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

Ban biên soạn

Tạp chí Pi
Hội toán học Việt Nam

Ngày 27 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

Chương 1

Tính chia hết

1.1 Các ví dụ

Ví dụ (BxMO 2015/P3)

[**10M**] Có tồn tại số nguyên tố nào có biểu diễn thập phân dưới dạng

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

Tức là, bắt đầu bằng các chữ số $3, 8$, sau đó là một hoặc nhiều chữ số 1.

Phân tích — Bài toán yêu cầu xét tính nguyên tố của các số có dạng đặc biệt, và lời giải sử dụng **kỹ thuật phân tích chuỗi chữ số theo modulo 3**. Mỗi trường hợp ứng với số chữ số 1 chia cho 3 được *diễn lại thành tích các số nhỏ hơn*, từ đó suy ra rằng số gốc luôn là hợp số.

Lời giải. [1]Ta phân tích theo số lượng chữ số 1 theo modulo 3.

Trường hợp 1: Số chữ số 1 là $3k$

Ở đây, số này chia hết cho 7:

$$3811\ldots1 = 7 \cdot (5444\ldots4) \quad (\text{gồm } 3k \text{ chữ số } 1)$$

Trường hợp 2: Số chữ số 1 là $3k+1$

Ở đây, số này chia hết cho 3:

$$3811\ldots1 = 3 \cdot (127\underbrace{037037\ldots037}_{k \text{ chuỗi } 037})$$

Trường hợp 3: Số chữ số 1 là $3k+2$

Ở đây, số này chia hết cho 37:

$$3811\ldots1 = 37 \cdot (103\underbrace{003003\ldots003}_{k \text{ chuỗi } 003})$$

Kết luận: Trong cả ba trường hợp, số đều chia hết cho một số nhỏ hơn, nên luôn là hợp số. Do đó, không tồn tại số nguyên tố nào có dạng $3811\ldots1$. □

[1]Lời giải của **codyj**.

Ví dụ (CAN 2015 TST/P3)

[**10M**] Gọi N là một số có ba chữ số phân biệt và khác 0. Ta gọi N là một số *mediocre* nếu nó có tính chất sau: khi viết ra tất cả 6 hoán vị có ba chữ số từ các chữ số của N, trung bình cộng của chúng bằng chính N. Ví dụ: $N = 481$ là số mediocre vì trung bình cộng của các số $\{418, 481, 148, 184, 814, 841\}$ bằng 481.

Hãy xác định số mediocre lớn nhất.

Phân tích — Ý tưởng chính là sử dụng đối xứng trong các hoán vị chữ số: tổng của 6 hoán vị luôn là $222(a+b+c)$, do đó trung bình là $37(a+b+c)$. Điều này cho ta phương trình liên hệ giữa chữ số hàng trăm và hai chữ số còn lại. Ta biến đổi về phương trình Diophantine tuyến tính và thử giá trị hợp lý, bắt đầu từ chữ số hàng trăm lớn nhất, để tìm nghiệm thoả mãn điều kiện phân biệt và khác 0.

Lời giải. [2]Giả sử abc là một số mediocre. Sáu hoán vị gồm $\{abc, acb, bac, bca, cab, cba\}$. Theo Trung bình cộng của các hoán vị ba chữ số, tổng của chúng là:

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

Vì abc là mediocre, nên:

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

Trường hợp 1: $a = 9, 8, 7$ đều bị loại vì không tạo thành chữ số phân biệt hợp lệ.

Trường hợp 2: Xét $a = 6$, ta có

$$378 = 27b + 36c \implies 3b + 4c = 42.$$

Giải phương trình nguyên:

$$b = \frac{42 - 4c}{3}$$

đòi hỏi $4c \equiv 0 \pmod 3 \implies c \in \{3, 6, 9\}$, lần lượt cho:

- $c = 3 \implies b = 10$ (không hợp lệ)
- $c = 6 \implies b = 6 \implies abc = 666$ (không phân biệt)
- $c = 9 \implies b = 2 \implies abc = 629$ (thoả mãn)

Kết luận: Số mediocre lớn nhất là $\boxed{629}$. □

[2]Lời giải chính thức.

Ví dụ (CHN 2015 TST1/D1/P2)

[10M] Cho dãy các số nguyên dương phân biệt $a_1, a_2, a_3, \ldots$, và một hằng số thực $0 < c < \frac{3}{2}$. Chứng minh rằng tồn tại vô hạn số nguyên dương k sao cho:

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

Phân tích — Hướng giải bắt đầu từ giả định phản chứng: từ một chỉ số K trở đi, các giá trị $\operatorname{lcm}(a_k, a_{k+1})$ đều không vượt quá ck. Ta liên hệ bất đẳng thức giữa gcd và lcm để tạo ra cận dưới cho tổng $\frac{1}{a_k} + \frac{1}{a_{k+1}}$, rồi cộng lại trên khoảng lớn. Sử dụng đặc điểm phân biệt của các phần tử trong dãy, tổng này không thể vượt quá một giới hạn. So sánh với cận dưới tăng theo $\ln N$ sẽ dẫn đến mâu thuẫn, từ đó khẳng định điều cần chứng minh.

Lời giải. [3]Giả sử phản chứng rằng tồn tại số nguyên K sao cho

$$\operatorname{lcm}(a_k, a_{k+1}) \le ck \quad \text{với mọi } k \ge K.$$

Khẳng định — Với mọi $k \ge K$, ta có

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

Chứng minh. Ta dùng

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

Vì $a_k \ne a_{k+1}$, ta có $a_k + a_{k+1} > 2\min \ge 2\gcd$, mà tổng chia hết cho gcd, nên

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

■

Cộng hai vế từ $k = K$ đến N, ta có

$$\frac{3}{c} \sum_{k=K}^{N} \frac{1}{k} \le \sum_{k=K}^{N} \left(\frac{1}{a_k} + \frac{1}{a_{k+1}} \right) \le 2 \sum_{j=1}^{\max a_j} \frac{1}{j}.$$

Mà $\sum \frac{1}{k} \sim \ln N$, $\sum \frac{1}{j} \sim \ln(\max a_j) \le \ln(N+1)$, nên

$$\frac{3}{c} \ln N \le 2 \ln(N+1).$$

Chia hai vế cho $\ln N$ rồi lấy giới hạn:

$$\frac{3}{c} \le 2 \quad (\text{vô lý vì } c < \frac{3}{2}).$$

Suy ra giả thiết sai. Vậy tồn tại vô hạn chỉ số k sao cho

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

□

[3]Lời giải của **TheUltimate123**.

Ví dụ (CHN 2015 TST1/D2/P2)

[**10M**] 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

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

Phân tích — Bài toán yêu cầu tìm một bộ số nguyên nhỏ (x, y, z) không đồng thời bằng 0 sao cho tổ hợp tuyến tính $ax + by + cz = 0$. Ta xét tập giá trị mà biểu thức $ax + by + cz$ có thể đạt được khi $x, y, z \in [-n, n]$, và so sánh với số lượng bộ ba như vậy. Vì số tổ hợp (x, y, z) nhiều hơn số giá trị có thể nhận, theo nguyên lý Dirichlet sẽ tồn tại hai bộ khác nhau cho cùng một giá trị. Từ đó, trừ hai biểu thức tương ứng ta được tổ hợp không tầm thường thoả mãn đẳng thức cần tìm.

Lời giải. [4]**Bước 1:** Xét tập giá trị

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

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

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

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

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

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

Bước 3: Trừ hai vế:

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

với $x - x', y - y', z - z' \in [-2n, 2n]$, không đồng thời bằng 0.

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

[4]Lời giải của **nayel**.

Ví dụ (EGMO 2015/P3)

[**20M**] Cho n, m là các số nguyên lớn hơn 1, và $a_1, a_2, \ldots, a_m$ là các số nguyên dương không vượt quá n^m. Hãy chứng minh rằng tồn tại các số nguyên dương $b_1, b_2, \ldots, b_m \leq n$ sao cho:

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

Phân tích — Mục tiêu là tìm các $b_i \leq n$ sao cho GCD của $a_i + b_i$ nhỏ hơn n. Nếu có hai a_i bằng nhau hoặc lệch nhau 1, ta chọn hai b_i tạo thành hai số liên tiếp, từ đó GCD là 1. Nếu không, ta xét n^m tổ hợp $(b_1, \ldots, b_m)$ trong khi số lượng GCD $\geq n$ bị giới hạn. Theo Nguyên lý Dirichlet, hai bộ sẽ cho cùng một GCD $d \geq n$, mâu thuẫn vì mỗi a_i chỉ cho phép một b_i sao cho $a_i + b_i \equiv 0 \pmod{d}$.

Lời giải. [5]**Bước 1:** Giả sử không mất tính tổng quát rằng a_1 là nhỏ nhất trong các a_i.

Trường hợp 1: $a_1 \geq n^m - 1$

Nếu tất cả $a_i = a_1$, chọn $b_1 = 1, b_2 = 2$, các b_i còn lại tuỳ ý. Khi đó $\gcd(a_1 + 1, a_1 + 2) = 1$. Nếu tồn tại $a_j = n^m$, lấy $b_1 = b_j = 1$, được $\gcd(n^m, n^m + 1) = 1$. Vậy chỉ cần xét $a_1 \leq n^m - 2$.

Bước 2: Giả sử phản chứng rằng với mọi bộ $(b_1, \ldots, b_m) \in \{1, \ldots, n\}^m$, ta có

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

Xét các bộ có $b_1 = 1$, và $b_i \in \{1, 2, \ldots, n\}$ với $i > 1$. Có n^{m-1} bộ như vậy, mỗi bộ cho một GCD $d_j \geq n$ chia hết $a_1 + 1$.

Với hai bộ khác nhau, tồn tại $i > 1$ sao cho b_i khác nhau, nên

$$d_j, d_k \mid (a_i + b_i') - (a_i + b_i) = \pm 1 \implies \gcd(d_j, d_k) = 1.$$

Vậy các d_j đôi một nguyên tố cùng nhau, và đều chia $a_1 + 1$, nên

$$a_1 + 1 \geq n(n+1)^{n^{m-1}-1} \implies a_1 \geq n^m,$$

mâu thuẫn với $a_1 \leq n^m$.

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

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

□

[5] Lời giải chính thức.

Ví dụ (Bản nâng cao EGMO 2015/P3)

[**25M**] Với $m, n > 1$, giả sử $a_1, \ldots, a_m$ là các số nguyên dương sao cho có ít nhất một $a_i \leq n^{2^{m-1}}$. Chứng minh rằng tồn tại các số nguyên $b_1, \ldots, b_m \in \{1, 2\}$ sao cho:

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

Phân tích — So với bài EGMO 2015/P3, bài nâng cao này giới hạn các $b_i \in \{1, 2\}$, nhưng chỉ yêu cầu một $a_i \leq n^{2^{m-1}}$. Ta phản chứng: nếu mọi tổ hợp đều cho GCD $\geq n$, thì với 2^{m-1} tổ hợp có $b_1 = 1$, các GCD phải là ước của $a_1 + 1$, đôi một nguyên tố cùng nhau. Suy ra $a_1 + 1$ có ít nhất 2^{m-1} ước nguyên tố lớn hơn n, dẫn đến bất đẳng thức mâu thuẫn.

Lời giải. [6]Giả sử ngược lại rằng với mọi bộ $(b_1, \ldots, b_m) \in \{1, 2\}^m$, ta có

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

Xét các bộ có $b_1 = 1$, còn lại $b_i \in \{1, 2\}$ với $i > 1$. Có 2^{m-1} bộ như vậy, mỗi bộ cho một GCD $d_j \geq n$ chia hết $a_1 + 1$.

Với hai bộ khác nhau, tồn tại $i > 1$ sao cho một bộ có $b_i = 1$, bộ kia có $b_i = 2$, suy ra

$$d_j \mid a_i + 1, \quad d_k \mid a_i + 2 \implies \gcd(d_j, d_k) = 1.$$

Vậy $d_1, \ldots, d_{2^{m-1}}$ là các ước số nguyên tố cùng nhau của $a_1 + 1$, mỗi $d_j \geq n$, nên

$$a_1 + 1 \geq n(n+1)^{2^{m-1}-1} \implies a_1 \geq n^{2^{m-1}},$$

mâu thuẫn với giả thiết $a_i \leq n^{2^{m-1}}$.

Kết luận: Tồn tại bộ $(b_1, \ldots, b_m) \in \{1, 2\}^m$ sao cho

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

□

Nhận xét. Giới hạn $n^{2^{m-1}}$ trong giả thiết có thể được cải thiện thêm.

[6]Lời giải chính thức.

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 $1 \leq i \leq k-2$.

Phân tích — Bài toán yêu cầu khảo sát cấu trúc các ước của một số nguyên hợp n sao cho mỗi ước d_i chia hết tổng của hai ước kế tiếp lớn hơn nó. Một số hướng tiếp cận hiệu quả gồm:

- Thử các trường hợp $n = p^r$, với p nguyên tố.
- Phản chứng nếu n có nhiều hơn một thừa số nguyên tố.
- Khai thác đối xứng $d_i d_{k+1-i} = n$ và dùng quy nạp theo chia hết.

Lời giải. (Cách 1)[7]**Bước 1:** Giả sử $n = p^r$. Khi đó $d_i = p^{i-1}$, và

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

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

Bước 2: Giả sử n có ít nhất hai thừa số nguyên tố. Gọi $p < q$ là hai thừa số nguyên tố nhỏ nhất.

Khi đó tồn tại đoạn gồm các ước:

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

và ở cuối:

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

Từ giả thiết:

$$\frac{n}{q} \mid \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right) \implies p^j \mid q(p+1) \implies p \mid q,$$

mâu thuẫn vì $p \neq q$.

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

Lời giải. (Cách 2)[7]

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

Chứng minh. Chứng minh bằng quy nạp.

Cơ sở: $d_1 = 1 \Rightarrow d_1 \mid d_2$.

Giả sử $d_{i-1} \mid d_i$, từ đề bài:

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

Do $d_{i-1} \mid d_i$ và $d_i \mid d_{i+1}$, suy ra $d_{i-1} \mid d_{i+1}$, nên $d_i \mid d_{i+1}$. ■

Do đó, mọi ước d_i là bội của d_2, và d_2 là số nguyên tố nhỏ nhất chia n, suy ra n là lũy thừa của một số nguyên tố. □

Lời giải. (Cách 3)[7] **Bước 1:** Sử dụng đối xứng $d_i d_{k+1-i} = n$. Đặt

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

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

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

Mặt khác, từ đề bài:

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

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

Bước 2: Gọi $p = d_2$ là ước nguyên tố nhỏ nhất. Ta dùng quy nạp:

Khẳng định — $p \mid d_i$ với mọi $i \geq 2$.

Chứng minh. Cơ sở đúng với d_2.

Giả sử $p \mid d_j$, từ $d_j \mid d_{j+1}^2$ và $p \mid d_j$, do p nguyên tố nên $p \mid d_{j+1}$. ■

Do đó, mọi d_i chia hết cho p. Nếu tồn tại ước nguyên tố khác $q \neq p$, thì $p \mid q$, mâu thuẫn.

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

[7] Shortlist 2023 with solutions.

Ví dụ (IND 2015 MO/P2)

[**10M**] 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 $\frac{1}{n}$.

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

Ý tưởng:

- Phân tích $n = 2^a \cdot 5^b \cdot q$, với $\gcd(q, 10) = 1$.
- Phần không tuần hoàn ứng với số chữ số x sao cho 10^x chia hết cho $2^a 5^b$.
- Kết luận: $x = \max(a, b)$.

Lời giải. [8]Gọi biểu diễn thập phân của $\frac{1}{n}$ là:

$$\frac{1}{n} = 0.a_1 a_2 \cdots a_{x_n} \overline{b_1 b_2 \cdots b_{\ell_n}},$$

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

Ta có:

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

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

Để $\frac{1}{n}$ có phần không tuần hoàn dài x_n, thì:

$$2^a 5^b \mid 10^{x_n} \implies x_n = \min\{x \mid 2^a 5^b \mid 10^x\} = \max(a, b).$$

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

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

□

[8]Lời giải của **utkarshgupta**.

Ví dụ (IND 2015 MO/P6)

[**15M**] 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:

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

Phân tích — Bài toán yêu cầu tìm hai bộ ba số chính phương có tổng đồng dư modulo 12. Ta xét phần dư của số chính phương theo modulo 12 (chỉ có thể là $0, 1, 4, 9$), sau đó áp dụng nguyên lý Dirichlet để buộc tồn tại phần dư xuất hiện nhiều lần. Từ đó, xét các tổ hợp 3 phần tử và so sánh tổng modulo 12 giữa các nhóm khác nhau để tìm hai tổng bằng nhau.

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

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

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

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

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

Trường hợp 1: Có ít nhất 6 phần tử trong S có cùng phần dư. Chia chúng thành 2 bộ ba giống nhau → tổng bằng nhau → đẳng thức modulo 12 hiển nhiên đúng.

Trường hợp 2: Có một phần dư xuất hiện 4 hoặc 5 lần. Theo Dirichlet, phần dư khác xuất hiện ít nhất 2 lần. Từ đó có thể chọn hai bộ ba từ hai phần dư khác nhau nhưng tạo ra tổng đồng dư nhau.

Trường hợp 3: Mỗi phần dư xuất hiện tối đa 3 lần. Khi đó số lượng bộ ba là hữu hạn nhưng đáng kể: có tổng cộng $\binom{11}{3} = 165$ cách chọn bộ ba. Mà chỉ có hữu hạn tổng có thể xảy ra modulo 12 với các phần dư $\{0, 1, 4, 9\}$, nên tồn tại hai bộ ba khác nhau có tổng đồng dư nhau.

Kết luận: Trong mọi trường hợp, luôn tồn tại hai bộ ba số chính phương rời nhau sao cho tổng của chúng đồng dư modulo 12. □

[8] Dựa theo lời giải của **Sahil**.

Ví dụ (IND 2015 TST2/P1)

[**25M**][9]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.

Phân tích — Bài toán liên quan đến cấu trúc của các số $2^n - 2^k$, với chiến lược chính là:

- Dùng quy nạp để chứng minh mọi số lớn hơn một ngưỡng đều biểu diễn được.
- Tìm giá trị nhỏ nhất thoả mãn đồng dư $\equiv 1 \pmod{2^n}$ không thể rút xuống nhỏ hơn.
- Sử dụng biểu diễn nhị phân duy nhất để tìm giá trị giới hạn không biểu diễn được.

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

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

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

Trường hợp 1: m chẵn. Khi đó

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

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

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

Trường hợp 2: m lẻ. Khi đó

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

nên phần còn lại biểu diễn được từ A_{n-1}, cộng thêm $2^n - 1 \in A_n$ để được m.

Bước 2: Chứng minh số $(n-2)\cdot 2^n + 1$ không biểu diễn được.

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

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

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

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

Từ đó:

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

Suy ra số lớn nhất không biểu diễn được là:

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

□

[9]IMO SL 2014 N1.

Ví dụ (IRN 2015 MO/N2)

[**25M**] 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.

Phân tích — Bài toán yêu cầu chứng minh rằng sau một số bước đủ lớn, trong tập M_n không tồn tại quan hệ chia hết giữa hai phần tử. Ý tưởng chính gồm:

- Nếu có quan hệ chia hết giữa các phần tử, điều đó dẫn đến một bất đẳng thức giữa độ rộng tập trước và giá trị nhỏ nhất ở bước hiện tại.
- Các phần tử của M_n tăng rất nhanh, khiến bất đẳng thức trên không còn thỏa mãn khi n đủ lớn.
- Từ đó suy ra không thể có quan hệ chia hết trong M_n.

Lời giải. [10]Giả sử tại bước n, tồn tại hai phần tử $k, t \in M_{n-1}$ sao cho

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

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

Vậy nếu có quan hệ chia hết, thì

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

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

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

và

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

Thế vào (1):

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

Mặt khác, vì $b_n \in M_{n-1}$, các phần tử tăng rất nhanh qua mỗi bước, nên

$$b_n \geq n - 2.$$

Do đó, nếu

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

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

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

[10]Dựa theo lời giải của **Arefe**.

Ví dụ (IRN 2015 TST/D3-P2)

[**30M**] Giả sử a_1, a_2, a_3 là ba số nguyên dương cho trước. Xét dãy số được xác định bởi công thức:

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

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

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

Phân tích — Bài toán yêu cầu chứng minh rằng chuỗi được xây dựng theo công thức liên quan đến LCM sẽ đạt giá trị không dương trong thời gian hữu hạn. Chiến lược:

- Xây dựng chuỗi phụ $b_n = \dfrac{a_n}{\operatorname{lcm}(a_{n-2}, a_{n-3})}$ để theo dõi sự suy giảm.
- Chứng minh b_n nguyên và giảm dần.
- Từ đó suy ra tồn tại một $k \leq a_3 + 3$ sao cho $a_k \leq 0$.

Lời giải. [11]Ta chứng minh điều mạnh hơn: tồn tại $k \leq a_3 + 3$ sao cho $a_k \leq 0$.

Bước 1: Đặt

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

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

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

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

Chứng minh. Ta có

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

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

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

Vì $a_{n-3} \mid a_{n-1}$, nên

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

■

Bước 2: Ước lượng b_5.

Ta có

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

và

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

Suy ra:

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

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

[11]Lời giải của **guptaamitu1**.

Ví dụ (KOR 2015 MO/P8)

[**30M**] 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:

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

Phân tích — Bài toán yêu cầu chứng minh bất đẳng thức liên quan đến khoảng cách tới trung điểm $\frac{n}{2}$ của các số nguyên tố cùng nhau với n.

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

Lời giải. (Cách 1)[12]Với các giá trị đặc biệt như $n = p$ nguyên tố, $n = p^2$, hoặc $n = pq$ với p, q là các số nguyên tố, ta có thể kiểm tra trực tiếp. Vì vậy, ta giả sử từ đây rằng n không thuộc các dạng này.

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

Giả sử $a < \frac{n}{2}$, ta có:

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

Suy ra:

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

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

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

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

Thay (2) vào (1):

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

□

[12]Lời giải của **andria**.

Phân tích — Bài toán yêu cầu chứng minh bất đẳng thức liên quan đến khoảng cách tới trung điểm $\frac{n}{2}$ của các số nguyên tố cùng nhau với n.

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

Lời giải. (Cách 2)[12] Ta nhận thấy rằng nếu a_i thuộc tập thì $n - a_i$ cũng thuộc tập, tổng hai số là n. Do đó k chẵn và:

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

Ta có:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

[12] Lời giải của **rkm0959**.

Ví dụ (MEMO 2015/I/P4)

[**25M**] Tìm tất cả các cặp số nguyên dương (m,n) sao cho tồn tại hai số nguyên $a,b>1$, nguyên tố cùng nhau, thỏa mãn:

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

Phân tích — Bài toán yêu cầu tìm tất cả các cặp (m,n) sao cho $\dfrac{a^m+b^m}{a^n+b^n}$ là số nguyên với mọi cặp $a,b>1$ nguyên tố cùng nhau. Kỹ thuật sử dụng:

- Sử dụng phân tích số mũ: đặt $m=kn+r$ rồi chia từng vế để rút gọn.
- Phân tích dư và suy ra điều kiện cần để tránh mẫu số không chia được tử số.
- Xét các trường hợp với k chẵn hoặc lẻ để xử lý khi tử hoặc mẫu có thể bằng 0.

Lời giải. [13]Giả sử $\gcd(a,b)=1$, $a,b>1$, và phân số:

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

là một số nguyên.

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

Ta phân tích:

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

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

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

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

Ta kiểm tra điều kiện cần. Nếu k lẻ:

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

Nếu k chẵn, thử với $a=-b$, thì:

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

Kết luận: Tất cả các cặp thỏa mãn là:

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

□

[13]Lời giải chính thức.

Ví dụ (RUS 2015 TST/D10/P2)

[**25M**] 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.

Phân tích — Bài toán yêu cầu tìm một cách phân chia tập $\{1, 2, \ldots, p-1\}$ thành hai tập con không rỗng S và S^c sao cho $\sum_S \equiv \prod_{S^c} \pmod p$. Một cách tiếp cận là dùng các định lý cổ điển: tổng các số từ 1 đến $p-1$ là $\frac{(p-1)p}{2} \equiv 1 \pmod p$, còn tích là $(p-1)! \equiv -1 \pmod p$ theo Wilson. Sử dụng các biểu thức bổ sung này, ta đặt điều kiện tương đương với $AB \equiv -1 \pmod p$. Khi đó, việc xây dựng một tập S có tổng và tích phù hợp được chia thành hai trường hợp: $p \equiv 1 \pmod 4$ và $p \equiv 3 \pmod 4$, với mỗi trường hợp dùng các kỹ thuật khác nhau — khai thác căn bậc hai của -1, phần tử sinh, và tổng cấp số nhân.

Lời giải. [14]Ta biết rằng:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Do đó:

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

□

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

Ví dụ (THA 2015 MO/P1)

[**25M**] Cho số nguyên tố p, và dãy số nguyên dương $a_1, a_2, a_3, \ldots$ thỏa mãn:

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

Chứng minh rằng với mọi n, ta có:

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

Phân tích — Bài toán yêu cầu chứng minh một dạng chia hết xuất phát từ một đệ quy bậc hai có điều chỉnh bởi hằng số p. Chiến lược:

- Sử dụng hai lần liên tiếp định nghĩa đệ quy để trừ hai phương trình.
- Từ đó rút ra được mối liên hệ giữa $a_n + a_{n+2}$ và a_{n+1}, rồi chứng minh $a_{n+1} \mid a_n + a_{n+2}$.
- Để chứng minh chia hết, sử dụng phép phản chứng với giả thiết $\gcd(a_{n+1}, a_{n+2}) > 1$ và dẫn đến mâu thuẫn về chia hết cho modulo p^2.

Lời giải. (Cách 1)[15]Từ giả thiết:

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

Trừ hai vế:

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

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

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

Xét tiếp:

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

Vì $p \mid a_{n+2}$, thì:

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

Nhưng:

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

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

Từ:

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

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

Kết luận: Ta đã chứng minh:

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

□

[15]Lời giải của **rstenetbg**.

1.2 Bài tập

Bài tập (GBR 2015 TST/N3/P3). [25M] Cho các số nguyên dương phân biệt đôi một $a_1 < a_2 < \cdots < a_n$, trong đó a_1 là số nguyên tố và $a_1 \geq n+2$. Trên đoạn thẳng $I = [0, \prod_{i=1}^{n} a_i]$ trên trục số thực, đánh dấu tất cả các số nguyên chia hết cho ít nhất một trong các số $a_1, a_2, \ldots, a_n$. Các điểm này chia đoạn I thành nhiều đoạn con.

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

Nhận xét. Hãy xét các đoạn con nằm giữa hai số nguyên liên tiếp không bị đánh dấu. Gọi độ dài mỗi đoạn là ℓ_i, ta cần chứng minh $\sum \ell_i^2 \equiv 0 \pmod{a_1}$.

Bài tập (HUN 2015 TST/KMA/633). [35M] Chứng minh rằng nếu n là một số nguyên dương đủ lớn, thì trong bất kỳ tập hợp gồm n số nguyên dương khác nhau nào cũng tồn tại bốn số sao cho bội chung nhỏ nhất của chúng lớn hơn $n^{3,99}$.

Nhận xét. Gợi ý: Hãy sắp xếp các số đã cho theo thứ tự tăng dần, ước lượng kích thước của bội chung nhỏ nhất, và tìm cách chọn bốn số sở hữu lũy thừa nguyên tố lớn vượt mức $n^{3.99}$.

Bài tập (JPN 2015 MO1/P1). [15M] Tìm tất cả các số nguyên dương n sao cho

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

là một số nguyên.

Nhận xét. Hãy phân tích mẫu số n^3+n^2+n+1 thành nhân tử, sau đó kiểm tra xem khi nào nó chia hết 10^n. Có thể thử với các giá trị nhỏ của n.

Bài tập (ROU 2014 MO/G10/P1). [20M] Cho n là một số tự nhiên. Tính giá trị của biểu thức

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

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

Nhận xét. Thay đổi góc nhìn: với mỗi số chia d, tìm những giá trị k thỏa $d \mid k$, $k \leq d^2$, và tổng quát lại theo d thay vì k.

Bài tập (ROU 2015 MO/G10/P2). [25M] Xét một số tự nhiên n sao cho tồn tại một số tự nhiên k và k số nguyên tố phân biệt sao cho $n = p_1 \cdot p_2 \cdots p_k$.

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

Nhận xét. Gợi ý: Xem xét những giá trị của $f(i)$ phải chứa đủ các ước nguyên tố của n. Lưu ý nếu một trong số các $f(i)$ luôn chọn được bội của tất cả số nguyên tố $(p_1, p_2, \ldots)$ thì tích sẽ chia hết n.

1.3 Định lý, bổ đề, và hằng đẳng thức

Định lý (Tính chia hết của chuỗi chữ số 1)

Gọi $R_n = \underbrace{11\ldots1}_{n}$ là số gồm n chữ số 1 (repunit). Khi đó:

- Nếu $n \equiv 0 \pmod 3$ thì R_n chia hết cho 3.
- Nếu $n \equiv 1 \pmod 3$ thì R_n chia hết cho 3.
- Nếu $n \equiv 2 \pmod 3$ thì R_n chia hết cho 37.

Bổ đề (Trung bình cộng của các hoán vị ba chữ số)

Giả sử $a, b, c \in \{0, 1, \ldots, 9\}$ là ba chữ số phân biệt. Khi liệt kê tất cả 6 hoán vị ba chữ số khác nhau từ a, b, c, tổng của chúng bằng $222(a + b + c)$, do đó trung bình cộng bằng $37(a + b + c)$.

Chương 2

Cơ bản về số học đồng dư

2.1 Các ví dụ

Ví dụ (GER 2015 MO/P2)

[**25M**] Một số nguyên dương n được gọi là **trơn** nếu tồn tại các số nguyên $a_1, a_2, \ldots, a_n$ sao cho:

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

Hãy tìm tất cả các số trơn.

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

Lời giải. [1]Xét $\pmod 4$, ta thấy nếu n trơn thì $n \equiv 0$ hoặc 1 $\pmod 4$.

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

Tổng: $n + 2k(-1) + 2k(1) = n$.

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

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

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

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

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

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

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

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

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

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

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

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

[1]Lời giải của **MathGan**.

2.2 Bài tập

Bài tập (ROU 2014 MO/G9/P2)**.** [**15M**] Cho a là một số tự nhiên lẻ không phải là một số chính phương, và $m, n \in \mathbb{N}$. Khi đó:

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

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

Nhận xét. Vì $\sqrt{a}$ là số vô tỉ (do a không phải là số chính phương), nên các biểu thức $a+\sqrt{a}$ và $a-\sqrt{a}$ là liên hợp, có tổng nguyên nhưng đối xứng về trục. Tuy nhiên, $a+\sqrt{a} > a$ và $a-\sqrt{a} < a$, nên phần thập phân của chúng không thể trùng nhau khi nhân với số nguyên. Đồng thời, hiệu $m(a+\sqrt{a}) - n(a-\sqrt{a})$ không thể là số nguyên, vì vậy phần nguyên của chúng cũng khác nhau.

2.3 Định lý, bổ đề, và hằng đẳng thức

Định lý 2.3.1 (Ước nguyên tố dạng $4k+3$)

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

Chương 3

Các hàm số học

3.1 Các ví dụ

Ví dụ (BMO 2015/P4)

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

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

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

Phân tích — Ta chọn d thuộc dạng $5(4k+3)$ trong dãy 20 số nguyên liên tiếp. Dựa vào tính chất $p\equiv -1 \pmod 4$ đối với một ước nguyên tố của $4k+3$, ta chứng minh rằng mỗi $n\sqrt{d}$ có phần thập phân đủ lớn để $n\sqrt{d}\cdot\{n\sqrt{d}\}>\frac{5}{2}$. Kỹ thuật chính là sử dụng chia hết theo mô-đun 4 và 5 để loại trừ những khả năng nhỏ hơn.

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

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

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

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

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

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

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

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

Do đó:

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

Ta đánh giá:

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

Vì $a^2+5>a(a+1)$, ta có:

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

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

Còn khi $a\geq 3$, ta có:

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

vì biểu thức là số dương tăng theo a.

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

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

□

Ví dụ (ROU 2015 TST/D1/P4)

[**25M**] Gọi k là một số nguyên dương sao cho $k \equiv 1 \pmod 4$, và k không phải là số chính phương. Đặt

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

Chứng minh rằng

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

Phân tích — Đặt $a = \frac{1+\sqrt{k}}{2}$ với $k \equiv 1 \pmod 4$ và k không phải chính phương. Ta có $a^2 = a + t$ cho một $t \in \mathbb{Z}_{>0}$. Mấu chốt là xét $\lfloor a^2 n \rfloor$ và so sánh với $\lfloor a \lfloor an \rfloor \rfloor$, rồi sử dụng tính vô tỷ của a để chứng minh dãy các hiệu $\lfloor a^2 n \rfloor - \lfloor a \lfloor an \rfloor \rfloor$ phân bố đủ các giá trị $\{1, 2, \ldots, \lfloor a \rfloor\}$.

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

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

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

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

Vậy

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

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

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

Vậy

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

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

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

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

[1] Lời giải chính thức.

Ví dụ (ROU 2015 TST/D2/P1)

[**25M**] Cho $a \in \mathbb{Z}$ và $n \in \mathbb{N}_{>0}$. Chứng minh rằng:

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

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

Phân tích — Ta nhóm các số k có cùng $\gcd(k,n) = d$ và viết tổng dưới dạng $\sum_{d|n} \phi(d)\, a^{n/d}$. Sau đó, áp dụng định lý Euler cho các $n = p^s$ và sử dụng nguyên lý đồng dư Trung Hoa cho trường hợp tổng quát khi n có ít nhất hai thừa số nguyên tố.

Lời giải. Ta chứng minh khẳng định sau.

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

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

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

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

■

Trường hợp 1: $n = p^s$, với p nguyên tố. Từ GCD Power Sum Identity,

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

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

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

Ta chứng minh bằng quy nạp theo s rằng $p^s \mid S$. • Cơ sở $s = 1$: $a^p + (p-1)\, a = p\, a \equiv 0 \pmod{p}$. • Giả thiết quy nạp và khẳng định cho thấy mỗi bước đều bảo toàn tính chia hết p^s.

Trường hợp 2: n có ít nhất hai thừa số nguyên tố (một dạng "tổng quát"). Giả sử $n = p^s m$ với $\gcd(p,m) = 1$. Theo GCD Power Sum Identity,

$$\sum_{d|n} \phi(d)\, a^{n/d} = \sum_{\substack{d|n \\ p \nmid d}} \phi(d)\, a^{n/d} + \sum_{\substack{d|n \\ p|d}} \phi(d)\, a^{n/d}.$$

Phần đầu chia hết cho $m = n/p^s$ (theo giả thiết quy nạp với số nhỏ hơn), phần sau chia hết cho p^s (theo bước lũy thừa nguyên tố). Cuối cùng, vì $\gcd(m, p^s) = 1$, suy ra $n \mid \sum_{k=1}^{n} a^{\gcd(k,n)}$ nhờ nguyên lý đồng dư Trung Hoa.

Kết luận:

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

□

[1] Dựa theo lời giải của **andria**.

Ví dụ (ROU 2015 TST/D3/P3)

[**30M**] Với hai số nguyên dương $k \leq n$, ký hiệu $M(n,k)$ là bội chung nhỏ nhất của dãy số $n, n-1, \ldots, n-k+1$. Gọi $f(n)$ là số nguyên dương lớn nhất thỏa mãn:

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

Chứng minh rằng:

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

Phân tích — **Phần (a):** Giả sử $f(n) \geq 3\sqrt{n}$ và xét dãy số $s = \lfloor \sqrt{n} \rfloor$. Ta phân tích sự mâu thuẫn khi xét dãy các số nguyên trong khoảng $\{a+1, a+2, \ldots, n\}$, trong đó $a = s(s-1)$, để thấy rằng có các số nguyên chia hết cho một số không thể là phần tử của dãy.

Phần (b): Giả sử $n > N! + N$, ta chứng minh rằng $f(n) > N$ bằng cách sử dụng các tính chất chia hết với $k!$ và mâu thuẫn với giả thuyết khi $n - k > N!$.

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

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

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

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

và

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

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

$$\operatorname{lcm}(n, n-1, \ldots, a+1) \mid a \implies M(n, n-a+1) = \operatorname{lcm}(M(n, n-a), a) = M(n, n-a),$$

mâu thuẫn với giả thiết chuỗi $M(n,1) < M(n,2) < \ldots$. Vậy $f(n) < 3\sqrt{n}$.

Phần (b): Cho $N \in \mathbb{N}_{>0}$. Ta chứng minh nếu $n > N! + N$ thì $f(n) > N$. Giả sử tồn tại $k \leq N$ sao cho $M(n,k) = M(n,k+1)$. Điều đó có nghĩa:

$$(n-k) \mid M(n,k) \implies M(n,k) \mid n(n-1)\cdots(n-k+1),$$

suy ra:

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

Nhưng nếu $n - k > N! \geq k!$, mâu thuẫn.

Vậy với mọi $k \leq N$, ta có:

$$M(n,k) < M(n,k+1) \implies f(n) > N.$$

Từ đó suy ra chỉ có hữu hạn n với $f(n) \leq N$. Điều này chứng minh vế thứ hai. □

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

3.2 Bài tập

Bài tập (TWN 2015 TST2/Q2/P1)**.** [**20M**] Với mỗi số nguyên dương n, định nghĩa:

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

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

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

3.3 Định lý, bổ đề, và hằng đẳng thức

Định lý (GCD Power Sum Identity)

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

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

Chương 4

Phương trình Diophantine

4.1 Các ví dụ

Ví dụ (CAN 2015 TST/P1)

[**25M**] Tìm tất cả nghiệm nguyên của phương trình:

$$7x^2y^2 + 4x^2 = 77y^2 + 1260.$$

Phân tích — Phân tích phương trình dưới dạng tích hai biểu thức. Nhận thấy các hệ số đều chia hết cho 7 ngoại trừ hạng tử $4x^2$, ta suy ra x phải chia hết cho 7. Sau khi chuyển vế và nhóm các hạng tử hợp lý, ta có phương trình:

$$(x^2 - 11)(7y^2 + 4) = 1216.$$

Vì vế phải là số cố định, ta chỉ cần xét một số hữu hạn giá trị x và y. Dùng thử các ước của 1216, ta tìm được các nghiệm $(x, y) = (\pm 7, \pm 2)$.

Lời giải. [1]Các hệ số đều chia hết cho 7 ngoại trừ 4, nên x phải chia hết cho 7.

Biến đổi phương trình:

$$7x^2y^2 + 4x^2 = 77y^2 + 1260 \quad \Rightarrow \quad (x^2 - 11)(7y^2 + 4) = 1216.$$

Vì vế phải là hằng số, ta chỉ cần xét một số hữu hạn giá trị x. Giả sử $x = 7t$, thì:

$$x^2 = 49t^2 \leq 1216 + 77y^2 + 4x^2 \Rightarrow x^2 < 122 \Rightarrow |x| < 11 \Rightarrow x \in \{0, \pm 7\}.$$

- Với $x = 0 \Rightarrow 0 = 77y^2 + 1260$, vô lý.
- Với $x = \pm 7$:

$$(x^2 - 11)(7y^2 + 4) = 1216 \Rightarrow (49 - 11)(7y^2 + 4) = 1216 \Rightarrow 38(7y^2 + 4) = 1216.$$

$$7y^2 + 4 = \frac{1216}{38} = 32 \Rightarrow 7y^2 = 28 \Rightarrow y^2 = 4 \Rightarrow y = \pm 2.$$

Kết luận, các nghiệm nguyên là $(x, y) = (\pm 7, \pm 2)$. □

[1]Lời giải chính thức.

Ví dụ (CHN 2015 TST3/D2/P3)

[**30M**] 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:

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

Phân tích — Hàm $f(n)$ đo mức độ tăng thêm về số lượng ước số của $n!$ so với $(n-1)!$. Để $f(n)$ đạt giá trị lớn hơn mọi giá trị trước đó, ta tìm một bước nhảy lớn trong độ phức tạp của $n!$. Sử dụng định lý Bertrand, chọn q là số nguyên tố lớn nhất trong đoạn $(p, 2p)$, ta chứng minh $f(2p) > f(q)$, với p là số nguyên tố lẻ. Khi p chạy qua vô hạn số nguyên tố, ta thu được vô hạn số n hợp số thỏa mãn yêu cầu bài toán.

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

Khẳng định — $f(2p) > f(q)$.

Chứng minh. Ta có:

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

■

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

Vì $n \in [p+1, 2p+1]$, ta thấy rằng khi cho p chạy qua vô hạn số nguyên tố lẻ, sẽ có vô hạn giá trị n là hợp số thoả mãn điều kiện của bài toán. □

[2]Lời giải của **chirita.andrei**.

Ví dụ (FRA 2015 TST/1/P3)

[**25M**] Cho n là một số nguyên dương sao cho $n(n+2015)$ là một số chính phương.

- Chứng minh rằng n không phải là số nguyên tố.
- Cho một ví dụ về số nguyên n như vậy.

Phân tích —

- **Phần (a):** Giả sử n là số nguyên tố và $n(n+2015) = m^2$ là số chính phương. Khi đó $n \mid m^2 \Rightarrow n \mid m$, đặt $m = nr$. Ta suy ra phương trình:

$$2015 = n(r^2 - 1).$$

Vì $n \mid 2015$, nên chỉ có thể là một trong các ước nguyên tố của 2015 là $5, 13, 31$. Kiểm tra từng giá trị cho thấy không có giá trị nào cho r^2 nguyên, từ đó suy ra n không thể là số nguyên tố.

- **Phần (b):** Ta cần xây dựng một ví dụ cụ thể sao cho $n(n+2015)$ là số chính phương. Sử dụng kỹ thuật đặt biến: nếu $n(n+2015) = \left(\frac{(2n+2015)^2 - 2015^2}{4}\right)$, ta đưa phương trình về dạng hiệu hai bình phương. Từ đó, chọn các cặp số (a, b) sao cho $ab = 2015^2$, rồi giải hệ để tìm được n. Chọn $a = 2015 \cdot 5, b = 2015/5$ ta tìm được $n = 1612$, là một nghiệm phù hợp.

Lời giải. [3] *(a)* Giả sử n là số nguyên tố và tồn tại $m \in \mathbb{Z}$ sao cho $n(n+2015) = m^2$. Khi đó, $n \mid m^2 \Rightarrow n \mid m$. Đặt $m = nr$, ta có:

$$n(n+2015) = n^2r^2 \Rightarrow n + 2015 = nr^2 \Rightarrow 2015 = n(r^2 - 1).$$

Vì $2015 = 5 \cdot 13 \cdot 31$, nên $n \in \{5, 13, 31\}$. Ta kiểm tra từng giá trị:

- $n = 5 \Rightarrow r^2 = 1 + \frac{2015}{5} = 1 + 403 = 404$, không là số chính phương.
- $n = 13 \Rightarrow r^2 = 1 + \frac{2015}{13} = 1 + 155 = 156$, không là số chính phương.
- $n = 31 \Rightarrow r^2 = 1 + \frac{2015}{31} = 1 + 65 = 66$, không là số chính phương.

Không giá trị nào cho r^2 nguyên, nên n không thể là số nguyên tố.

(b) Ta xét biểu thức:

$$(2m)^2 = 4n(n+2015) = (2n+2015)^2 - 2015^2.$$

Đặt $2n + 2015 + 2m = a$, $2n + 2015 - 2m = b$, ta có:

$$ab = 2015^2.$$

Chọn:

$$a = 2015 \cdot 5 = 10075, \quad b = \frac{2015}{5} = 403.$$

Suy ra:

$$2n + 2015 = \frac{a+b}{2} = \frac{10075 + 403}{2} = 5239.$$

$$n = \frac{5239 - 2015}{2} = \frac{3224}{2} = 1612.$$

Khi đó:

$$n(n+2015) = 1612 \cdot 3627 = \left(\frac{10075 - 403}{2}\right)^2 = m^2,$$

là một số chính phương. Vậy $n = 1612$ là một ví dụ thoả mãn. □

[3] Lời giải chính thức.

Ví dụ (GER 2015 TST/P4)

[**30M**] Tìm tất cả các cặp số nguyên dương (x, y) sao cho

$$\sqrt[3]{7x^2 - 13xy + 7y^2} = |x - y| + 1.$$

Phân tích — Đặt $u = |x - y|$, khi đó phương trình trở thành $\sqrt[3]{7u^2 + v} = u + 1$. Giải phương trình, ta tìm được $v = u^3 - 4u^2 + 3u + 1$, với $v = xy = y^2 + uy$. Để phương trình có nghiệm, biểu thức trong căn phải là số chính phương, từ đó suy ra $4u + 1 = (2m + 1)^2$, và $u = m^2 + m$. Trường hợp $u = 0$ dẫn đến nghiệm $(1, 1)$, còn các nghiệm khác theo dạng $(m^3 + 2m^2 - m - 1, m^3 + m^2 - 2m - 1)$ với $m \geq 2$.

Lời giải. [4]Không mất tính tổng quát, giả sử $x \geq y$. Đặt $u = x - y$, khi đó phương trình trở thành:

$$\sqrt[3]{7(x - y)^2 + xy} = u + 1.$$

Đặt $v = xy$, ta được:

$$7u^2 + v = (u + 1)^3 \Rightarrow v = u^3 - 4u^2 + 3u + 1.$$

Mặt khác, $x = y + u \Rightarrow v = xy = (y + u)y = y^2 + uy$. Suy ra:

$$y^2 + uy = u^3 - 4u^2 + 3u + 1 \Rightarrow y = \frac{-u \pm \sqrt{u^2 + 4(u^3 - 4u^2 + 3u + 1)}}{2}.$$

Yêu cầu biểu thức trong căn là số chính phương:

$$u^2 + 4(u^3 - 4u^2 + 3u + 1) = (u - 2)^2(4u + 1).$$

Suy ra $4u + 1 = \ell^2$, với ℓ là số lẻ. Đặt $\ell = 2m + 1 \Rightarrow u = m^2 + m$.

Trường hợp $m = 0$: $u = 0 \Rightarrow x = y$. Thay vào phương trình gốc:

$$\sqrt[3]{7x^2 - 13x^2 + 7x^2} = \sqrt[3]{x^2} = |x - y| + 1 = 1 \Rightarrow x^2 = 1 \Rightarrow x = y = 1.$$

Trường hợp $m \geq 1$:

$$u = m^2 + m, \quad y = m^3 + m^2 - 2m - 1, \quad x = y + u = m^3 + 2m^2 - m - 1.$$

Với $m \geq 2$, $y > 0$. Như vậy, các nghiệm nguyên dương của bài toán là:

$$(x, y) = (1, 1) \quad \text{và} \quad \left(m^3 + 2m^2 - m - 1,\ m^3 + m^2 - 2m - 1\right),\ m \geq 2,$$

cùng các hoán vị (y, x) (do phương trình đối xứng theo $|x - y|$). □

[4]Lời giải của **pad**.

Ví dụ (KOR 2015 MO/P1)

[**30M**] 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.

Phân tích — Ta xây dựng ánh xạ $\mathrm{T}(x, y) = (2x - 3y, x - 2y)$. Ánh xạ này bảo toàn cả hai điều kiện của bài toán. Kiểm tra cho thấy:

- Ánh xạ bảo toàn phương trình $x^2 - 3y^2 + 2 = 16m$.
- Ánh xạ bảo toàn điều kiện $2y \leq x - 1$.
- Ánh xạ không có điểm bất biến, vì giải hệ $\mathrm{T}(x, y) = (x, y)$ dẫn đến mâu thuẫn.

Vì vậy, mọi nghiệm đều xuất hiện thành từng cặp hoán vị, suy ra số lượng nghiệm là chẵn hoặc bằng 0.

Lời giải. [5]Nếu không có nghiệm thì rõ ràng số lượng là 0. Giả sử tồn tại ít nhất một nghiệm $(x, y) \in \mathbb{Z}^2_{>0}$ thỏa mãn hai điều kiện. Định nghĩa ánh xạ:

$$\mathrm{T}(x, y) = (x', y') = (2x - 3y,\ x - 2y).$$

Bước 1. Kiểm tra (x', y') vẫn là số nguyên dương: Từ bất đẳng thức $2y \leq x - 1 \Rightarrow x \geq 2y + 1$, suy ra:

$$\left.\begin{array}{rcl} x' & = & 2x - 3y \geq 2(2y + 1) - 3y = 4y + 2 - 3y = y + 2 \geq 3 \\ y' & = & x - 2y \geq 2y + 1 - 2y = 1. \end{array}\right\} \implies x', y' \in \mathbb{Z}_{>0}$$

Bước 2. Kiểm tra bảo toàn phương trình:

$$\begin{aligned} &(2x - 3y)^2 - 3(x - 2y)^2 + 2 = 4x^2 - 12xy + 9y^2 - 3(x^2 - 4xy + 4y^2) + 2 \\ &= 4x^2 - 12xy + 9y^2 - 3x^2 + 12xy - 12y^2 + 2 = x^2 - 3y^2 + 2 = 16m \implies (i) \end{aligned}$$

Bước 3. Kiểm tra điều kiện (ii) sau ánh xạ:

$$\begin{aligned} &2y' = 2(x - 2y) = 2x - 4y, \quad x' - 1 = 2x - 3y - 1. \\ &2x - 4y \leq 2x - 3y - 1 \iff -4y \leq -3y - 1 \iff -y \leq -1 \iff y \geq 1 \implies y \in \mathbb{Z}_{>0} \end{aligned}$$

Bước 4. Chứng minh T là một ánh xạ nghịch đảo (involution):

$$\begin{aligned} \mathrm{T}(\mathrm{T}(x, y)) &= \mathrm{T}(2x - 3y,\ x - 2y) = (2(2x - 3y) - 3(x - 2y),\ (2x - 3y) - 2(x - 2y)) \\ &= (4x - 6y - 3x + 6y,\ 2x - 3y - 2x + 4y) = (x, y). \end{aligned}$$

Bước 5. Không có điểm bất biến: Giả sử $\mathrm{T}(x, y) = (x, y) \Rightarrow x = 2x - 3y,\ y = x - 2y$. Giải hệ này:

$$\begin{aligned} &x = 3y, \quad y = 3y - 2y = y \implies x^2 - 3y^2 + 2 = 9y^2 - 3y^2 + 2 = 6y^2 + 2. \\ &\implies 6y^2 + 2 \equiv 0 \pmod{16} \Rightarrow 6y^2 \equiv -2 \pmod{16}, \end{aligned}$$

nhưng $6y^2 \pmod{16} \in \{0, 6, 8, 14, 2, 10, 12\}$, không có giá trị nào cho ra $-2 \equiv 14$. Mâu thuẫn.

Vậy không có điểm bất biến, và ánh xạ chia các nghiệm thành từng cặp hoán vị. Do đó số nghiệm là số chẵn, hoặc bằng 0. □

[5]Lời giải chính thức.

Ví dụ (MEMO 2015/T/P7)

[**25M**] Tìm tất cả các cặp số nguyên dương (a, b) sao cho:

$$a! + b! = a^b + b^a.$$

Phân tích — Ta xét ba trường hợp sau:

- **Trường hợp $a = b$:** Phương trình trở thành $2a! = 2a^a$, với $a \geq 2$ thì $a! < a^a$, nên không thỏa mãn. Chỉ có $a = 1 \Rightarrow (a, b) = (1, 1)$ là nghiệm.
- **Trường hợp $a = 1$:** Khi đó $1 + b! = 1 + b \Rightarrow b! = b$, suy ra $b = 2$. Do đó, $(a, b) = (1, 2)$ và $(a, b) = (2, 1)$ là nghiệm.
- **Trường hợp $1 < a < b$:** Ta có $a! + b! < a^b + b^a$ vì $a! < a^b$ và $b! < b^a$. Do đó, không có nghiệm.

Cũng có thể xét một cách khác với $p \mid a$ và sử dụng phân tích p-adic, dẫn đến mâu thuẫn. Kết luận, các nghiệm duy nhất là $(a, b) = (1, 1), (1, 2), (2, 1)$.

Lời giải. [6] *Trường hợp $a = b$:* Khi đó:

$$2a! = 2a^a \quad \Rightarrow \quad a! = a^a.$$

Với $a \geq 2$, ta có $a! < a^a$, nên không thỏa mãn. Chỉ có $a = 1 \Rightarrow (a, b) = (1, 1)$ là nghiệm.

Trường hợp $a = 1$:

$$1! + b! = 1 + b! = 1^b + b^1 = 1 + b \Rightarrow b! = b \Rightarrow b = 2.$$

Suy ra $(a, b) = (1, 2)$ là nghiệm. Tương tự, $b = 1 \Rightarrow (a, b) = (2, 1)$ cũng là nghiệm.

Giả sử $1 < a < b$: Khi đó:

$$a! + b! < a^b + b^a,$$

do $a! < a^b$ và $b! < b^a$, nên phương trình không thể đúng.

Một cách khác: giả sử (a, b) là nghiệm với $1 < a < b$, xét một số nguyên tố $p \mid a$. Khi đó:

$$p \mid b! \Rightarrow p \mid b^a \Rightarrow p \mid a^b + b^a.$$

Xét số mũ p hai vế:

- Vế phải: $\nu_p(a^b + b^a) \geq a$.
- Vế trái: $\nu_p(a! + b!) = \nu_p(a!)$ (vì $b!$ chia hết cho $a!$). Nhưng $\nu_p(a!) = \sum_{k=1}^{\infty} \left\lfloor \frac{a}{p^k} \right\rfloor < a$.

Mâu thuẫn, nên loại trường hợp $1 < a < b$.

Kết luận: Các nghiệm duy nhất là:

$$\boxed{(a, b) \in \{(1, 1), (1, 2), (2, 1)\}}.$$

□

[6] Lời giải chính thức.

Ví dụ (USA 2015 MO/P1)

[**15M**] Giải trong tập số nguyên phương trình

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

Phân tích — Start by letting $x + y = 3t$. Substitute into the equation, simplify, and arrive at a form where $4t + 1$ must be a perfect square. Let $4t + 1 = (2n + 1)^2$, which leads to $t = n^2 + n$. Solve for x and y in terms of n, yielding the general solution for integer pairs (x, y).

Lời giải. [7]Đặt $x + y = 3t$. Khi đó:

$$x^2 + xy + y^2 = (t+1)^3 \quad \Longrightarrow \quad x^2 + x(3t - x) + (3t - x)^2 = (t+1)^3.$$

Rút gọn và chuyển vế:

$$(2x - 3t)^2 = (t-2)^2(4t+1).$$

Đặt $4t + 1 = (2n + 1)^2 \Rightarrow t = n^2 + n$. Thay vào:

$$2x - 3(n^2 + n) = \pm\left((n^2 + n - 2)(2n + 1)\right).$$

Vế phải có thể rút gọn thành:

$$2n^3 + 3n^2 - 3n - 2,$$

và giải ra:

$$x = n^3 + 3n^2 - 1 \quad \text{hoặc} \quad x = -n^3 + 3n + 1.$$

Vì $y = 3t - x = 3(n^2 + n) - x$, ta thu được hai cặp nghiệm đối xứng:

$$(x, y) = \left(n^3 + 3n^2 - 1,\ -n^3 + 3n + 1\right) \quad \text{và} \quad (-n^3 + 3n + 1,\ n^3 + 3n^2 - 1),$$

với mọi $n \in \mathbb{Z}$. □

[7]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.

Phân tích — Giả sử $ac + bd$ là một số nguyên tố. Ta biến đổi biểu thức

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

thu được tích bốn nhân tử. Vì các biến phân biệt, không nhân tử nào bằng 0. Ta suy ra $ac + bd \mid e^5(cd - ab)(cd + ab)$. Nếu $ac + bd$ là số nguyên tố, nó phải chia e^5, nhưng điều này mâu thuẫn với tính chất lũy thừa bậc 5 của e, do đó $ac + bd$ không thể là số nguyên tố, tức là hợp số.

Lời giải. [8]Giả sử ngược lại rằng $ac + bd$ là một số nguyên tố.

Không mất tính tổng quát, giả sử $a > d$. Từ $a^4 + b^4 = c^4 + d^4$, 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 $a^4 + b^4 = c^4 + d^4 = e^5$, nên:

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

Nếu $ac - bd = 0$ hoặc $ad - bc = 0$, thì ta có tỉ lệ $\frac{a}{b} = \frac{c}{d}$ hoặc $\frac{a}{b} = \frac{d}{c}$, mâu thuẫn với giả thiết các số đều phân biệt. Vậy mọi nhân tử đều khác 0.

Khi đó, $ac + bd \mid e^5(cd - ab)(cd + ab)$. Nhưng vì $ac + bd > cd + ab$, ta thấy $ac + bd \nmid cd + ab$ và cũng không chia hết $cd - ab$. Suy ra $ac + bd \mid e^5$. Gọi $ac + bd = p$, khi đó $p \mid e^5 \Rightarrow p \leq e$.

Nhưng:

$$e = \sqrt[5]{a^4 + b^4} \leq \sqrt[5]{2a^4} = a^{4/5} \cdot 2^{1/5} < a.$$

Vì $ac + bd > ab$, thì $p > ab$, mâu thuẫn với $p \leq e < a \leq ab$.

Vậy $ac + bd$ không thể là số nguyên tố, tức là nó là hợp số. □

[8]Lời giải chính thức.

4.2 Bài tập

Bài tập (BGR 2015 EGMO TST/P4). [30M] [9]Chứng minh rằng với mọi số nguyên dương m, tồn tại vô số cặp số nguyên dương (x, y) nguyên tố cùng nhau sao cho:

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

Nhận xét. Tìm cách xây dựng (hoặc suy luận) các nghiệm từ công thức tham số. Thử coi (x, y) vừa đủ điều kiện chia, kết hợp với sự nguyên tố cùng nhau của (x, y). Xem định lý Euclid về vô hạn số nguyên tố để tạo dãy vô hạn đáp ứng yêu cầu.

Bài tập (BGR 2015 EGMO TST/P6). [30M] Chứng minh rằng với mọi số nguyên dương $n \geq 3$, tồn tại n số nguyên dương phân biệt sao cho tổng các lập phương của chúng cũng là một lập phương hoàn hảo.

Nhận xét. Thử xây dựng một họ các bộ n số (có thể đồng dư hoặc biến thiên theo tham số) sao cho tổng lập phương thu được là (một giá trị tham số)^3. Các ví dụ quen thuộc là các "nhóm" số mà tổng lập phương khéo léo triệt tiêu và cộng dồn thành một khối lập phương.

Bài tập (FRA 2015 TST/3/P6). [25M] Tìm tất cả các cặp số nguyên (x, y) thỏa mãn:

$$x^2 = y^2(y^4 + 2y^2 + x).$$

Nhận xét. Thử cô lập x để bộc lộ tính chất của x liên quan đến đa thức bậc cao của y. Có thể suy luận y không quá lớn hoặc dùng cách phân tích trường hợp $(y = 0)$, $(y \neq 0)$ và khống chế cỡ của x để tìm nghiệm hữu hạn.

Bài tập (FRA 2015 TST/3/P9). [35M] Tìm tất cả các bộ ba (p, x, y), trong đó p là số nguyên tố và x, y là hai số nguyên dương, sao cho:

$$x^{p-1} + y \quad \text{và} \quad x + y^{p-1}$$

đều là các luỹ thừa của p.

Nhận xét. Khảo sát trước các trường hợp nhỏ cho x hay y (chẳng hạn 1 hoặc p) và kiểm tra tính chất đồng thời của hai biểu thức trở thành lũy thừa của p. Có thể dùng định lý LTE hoặc cân nhắc modulo p và modulo p^2 để khống chế số mũ và tính chia hết.

Bài tập (GBR 2015 TST/F1/P2). [20M] Cho dãy số nguyên $(a_n)_{n\geq 0}$ thỏa mãn:

$$a_0 = 1, \quad a_1 = 3, \quad \text{và} \quad a_{n+2} = 1 + \left\lfloor \frac{a_{n+1}^2}{a_n} \right\rfloor \text{ với mọi } n \geq 0.$$

Chứng minh rằng với mọi $n \geq 0$, ta có: $a_n a_{n+2} - a_{n+1}^2 = 2^n$.

Nhận xét. Gợi ý: Thử áp dụng quy nạp theo n, và phân tích biểu thức $a_{n+2} - 1 = \left\lfloor \frac{a_{n+1}^2}{a_n} \right\rfloor$ để liên hệ với a_n, từ đó tính sai khác $a_n a_{n+2} - a_{n+1}^2$ và chứng minh bằng lũy thừa của 2.

Bài tập (ROU 2014 MO/G7/P1). [25M] Tìm tất cả các số nguyên tố p và q, với $p \leq q$, sao cho

$$p(2q + 1) + q(2p + 1) = 2(p^2 + q^2).$$

[9]IMO SL 1992 P1.

Nhận xét. Thử xét phương trình theo modulo p hoặc q, rồi phân tích trường hợp nhỏ cho các cặp số nguyên tố.

Bài tập (ROU 2014 MO/G7/P3). [**25M**] Tìm tất cả các số nguyên dương n sao cho:

$$17^n + 9^{n^2} = 23^n + 3^{n^2}.$$

Nhận xét. Nhận xét rằng $17^n < 23^n$ với $n \geq 1$, và $9^{n^2} > 3^{n^2}$ với $n \geq 1$. So sánh từng cặp và tìm điểm cân bằng. Thử các giá trị nhỏ của n, vì n^2 tăng rất nhanh trong luỹ thừa.

Bài tập (ROU 2014 MO/G8/P3). [**15M**] Tìm số nguyên nhỏ nhất n sao cho tập hợp

$$A = \{n, n+1, n+2, \ldots, 2n\}$$

chứa năm phần tử $a < b < c < d < e$ thỏa mãn

$$\frac{a}{c} = \frac{b}{d} = \frac{c}{e}.$$

Nhận xét. Gọi tỉ số chung là r, ta có:

$$\frac{a}{c} = \frac{b}{d} = \frac{c}{e} = r \implies a = rc, \quad b = rd, \quad e = \frac{c}{r} \implies ae = c^2, \quad be = cd.$$

Bài tập (ROU 2014 MO/G9/P1). [**30M**] Tìm các số nguyên $x, y, z \in \mathbb{Z}$ sao cho

$$x^2 + y^2 + z^2 = 2^n(x + y + z)$$

với $n \in \mathbb{N}$.

Nhận xét. Thử đưa toàn bộ phương trình về một vế và nhóm các biểu thức theo từng biến. Xét biến đổi hoàn chỉnh bình phương để tạo điều kiện cho việc đánh giá hoặc tìm các nghiệm nhỏ. Ngoài ra, kiểm tra các trường hợp đặc biệt như $x = y = z$ hoặc $x + y + z = 0$ có thể giúp tìm nghiệm đặc biệt.

Bài tập (RUS 2015 TST/D10/P3). [**30M**] Tìm tất cả các số nguyên k sao cho tồn tại vô số bộ ba số nguyên (a, b, c) thỏa mãn:

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

Nhận xét. Hãy xét một cách xây dựng (hoặc tham số hoá) các nghiệm (a, b, c) - thí dụ, giả sử $(a^2 - k) = \alpha$, $(b^2 - k) = \beta$, thì $\alpha\beta = c^2 - k$. Cần tìm α, β để vô hạn (a, b, c) xuất hiện. Kiểm tra cách $(\alpha, \beta) = (t^2, \ldots)$ hoặc $\alpha = \beta$.

Chương 5

Số học đồng dư nâng cao

5.1 Các ví dụ

Ví dụ (APMO 2015/P3)

[**30M**] Một dãy số thực $a_0, a_1, \ldots$ được gọi là **tốt** nếu thỏa mãn ba điều kiện sau:

(i) a_0 là một số nguyên dương.

(ii) Với mỗi số nguyên không âm i, ta có:

$$a_{i+1} = 2a_i + 1 \quad \text{hoặc} \quad a_{i+1} = \frac{a_i}{a_i + 2}.$$

(iii) Tồn tại số nguyên dương k sao cho $a_k = 2014$.

Tìm số nguyên dương nhỏ nhất n sao cho tồn tại một dãy tốt $(a_0, a_1, \ldots)$ với $a_n = 2014$.

Phân tích — Ta xét a_0 và biến đổi theo dãy phân số. Đặt $b_i = \frac{1}{a_i+1}$, ta thấy dãy b_i có dạng đệ quy với hai lựa chọn $\varepsilon_i \in \{0, 1\}$, và b_k phải bằng $\frac{1}{2015}$. Vấn đề trở thành việc tìm giá trị nhỏ nhất của k sao cho $2015 \mid 2^k - 1$, tức là tìm $\text{ord}_{2015}(2) = k$.

Lời giải. (Cách 1)[1]Ta có:

$$a_{i+1} + 1 = 2(a_i + 1) \quad \text{hoặc} \quad a_{i+1} + 1 = \frac{a_i + 2}{a_i + 1}.$$

Suy ra:

$$\frac{1}{a_{i+1} + 1} = \frac{1}{2(a_i + 1)} \quad \text{hoặc} \quad \frac{1}{a_{i+1} + 1} = \frac{1}{2}.$$

Suy ra:

$$\frac{1}{a_k + 1} = \frac{1}{2^k}\left(\frac{1}{a_0 + 1} + \sum_{i=1}^{k} \varepsilon_i \cdot 2^{i-1}\right), \tag{1}$$

với $\varepsilon_i \in \{0, 1\}$.

Đặt $a_k = 2014 \implies a_k + 1 = 2015$, nhân (1) với $2^k \cdot 2015$, ta có:

$$2^k = 2015\left(\frac{1}{a_0 + 1} + \sum_{i=1}^{k} \varepsilon_i \cdot 2^{i-1}\right) \implies \frac{1}{a_0 + 1} = \frac{2^k}{2015} - \sum_{i=1}^{k} \varepsilon_i \cdot 2^{i-1}.$$

Để $a_0 + 1 \in \mathbb{Z}$, cần $2015 \mid 2^k$, tức là:

$$2015 \mid 2^k - 1.$$

Phân tích: $2015 = 5 \cdot 13 \cdot 31$, với:

$$2^4 \equiv 1 \pmod 5, \quad 2^{12} \equiv 1 \pmod{13}, \quad 2^{30} \equiv 1 \pmod{31} \implies \text{lcm}(4, 12, 30) = 60.$$

Vì $\text{ord}_{2015}(2) = 60$, nên số nhỏ nhất là:

$$\boxed{k = 60}$$

□

Phân tích — Cách tiếp cận thứ hai là đi ngược từ $a_k = 2014$ về a_0 bằng biểu diễn phân số $\frac{m_i}{n_i}$. Mỗi bước xây dựng dãy phân số tuân theo truy hồi đơn giản, bảo toàn tổng $m_i + n_i = 2015$, với $\gcd(m_i, n_i) = 1$.

Quan sát cho thấy:

$$(m_i, n_i) \equiv (-2^i, 2^i) \pmod{2015} \Rightarrow 2^k \equiv 1 \pmod{2015}.$$

Từ đó xác định được giá trị nhỏ nhất của k cần tìm.

Lời giải. (Cách 2)[1] Đặt $a_k = \frac{2014}{1} = \frac{m_0}{n_0}$, và định nghĩa dãy ngược:

$$a_{k-i} = \frac{m_i}{n_i}, \quad i \geq 0$$

với truy hồi:

$$(m_{i+1}, n_{i+1}) = \begin{cases} (m_i - n_i,\ 2n_i) & \text{nếu } m_i > n_i \\ (2m_i,\ n_i - m_i) & \text{nếu } m_i < n_i. \end{cases}$$

Ta có:

$$m_i + n_i = 2015, \quad \gcd(m_i, n_i) = 1 \implies (m_i, n_i) \equiv (-2^i, 2^i) \pmod{2015} \implies 2^k \equiv 1 \pmod{2015}.$$

Nên số nhỏ nhất là:

$$\boxed{k = 60}$$

□

[1] Lời giải chính thức.

Ví dụ (CAN 2015 MO/P5)

[**30M**] Cho p là một số nguyên tố sao cho $\frac{p-1}{2}$ cũng là số nguyên tố, và cho a, b, c là các số nguyên không chia hết cho p. Chứng minh rằng có nhiều nhất $1+\sqrt{2p}$ số nguyên dương n sao cho $n < p$ và $p \mid (a^n + b^n + c^n)$.

Phân tích — Ta cần đếm số nghiệm nguyên dương $n < p$ sao cho $a^n + b^n + c^n \equiv 0 \pmod{p}$. Phương pháp giải chủ yếu sử dụng định lý Fermat nhỏ, phân tích bậc lũy thừa của các số modulo p và số lượng cặp sai khác giữa các nghiệm n. Cuối cùng, ta suy ra rằng số lượng nghiệm là $\sqrt{2p}+1$ hoặc ít hơn.

Lời giải. (Cách 1)[2]Giả sử trước hết rằng $ac+bd$ là một số nguyên tố.

Không mất tính tổng quát, giả sử $a > d$. Từ $a^4+b^4 = c^4+d^4$, 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 $a^4+b^4 = c^4+d^4 = e^5$, nên:

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

Nếu $ac-bd=0$ hoặc $ad-bc=0$, thì ta có tỷ lệ $\frac{a}{b} = \frac{c}{d}$ hoặc $\frac{a}{b} = \frac{d}{c}$, mâu thuẫn với giả thiết các số đều phân biệt. Vậy mọi nhân tử đều khác 0.

Khi đó, $ac+bd \mid e^5(cd-ab)(cd+ab)$. Nhưng vì $ac+bd > cd+ab$, ta thấy $ac+bd \nmid cd+ab$ và cũng không chia hết $cd-ab$. Suy ra $ac+bd \mid e^5$. Gọi $ac+bd = p$, khi đó $p \mid e^5 \Rightarrow p \le e$.

Nhưng:

$$e = \sqrt[5]{a^4+b^4} \le \sqrt[5]{2a^4} = a^{4/5} \cdot 2^{1/5} < a.$$

Vì $ac+bd > ab$, thì $p > ab$, mâu thuẫn với $p \le e < a \le ab$.

Vậy $ac+bd$ không thể là số nguyên tố, tức là nó là hợp số. □

[2]Lời giải chính thức.

Ví dụ (EMC 2015/P1)

[**20M**] Cho tập $A = \{a, b, c\}$ gồm ba số nguyên dương. Chứng minh rằng tồn tại tập con $B = \{x, y\} \subset A$ sao cho với mọi số nguyên dương lẻ m, n, ta có:

$$10 \mid x^m y^n - x^n y^m.$$

Phân tích — Ta cần tìm hai phần tử x, y sao cho $x^m y^n - x^n y^m \equiv 0 \pmod{10}$ với mọi số lẻ m, n. Phương pháp giải bao gồm:

- Chứng minh chia hết cho 2 bằng cách phân tích chẵn lẻ của x và y.
- Dùng nguyên lý Dirichlet để xử lý modulo 5, chọn cặp sao cho $x + y \equiv 0 \pmod{5}$.

Kết hợp chia hết cho 2 và 5, ta có $10 \mid x^m y^n - x^n y^m$.

Lời giải. (Cách 1)[3]Xét $f(x, y) = x^m y^n - x^n y^m$. Nếu $m = n$, ta có $f(x, y) = 0$, chia hết cho 10 với mọi x, y, nên ta giả sử $n > m$.

Vì m, n lẻ $\implies$ $n - m$ chẵn. Khi đó:

$$f(x, y) = x^m y^m (y^{n-m} - x^{n-m}) = x^m y^m (y^2 - x^2) Q(x, y) = x^m y^m (y - x)(y + x) Q(x, y),$$

với $Q(x, y) \in \mathbb{Z}[x, y]$.

Xét chia hết cho 2: Nếu x hoặc y chẵn $\implies$ $2 \mid f(x, y)$. Nếu x, y đều lẻ, thì $x \pm y$ chẵn $\implies$ $2 \mid f(x, y)$ cho nên Luôn có $2 \mid f(x, y)$.

Xét chia hết cho 5:

Trường hợp 1: Tồn tại phần tử trong A chia hết cho 5. Chọn phần tử đó và một phần tử bất kỳ khác, khi đó $5 \mid x$ hoặc y cho nên $5 \mid f(x, y)$.

Trường hợp 2: Không phần tử nào chia hết cho 5 cho nên mỗi phần tử $\not\equiv 0 \pmod{5}$. Do A có 3 phần tử, mỗi phần dư $\pmod{5} \in \{1, 2, 3, 4\}$. Áp dụng nguyên lý Dirichlet:

- Nếu tồn tại hai phần tử cùng dư modulo 5: chọn cặp đó cho nên $x \equiv y \pmod{5}$ $\implies$ $x - y \equiv 0 \pmod{5}$ $\implies$ $5 \mid f(x, y)$.
- Nếu cả ba phần tử khác nhau modulo 5 cho nên chắc chắn tồn tại một trong hai cặp $(1, 4)$ hoặc $(2, 3)$ thuộc A. Vì $1+4 \equiv 0 \pmod{5}$, $2+3 \equiv 0 \pmod{5}$ cho nên chọn cặp đó: $x+y \equiv 0 \pmod{5}$ $\implies$ $5 \mid f(x, y)$.

Kết luận: Trong mọi trường hợp, tồn tại $\{x, y\} \subset A$ sao cho:

$$\boxed{10 \mid x^m y^n - x^n y^m \quad \text{với mọi số lẻ } m, n}$$

□

[3]Lời giải chính thức.

Ví dụ (FRA 2015 RMM/P3)

[**30M**] Cho số nguyên tố $p \geq 5$. Chứng minh rằng tập hợp

$$K = \left\{a \in \mathbb{Z} \mid a^{p-1} \equiv 1 \pmod{p^2}\right\}$$

chứa ít nhất hai số nguyên tố lẻ phân biệt nhỏ hơn p.

Phân tích — Cần chứng minh rằng trong tập K, có ít nhất hai số nguyên tố lẻ phân biệt nhỏ hơn p. Ta sử dụng ý tưởng sau:

- Xét nhóm con K của $\mathbb{Z}_p^*$ mở rộng modulo p^2.
- Dùng khai triển nhị thức để tìm điều kiện về $(a+kp)^{p-1} \equiv 1 \pmod{p^2}$.
- Xác định các số nguyên tố nhỏ hơn p và chỉ ra mâu thuẫn khi giả sử có ít hơn hai số như vậy trong K.

Kết hợp các yếu tố trên, ta chứng minh được yêu cầu bài toán.

Lời giải. (Cách 1)[4]Trước hết, bài toán là hiển nhiên nếu $p = 5$, vì khi đó

$$2^{p-1} \equiv 16 \not\equiv 1 \pmod{p^2} \quad \text{và} \quad 3^{p-1} \equiv 6 \not\equiv 1 \pmod{p^2}.$$

Giả sử từ đây $p \geq 7$. Đặt

$$K = \{\, n \in \mathbb{Z} \mid n^{p-1} \equiv 1 \pmod{p^2}\}.$$

(a) K đóng dưới phép nhân.

(b) Nếu $a \in K$ (tức $a \not\equiv 0 \pmod{p}$) và $k \in \mathbb{Z}$, ta tính:

$$(a+kp)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}\,k\,p \equiv 1 - kp\,a^{p-2} \pmod{p^2}.$$

Vậy $a + kp \in K \iff k \in p\mathbb{Z}$.

Tiếp theo, vì $\{-1, 1\} \subset K$, phải có $\{p-1, p+1\} \not\subset K$. Thế nên tồn tại hai số nguyên tố $q \mid (p-1)$ và $r \mid (p+1)$ với $\{q, r\} \cap K = \emptyset$. Khi $q \neq r$, ta được hai số nguyên tố lẻ phân biệt $\leq p$. Nếu $q = r$, thì $q = 2$, cũng suy ra $2 \notin K$.

Trong trường hợp còn lại (tức mọi số nguyên tố lẻ $\leq p-1$ đều thuộc K) sẽ dẫn đến mâu thuẫn: ta chọn $\theta = 1$ hoặc 5 tùy $p \mod 3$, từ đó suy ra $2p + \theta \in K$ trong khi $\theta \in K$ và $\theta \notin p\mathbb{Z}$, gây nghịch lý.

Vậy kết luận, ắt phải có hai số nguyên tố lẻ $< p$ nằm trong K. □

[4]Lời giải chính thức.

Ví dụ (GER 2015 MO/P4)

[**20M**] Cho số nguyên dương k. Định nghĩa n_k là số có dạng thập phân $70\underbrace{00\ldots0}_{k \text{ chữ số } 0}1$. Chứng minh rằng:

- Không có số nào trong các số n_k chia hết cho 13.
- Có vô số số n_k chia hết cho 17.

Phân tích — Xét $n_k = 70\underbrace{00\ldots0}_{k \text{ chữ số } 0}1 = 7 \cdot 10^{k+1} + 1$.

- Với modulo 13: Cần $10^{k+1} \equiv 11 \pmod{13}$, nhưng chu kỳ $10^t \pmod{13}$ không có giá trị 11, nên không có k thỏa mãn.
- Với modulo 17: Cần $10^{k+1} \equiv 12 \pmod{17}$, và chu kỳ $10^t \pmod{17}$ có giá trị 12 tại $t = 15$, nên $k + 1 \equiv 15 \pmod{16}$, dẫn đến vô số n_k chia hết cho 17.

Lời giải. [5]

$$n_k = 7 \cdot 10^{k+1} + 1.$$

(a) Ta cần xét $n_k \equiv 0 \pmod{13} \iff 7 \cdot 10^{k+1} \equiv -1 \pmod{13}$.

Khi $7^{-1} \equiv 2 \pmod{13}$, điều này tương đương $10^{k+1} \equiv 11 \pmod{13}$.

Dãy $\{10^t \bmod 13\}$ có chu kỳ 6:

$$10^1 \equiv 10,\ 10^2 \equiv 9,\ 10^3 \equiv 12,\ 10^4 \equiv 3,\ 10^5 \equiv 4,\ 10^6 \equiv 1, \ldots$$

không bao giờ bằng 11. Vậy không tồn tại k để $n_k \equiv 0 \pmod{13}$.

(b) Tương tự, $n_k \equiv 0 \pmod{17} \iff 7 \cdot 10^{k+1} \equiv -1 \pmod{17} \iff 10^{k+1} \equiv -7^{-1} \pmod{17}$.

Bởi $7^{-1} \equiv 5 \pmod{17} \implies -7^{-1} \equiv -5 \equiv 12 \pmod{17}$.

Xem $\{10^t \bmod 17\}$ có chu kỳ 16, tìm $10^{k+1} \equiv 12$. Quả thật $10^{15} \equiv 12 \pmod{17}$.

Vậy $k + 1 \equiv 15 \pmod{16} \implies k \equiv 14 \pmod{16}$. Suy ra vô hạn k chia hết cho 17. □

[5] Dựa theo giải của **RagvaloD**.

Ví dụ (IMO 2015/N1)

[**30M**] Xác định tất cả các số nguyên dương M sao cho dãy số $a_0, a_1, a_2, \ldots$ được xác định bởi

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

chứa ít nhất một số nguyên.

Phân tích — Để a_k chứa số nguyên, ta xét $b_k = 2a_k$. Dãy b_k tạo thành số lẻ, với quy nạp chứng minh rằng $b_k \equiv 3 \pmod{2^m}$ với mọi m. Điều này dẫn đến $b_k = 3$, suy ra $a_k = \frac{3}{2}$ khi $M = 1$. Do đó, chỉ có $M = 1$ thỏa mãn.

Lời giải. (Cách 1)[6]Đặt $b_k = 2a_k \implies b_{k+1} = b_k \left\lfloor \frac{b_k}{2} \right\rfloor$.

Vì $b_0 = 2a_0 = 2M + 1$ là số nguyên lẻ, suy ra mọi b_k là số nguyên, và nếu giả sử dãy a_k không bao giờ là số nguyên, thì tất cả b_k phải là số lẻ.

Khi đó:

$$\left\lfloor \frac{b_k}{2} \right\rfloor = \frac{b_k - 1}{2} \implies b_{k+1} = b_k \cdot \frac{b_k - 1}{2} = \frac{b_k(b_k - 1)}{2}. \tag{1}$$

Ta sẽ chứng minh:

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

Chứng minh. Chứng minh bằng **??** theo m.

Bước cơ sở: $m = 1 \implies b_k$ là số lẻ, nên $b_k \equiv 1$ hoặc $3 \pmod 2$, nhưng vì $b_0 = 2M + 1 \equiv 3 \pmod 2$ nếu $M = 1$, nên đúng.

Bước quy nạp: Giả sử $b_k \equiv 3 \pmod{2^m} \implies b_k = 2^m d_k + 3$ với $d_k \in \mathbb{Z}$.

Khi đó:

$$b_{k+1} = \frac{b_k(b_k - 1)}{2} = \frac{(2^m d_k + 3)(2^m d_k + 2)}{2} \equiv 3 \cdot 2^m d_k + 3 \pmod{2^{m+1}}.$$

Suy ra d_k phải chẵn $\implies b_{k+1} \equiv 3 \pmod{2^{m+1}}$. Khẳng định được chứng minh. ■

Vì $b_k \equiv 3 \pmod{2^m}$ với mọi m, nên $b_k = 3 \implies a_k = \frac{3}{2} \implies M = 1$.

Kết luận:

$$\boxed{M = 1}$$

là giá trị duy nhất sao cho dãy a_k chứa một số nguyên. □

[6] Shortlist 2015 with solutions.

Ví dụ (IND 2015 TST3/P2)

[**30M**] 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.

Phân tích — Ta xét các trường hợp riêng biệt:

- Với $p = 2$, dễ dàng nhận thấy rằng luôn tồn tại vô số nghiệm.
- Với $p > 2$, ta phân tích các biểu thức $x^{p-1} + y = p^a$ và $x + y^{p-1} = p^b$, kết hợp với phân tích p-adic và định lý Fermat nhỏ để suy ra các giới hạn.
- Qua các phép thử, ta nhận thấy nghiệm duy nhất là $(3, 2, 5)$ với $p = 3$.

Lời giải. [7]**Trường hợp $p = 2$:** Với $x, y \in \mathbb{Z}_{>0}$, ta có:

$$x^{p-1} + y = x + y, \quad x + y^{p-1} = x + y \implies \text{cùng bằng tổng } x + y$$

Vì lũy thừa của 2 xuất hiện dày đặc, nên luôn tồn tại (x, y) sao cho tổng là lũy thừa của 2. Trường hợp này cho vô số nghiệm.

Giả sử từ đây $p > 2$. Đặt:

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

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

Xét:

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

Xét modulo p^a, do $p - 1$ chẵn:

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

Áp dụng định lý Fermat nhỏ: $x^{p-1} \equiv 1 \pmod{p} \implies x^{p(p-2)} \equiv 1 \pmod{p} \implies p \mid x + 1$.

Đặt $x + 1 = p^r \implies r = \nu_p(x + 1)$, ta xét lũy thừa lớn nhất của p chia hết $x^{p(p-2)} + 1$. Sử dụng khai triển nhị thức:

$$x = -1 \implies x^{p(p-2)} = (-1)^{p(p-2)} = 1 \implies x^{p(p-2)} + 1 = 2 \text{ không chia hết cho } p$$

Nhưng vì $p \mid x + 1 \implies p^r \le x + 1 \le p^a \implies a = r$ hoặc $r + 1$.

Nếu $a = r \implies x + 1 = p^a \implies x = p^a - 1 \implies y = p^a - x^{p-1}$

Một vài thử nghiệm: - $p = 3 \implies x = 2 \implies x^{p-1} = 4$, $y = 5 \implies x^{p-1} + y = 9 = 3^2$, $x + y^{p-1} = 2 + 25 = 27 = 3^3$

Nếu $p \ge 5$, thử với $x = p - 1 \implies x^{p-1} \ge (p-1)^4 \gg p^2 \implies x^{p-1} + y > p^a \implies$ mâu thuẫn.

Kết luận:

> Các bộ ba thỏa mãn là:
> $(p, x, y) = (2, x, y)$, với $x + y$ là lũy thừa của 2, và
> $(3, 2, 5)$

□

[7] IMO SL 2014 N5.

Ví dụ (IND 2015 TST4/P3)

[25M] 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.

Phân tích — Ta xét hai trường hợp:

- Với $p = 2$, $x + y$ luôn là lũy thừa của 2, có vô số nghiệm.
- Với $p > 2$, đặt $x^{p-1} + y = p^a$ và $x + y^{p-1} = p^b$, từ đó suy ra giới hạn cho x, y bằng các phương pháp p-adic và định lý Fermat nhỏ.

Các phép thử cho $p = 3$ dẫn đến nghiệm duy nhất là $(3, 2, 5)$, trong khi với $p \geq 5$, không có nghiệm nào thỏa mãn.

Lời giải. [8]**Trường hợp $p = 2$:** Với $x, y \in \mathbb{Z}_{>0}$, ta có:

$$x^{p-1} + y = x + y, \quad x + y^{p-1} = x + y \implies \text{cùng bằng tổng } x + y$$

Vì lũy thừa của 2 xuất hiện dày đặc, nên luôn tồn tại (x, y) sao cho tổng là lũy thừa của 2. Trường hợp này cho vô số nghiệm.

Giả sử từ đây $p > 2$. Đặt:

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

Giả sử $x \leq y \implies x^{p-1} + y \leq x + y^{p-1} \implies a \leq b \implies p^a \mid p^b$.

Xét:

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

Xét modulo p^a, do $p - 1$ chẵn:

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

Áp dụng định lý Fermat nhỏ: $x^{p-1} \equiv 1 \pmod{p} \implies x^{p(p-2)} \equiv 1 \pmod{p} \implies p \mid x + 1$.

Đặt $x + 1 = p^r \implies r = \nu_p(x + 1)$, ta xét lũy thừa lớn nhất của p chia hết $x^{p(p-2)} + 1$. Sử dụng khai triển nhị thức:

$$x = -1 \implies x^{p(p-2)} = (-1)^{p(p-2)} = 1 \implies x^{p(p-2)} + 1 = 2 \text{ không chia hết cho } p$$

Nhưng vì $p \mid x + 1 \implies p^r \leq x + 1 \leq p^a \implies a = r$ hoặc $r + 1$.

Nếu $a = r \implies x + 1 = p^a \implies x = p^a - 1 \implies y = p^a - x^{p-1}$

Một vài thử nghiệm:

$$p = 3 \implies x = 2 \implies x^{p-1} = 4,\ y = 5 \implies x^{p-1} + y = 9 = 3^2,\ x + y^{p-1} = 2 + 25 = 27 = 3^3.$$

Nếu $p \geq 5$, thử với $x = p - 1 \implies x^{p-1} \geq (p-1)^4 \gg p^2 \implies x^{p-1} + y > p^a \implies$ mâu thuẫn.

Kết luận:

> Các bộ ba thỏa mãn là:
> $(p, x, y) = (2, x, y)$, với $x + y$ là lũy thừa của 2, và $(3, 2, 5)$

□

[8] IMO SL 2014 N5.

Ví dụ (IRN 2015 MO/N4)

[**35M**] 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 $k = \ell$.

Phân tích — Ta cần chứng minh rằng nếu hai biểu thức $n^k + a^n + c$ và $n^\ell + b^n + d$ luôn có cùng tập thừa số nguyên tố với mọi n, thì các tham số phải giống hệt nhau.

Hướng tiếp cận:

- Xét các giá trị lớn của n, và sử dụng mô hình đồng dư modulo một số nguyên tố p thích hợp.
- Xây dựng một đa thức $P(s)$ và chứng minh rằng nó phải đồng nhất bằng 0.
- Từ đó rút ra điều kiện bắt buộc giữa các hệ số.

Lời giải. [9]Giả sử tồn tại các bộ số (a, b, c, d, k, ℓ) thỏa mãn điều kiện đề bài nhưng không đồng nhất.

Xét $n = (kp - t)(p - 1) + s$, với p là số nguyên tố lớn, $t, s \in \mathbb{N}$ cố định. Khi đó:

$$n \equiv s \pmod{p-1} \implies a^n \equiv a^s, \quad b^n \equiv b^s \pmod{p},$$
$$n \equiv t + s \pmod{p} \implies n^k \equiv (t+s)^k, \quad n^\ell \equiv (t+s)^\ell \pmod{p}.$$

Ta có:

$$n^k + a^n + c \equiv (t+s)^k + a^s + c \pmod{p}, \quad n^\ell + b^n + d \equiv (t+s)^\ell + b^s + d \pmod{p}.$$
$$p \mid n^k + a^n + c \implies (t+s)^k \equiv -a^s - c \pmod{p}, \quad (t+s)^\ell \equiv -b^s - d \pmod{p}.$$

Nâng hai vế lên bội chung:

$$(-(a^s + c))^\ell \equiv (-(b^s + d))^k \pmod{p} \implies p \mid (a^s + c)^\ell - (b^s + d)^k.$$

Đặt:

$$P(s) := (a^s + c)^\ell - (b^s + d)^k.$$

Nếu $P(s) \not\equiv 0$, thì $P(s)$ là đa thức khác hằng $\Rightarrow$ có vô hạn thừa số nguyên tố.

Nhưng với mỗi s, có thể chọn t, p sao cho $p \mid n^k + a^n + c \Rightarrow p \mid P(s)$, điều này mâu thuẫn trừ khi $P(s) = 0$ với mọi $s \in \mathbb{N}$.

Vậy:

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

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

$$(a^s + c)^{\ell'} = (b^s + d)^{k'}.$$

Giả sử $k' > 1$, với s đủ lớn thì $a^s \gg c$, nên $a^s + c$ không thể là lũy thừa bậc k', mâu thuẫn.

Tương tự với $\ell' > 1$. Vậy $k' = \ell' = 1 \Rightarrow k = \ell$, và:

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

Hiệu vế trái thay đổi theo s nếu $a \neq b$, trong khi vế phải là hằng số suy ra mâu thuẫn cho nên $a = b,\ c = d$.

Kết luận cuối cùng:

$$\boxed{a = b, \quad c = d, \quad k = \ell}$$

□

Ví dụ (POL 2015 MO/P3)

[**25M**] Cho $a_n = |n(n+1) - 19|$ với $n = 0, 1, 2, \ldots$ và $n \neq 4$. Chứng minh rằng nếu $\gcd(a_n, a_k) = 1$ với mọi $k < n$, thì a_n là một số nguyên tố.

Phân tích — Dãy $a_n = |n(n+1) - 19|$ được xây dựng từ một biểu thức bậc hai và có tính đơn điệu từng đoạn.

Ý tưởng giải:

- Nếu a_n không phải là số nguyên tố, tồn tại một ước nguyên tố $p \mid a_n$.
- Vì $a_n < (n+1)^2$, ta có $p < n+1$ và tồn tại $k < n$ sao cho $k \equiv n \pmod{p}$.
- Khi đó, $a_k \equiv a_n \pmod{p} \Rightarrow p \mid a_k \Rightarrow p \mid \gcd(a_k, a_n)$, mâu thuẫn với giả thiết.

Lời giải. [10]Ta nhận thấy $a_n = 1$ chỉ xảy ra tại $n = 4$, vì:

$$n(n+1) = 19 \iff n^2 + n - 19 = 0 \Rightarrow n = \frac{-1 \pm \sqrt{1+76}}{2} = 4.$$

Mà $n = 4$ đã bị loại trong đề bài.

Với $n \neq 4$, giả sử ngược lại rằng a_n không phải là số nguyên tố. Khi đó tồn tại một số nguyên tố p sao cho $p \mid a_n$.

Vì $a_n = |n(n+1) - 19| < (n+1)^2$, nên $p^2 \leq a_n < (n+1)^2 \Rightarrow p < n+1 \Rightarrow p \leq n$.

Tồn tại $k < n$ sao cho $k \equiv n \pmod{p}$. Khi đó:

$$a_k \equiv a_n \pmod{p} \Rightarrow p \mid a_k \Rightarrow p \mid \gcd(a_n, a_k),$$

mâu thuẫn với giả thiết $\gcd(a_n, a_k) = 1$.

Kết luận: a_n phải là số nguyên tố. □

Nhận xét. Giá trị 19 không đóng vai trò then chốt trong lý luận — nó chỉ là một hằng số cố định tạo ra một dãy số có tính chất nguyên tố thú vị. Một ví dụ nổi tiếng hơn là $n(n+1) + 41$, do Euler đề xuất, cho ra các số nguyên tố với nhiều giá trị nhỏ của n.

[9]Lời giải của **mojyla222**.
[10]Lời giải của **mavropnevma**.

Ví dụ (RMM 2015/P5)

[**25M**] Cho số nguyên tố $p \geq 5$. Với mỗi số nguyên dương k, định nghĩa $R(k)$ là phần dư khi chia k cho p, tức là $0 \leq R(k) < p$. Tìm tất cả các số nguyên dương $a < p$ sao cho với mọi $m = 1, 2, \ldots, p-1$, ta có:

$$m + R(ma) > a.$$

Phân tích — Ta cần tìm các giá trị $a \in \{1, 2, \ldots, p-1\}$ sao cho bất đẳng thức $m + R(ma) > a$ đúng với mọi $1 \leq m < p$. Hướng tiếp cận:

- Xét trường hợp đặc biệt $a = p - 1$.
- Với $a < p - 1$, phân tích cấu trúc $p = aq + r$ với $0 < r < a$, và kiểm soát phần dư $R(ma)$.
- Chứng minh rằng chỉ những $a = \left\lfloor \frac{p}{q} \right\rfloor$ với $q \in \{2, \ldots, p-1\}$ là chấp nhận được.

Lời giải. [11]Ta chia làm hai phần: chứng minh điều kiện đủ và điều kiện cần.

Phần 1: Chứng minh điều kiện đủ.

Trường hợp 1: $a = p - 1$.

Ta có:

$$ma \equiv -m \pmod{p} \Rightarrow R(ma) = p - m \Rightarrow m + R(ma) = p > a.$$

Trường hợp 2: $a = \left\lfloor \frac{p}{q} \right\rfloor$ *với* $q \in \{2, \ldots, p-1\}$.

Giả sử $p = aq + r$ với $0 < r < q$, xét $m = xq + y$ với $0 \leq x$, $1 \leq y \leq q$, ta có:

$$ma = a(xq + y) = x(p - r) + ay \Rightarrow R(ma) = ay - xr < aq < p.$$

Suy ra:

$$m + R(ma) \geq xq + y + ay - xr = x(q - r) + y(a + 1) > a.$$

Vậy bất đẳng thức luôn đúng.

Phần 2: Chứng minh điều kiện cần.

Giả sử a thỏa mãn bất đẳng thức, đặt $p = aq + r$ với $0 < r < a$. Chọn $m = q + 1$ (vì $m < p$):

$$ma = a(q + 1) = p + (a - r) \Rightarrow R(ma) = a - r,$$
$$m + R(ma) = q + 1 + a - r > a \Rightarrow r < q + 1.$$

Từ $p = aq + r$, suy ra $a = \left\lfloor \frac{p}{q} \right\rfloor$.

Kết luận: Các giá trị thỏa mãn là:

$$\boxed{a = \left\lfloor \frac{p}{q} \right\rfloor \text{ với } q \in \{2, \ldots, p-1\}, \quad \text{hoặc} \quad a = p - 1.}$$

□

[11]Lời giải chính thức.

Ví dụ (ROU 2015 TST/D2/P1)

[**25M**] Cho $a \in \mathbb{Z}$ và $n \in \mathbb{N}_{>0}$. Chứng minh rằng:

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

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

Phân tích — Ta nhóm các chỉ số k theo giá trị $d = \gcd(k,n)$. Mỗi giá trị a^d xuất hiện đúng $\phi(n/d)$ lần trong tổng, nên ta có:

$$\sum_{k=1}^{n} a^{\gcd(k,n)} = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) a^d.$$

Để chứng minh tổng này chia hết cho n, ta xét các ước nguyên tố p của n và chứng minh tổng chia hết cho $p^{v_p(n)}$ với mỗi p. Từ đó suy ra tổng chia hết cho n theo định lý cơ bản của số học.

Lời giải. Với mỗi ước $d \mid n$, số lần a^d xuất hiện là $\phi(n/d)$. Vậy:

$$\sum_{k=1}^{n} a^{\gcd(k,n)} = \sum_{d \mid n} \phi\left(\frac{n}{d}\right) a^d.$$

Xét một ước nguyên tố $p \mid n$, gọi $j = v_p(n)$. Mỗi ước $d \mid n$ có thể viết dưới dạng $d = p^i d'$, với $0 \le i \le j$ và $(d', p) = 1$. Khi đó:

$$\sum_{d \mid n} \phi\left(\frac{n}{d}\right) a^d = \sum_{\substack{d' \mid n \\ (d',p)=1}} \sum_{i=0}^{j} \phi\left(\frac{n}{p^i d'}\right) a^{p^i d'}.$$

Với $x = a^{d'}$, $\phi(n/(p^i d')) = \phi(n/(p^j d'))\,\phi(p^{j-i})$. Áp dụng Tổng Euler lũy thừa theo modulo:

$$\sum_{i=0}^{j} \phi(p^{j-i})\, x^{p^i} \equiv 0 \pmod{p^j}.$$

Nên toàn bộ tổng chia hết cho p^j. Lặp lại với mọi $p \mid n$, suy ra:

$$\sum_{k=1}^{n} a^{\gcd(k,n)} \equiv 0 \pmod{n}.$$

□

Ví dụ (RUS 2015 TST/D7/P5)

[35M] 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.

Phân tích — Bài toán yêu cầu chứng minh rằng không phải mọi $a < p-1$ đều thỏa mãn $a^{p-1} \equiv 1 \pmod{p^2}$ hoặc $(a+1)^{p-1} \equiv 1 \pmod{p^2}$. Phương pháp hiệu quả là giả sử ngược lại — rằng mọi $a \in \{1, \ldots, p-2\}$ đều thỏa mãn ít nhất một trong hai điều kiện — rồi sử dụng khai triển nhị thức để xây dựng mâu thuẫn thông qua đánh giá đồng dư modulo p^2.

Lời giải. [12]Giả sử tồn tại a sao cho $p^2 \mid a^{p-1}-1$. Ta chứng minh:

Khẳng định — $p^2 \nmid (p-a)^{p-1}$.

Chứng minh. Sử dụng khai triển nhị thức:

$$(p-a)^{p-1} \equiv a^{p-1} - 1 + pa^{p-2} \pmod{p^2}.$$

Vì $p^2 \mid a^{p-1}-1 \Rightarrow (p-a)^{p-1} \equiv pa^{p-2} \not\equiv 0 \pmod{p^2}$. Đpcm. ■

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

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

Ta có $p^2 \mid 1^{p-1}-1=0 \Rightarrow$ giả sử phản chứng áp dụng tại $a=1$.

Từ khẳng định, $p^2 \nmid (p-1)^{p-1}-1 \Rightarrow p^2 \mid (p-2)^{p-1}-1$.

Khai triển:

$$(p-2)^{p-1} \equiv 2^{p-1} - p(p-1)2^{p-2} \pmod{p^2} \Rightarrow p^2 \mid 2^{p-1} - 1 + p2^{p-2}.$$

Nhân hai vế với $2^{p-1}+1$, ta được:

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

Mặt khác, lặp lại bước suy luận ta thu được:

$$p^2 \mid 3^{p-1}-1 \Rightarrow p^2 \nmid (p-3)^{p-1}-1 \Rightarrow p^2 \mid (p-4)^{p-1}-1 \Rightarrow p^2 \mid 4^{p-1}-1+p4^{p-2}. \tag{2}$$

So sánh (1) và (2):

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

Nhưng theo định lý Fermat nhỏ:

$$4^{p-1} \equiv 1, \quad 2^{p-1} \equiv 1 \pmod{p} \Rightarrow 4(4^{p-2}+2^{p-2}) \equiv 4 + 2 \cdot 2 \equiv 8 \not\equiv 0 \pmod{p},$$

cho nên mâu thuẫn.

Kết luận: Giả thiết phản chứng sai $\Rightarrow$

$$\boxed{\text{Tồn tại } a < p-1 \text{ sao cho } a^{p-1}-1 \text{ và } (a+1)^{p-1}-1 \text{ đều không chia hết cho } p^2.}$$

□

[12]Lời giải của **HoshimiyaMukuro**.

Ví dụ (THA 2015 MO/P5)

[**25M**] Với mỗi số thực x, ký hiệu $\lfloor x \rfloor$ là phần nguyên của x, tức là số nguyên lớn nhất không vượt quá x. Chứng minh rằng:

$$\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor$$

là số chẵn với mọi số nguyên dương n.

Phân tích — Bài toán yêu cầu chứng minh rằng phần nguyên của biểu thức $\frac{(n-1)!}{n(n+1)}$ luôn là số chẵn. Ta chia thành các trường hợp dựa trên tính chất nguyên tố hay hợp số của n và $n+1$ và áp dụng:

- Kiểm tra trực tiếp các giá trị nhỏ $n \leq 6$.
- Định lý Wilson: với số nguyên tố p, ta có $(p-1)! \equiv -1 \pmod{p}$.
- Với $n, n+1$ là hợp số, khi đó $n(n+1) \mid (n-1)!$, do đó biểu thức là số nguyên.
- Khi biểu thức là số nguyên, cần chứng minh nó chẵn — điều này thường suy ra từ việc $(n-1)!$ chứa nhiều thừa số chẵn.

Lời giải. [13]Ta xét các trường hợp.

Trường hợp 1: $n \leq 6$**.** Trực tiếp tính cho $n = 1, 2, \ldots, 6$, dễ thấy:

$$\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor = 0,$$

là số chẵn.

Trường hợp 2: $n \geq 8$**,** n **và** $n+1$ **là hợp số.** Khi đó tồn tại $a, b, c, d < n$ sao cho $n = ab$, $n+1 = cd$. Suy ra $n(n+1) \mid (n-1)!$. Do đó $\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor \in \mathbb{Z}$. Mặt khác, $(n-1)!$ chia hết cho 2 với $n \geq 8$, nên thương là số chẵn.

Trường hợp 3: $n \geq 7$**,** n **là số nguyên tố.** Khi đó áp dụng định lý Wilson:

$$(n-1)! \equiv -1 \pmod{n} \implies (n-1)! = nq - 1 \text{ với } q \in \mathbb{Z}.$$

Ta có:

$$\frac{(n-1)!}{n(n+1)} = \frac{q - \frac{1}{n}}{n+1} = \frac{q}{n+1} - \frac{1}{n(n+1)}.$$

Phần nguyên của biểu thức là $\left\lfloor \frac{q}{n+1} - \frac{1}{n(n+1)} \right\rfloor = \left\lfloor \frac{q}{n+1} \right\rfloor$ hoặc nhỏ hơn 1. Vì q là nguyên, và $(n-1)!$ rất lớn, giá trị này là số nguyên dương. Do $(n-1)!$ chẵn, còn $n(n+1)$ lẻ chẵn, thì thương là số chẵn.

Trường hợp 4: $n+1$ **là số nguyên tố (tức** $n = p-1$**).** Theo Wilson: $(p-1)! \equiv -1 \pmod{p}$, mà $(p-1)! = (n)! \Rightarrow n! \equiv -1 \pmod{n+1}$. Vậy:

$$n! = (n+1)t - 1 \text{ với } t \in \mathbb{Z}, \quad \frac{n!}{n(n+1)} = \frac{t - \frac{1}{n+1}}{n}.$$

Do đó, phần nguyên là $\left\lfloor \frac{t}{n} - \frac{1}{n(n+1)} \right\rfloor = \left\lfloor \frac{t}{n} \right\rfloor$, là số nguyên. Vì $n!$ chẵn và $n(n+1)$ chia hết cho 2, ta lại kết luận thương là số chẵn.

Kết luận:

$$\boxed{\left\lfloor \frac{(n-1)!}{n(n+1)} \right\rfloor \text{ là số chẵn với mọi } n \in \mathbb{Z}_{>0}.}$$

□

5.2 Bài tập

Bài tập (HUN 2015 TST/KMA/640). [30M] Hãy xác định tất cả các số nguyên tố p và các số nguyên dương n sao cho các số có dạng $(k+1)^n - 2k^n$ với $k = 1, 2, \ldots, p$ tạo thành một hệ đầy đủ các số dư modulo p.

Nhận xét. Hãy thử khảo sát với các giá trị nhỏ của p, chẳng hạn $p = 2, 3, 5$, và xem biểu thức $(k+1)^n - 2k^n$ có cho ra đủ p phần dư khác nhau modulo p hay không. Nếu không, ta loại trừ. Nếu có, cần kiểm tra xem tính chất đó có đúng với các giá trị lớn hơn hay không.

Bài tập (JPN 2015 MO1/P3). [30M] 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.

Nhận xét. (a) Quan sát rằng điều kiện $a_n + a_{n+1} < a_{n+2}$ dẫn đến tốc độ tăng nhanh của dãy. Từ đó, có thể áp dụng định lý số nguyên tố và ước lượng mật độ số nguyên tố để loại trừ vô hạn trường hợp.

(b) Ta có thể xây dựng dãy bằng phương pháp quy nạp. Tại mỗi bước, chọn a_{n+1} đủ lớn để tránh chia hết cho tất cả các ước nguyên tố của các số đã có. Hãy cân nhắc lựa chọn số nguyên tố mới, và kiểm tra xem điều kiện tăng mạnh có được giữ không.

Bài tập (THA 2015 MO/P8). [25M] Cho m, n là các số nguyên dương sao cho $m - n$ là số lẻ. Chứng minh rằng biểu thức

$$(m + 3n)(5m + 7n)$$

không thể là số chính phương.

Nhận xét. Sử dụng lập luận modulo 4 hoặc modulo 8 để loại trừ khả năng biểu thức là một số chính phương. Ngoài ra, hãy xét tính chẵn/lẻ của hai thừa số, và tổng quát hoá bằng phân tích đồng dư.

Bài tập (TWN 2015 TST2/Q2/P1). [30M] Cho dãy số $\{a_n\}$ xác định bởi:

$$a_{n+1} = a_n^3 + 103, \quad \text{với } n = 1, 2, 3, \ldots$$

Chứng minh rằng có nhiều nhất một số hạng a_n là số chính phương.

Nhận xét. Hãy thử kiểm tra các giá trị nhỏ của a_1, rồi khảo sát tốc độ tăng trưởng của dãy. Sử dụng mâu thuẫn: nếu hai số chính phương xuất hiện trong dãy, có thể dẫn đến bất khả về dạng số học.

[13] APMO 2004 P4.

5.3 Định lý, bổ đề, và hằng đẳng thức

Bổ đề 5.3.1 (Tổng Euler lũy thừa theo modulo)
Với mọi số nguyên tố p và số nguyên $j \geq 1$, và với mọi $x \in \mathbb{Z}$, ta có:

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

Chương 6

Luỹ thừa lớn nhất

6.1 Các ví dụ

Ví dụ (CHN 2015 MO/P4)

[**25M**] Xác định tất cả các số nguyên k sao cho tồn tại vô hạn số nguyên dương n không thỏa mãn:

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

Phân tích — Dùng định lý Kummer về số mũ của một số nguyên tố trong nhị thức, ta xét giá trị $\nu_2\left(\binom{2n}{n}\right)$. Chọn $n = 2^\alpha - k$, khi đó $n+k = 2^\alpha$, có $\nu_2(n+k) = \alpha$.

Mặt khác, định lý Kummer nói rằng:

$$\nu_2\left(\binom{2n}{n}\right) = \text{số chữ số “nhớ” khi cộng } n+n \text{ trong hệ nhị phân} < \alpha.$$

Từ đó, với $k \neq 1$, ta luôn có thể chọn α lớn để $\nu_2(n+k) > \nu_2\left(\binom{2n}{n}\right)$, suy ra không chia hết.

Trường hợp duy nhất không xảy ra điều này là $k = 1$, khi đó biểu thức trở thành $(n+1) \mid \binom{2n}{n}$, luôn đúng vì là số Catalan.

Lời giải. [1]Ta xét ba trường hợp:

Trường hợp 1: $k = 0$. Chọn $n = 2^\alpha$, với $\alpha \geq 2$. Khi đó:

$$\nu_2(n+k) = \alpha, \quad \nu_2\left(\binom{2n}{n}\right) = 1 \quad (\text{do Kummer}) \Rightarrow n+k \nmid \binom{2n}{n}.$$

Có vô hạn α, nên tồn tại vô hạn n vi phạm chia hết.

Trường hợp 2: $k \neq 0, 1$. Chọn $n = 2^\alpha - k$ với $\alpha \geq \log_2(|k|) + 3$, đủ lớn để:

$$n+k = 2^\alpha \Rightarrow \nu_2(n+k) = \alpha.$$

Dùng định lý Kummer:

$$\nu_2\left(\binom{2n}{n}\right) \leq \alpha - 1 \Rightarrow \text{không chia hết.}$$

Vậy có vô hạn n sao cho $n+k \nmid \binom{2n}{n}$.

Trường hợp 3: $k = 1$. Khi đó:

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

là số nguyên, tức $n+1 \mid \binom{2n}{n}$ với mọi n. Không tồn tại vô hạn n vi phạm chia hết.

Kết luận:

$$\boxed{\text{Tồn tại vô hạn } n \text{ sao cho } n+k \nmid \binom{2n}{n} \iff k \neq 1.}$$

□

[1]Lời giải của yunxiu.

Ví dụ (CHN 2015 TST3/D1/P3)

[**25M**] 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 viết dưới dạng tích của hai (hoặc nhiều) phần tử khác trong S. 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.

Phân tích — Gọi $g = \gcd(a, b)$, và viết $a = ga'$, $b = gb'$. Với giả thiết rằng g có ít nhất hai thừa số nguyên tố.

Ta chia làm hai trường hợp:

- Nếu $\gcd(b', g) > 1$, thì tồn tại số nguyên tố $p \mid b' \cap g$. Do đó $\nu_p(x) = \nu_p(g)$ với mọi $x \in S$, khiến không thể phân tích x thành tích các phần tử khác trong S.
- Nếu $\gcd(b', g) = 1$, chọn hai số nguyên tố $p, q \mid g$. Với mỗi phần tử $x \in S$, ta dùng thao tác biến đổi $(u, v) \mapsto (p^{\varphi(b')}u, v/p^{\varphi(b')})$ để điều chỉnh chỉ số ν_p, ν_q, giới hạn chúng, từ đó giới hạn số lượng thừa số không thể phân tích.

Ta thu được một cận trên t cho số lượng thừa số không thể phân tích.

Lời giải. [2]Gọi $g = \gcd(a, b)$, rồi viết $a = ga'$, $b = gb'$. Theo giả thiết, g có ít nhất hai thừa số nguyên tố. Xét hai trường hợp:

Trường hợp 1: $\gcd(b', g) > 1$. Chọn một số nguyên tố p sao cho $p \mid b'$ và $p \mid g$. Vì $p \nmid a'$, ta có $\nu_p(a) = \nu_p(g) < \nu_p(b)$. Khi đó với mọi $x \equiv a \pmod b$, ta có $\nu_p(x) = \nu_p(a)$. Do đó, x không thể là tích của hai phần tử khác có cùng chỉ số p, nên mỗi $x \in S$ là phần tử không thể phân tích.

Trường hợp 2: $\gcd(b', g) = 1$. Chọn hai số nguyên tố $p, q \mid g$. Xét một phần tử $x \in S$. Nếu x đã là phần tử không thể phân tích thì xong. Nếu không, tức là $x = uv$ với $u, v \in S$. Ta thực hiện thao tác chuyển đổi:

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

Vì $\gcd(b', p) = 1$, ta có $p^{\varphi(b')} \equiv 1 \pmod{b'}$, nên u vẫn thuộc lớp đồng dư $a \pmod b$. Lặp lại quá trình này đến khi:

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

Mỗi lần phân tích thêm đều yêu cầu chỉ số nguyên tố lớn hơn hoặc bằng $\nu_p(g)$ (hoặc $\nu_q(g)$) cho các thừa số, nên tổng số thừa số bị chặn trên bởi:

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

Vì t là hữu hạn, mọi phần tử trong S có thể được biểu diễn thành tích của không quá t phần tử không thể phân tích. □

[2]Lời giải của **MarkBcc168**.

Ví dụ (IMO 2015/N1)

[**20M**] Xác định tất cả các số nguyên dương M sao cho dãy số $a_0, a_1, a_2, \ldots$ được xác định bởi

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

chứa ít nhất một số nguyên.

Phân tích — Đặt $b_k = 2a_k$. Khi đó $b_0 = 2a_0 = 2M + 1$, là số nguyên lẻ, suy ra mọi b_k đều là số nguyên.

Nếu dãy (a_k) không bao giờ là số nguyên, thì các b_k đều là số lẻ. Khi đó công thức truy hồi trở thành:

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

Ta chứng minh bằng phương pháp mâu thuẫn rằng không thể xảy ra điều này mãi mãi, vì hiệu $b_k - 3$ giảm nhanh hơn cấp số nhân, dẫn đến mâu thuẫn với nguyên lý cực hạn.

Do đó $b_0 - 3 \leq 0 \Rightarrow b_0 = 3 \Rightarrow M = 1$ là giá trị nhỏ nhất thỏa mãn. Với $M = 1$, $a_0 = \frac{3}{2}$, và ta có $a_1 = \frac{9}{2}$, $a_2 = \frac{405}{2}$, $a_3 = \frac{82005}{2}$, v.v... không có số nguyên nào xuất hiện. Từ đó suy ra chỉ khi $M = 1$, dãy không chứa số nguyên.

Vậy để dãy chứa ít nhất một số nguyên thì cần và đủ $\boxed{M \neq 1}$.

Lời giải. (Cách 2)[3]Xét $b_k = 2a_k$. Khi đó,

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

Nếu dãy (a_k) không chứa số nguyên, thì mọi b_k là số lẻ và ta có:

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

Xét hiệu $b_k - 3$, ta thấy:

$$b_0 - 3 = 2M + 1 - 3 = 2(M - 1),$$

mà theo truy hồi trên, hiệu $b_k - 3$ giảm nhanh theo bậc số mũ. Điều này mâu thuẫn với nguyên lý cực hạn, vì một dãy số nguyên dương không thể giảm mãi mà vẫn dương.

Suy ra, chỉ có thể xảy ra khi $b_0 - 3 \leq 0 \Rightarrow b_0 \leq 3 \Rightarrow M = 1$. Khi đó $a_0 = \frac{3}{2}$, và dãy tiếp theo không bao giờ đạt giá trị nguyên.

Vậy điều kiện để dãy chứa ít nhất một số nguyên là:

$$\boxed{M \neq 1}.$$

□

[3]Lời giải chính thức – IMO Shortlist 2015.

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:

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

đều là lũy thừa của 2.

Phân tích — Bài toán yêu cầu tìm tất cả các bộ ba $(a, b, c) \in \mathbb{Z}^3_{>0}$ sao cho ba biểu thức đối xứng $ab - c$, $bc - a$, và $ca - b$ đều là lũy thừa của 2.

Hướng giải sử dụng:

- Giả sử $a \leq b \leq c$ để tránh xét các hoán vị trùng lặp.
- Thử trực tiếp các giá trị nhỏ của a như $2, 3, 4$, rồi giới hạn khả năng của b, c.
- Dùng các bất đẳng thức và điều kiện số học (chia hết, chẵn/lẻ) để loại trừ trường hợp.

Lời giải. [4]Các nghiệm thỏa mãn là: $(2, 2, 2)$, $(2, 2, 3)$, $(2, 6, 11)$, $(3, 5, 7)$, và các hoán vị của chúng.

Giả sử $a \leq b \leq c$, đặt:

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

Nếu $a = 1 \Rightarrow b - c = 2^m$, điều này không thể xảy ra vì vế trái có thể âm. Vậy $a \geq 2$.

Khi đó:

$$ca - b \geq (a - 1)c \geq 2 \Rightarrow n, p \geq 1.$$

Trường hợp 1: $a = b \geq 3$. Lúc này:

$$ac - b = a(c - 1) \Rightarrow a \mid 2^n. \text{ Vì } a \geq 3 \ implies\text{mâu thuẫn } a \neq b.$$

Trường hợp 2: $a = 2$. Ta có:

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

Nếu $p = 1 \Rightarrow bc = 4 \Rightarrow b = c = 2 \Rightarrow (2, 2, 2)$ là nghiệm.

Nếu $p > 1 \Rightarrow bc$ chẵn, và do đó c lẻ (vì b chẵn). Điều này buộc $m = 0$.

Thử các giá trị nhỏ của n để giải hệ phương trình:

$$2b - c = 1, \quad 2c - b = 2^n \implies (b, c) = (2, 3),\ (6, 11) \Rightarrow (2, 2, 3),\ (2, 6, 11).$$

Trường hợp 3: $a = 3$. Ta có:

$$3b - c = 2^m, \quad 3c - b = 2^n, \quad bc - 3 = 2^p.$$
$$b = 5,\ c = 7 \Rightarrow ab - c = 15 - 7 = 8,\ bc - a = 35 - 3 = 32,\ ca - b = 21 - 5 = 16,$$

đều là lũy thừa của 2. Nên $(3, 5, 7)$ là nghiệm.

Trường hợp 4: $a \geq 4$. Trong trường hợp này, $ca - b \geq (a - 1)c$ là rất lớn nên dễ vượt quá lũy thừa của 2 gần nhất. Hơn nữa, giới hạn từ $ab - c = 2^m$ sẽ mâu thuẫn với tốc độ tăng của ab, do đó không thể xảy ra.

Kết luận: Các bộ ba thỏa mãn là:

$$\boxed{(a, b, c) \in \{(2, 2, 2),\ (2, 2, 3),\ (2, 6, 11),\ (3, 5, 7)\} \text{ và các hoán vị.}}$$

□

[4]Lời giải chính thức.

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:

$$d_i \mid (d_{i+1} + d_{i+2}) \quad \text{với mọi } 1 \leq i \leq k-2.$$

Phân tích — Bài toán yêu cầu tìm các số nguyên hợp dương n sao cho mọi bộ ba ước liên tiếp (d_i, d_{i+1}, d_{i+2}) trong dãy các ước số dương tăng dần của n, đều thỏa mãn $d_i \mid (d_{i+1} + d_{i+2})$.

Hướng tiếp cận:

- Kiểm tra trước các số dạng $n = p^r$ với p là số nguyên tố, thấy rằng chúng đều thỏa mãn điều kiện.
- Giả sử n có ít nhất hai thừa số nguyên tố phân biệt, xét các ước liên tiếp và đưa về đánh giá chuẩn p-adic.
- Sử dụng mâu thuẫn về chỉ số p-adic để loại trừ trường hợp n có nhiều hơn một thừa số nguyên tố.

Lời giải. Trước tiên, ta chứng minh rằng mọi số dạng $n = p^r$ với $r \geq 2$ (tức là lũy thừa bậc cao của một số nguyên tố) đều thỏa mãn điều kiện.

Thật vậy, các ước số dương của p^r là:

$$1 = p^0 < p^1 < p^2 < \cdots < p^r.$$

Ta có:

$$p^i \mid (p^{i+1} + p^{i+2}) = p^i(p + p^2),$$

nên điều kiện $d_i \mid (d_{i+1} + d_{i+2})$ được thỏa mãn với mọi i.

Bây giờ giả sử n là hợp số có ít nhất hai thừa số nguyên tố phân biệt. Gọi $p < q$ là hai thừa số nguyên tố nhỏ nhất của n. Khi đó n chia hết cho pq, nên có các ước:

$$d = \frac{n}{q}, \quad d' = \frac{n}{p^j} \text{ với một số } j, \quad d'' = \frac{n}{p^{j-1}}.$$

Điều kiện bài toán yêu cầu:

$$\frac{n}{q} \mid \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right) = \frac{n}{p^j}(p+1).$$

Xét chuẩn p-adic hai vế:

$$\nu_p\left(\frac{n}{q}\right) = \nu_p(n) \quad \text{vì } p \nmid q, \text{ trong khi: } \nu_p\left(\frac{n}{p^j}(p+1)\right) = \nu_p(n) - j.$$

Vì $p \nmid (p+1)$, nên $\nu_p(p+1) = 0$. Suy ra:

$$\nu_p\left(\frac{n}{q}\right) > \nu_p\left(\frac{n}{p^j}(p+1)\right),$$

điều này mâu thuẫn với giả thiết rằng $\frac{n}{q} \mid \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right)$.

Do đó, n không thể có nhiều hơn một thừa số nguyên tố.

Kết luận: Mọi số n thỏa mãn bài toán là các số có dạng:

$$\boxed{n = p^r, \text{ với } p \text{ nguyên tố, } r \geq 2.}$$

□

[4] Shortlist 2023 with solutions.

Ví dụ (RUS 2015 MO11/P2)

[**25M**] 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?

Phân tích — Xét bài toán về tính chẵn lẻ của tổng các tử số trong các phân số tối giản dạng $\frac{k}{n}$ với $1 \le k < n$ và $\gcd(k, n) = 1$. Tổng này được gọi là $f(n)$. Bài toán yêu cầu kiểm tra tính chẵn lẻ của $f(n)$ và $f(2015n)$, và tìm xem có giá trị $n > 1$ nào sao cho chúng khác tính chẵn lẻ.

Ý tưởng chính gồm:

- Phân tích cách tử số thay đổi khi nhân thêm một hằng số (như 2015) vào mẫu số.
- Sử dụng định lý về định giá 2-adic (v_2) để xác định khi nào một tử số là số lẻ.
- Thấy rằng nếu n chẵn, thì tồn tại số lượng tử số lẻ khác nhau giữa $f(n)$ và $f(2015n)$, nên tính chẵn lẻ của chúng sẽ khác nhau.

Lời giải. (Cách 1)[5]Mỗi phân số $\frac{k}{n}$ tối giản có tử số là $\frac{k}{\gcd(k,n)}$. Tổng $f(n)$ là tổng các tử số này với $1 \le k < n$ và $\gcd(k, n) = 1$. Tương tự định nghĩa $f(2015n)$.

Xét khi nào $\frac{k}{\gcd(k,2015n)}$ là số lẻ. Gọi $v_2(k)$ là số mũ của 2 trong phân tích thừa số nguyên tố của k, thì:

$$v_2\left(\frac{k}{\gcd(k, 2015n)}\right) = v_2(k) - \min\left(v_2(k), v_2(2015n)\right).$$

Nên $\frac{k}{\gcd(k,2015n)}$ lẻ nếu và chỉ nếu $v_2(k) \le v_2(2015n)$: k không chia hết cho bậc cao hơn của 2 so với n.

Vì $2015 = 5 \cdot 13 \cdot 31$, nên $v_2(2015n) = v_2(n)$. Ta thấy số lượng k trong $\{1, 2, \ldots, 2015n - 1\}$ sao cho $v_2(k) \le v_2(n)$ là một số lẻ. Do đó, tổng $f(2015n)$ sẽ có số lẻ tử số lẻ — suy ra $f(2015n)$ lẻ, còn $f(n)$ chẵn (hoặc ngược lại). Kết luận, chúng luôn khác tính chẵn lẻ. □

Lời giải. (Cách 2)[6]Gọi $v_2(n) = \alpha$, tức $n = 2^\alpha \cdot \beta$ với β lẻ.

Ta dùng kết quả sau: $\frac{k}{n}$ có tử số lẻ nếu và chỉ nếu $v_2(k) \le \alpha$. Vậy số lượng tử số lẻ trong $f(n)$ là:

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

Vì $2015n = 2015 \cdot 2^\alpha \cdot \beta$, ta tính:

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

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

Mà β là số lẻ, nên $1007 \cdot \beta \equiv 1 \pmod 2 \Rightarrow \lfloor \cdot \rfloor$ của hai vế khác nhau modulo 2.

Vậy $f(n)$ và $f(2015n)$ luôn khác tính chẵn lẻ.

Kết luận: Với mọi $n > 1$, tồn tại sự khác biệt về tính chẵn lẻ giữa $f(n)$ và $f(2015n)$. □

[5]Lời giải của **JAnatolGT_00**.
[6]Lời giải của **kreegyt**.

Ví dụ (TWN 2015 TST3/D1/P3)

[**25M**] Cho số nguyên $c \geq 1$. Xét dãy số nguyên dương được xác định bởi:

$$a_1 = c, \quad a_{n+1} = a_n^3 - 4c \cdot a_n^2 + 5c^2 \cdot a_n + c \text{ với mọi } n \geq 1.$$

Chứng minh rằng với mỗi số nguyên $n \geq 2$, tồn tại một số nguyên tố p chia hết a_n nhưng không chia hết bất kỳ số nào trong các số $a_1, a_2, \ldots, a_{n-1}$.

Phân tích — Đặt $b_n = \frac{a_n}{c}$. Khi đó dãy thỏa đệ quy:

$$b_1 = 1, \quad b_{n+1} = c^2\, b_n(b_n^2 - 4b_n + 5) + 1.$$

Ta sẽ chứng minh:

- Mỗi b_n là số nguyên dương.
- Với mọi m, n, ta có $b_{m+n} \equiv b_m \pmod{b_n}$, và nếu $m \geq 2$, thì $b_{m+n} \equiv b_m \pmod{b_n^2}$.
- Từ đó suy ra: nếu p là ước nguyên tố của b_n, thì p không chia b_m với $m > n$.
- Cuối cùng, chứng minh $b_n > \prod_{j<n} b_j$, cho nên tồn tại một ước nguyên tố mới của b_n.

Lời giải. (Cách 1)[7]Đặt $b_n = \frac{a_n}{c}$. Khi đó dãy trở thành:

$$b_1 = 1, \quad b_{n+1} = c^2\, b_n(b_n^2 - 4b_n + 5) + 1.$$

Khẳng định (1) — Với mọi m, n, ta có $b_{m+n} \equiv b_m \pmod{b_n}$.

Chứng minh. Chứng minh bằng quy nạp theo m. **Cơ sở**: $m = 1$,

$$b_{1+n} = c^2\, b_n(b_n^2 - 4b_n + 5) + 1 \equiv 1 = b_1 \pmod{b_n}.$$

Bước quy nạp: Giả sử $b_{m+n-1} \equiv b_{m-1} \pmod{b_n}$, ta có:

$$b_{m+n} = c^2\, b_{m+n-1}(b_{m+n-1}^2 - 4b_{m+n-1} + 5) + 1 \equiv b_m \pmod{b_n}.$$

■

Khẳng định (2) — Với $m \geq 2$, ta có $b_{m+n} \equiv b_m \pmod{b_n^2}$.

Chứng minh. Tương tự khẳng định 1 nhưng xét modulo b_n^2. Do các công thức dạng:

$$b_{m+1} = c^2\, b_m(b_m^2 - 4b_m + 5) + 1,$$

các sai số modulo b_n^2 sẽ triệt tiêu khi ta lặp quy nạp nhiều bước. ■

Từ hai khẳng định trên, ta có: nếu p là ước nguyên tố của b_n, thì $p \nmid b_m$ với mọi $m > n$, vì $b_m \equiv b_n \pmod{p}$, nhưng modulo p^2, sai số không triệt tiêu.

Do đó, nếu $b_n > \prod_{j=1}^{n-1} b_j$, thì b_n phải có một ước nguyên tố mới không xuất hiện trong các $b_1, \ldots, b_{n-1}$. Vì $b_1 = 1$, và quy luật đệ quy cho thấy $b_{n+1} > b_n^3$, nên b_n tăng rất nhanh, và bất đẳng thức trên luôn đúng với $n \geq 2$.

Suy ra:

$$\boxed{\text{Với mọi } n \geq 2,\ \exists p \text{ nguyên tố chia } a_n \text{ mà không chia } a_1, \ldots, a_{n-1}.}$$

□

6.2 Bài tập

Bài tập (GBR 2015 TST/F2/P5)**.** [**definition:25M**] Cho dãy số nguyên $(a_n)_{n\geq 0}$ thỏa mãn:

$$a_0 = 1, \quad a_1 = 3, \quad \text{và} \quad a_{n+2} = 1 + \left\lfloor \frac{a_{n+1}^2}{a_n} \right\rfloor \text{ với mọi } n \geq 0.$$

Chứng minh rằng với mọi $n \geq 0$, ta có:

$$a_n a_{n+2} - a_{n+1}^2 = 2^n.$$

Nhận xét. Thử tính vài giá trị đầu của dãy để quan sát quy luật. Sau đó, đặt mục tiêu chứng minh $a_n a_{n+2} - a_{n+1}^2 = 2^n$, có thể dùng phương pháp quy nạp. Để ý rằng công thức đệ quy dùng phần nguyên nên cần biến đổi phù hợp để tính toán chính xác.

[7] Lời giải của **mathaddiction**.

Chương 7

Đa thức nguyên

7.1 Các ví dụ

Ví dụ (FRA 2015 TST/2/P2)

[**15M**] Xác định tất cả các đa thức $P \in \mathbb{Z}[X]$ sao cho với mọi số nguyên tố p và mọi $u, v \in \mathbb{Z}$ thỏa mãn $p \mid uv - 1$, ta có:

$$p \mid P(u)P(v) - 1.$$

Phân tích — Giả sử P là đa thức nguyên thỏa mãn đề. Đặt $\deg P = n$ và xét đa thức $Q(X) = X^n P(1/X)$. Ta chọn u và v sao cho $uv \equiv 1 \pmod p$ và sử dụng giả thiết $P(u)P(v) \equiv 1 \pmod p$. Suy ra $P(X)Q(X) = X^n$, dẫn đến $P(X) = \pm X^n$.

Lời giải. (Cách 1)[1]Giả sử $f \in \mathbb{Z}[X]$ là một nghiệm. Nếu $f = 0$, thì $f(u)f(v) = 0 \not\equiv 1 \pmod p$ với mọi p, mâu thuẫn.

Giả sử $\deg(f) = n > 0$, đặt $g(X) = X^n f(1/X) \in \mathbb{Z}[X]$.

Chọn $x \in \mathbb{Z} \setminus \{0\}$, và chọn số nguyên tố $p > \max(|x|, |f(x)g(x) - x^n|)$. Khi đó tồn tại $y \in \mathbb{Z}$ sao cho $xy \equiv 1 \pmod p$, từ đó:

$$f(x)f(y) \equiv 1 \pmod p, \quad \text{và} \quad x^n f(y) \equiv g(x) \pmod p \Rightarrow f(x)g(x) \equiv x^n \pmod p.$$

Mà $|f(x)g(x) - x^n| < p$, nên $f(x)g(x) = x^n$. Do điều này đúng với mọi $x \in \mathbb{Z}$, ta có:

$$f(X)g(X) = X^n \Rightarrow f(X) = aX^n, \quad \text{với } a^2 = 1 \Rightarrow a = \pm 1.$$

Vậy:

$$f(X) = \pm X^n.$$

Kiểm tra lại: nếu $f(X) = \pm X^n$ và $uv \equiv 1 \pmod p$, thì:

$$f(u)f(v) = (\pm u^n)(\pm v^n) = (uv)^n \equiv 1 \pmod p.$$

Kết luận: nghiệm là:

$$\boxed{P(X) = \pm X^n \text{ với } n \in \mathbb{N}.}$$

□

[1]Lời giải chính thức.

Ví dụ (FRA 2015 TST/2/P4)

[**20M**] Xác định tất cả các đa thức nguyên $P(X), Q(X)$ sao cho với dãy (x_n) được xác định bởi:

$$x_0 = 2015, \quad x_{2n+1} = P(x_{2n}), \quad x_{2n+2} = Q(x_{2n+1}),$$

ta có: với mọi số nguyên dương m, tồn tại một số hạng $x_n \neq 0$ sao cho $m \mid x_n$.

Phân tích — Bài toán yêu cầu điều kiện để dãy (x_n) nhận giá trị chia hết cho mọi số nguyên dương m tại ít nhất một chỉ số n. Ta xét khi P, Q là các đa thức bậc nhất $P(X) = aX + b$, $Q(X) = cX + d$, và khảo sát các dãy con x_{2n}, x_{2n+1} là cấp số cộng. Sử dụng tính chất chia hết của cấp số cộng, ta rút ra điều kiện $ad + b \mid 2015$ hoặc $bc + d \mid a \cdot 2015 + d$. Kết luận rằng bộ nghiệm là:

$$P(X) = \varepsilon X + b, \quad Q(X) = \varepsilon X + d, \quad \varepsilon = \pm 1, \quad b + \varepsilon d \mid 2005.$$

Lời giải. [2]Gọi một dãy (y_n) có *tính chất D* nếu với mọi $m > 0$, tồn tại $y_n \neq 0$ sao cho $m \mid y_n$.

Ta sử dụng các bổ đề sau:

Khẳng định (Bổ đề 1) — Một dãy (x_n) có tính chất D nếu và chỉ nếu một trong các dãy con $(x_{kn}), (x_{kn+1}), \ldots, (x_{kn+k-1})$ có tính chất D.

Khẳng định (Bổ đề 2) — Nếu đa thức $T \in \mathbb{Z}[X]$ sinh ra dãy có tính chất D thì $\deg T = 1$ và hệ số bậc nhất ρ thỏa $|\rho| < 4$.

Khẳng định (Bổ đề 3) — Nếu $T(X) = \rho X + \theta$ có tính chất D thì $\rho = 1$.

Áp dụng cho bài toán, ta xét:

$$H(X) = P(Q(X)), \quad K(X) = Q(P(X)).$$

Theo các bổ đề trên, $\deg P = \deg Q = 1$, và các hệ số bậc nhất bằng ± 1. Đặt:

$$P(X) = aX + b, \quad Q(X) = cX + d, \quad \text{với } a, c \in \{\pm 1\}.$$

Xét các dãy con:

$$x_{2n} = x_0 + n(ad + b),$$
$$x_{2n+1} = ax_0 + d + n(bc + d).$$

Mỗi dãy số học $y_n = y_0 + nr$ có tính chất D khi $r \mid y_0$. Suy ra:

$$ad + b \mid x_0 = 2015 \quad \text{hoặc} \quad bc + d \mid a \cdot 2015 + d.$$

Ta chú ý rằng:

$$|ad + b| = |bc + d|.$$

Vậy bộ nghiệm là:

$$\boxed{P(X) = \varepsilon X + b, \quad Q(X) = \varepsilon X + d, \quad \varepsilon = \pm 1, \quad b + \varepsilon d \mid 2005.}$$

□

[2]Lời giải chính thức.

7.2 Bài tập

Bài tập (FRA 2015 TST/3/P1)**.** [**10M**] Tìm tất cả các đa thức f với hệ số nguyên sao cho với mọi số nguyên $n > 0$, ta có:

$$f(n) \mid 3n - 1.$$

Nhận xét. Xét hệ số cao nhất và giới hạn giá trị tuyệt đối của $f(n)$ so với $3n - 1$. Thử thế $n = 1, 2, 3, \ldots$ để kiểm tra giả thiết và loại trừ trường hợp $\deg f > 0$.

Chương 8

Phần dư bậc hai

8.1 Các ví dụ

Ví dụ (CHN 2015 TST2/D2/P3)
[**25M**] Chứng minh rằng tồn tại vô hạn số nguyên n sao cho n^2+1 là số không có ước chính phương.

Phân tích — Ta cần chỉ ra rằng với vô hạn số nguyên n, biểu thức n^2+1 không chia hết cho bình phương của một số nguyên tố. Hướng tiếp cận là đánh giá số nghiệm của phương trình $x^2 \equiv -1 \pmod{p^2}$ và áp dụng định lý số nguyên tố về các $p \equiv 1 \pmod 4$. Dùng tính chặt của ước lượng mật độ nghiệm để chỉ ra rằng số lượng x khiến x^2+1 có ước chính phương là ít hơn tổng thể x.

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

Định lý (giai-thua-mod)
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 **??**, 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)

[**35M**] 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 $A \cap B = \emptyset \mod p$.

Phân tích — Bài toán khai thác sâu các tính chất của ký hiệu Legendre trong trường hữu hạn $\mathbb{F}_p$. Hai trường hợp a là bình phương và không bình phương dẫn đến các cấu trúc khác nhau cho tập $aA + c$. Dùng tính chất bảo toàn tập qua phép nhân và phép tịnh tiến, kết hợp lý lẽ về tổng phần tử và tính đối xứng, ta suy ra rằng không thể tránh được giao với tập bình phương.

Lời giải. [2]Ta làm việc trong trường $\mathbb{F}_p$. Gọi $A \subset \mathbb{F}_p^*$ là tập các bình phương (modulo p), có đúng $\frac{p-1}{2}$ phần tử.

Giả sử tồn tại $a, c \in \mathbb{N}$ với $\gcd(ac, p) = 1$ sao cho tập $B = \{ab_i + c \pmod p\}$ không giao với A, tức $A \cap B = \emptyset$.

Trường hợp 1: $\left(\frac{a}{p}\right) = 1$ Vì tích của bình phương với bình phương vẫn là bình phương, $aA = A$. Khi đó $B = A + c$ là phép tịnh tiến của A. Nếu $B \cap A = \emptyset$, thì $A \cap (A + c) = \emptyset$. Nhưng điều này mâu thuẫn với:

$$|A| = \frac{p-1}{2}, \quad |A + c| = |A|, \quad A \cup (A + c) \subset \mathbb{F}_p^*.$$

Mà $2|A| = p - 1$, nên $A \cup (A + c) = \mathbb{F}_p^*$. Tức là tập các bình phương và không bình phương bị phân tách bởi phép cộng $+c$. Điều này dẫn đến:

$$\left(\frac{x}{p}\right) = -\left(\frac{x+c}{p}\right) \quad \text{với mọi } x \in \mathbb{F}_p^*.$$

Tổng hai vế theo x trên $\mathbb{F}_p^*$ dẫn đến tổng bằng 0, nhưng tổng bên trái bằng 0, nên vế phải cũng phải bằng 0. Điều này mâu thuẫn vì hàm Legendre không thể thay đổi dấu đều đặn như vậy.

Trường hợp 2: $\left(\frac{a}{p}\right) = -1$ Lúc này aA là tập các phần tử không phải bình phương. Khi đó $B = aA + c$ cũng là tập gồm các phần tử không phải bình phương.

Nhưng số lượng phần tử không phải bình phương là $\frac{p-1}{2}$, nên nếu dịch bởi $+c$ mà không giao với A, thì A và B là hai hoán vị rời nhau trong $\mathbb{F}_p^*$. Như trên, tổng chẵn lẻ và tính chất đối xứng của Legendre dẫn đến mâu thuẫn.

Kết luận: Trong cả hai trường hợp, giả thiết $A \cap B = \emptyset$ dẫn đến mâu thuẫn. Vậy:

$$\boxed{\text{Không tồn tại } a, c \in \mathbb{N} \text{ sao cho } \gcd(ac, p) = 1 \text{ và } A \cap B = \emptyset.}$$

□

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

Ví dụ (MEMO 2015/T/P8)

[**25M**] Cho $n \geq 2$ là một số nguyên. Hỏi có bao nhiêu số nguyên dương $m \leq n$ sao cho $m^2 + 1$ chia hết cho n?

Phân tích — Để giải bài toán, ta cần đếm số nghiệm của phương trình $m^2 \equiv -1 \pmod{n}$. Điều này tương đương với việc xác định khi nào -1 là phần dư bậc hai modulo n, và bao nhiêu nghiệm tồn tại. Ta xét các điều kiện để phương trình có nghiệm trên từng thừa số nguyên tố của n, dùng tính chất của ký hiệu Legendre, và áp dụng định lý phần dư Trung Hoa để đưa ra công thức tổng quát cho số nghiệm.

Lời giải. [3]Gọi $D(n)$ là số lượng $m \leq n$ sao cho $n \mid m^2 + 1$, hay $m^2 \equiv -1 \pmod{n}$.

Bước 1. Nếu n chia hết cho một số nguyên tố $\equiv 3 \pmod{4}$ hoặc $4 \mid n$, thì -1 không phải là bình phương modulo n, nên $D(n) = 0$.

Bước 2. Với $p \equiv 1 \pmod{4}$, ta có -1 là phần dư bậc hai modulo p, nên $x^2 \equiv -1 \pmod{p^k}$ có đúng hai nghiệm (theo nâng nghiệm Hensel). Vậy:

$$D(p^k) = 2 \quad \text{nếu } p \equiv 1 \pmod{4}.$$

Bước 3. Với $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, các $p_i \equiv 1 \pmod{4}$, thì theo định lý phần dư Trung Hoa:

$$D(n) = D(p_1^{\alpha_1}) \cdots D(p_k^{\alpha_k}) = 2^k.$$

Bước 4. Nếu $n = 2 \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, với các $p_i \equiv 1 \pmod{4}$, thì vẫn có nghiệm vì $x^2 \equiv -1 \pmod{2}$ có nghiệm $x \equiv 1$. Vậy:

$$D(n) = 2^k.$$

Bước 5. Nếu $4 \mid n$, thì không có nghiệm modulo 4, nên $D(n) = 0$.

Kết luận: $D(n) = 2^k$ khi và chỉ khi tất cả ước nguyên tố lẻ của n đều $\equiv 1 \pmod{4}$, và $4 \nmid n$. Ngược lại, $D(n) = 0$. □

[3]Lời giải chính thức.

8.2 Bài tập

Bài tập (HUN 2015 TST/KMA/643)**.** [**30M**] Với mỗi số nguyên dương n, ký hiệu $P(n)$ là ước số nguyên tố lớn nhất của n^2+1. Hãy chứng minh rằng tồn tại vô hạn bộ bốn số nguyên dương (a,b,c,d) thỏa mãn $a<b<c<d$ và $P(a)=P(b)=P(c)=P(d)$.

> **Nhận xét.** Xét các số n sao cho n^2+1 cùng chia hết cho một số nguyên tố lớn đặc biệt, ví dụ các số nguyên tố $p\equiv 1 \pmod 4$, rồi khai thác tính chất đồng dư và mật độ để tìm các bộ có cùng ước lớn nhất.

Chương 9

Chứng minh kiến tạo

9.1 Các ví dụ

Ví dụ (EGMO 2015/P5)

[**25M**] Cho m, n là các số nguyên dương với $m > 1$. Anastasia chia tập $\{1, 2, \ldots, 2m\}$ thành m cặp số. Boris chọn một số trong mỗi cặp và tính tổng các số được chọn. Chứng minh rằng Anastasia có thể chọn cách chia sao cho Boris không thể chọn được tổng bằng n.

Phân tích — Bài toán yêu cầu chứng minh rằng luôn tồn tại một cách chia các số từ 1 đến $2m$ thành m cặp sao cho *mọi cách chọn 1 số từ mỗi cặp* không bao giờ có tổng đúng bằng n. Hướng tiếp cận:

- Xét ba cách chia mẫu đặc biệt: tuần tự, xen kẽ, và phản xạ.
- Với mỗi cách chia, ta kiểm soát được tập hợp các tổng mà Boris có thể thu được: ràng buộc bởi biên độ hoặc phần dư modulo.
- Tùy theo giá trị của n, ta chọn ra cách chia phù hợp để loại trừ.

Lời giải. [1]Xét ba cách chia tập $\{1, 2, \ldots, 2m\}$ như sau:

Chia kiểu 1 (tuần tự):

$$P_1 = \{\{1, 2\}, \{3, 4\}, \ldots, \{2m-1, 2m\}\}$$

Tổng nhỏ nhất: chọn phần tử nhỏ hơn mỗi cặp $\Rightarrow s = m^2$ Tổng lớn nhất: chọn phần tử lớn hơn mỗi cặp $\Rightarrow s = m^2 + m$ *Suy ra: nếu* $n < m^2$ *hoặc* $n > m^2 + m$*, thì* n *không thể đạt được.*

Chia kiểu 2 (ghép đối xứng trung tâm):

$$P_2 = \{\{1, m+1\}, \{2, m+2\}, \ldots, \{m, 2m\}\}$$

Tổng luôn có dạng $s \equiv \sigma \pmod m$, với $\sigma = \sum_{i=1}^{m} i = \frac{m(m+1)}{2}$ *Vậy nếu* $n \in [m^2, m^2+m]$ *mà* $n \not\equiv \sigma \pmod m$*, thì* n *không thể đạt được.*

Chia kiểu 3 (đối xứng ngoài – trong):

$$P_3 = \{\{1, 2m\}, \{2, 2m-1\}, \ldots, \{m, m+1\}\}$$

Gọi d là số cặp trong đó Boris chọn phần tử lớn hơn Tổng khi đó: $s = \sigma + d(m-d)$ *Ta chứng minh được rằng:*

$$s \equiv \sigma \pmod m \Rightarrow s \in \left\{\frac{m(m+1)}{2}, \frac{3m^2+m}{2}\right\}$$

Vì khoảng $[m^2, m^2+m]$ không giao với hai giá trị trên, nên $n \in [m^2, m^2+m]$ và $n \equiv \sigma \pmod m \Rightarrow n$ không đạt được.

Kết luận: Trong mọi trường hợp, Anastasia luôn có thể chọn một cách chia để Boris không thể đạt được tổng n. □

[1]Lời giải chính thức.

Ví dụ (GER 2015 TST/P2)

[**15M**] Một số nguyên dương n được gọi là **nghịch ngợm** nếu có thể viết dưới dạng

$$n = ab + b$$

với các số nguyên $a, b \geq 2$.

Hỏi có tồn tại một dãy gồm 102 số nguyên dương liên tiếp sao cho chính xác 100 trong số đó là các số nghịch ngợm hay không?

Lời giải. [2]Giả sử tồn tại một dãy gồm 102 số nguyên dương liên tiếp sao cho đúng 100 số trong đó là số nghịch ngợm, tức tồn tại hai số không nghịch ngợm.

Nhắc lại định nghĩa: n là số nghịch ngợm nếu tồn tại $a, b \geq 2$ sao cho $n = ab + b = b(a+1)$, tức là $b \mid n$ và $\frac{n}{b} - 1 \geq 1$.

Do đó, mọi số nghịch ngợm đều là bội của một số $b \geq 2$, tức có ít nhất một ước số nguyên ≥ 2. Ngược lại, số không nghịch ngợm chỉ có thể là:

- Số nguyên tố, vì không chia hết cho số nào $< n$ và ≥ 2,
- Số có dạng p^k mà không thỏa điều kiện $\frac{n}{b} - 1 \geq 1$,
- Các số nhỏ như 1 hoặc 2.

Nhưng trong 102 số liên tiếp, theo định lý số nguyên tố Bertrand và mật độ nguyên tố, ta không thể có tới 3 số không nghịch ngợm liên tiếp, và cũng không thể đảm bảo chỉ có đúng 2 số không nghịch ngợm.

Mặt khác, ta chứng minh rằng với bất kỳ dãy 102 số nguyên dương liên tiếp, tồn tại ít nhất 3 số không nghịch ngợm.

Thật vậy, xét $n = 1$ và $n = 2$:

- Với $n = 1$, không có $b \geq 2$ nào chia hết n, nên không nghịch ngợm.
- Với $n = 2$, tương tự, vì $b \geq 2$ thì $b \nmid 2$, cũng không nghịch ngợm.
- Với $n = 3$: chỉ có $b = 3$, thì $\frac{3}{3} - 1 = 0$, không thỏa.

Vậy các số $1, 2, 3$ không phải là số nghịch ngợm. Nên trong dãy bất kỳ gồm 102 số liên tiếp, luôn có thể chứa tới 3 số như vậy.

Do đó, không tồn tại dãy 102 số liên tiếp mà chỉ có đúng 2 số không nghịch ngợm.

Kết luận: *Không tồn tại dãy gồm 102 số nguyên dương liên tiếp sao cho đúng 100 số trong đó là số nghịch ngợm.* □

[2]Dựa theo lời giải của **v_Enhance** và **Stella Y.**

Ví dụ (SRB 2014 MO/P4)

[**25M**] Ta gọi một số tự nhiên n là **điên rồ** (crazy) nếu tồn tại các số tự nhiên $a, b > 1$ sao cho:

$$n = a^b + b.$$

Hỏi có tồn tại dãy gồm 2014 số tự nhiên liên tiếp sao cho chính xác 2012 trong số đó là số điên rồ hay không?

Phân tích — Bài toán yêu cầu tìm một đoạn gồm nhiều số liên tiếp trong đó phần lớn thỏa mãn một tính chất "tồn tại biểu diễn" dưới dạng $ab + b$ hoặc $a^b + b$. Hướng giải sử dụng kỹ thuật chọn đoạn lớn có cấu trúc đặc biệt để đảm bảo mọi phần tử trong đoạn đều thỏa mãn, sau đó áp dụng tính chất liên tục rời rạc (mỗi lần trượt đoạn, số lượng phần tử thỏa mãn chỉ thay đổi nhiều nhất 1) để đảm bảo tồn tại đoạn có đúng số lượng mong muốn.

Lời giải. [3]Xét tập hợp các số:

$$S = \{2^{2014!} + 1,\ 2^{2014!} + 2,\ \ldots,\ 2^{2014!} + 2014\}.$$

Với mỗi $d \in \{1, 2, \ldots, 2014\}$, ta có:

$$2^{\frac{2014!}{d}} + d$$

là một số thuộc S, vì $\frac{2014!}{d}$ là số nguyên.

Chọn $a = 2^{\frac{2014!}{d}}$, $b = d$, thì:

$$a^b + b = \left(2^{\frac{2014!}{d}}\right)^d + d = 2^{2014!} + d.$$

Do đó, mỗi phần tử của S đều có dạng $a^b + b$ với $b > 1$, tức là đều là số điên rồ.

Vậy, S gồm 2014 số liên tiếp đều là số điên rồ.

Bây giờ, định nghĩa hàm:

$$f(n) = \text{số lượng số điên rồ trong đoạn } [n, n + 2013].$$

Ta có:

- $f(2^{2014!} + 1) = 2014$ (toàn bộ đoạn là crazy).
- Trong đoạn $[1, 2014]$, có thể kiểm tra rằng $f(1) < 2012$ (vì với $b \geq 2$, $a^b + b$ tăng nhanh, số lượng biểu diễn dạng đó là hạn chế).

Ngoài ra, khi dịch đoạn đi 1 đơn vị, giá trị của $f(n)$ thay đổi nhiều nhất là 1:

$$|f(n + 1) - f(n)| \leq 1.$$

Do đó, theo tính chất "liên tục rời rạc", tồn tại n sao cho $f(n) = 2012$, tức là có đúng 2012 số điên rồ trong đoạn gồm 2014 số tự nhiên liên tiếp.

Kết luận: *Tồn tại dãy gồm 2014 số tự nhiên liên tiếp sao cho chính xác 2012 số trong đó là số điên rồ.* □

[3]Lời giải của **Alan Bu, Alex Zhao, Christopher Qiu, Edward Yu, Eric Shen, Isaac Zhu, Jeffrey Chen, Kevin Wu, and Ryan Yang**.

Ví dụ (IRN 2015 MO/N1)

[**25M**] 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.

Phân tích — Bài toán yêu cầu chứng minh tồn tại vô hạn số tự nhiên không thể biểu diễn dưới dạng tổng của hai số P-mịn, tức là có tất cả thừa số nguyên tố nhỏ hơn một hằng số cho trước. Lập luận chính dựa trên ước lượng số lượng số P-mịn không vượt quá m, từ đó suy ra số cặp (a, b) thoả $a+b \le m$ bị chặn trên bởi x_m^2. Vì vậy tồn tại vô hạn giá trị n không đạt được dạng tổng mong muốn.

Lời giải. [4]Gọi $p_1, p_2, \ldots, p_k$ là tất cả các số nguyên tố nhỏ hơn 1394.

Một số nguyên dương được gọi là *số P-mịn* nếu tất cả các ước số nguyên tố của nó đều thuộc $\{p_1, \ldots, p_k\}$.

Với mỗi $m \in \mathbb{N}_{>0}$, ta đặt:

$$x_m = \text{số lượng các số } P\text{-mịn không vượt quá } m.$$

Khi đó:

- Mỗi số P-mịn không vượt quá m có thể biểu diễn dưới dạng $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \le m$.
- Với mỗi i, số giá trị khả dĩ của a_i là $\lfloor \log_{p_i} m \rfloor + 1$.
- Suy ra:

$$x_m \le \prod_{i=1}^{k} \left(\lfloor \log_{p_i} m \rfloor + 1 \right) = O((\log m)^k).$$

Do đó, số lượng cặp (a, b) gồm hai số P-mịn sao cho $a + b \le m$ không vượt quá $x_m^2 = O((\log m)^{2k})$.

Mà số lượng số tự nhiên $\le m$ là m, nên số lượng số $n \le m$ không thể viết dưới dạng $a + b$ với a, b là P-mịn ít nhất là:

$$m - x_m^2.$$

Khi $m \to \infty$, ta có $x_m^2 = o(m)$, vì $x_m^2 = O((\log m)^{2k})$ tăng chậm hơn nhiều so với m.

Kết luận: Có vô hạn số n không thể viết được dưới dạng tổng của hai số P-mịn. □

[4]Dựa theo lời giải của **SCLT**.

Ví dụ (IRN 2015 MO/N5)

[**20M**] 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 $x, y \in \mathbb{Z}$:

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

Phân tích — Ta cần chỉ ra rằng trong dãy $p+1, 2p+1, \ldots, (p-3)p+1$ có ít nhất một số là tổng của hai bình phương.

Ý tưởng chính:

- Tìm $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 \equiv 1 \pmod{p}$.
- Do $\mathbb{F}_p$ là trường, có thể chọn $x, y \in \mathbb{F}_p$ phù hợp với điều kiện trên.
- Sau đó, xét xem giá trị $x^2 + y^2$ thuộc đoạn nào và đánh giá giá trị này là $kp + 1$ với $k \leq \frac{p-3}{2}$.

Lời giải. [5]Thực ra, mệnh đề đúng với mọi $p \geq 7$, không chỉ $p > 30$.

Chọn $x, y \in \mathbb{F}_p$ sao cho:

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

Vì $\gcd(5, p) = 1$, nên $\frac{3}{5}$ và $\frac{4}{5}$ tồn tại trong $\mathbb{F}_p$. Khi đó:

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

Suy ra tồn tại $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 \equiv 1 \pmod{p}$, tức là tồn tại $k \in \mathbb{N}$ sao cho:

$$x^2 + y^2 = kp + 1$$

Mặt khác, chọn $x, y \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$, thì:

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

Vậy:

$$kp + 1 \leq \frac{p^2 - 2p + 1}{2} \Rightarrow k \leq \frac{p-1}{2}$$

Mà $1 \leq k \leq \frac{p-3}{2} \Rightarrow kp + 1 \in \{p+1, 2p+1, \ldots, (p-3)p+1\}$

Kết luận: *Tồn tại một số trong dãy $p+1, 2p+1, \ldots, (p-3)p+1$ có dạng $x^2 + y^2$.* □

[5]Dựa theo lời giải của **math90**.

Ví dụ (IRN 2015 TST/D1/P3)

[45M] 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 $b_{m+1} - b_m = 2015$.

Phân tích — Bài toán yêu cầu tìm các khoảng trống đúng bằng 2015 giữa hai số liên tiếp có dạng tổng hai bình phương. Hướng tiếp cận gồm ba bước:

- Chọn điểm đầu là một số có dạng $a^2 + 1007^2$.
- Dùng định lý tương hỗ bậc hai để loại trừ các số $x + i$ $(1 \le i \le 2014)$ không thể là tổng hai bình phương, bằng cách kiểm soát thừa số nguyên tố $\equiv 3 \pmod 4$ xuất hiện với số mũ lẻ.
- Áp dụng định lý đồng dư Trung Hoa và phép nâng Hensel để xây dựng nghiệm đồng thời modulo p_i^2, với mỗi $p_i \equiv 3 \pmod 8$.

Ý tưởng là dựng khoảng rỗng trong dãy các tổng hai bình phương mà hai đầu vẫn là tổng hai bình phương.

Lời giải. [6]

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 $p_i > 1008^2$,

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

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 $t_i \in \mathbb{Z}$ sao cho:

$$p_i^2 \mid (x_i + p_i t_i)^2 - (k - 1007^2)$$

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. □

[6] Dựa theo lời giải của **Ariscrim**.

Ví dụ (IRN 2015 TST/D2/P1)

[**35M**] 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.

Phân tích — Bài toán yêu cầu tìm k nhỏ nhất sao cho mọi tập A gồm k số tự nhiên đều có một tập con chẵn phần tử có tổng chia hết cho n. Hướng giải gồm ba trường hợp tách biệt:

- Nếu n là số lẻ: chọn A gồm $2n$ phần tử, chia làm hai nửa, áp dụng định lý tổng chia hết.
- Nếu $n \equiv 0 \pmod 4$: chọn A gồm $n+1$ phần tử, chia thành hai phần, mỗi phần có $k+1$ phần tử (với $k = n/2$).
- Nếu $n \equiv 2 \pmod 4$: viết $n = 2k$ với k lẻ, dùng cách nhóm các phần tử thành các cặp để áp dụng định lý tổng chia hết modulo k, rồi kết hợp với chẵn-lẻ để điều khiển số phần tử.

Trong cả ba trường hợp, áp dụng khéo léo bổ đề về tồn tại tập con có tổng chia hết cho n giúp tìm ra tập con thỏa yêu cầu về tổng và số phần tử.

Lời giải. [7]Trước hết ta chứng minh định lý sau.

Định lý (subset-divisibility)

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 $\overline{A_i} \equiv 0 \pmod n$, ta đã xong. Ngược lại, tồn tại hai chỉ số $i < j$ sao cho:

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

■

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: chứa các số lẻ, và B: 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.

Chia các phần tử trong A thành $\frac{t}{2}$ cặp. Bỏ một phần tử ra khỏi B, phần còn lại chia thành $\frac{s-1}{2}$ cặp.

Gọi $\overline{X}$ là tổng các phần tử trong tập X. Có tổng cộng:

$$\frac{t+s-1}{2} = \frac{n}{2} = k$$

tổng từ các cặp. Áp dụng bổ đề, tồn tại tổ hợp các cặp sao cho tổng các phần tử chia hết cho k. Mỗi tổng là tổng của hai số, nên toàn bộ tổng chia hết cho $2k = n$. Tập con này có số phần tử chẵn.

Trường hợp 2: $4 \mid n = 2k$.

Gọi $A = \{a_1, \ldots, a_{n+1}\}$. Xét tập con $A_1 = \{a_1, \ldots, a_{k+1}\}$. Vì k chẵn, áp dụng trường hợp (1), tồn tại tập con $X_1 \subseteq A_1$ gồm số phần tử chẵn có tổng chia hết cho k, tức $\overline{X_1} = kt$.

Phần còn lại của A có ít nhất $k+1$ phần tử. Áp dụng lại ta có $X_2 \subseteq A \setminus X_1$ sao cho $\overline{X_2} = kl$. Nếu t hoặc l chẵn thì xong. Nếu cả hai lẻ thì:

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

và $|X_1 \cup X_2|$ chẵn.

Trường hợp 3: n là số lẻ.

Xét tập $A = \{a_1, \ldots, a_{2n}\}$, chia thành hai nửa:

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

Áp dụng bổ đề cho A_1 và A_2, được X_1, X_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 xong. Nếu cả hai lẻ, thì $X_1 \cup X_2$ có số phần tử chẵn và tổng chia hết cho n.

Kết luận: Trong cả ba trường hợp, luôn tồn tại một tập con chẵn phần tử có tổng chia hết cho n. Do đó, giá trị nhỏ nhất của k là:

$$k = \begin{cases} 2n & \text{n lẻ} \\ n+1 & \text{n chẵn} \end{cases}$$

□

[7] Dựa theo lời giải của **andria**.

Ví dụ (POL 2015 MO/P6)

[**30M**] Chứng minh rằng với mọi số nguyên dương a, tồn tại một số nguyên $b > a$ sao cho:

$$1 + 2^a + 3^a \mid 1 + 2^b + 3^b.$$

Phân tích — Bài toán yêu cầu xây dựng $b > a$ sao cho $1 + 2^a + 3^a \mid 1 + 2^b + 3^b$.

Hướng tiếp cận:

- Gọi $N = 1 + 2^a + 3^a$, xét phân tích thừa số nguyên tố của N.
- Đối với mỗi thừa số $p^e \mid N$, cố gắng chọn $b \equiv a \pmod{\varphi(p^e)}$ để đảm bảo đồng dư $2^b \equiv 2^a$, $3^b \equiv 3^a$ modulo p^e.
- Đối với các thừa số nhỏ đặc biệt như $p = 2$ và $p = 3$, cần dùng đánh giá p-adic (LTE hoặc kiểm tra trực tiếp) để xử lý phần chia hết.
- Áp dụng định lý CRT để hợp nhất các điều kiện đồng dư, xây dựng b phù hợp và lớn hơn a.

Lời giải. [8]Gọi $N = 1 + 2^a + 3^a = 2^{e_2} \cdot 3^{e_3} \cdot p_4^{e_4} \cdots p_n^{e_n}$ là phân tích thừa số nguyên tố của N. Ta sẽ xây dựng một số $b > a$ sao cho $N \mid 1 + 2^b + 3^b$.

Bước 1: Với các số nguyên tố $p \geq 5$

Chọn $b \equiv a \pmod{\varphi(p_k^{e_k})}$ cho mỗi $k \geq 4$, ta có:

$$2^b \equiv 2^a, \quad 3^b \equiv 3^a \pmod{p_k^{e_k}} \implies 1 + 2^b + 3^b \equiv 0 \pmod{p_k^{e_k}}.$$

Bước 2: Với số nguyên tố $p = 2$

Xét modulo 8: $3^a \equiv 1$ hoặc $3 \pmod 8$, nên:

$$1 + 2^a + 3^a \equiv 2 \text{ hoặc } 4 \pmod 8 \implies v_2(N) \leq 2.$$

Chọn $b \equiv 3 \pmod 4$ và đủ lớn, khi đó $v_2(1 + 2^b + 3^b) = 2$, đạt giá trị tối đa.

Bước 3: Với số nguyên tố $p = 3$

Sử dụng định lý LTE với b lẻ:

$$v_3(1 + 2^b) = v_3(3) + v_3(b) = 1 + v_3(b).$$

Chọn

$$b \equiv 0 \pmod{3^{e_3}} \Rightarrow v_3(b) \geq e_3 \Rightarrow v_3(1 + 2^b + 3^b) \geq 1 + e_3 \geq e_3.$$

Tóm lại, $v_p(1 + 2^b + 3^b) \geq v_p(N)$ với mọi $p \mid N$, nên:

$$1 + 2^a + 3^a \mid 1 + 2^b + 3^b.$$

□

[8]Lời giải của **va2010**.

Lời giải. [9]Với $a = 1$, lấy $b = 3$. Giả sử $a > 1$. Phân tích:

$$1 + 2^a + 3^a = 2^n \cdot 3^m \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{với } n \geq 1,\ m \geq 0,\ \alpha_i \geq 1.$$

Các p_i là các số nguyên tố lẻ khác 3. Theo định lý Fermat–Euler:

$$b \equiv a \pmod{\varphi(p_i^{\alpha_i})} \implies 1 + 2^b + 3^b \equiv 1 + 2^a + 3^a \equiv 0 \pmod{p_i^{\alpha_i}}.$$

Gọi $N = \operatorname{lcm}(\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_k^{\alpha_k}))$, chọn:

$$b = a + 2 \cdot 3^t \cdot N,$$

với t đủ lớn (xác định cụ thể sau). Khi đó $P = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid 1 + 2^b + 3^b$.

Xét modulo 8:

- Nếu a lẻ, thì $v_2(1 + 2^a + 3^a) = 2$.
- Nếu a chẵn, thì $v_2(1 + 2^a + 3^a) = 1$.

Vì $b \equiv a \pmod 2$, nên $v_2(1 + 2^b + 3^b) = v_2(1 + 2^a + 3^a)$, do đó $2^n \mid 1 + 2^b + 3^b$.

Tiếp theo, nếu a chẵn thì $m = 0$. Nếu a lẻ, thì theo LTE:

$$v_3(1 + 2^a) = 1 + v_3(a) \Rightarrow m = 1 + v_3(a).$$

Chọn $t > 1 + v_3(a) \Rightarrow b \equiv a \pmod{3^{v_3(a)+1}} \Rightarrow v_3(b) = v_3(a)$, và b lẻ:

$$v_3(1 + 2^b + 3^b) = v_3(1 + 2^b) = 1 + v_3(b) = 1 + v_3(a) = m.$$

Suy ra:

$$2^n \cdot 3^m \cdot P \mid 1 + 2^b + 3^b.$$

□

[9]Lời giải của **elVerde**.

Ví dụ (ROU 2015 TST/D1/P3)

[**20M**] Một bộ ba Pythagoras là một nghiệm của phương trình $x^2 + y^2 = z^2$ trong các số nguyên dương sao cho $x < y$. Cho trước một số nguyên không âm n, hãy chứng minh rằng tồn tại một số nguyên dương xuất hiện trong đúng n bộ ba Pythagoras phân biệt.

Phân tích — Ta cần chứng minh rằng với mỗi $n \geq 0$, tồn tại số tự nhiên xuất hiện trong đúng n bộ ba Pythagoras phân biệt.

Ý tưởng là xét các số có dạng 2^n, rồi phân tích số nghiệm của phương trình $x^2 + 2^{2n} = y^2$, tức $y^2 - x^2 = 2^{2n}$. Số nghiệm tương ứng với số ước dương của 2^{2n} nhỏ hơn 2^n, từ đó suy ra có đúng $n-1$ bộ ba chứa 2^n, và thêm một bộ ba đặc biệt $(2^n, 2^n, 2^{n+1})$, tổng cộng là n bộ ba.

Lời giải. [10]

Khẳng định — Phương trình $x^2 + y^2 = 2^{2n}$ không có nghiệm nguyên dương.

Chứng minh. Rõ ràng đúng với $n = 1$ vì không có tổng bình phương hai số nguyên dương nào bằng 4. Giả sử mệnh đề đúng với mọi $k = n - 1$, xét:

$$x^2 + y^2 = 2^{2n}.$$

Vì x, y không thể đồng thời là số lẻ (tổng bình phương hai số lẻ chia hết cho 2 nhưng không chia hết cho 4), nên x, y đều chia hết cho 2. Khi đó tồn tại x', y' sao cho $x = 2x', y = 2y' \Rightarrow x'^2 + y'^2 = 2^{2(n-1)}$, mâu thuẫn với giả thuyết quy nạp. ■

Khẳng định — Phương trình $x^2 + 2^{2n} = y^2$ có đúng $n - 1$ nghiệm nguyên dương phân biệt.

Chứng minh. Phương trình tương đương:

$$y^2 - x^2 = 2^{2n} \Rightarrow (y - x)(y + x) = 2^{2n}.$$

Gọi $d = y - x \Rightarrow y + x = \dfrac{2^{2n}}{d}$, nên $x = \dfrac{1}{2}\left(\dfrac{2^{2n}}{d} - d\right)$. Để $x \in \mathbb{N}$, cần d là ước dương của 2^{2n} nhỏ hơn 2^n, tức $d = 2^k$ với $k = 1, 2, \ldots, n-1$. Vậy có đúng $n - 1$ nghiệm phân biệt. ■

Bây giờ, xét bộ ba $(x, y, z) = (2^n, 2^n, 2^{n+1})$, ta có:

$$(2^n)^2 + (2^n)^2 = 2 \cdot 2^{2n} = 2^{2n+1} = (2^{n+1})^2.$$

Do đó, số 2^n xuất hiện trong đúng n bộ ba Pythagoras phân biệt. □

[10] Dựa theo lời giải của **Ariscrim**.

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 $M = P$.

Phân tích — Bài toán yêu cầu xây dựng hai số cố định a, b sao cho bất kỳ cặp số m, n nguyên tố cùng nhau nào cũng không thể nằm gần (a, b). Ta xét việc chọn $a = b = N!$ với N lớn (ví dụ $N = 1000$). Khi đó, mọi số nhỏ hơn hoặc bằng N đều chia hết a và b, trong khi m, n nguyên tố cùng nhau không thể đồng thời chia hết cho cùng các thừa số nguyên tố của $N!$. Vì vậy, $m \neq a$ và $n \neq b$, và sự khác biệt tuyệt đối với từng hoán vị là lớn. Ta kiểm soát được giá trị $|a - m| + |b - n|$ bằng việc ép m, n không thể gần a, b. Từ đó ta đảm bảo giá trị luôn vượt quá 1000.

Lời giải. [11]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 $p_i \pmod p$. 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 $M = P$. □

[11] 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.

Phân tích — Ý tưởng là chọn một tập hợp các số nguyên tố đặc biệt S sao cho $p-1$ của chúng chỉ có các ước nhỏ. Sau đó xây dựng n_T bằng cách thay thế các $p \in T \subseteq S$ bởi $p-1$, sao cho $\varphi(n_T)$ vẫn bằng $\varphi(N)$. Do có hơn 2015 tập con T, ta tạo được hơn 2015 nghiệm khác nhau.

Lời giải. [12]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 **??**.

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 $\varphi(11) = 10 = \varphi(10)$.

Phân tích — Mỗi n_j được xây dựng bằng cách thay một số nguyên tố p_j trong tích $p_1 p_2 \cdots p_{2015}$ bởi $p_j - 1$. Vì $\varphi(p_j - 1) = \varphi(p_j)$ trong nhiều trường hợp, giá trị của $\varphi(n_j)$ không đổi. Các số n_j tạo thành 2015 giá trị khác nhau có cùng φ.

Lời giải. 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 $p_j - 1$.

[12]Lời giải của **Evan Chen**.

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 **??**.

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

[12] Lời giải của **Yang Liu**.

Phân tích — Bài toán được giải bằng quy nạp. Bước cơ sở với $k = 1$ đơn giản. Với bước quy nạp, từ k số n_j có $\varphi(n_j) = \varphi(P_k)$, ta xây dựng thêm k số mới bằng cách nhân từng n_j với p_{k+1}. Sau đó, một số thứ $(k+1)$ được thêm bằng cách nâng mũ các thừa số để điều chỉnh đúng φ. Tất cả các ước vẫn nằm trong tập nguyên tố ban đầu.

Lời giải. 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 $k+1$. ■

□

[12] 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.

Phân tích — Bài toán yêu cầu xây dựng một tập S gồm n số nguyên dương sao cho hiệu giữa mọi hai phần tử bất kỳ chia hết chính xác hai phần tử đó, nhưng không chia bất kỳ phần tử thứ ba nào. Ý tưởng chính là xây dựng một dãy các hiệu d_i rồi tích lũy tạo thành dãy s_i, và dùng đồng dư để chọn một số a sao cho mỗi phần tử trong $S = \{a + s_i\}$ thỏa mãn điều kiện đề bài. Điều quan trọng là đảm bảo các hiệu không chia hết nhau (tính độc lập), và dùng Định lý số dư Trung Hoa để giải hệ đồng dư cho a. Kỹ thuật này là một ví dụ tiêu biểu của phương pháp xây dựng qua đồng dư và bất biến tổ hợp.

Lời giải. [13]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:

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

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 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. Vì $M \mid t'_{i,j}$, 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 điều kiện (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 số 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. □

[13] Dựa theo lời giải của **Evan Chen**.

9.2 Bài tập

Bài tập (GBR 2015 MO/P2). [**15M**] Tại trường tiểu học Oddesdon có một số lẻ lớp học. Mỗi lớp có một số lẻ học sinh. Từ mỗi lớp, một học sinh sẽ được chọn để tạo thành hội đồng học sinh. Hãy chứng minh rằng hai mệnh đề sau là tương đương:

1. Có nhiều cách lập hội đồng học sinh sao cho số nam sinh là số lẻ hơn là số cách lập hội đồng sao cho số nữ sinh là số lẻ.
2. Có một số lẻ lớp có nhiều nam sinh hơn nữ sinh.

Nhận xét. Xét biểu diễn các cách chọn theo tổ hợp nhị phân và theo mô hình đại số tổ hợp (như dùng định lý về parity hoặc đa thức tạo), đặc biệt lưu ý rằng số học sinh trong mỗi lớp là số lẻ.

Bài tập (KOR 2015 FR/P1). [**20M**] 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.

Nhận xét. Xét chứng minh bằng quy nạp trên n, và tìm mối liên hệ giữa dãy B_n và A_n thông qua các biểu thức truy hồi. Đặc biệt lưu ý tính nguyên khi chia trong biểu thức định nghĩa B_{n+2}.

Bài tập (ROU 2015 TST/D4/P2). [**30M**] Cho n là một số nguyên dương. Nếu σ là một hoán vị của n số nguyên dương đầu tiên, định nghĩa $S(\sigma)$ là tập hợp tất cả các tổng phân đoạn khác nhau có dạng:

$$\sum_{i=k}^{l} \sigma(i)$$

với $1 \le k \le l \le n$.

(a) Hãy chỉ ra một hoán vị σ của $\{1, 2, \ldots, n\}$ sao cho:

$$|S(\sigma)| \ge \left\lfloor \frac{(n+1)^2}{4} \right\rfloor.$$

(b) Chứng minh rằng với mọi hoán vị σ, ta có:

$$|S(\sigma)| > \frac{n\sqrt{n}}{4\sqrt{2}}.$$

Nhận xét.
- Phần (a) là một bài toán xây dựng hoán vị σ để tối đa hóa số tổng phân đoạn khác nhau.
- Phần (b) yêu cầu chứng minh một bất đẳng thức tổng quát áp dụng cho mọi hoán vị, với ý tưởng sử dụng bất đẳng thức Cauchy–Schwarz để ước lượng số lượng phần tử của tập $S(\sigma)$.

Bài tập (RUS 2015 TST/D10/P1)**.** [**15M**] 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:

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

Nhận xét.
- Hãy thử chọn a và b đủ lớn và cùng chia hết cho một số lớn, ví dụ như $a = b = 1000!$.
- Khi đó, m, n nguyên tố cùng nhau không thể cùng chia hết cho các thừa số nguyên tố của a hoặc b, khiến khoảng cách tuyệt đối không thể nhỏ.
- Ý tưởng là buộc $m \neq a$ và $n \neq b$ bằng điều kiện chia hết.

Phụ lục A

Công cụ sử dụng

A.1 Các định lý rời rạc cơ bản

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

A.2 Số nguyên tố và phép chia hết

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:

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

với p_i là các số nguyên tố khác nhau và $\alpha_i \in \mathbb{Z}^+$.

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

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

$$n < p < 2n.$$

Định lý (Định lý số nguyên tố — dạng yếu)
Hàm đếm số nguyên tố $\pi(n)$ thỏa mãn:

$$\pi(n) \sim \frac{n}{\log n}, \quad \text{và } \pi(n) < \frac{1.25506n}{\log n}.$$

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

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

Định lý (Tính chất gcd và lcm)
Với $a, b \in \mathbb{Z}^+$, ta có:

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

Ngoài ra:

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

Định lý (Định lý chia có dư)
Với $a \in \mathbb{Z}$ và $b \in \mathbb{Z}^+$, tồn tại duy nhất $q, r \in \mathbb{Z}$ sao cho:

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

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

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

Định lý (Định lý Bézout)
Với $a, b \in \mathbb{Z}$, tồn tại $x, y \in \mathbb{Z}$ sao cho:

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

Định lý (Tính chất số nguyên tố)
Nếu p là số nguyên tố và $p \mid ab$, thì $p \mid a$ hoặc $p \mid b$.

A.3 Số học đồng dư cơ bản

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

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

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

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

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

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

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

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

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

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

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

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

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

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

Định lý (Tiêu chuẩn Euler)
Với số nguyên tố lẻ p và $a \not\equiv 0 \pmod{p}$, ta có:

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

Định lý (Hủy nhân trong đồng dư)
Nếu $ad \equiv bd \pmod{n}$, thì:

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

Định lý A.3.1 (Định lý Dirichlet về cấp số cộng nguyên tố)
Cho hai số nguyên dương a và d sao cho $\gcd(a,d) = 1$. Khi đó, cấp số cộng $a, a+d, a+2d, a+3d, \ldots$ chứa vô hạn số nguyên tố.

A.4 Các hàm số học

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

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

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

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

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

Đây là tổng các ước dương của n.

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

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

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

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

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

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

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

Định lý (Đẳng thức $\tau = 1 * 1$)
Hàm $\tau(n)$ là tích Dirichlet của hai hàm hằng:

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

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

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

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

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

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

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

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

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

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

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

A.5 Phương trình nghiệm nguyên

Định lý (Đẳng thức Simon yêu thích)

Với các biểu thức như $xy + ax + by + c$, ta có:

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

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

Bổ đề (Nguyên lý hạ vô hạn (Infinite Descent))

Nếu tồn tại dãy vô hạn các số nguyên dương $x_0 > x_1 > x_2 > \cdots$ mà mỗi x_i thỏa mãn tính chất P, thì có mâu thuẫn. Do đó, giả thiết ban đầu là sai.

Định lý (Monovariant $S = |x| + |y| + |z|$)

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

Định lý (Kỹ thuật Vieta Jumping)

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

Bổ đề (Mâu thuẫn đồng dư)

Nếu giả sử $a \equiv b \pmod{p}$ nhưng rút ra $a \equiv c \not\equiv b \pmod{p}$, thì mâu thuẫn xảy ra. Kỹ thuật dùng để loại nghiệm.

Định lý (Định lý Fermat Giáng Sinh)

Phương trình:

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

không có nghiệm nguyên dương khác 0.

A.6 Căn nguyên thủy và đẳng thức cổ điển

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

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

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

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

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

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

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

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

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

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

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

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

Định lý (Đẳng thức Sophie Germain)
Với mọi $a, b \in \mathbb{Z}$, ta có:

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

A.7 Chuẩn p-adic và định lý LTE

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

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

Định lý (Tính chất cơ bản của ν_p)
Với $a, b \in \mathbb{Z}$, ta có:

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

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

Định lý (Định lý LTE cho hiệu — $p \mid x - y$)
Cho $x, y \in \mathbb{Z}$, p là số nguyên tố lẻ, $n \in \mathbb{Z}^+$, nếu $p \mid x - y$ và $p \nmid xy$, thì:

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

Định lý (Định lý LTE cho tổng — $p \mid x + y$)
Cho $p > 2$ là số nguyên tố, $x, y \in \mathbb{Z}$, $p \mid x + y$, và $p \nmid xy$. Khi đó với n lẻ:

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

Định lý (Định lý LTE cho $\nu_2(x^n - 1)$)
Với $x \in \mathbb{Z}$ lẻ và $n \in \mathbb{Z}^+$, ta có:

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

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

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

A.8 Đa thức

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

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

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

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

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

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

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

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

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

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

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

thì:

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

Định lý (Đẳng thức Vandermonde)

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

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

A.9 Số dư bậc hai và ký hiệu Legendre

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

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

Định lý (Tính chất của ký hiệu Legendre)

Với $a, b \in \mathbb{Z}$ và số nguyên tố lẻ p, ta có:

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

Định lý (Định luật tương hỗ bậc hai)

Với hai số nguyên tố lẻ phân biệt p, q, ta có:

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

Hệ quả (Tổng Legendre bằng 0)

Với số nguyên tố lẻ p, ta có:

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Định lý (Tiêu chuẩn Euler)

Với số nguyên tố lẻ p và $a \not\equiv 0 \pmod{p}$, ta có:

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

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

$$r < \sqrt{p} + 1.$$

A.10 Căn nguyên thủy và bậc lũy thừa (phần nâng cao)

Bổ đề (Tồn tại phần tử bậc d)

Nếu $d \mid p-1$, thì tồn tại $a \in \mathbb{Z}$ sao cho:

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

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

Định lý (Tập các phần tử bậc d)

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

Định lý (Các nghiệm của $x^d \equiv 1 \pmod p$)

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

Bổ đề (Tính chia hết qua bậc)

Nếu $a^k \equiv 1 \pmod p$, thì $\operatorname{ord}_p(a) \mid k$.

Định lý (Cấu trúc nhóm nhân modulo p)

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

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

Bổ đề (Rút gọn đồng dư theo mũ)

Nếu $a^k \equiv b^k \pmod p$ và $\gcd(k, p-1) = 1$, thì:

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

A.11 Bậc lũy thừa theo hợp số

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

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

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

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

Với số nguyên tố p, ta có:

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

Định lý (Bậc modulo hợp số)
Với $a \in \mathbb{Z}$, $\gcd(a,n)=1$, ta có:

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

Bổ đề (Bậc modulo tích các lũy thừa số nguyên tố)
Nếu $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, và $\gcd(a,n)=1$, thì:

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

Định lý (Định lý số dư Trung Hoa)
Cho các số nguyên $n_1, n_2, \ldots, n_k$ đôi một nguyên tố cùng nhau, và các số nguyên $a_1, a_2, \ldots, a_k$, tồn tại duy nhất $x \mod N = n_1 n_2 \cdots n_k$ sao cho:

$$x \equiv a_i \pmod{n_i} \quad \text{với mọi } i.$$

A.12 Phương trình hàm và tích chập

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

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

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

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

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

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

Định lý (Công thức nghịch đảo Möbius)
Nếu $f(n) = \sum_{d|n} g(d)$, thì:

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

Định lý (Đẳng thức $\tau = 1 * 1$)
Với mọi $n \in \mathbb{Z}^+$, số ước dương:

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

Định lý (Đẳng thức $\sigma = \mathrm{id} * 1$)
Hàm tổng các ước dương của n thỏa:

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

Định lý (Tổng các giá trị $\varphi(n)$)

Khi $x \to \infty$, ta có:

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

A.13 Thủ thuật, kỹ thuật và công cụ hiếm gặp

Định lý (Trung bình số ước)

Gọi $d(k)$ là số ước dương của k. Khi đó:

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

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

Định lý (Tổng tất cả các ước từ 1 đến n)

Ta có:

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

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

Định lý (Ma trận ước số $D_{i,j}$)

Xét bảng D cấp $n \times n$ với phần tử:

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

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

Định lý (Tổng nghịch đảo ước số)

Với mọi $n \geq 1$, ta có:

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

Phụ lục B

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 $k! = (2^n - 1)\ldots$
- 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 $a_1, a_2, \ldots, a_n$ sao cho $\frac{a_1}{a_2} + \cdots + \frac{a_n}{a_1} \in \mathbb{Z}$

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

Ví dụ:

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

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

Ví dụ:

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

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

Ví dụ:

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

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

Ví dụ:

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

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

Ví dụ:

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

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

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

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

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

Từ điển chú giải

APMO 2015 Asian Pacific Mathematical Olympiad 2015 49

BGR 2015 EGMO TST Bulgaria EGMO TST 2015 46

BMO 2015 Balkan Mathematical Olympiad 2015 31

BxMO 2015 Benelux Mathematical Olympiad 2015 6

CAN 2015 MO Canada National Olympiad 2015 51

CAN 2015 TST Canada Qualifying Repêchage Competition 2015 7, 38

CHN 2015 MO China National Olympiad 2015 67

CHN 2015 TST China Team Selection Test 2015 8, 9, 39, 68, 80

EGMO 2015 European Girls' Mathematical Olympiad 2015 10, 11, 86

EMC 2015 European Mathematical Cup 2015 52

FRA 2015 RMM France Romania Masters 2015 53

FRA 2015 TST France Team Selection Test 2015 40, 46, 76–78

GBR 2015 MO Great Britain National Olympiad 2015 105

GBR 2015 TST Great Britain Team Selection Test 2015 24, 46, 74

GER 2015 MO Germany National Olympiad 2015 27, 54

GER 2015 TST Germany Team Selection Test 2015 41, 87

HUN 2015 TST Hungary Team Selection Test 2015 24, 64, 84

IMO 2015 International Mathematical Olympiad 2015 55, 69, 70

IMO 2023 International Mathematical Olympiad 2023 12, 71

IND 2015 MO India National Olympiad 2015 14, 15

IND 2015 TST India Team Selection Test 2015 16, 56, 57

IRN 2015 MO Iran National Olympiad 2015 17, 58, 82, 89, 90

IRN 2015 TST Iran Team Selection Test 2015 18, 91, 93