Diễn đàn THUVIENTOAN.NET

CHUYÊN ĐỀ SỐ HỌC

Tháng 10/2013

Mục lục

Lời nói đầu

"Số học là bà hoàng của Toán học"

Có thể nói Số học là lĩnh vực xuất hiện sớm nhất trong lịch sử Toán học. Khi con người bắt đầu làm việc với những con số thì khi ấy, Số học ra đời.Trải qua hàng nghìn năm phát triển, Số học vẫn giữ được vẻ đẹp thuần khiết của nó. Vẻ đẹp ấy được thể hiện qua cách phát biểu đơn giản của bài toán, đến nỗi một học sinh lớp 6 cũng có thể hiểu được. Thế nhưng, vẻ đẹp ấy thường tiềm ẩn những thử thách sâu thẳm bên trong để thách thức trí tuệ loài người...

Hãy nói về Định lý Fermat lớn, một định lý đã quá nổi tiếng trong thế giới Toán học. Trong một tuyển tập văn học với tựa đề *Thoả ước với Quỷ* có truyện ngắn *Con Quỷ và Simon Flagg* của Arthur Poges. Trong truyện ngắn này con Quỷ có đề nghị Simon Flagg đặt cho nó một câu hỏi. Nếu con Quỷ trả lời được trong vòng 24 giờ, nó sẽ lấy đi linh hồn của Simon, còn nếu nó đầu hàng nó sẽ trả cho Simon 100.000 đôla. Simon đã đặt cho con Quỷ câu hỏi: " Định lý cuối cùng của Fermat có đúng không?" Nghe xong, con Quỷ biến mất và bay vút đi khắp vũ trụ để tiếp thu tất cả tri thức toán học đã từng được sáng tạo ra. Ngày hôm sau con Quỷ quay trở lại và thú nhận: *"Simon, ngươi đã thắng", con Quỷ buồn rầu nói và nhìn Si mon với con mắt đầy thán phục. "Ngay cả ta, ta cũng không có đủ kiến thức toán học để trong một thời gian ngắn như thế có thể giải đáp được một bài toán khó như vậy. Càng nghiên cứu sâu nó càng rắc rối hơn... Chà! Ngươi có biết"-Con Quỷ tâm sự- "ngay cả những nhà toán học giỏi nhất trên các hành tinh khác, họ còn uyên bác hơn những nhà toán học của các ngươi nhiều, cũng không giải nổi câu đố đó không? Thì đấy, một gã trên sao Thổ nhìn giống như một cây nấm trên cà kheo, gã có thể giải nhẩm các phương trình vi phân đạo hàm riêng, mà cũng phải đầu hàng đó thôi."*

Chính vì có cách phát biểu đơn giản nhưng cần những suy luận sâu sắc và tinh tế nên những bài toán Số học trong các kì thi Olympic thường được dùng để phân loại học sinh. Tuy rằng trên thị trường đã có rất nhiều cuốn sách viết về Số học, nhưng nhu cầu sách về lĩnh vực này chưa bao giờ vơi đi. Đặc biệt, ngày càng nhiều càng phương pháp mới xuất hiện, cần một đầu sách không những phát triển những phương pháp cũ mà còn có thể giới thiệu những phương pháp mới hoặc những cái nhìn mới về những vấn đề cũ.

"Chuyên đề Số học" của Diễn đàn Mathscope ra đời chính là để đáp ứng nhu cầu đó của đông đảo học sinh, sinh viên và giáo viên trên khắp cả nước. Chuyên đề được thực hiện bởi các thành viên của Diễn đàn Mathscope, bao gồm các chủ đề: Cấp và căn nguyên thuỷ, Các bài toán số học hoán vị vòng quanh, Dãy số số học, Hàm số học, Bổ đề nâng số mũ LTE, Phần nguyên,

Thặng dư chính phương, Phương pháp bước nhảy Viete. Hi vọng đây sẽ là một tài liệu hữu ích cho các bạn đọc gần xa trong việc ôn luyện cho các kì thi Olympic.

Để hoàn thành chuyên đề này, ban biên tập xin gửi lời cảm ơn sâu sắc đến tác giả của các bài viết, các thành viên đã tham gia thảo luận, đóng góp trên Diễn đàn. Đặc biệt, xin gửi lời cảm ơn sâu sắc đến Ban quản trị của Diễn đàn Mathscope đã luôn tạo điều kiện tốt nhất cho ban biên tập để hoàn thành chuyên đề này. Cuốn sách này chính là thành quả quá trình lao động nghiêm túc của các thành viên trong ban biên tập, nhưng hơn hết đây vẫn là một sản phẩm đáng quý của cộng đồng thuvientoan.net nói riêng và cộng đồng Toán học Việt Nam nói chung.

Tuy đã được kiểm tra kĩ càng nhưng chuyên đề không tránh khỏi những sai sót. Mọi góp ý về chuyên đề xin được gửi lên Diễn đàn thuvientoan.net hoặc gửi về hộp mail thuvientoan.net@gmail.com. Xin chân thành cảm ơn.

Thành phố Hồ Chí Minh, ngày Phụ nữ Việt Nam 20-10-2013

Chuyên đề 1:
Bước nhảy Viete

Phạm Huy Hoàng [1]

Mở đầu

Trong các kì thi học sinh giỏi, các bài toán về phương trình Diophante bậc hai đã không còn xa lạ. Phương trình Pell là một trong các ví dụ nổi bật nhất về phương trình Diophante bậc hai, tuy nhiên do lượng bài toán về phương trình Pell đã khá nhiều, nên trong kì thi IMO 1988 đã xuất hiện một dạng bài phương trình Diophante bậc hai rất mới mẻ thời bấy giờ:

> *Cho a, b là hai số nguyên dương thỏa mãn $ab+1|a^2+b^2$. Chứng minh rằng*
>
> $$\frac{a^2+b^2}{ab+1}$$
>
> *là số chính phương.*

Bài toán này được coi là khó nhất trong các kì thi IMO trước năm 1988 và cũng là bài toán khó nhất trong kì thi này. Tác giả *Authur Engel* đã từng bình luận về bài toán này (nguyên văn):

> " Nobody of the six members of the Australian problem committee could solve it. Two of the members were George Szekeres and his wife, both famous problem solvers and problem creators. Since it was a number theoretic problem it was sent to the four most renowned Australian number theorists. They were asked to work on it for six hours. None of them could solve it in this time. The problem committee submitted it to the jury of the XXIX IMO marked with a double asterisk, which meant a superhard problem, possibly too hard to pose. After a long discussion, the jury finally had the courage to choose it as the last problem of the competition. Eleven students gave perfect solutions."

Dịch ra tiếng Việt nôm na là:

> "Không có ai trong số sáu thành viên của hội đồng giám khảo của Úc giải được bài toán này. Hai thành viên nổi bật trong đó, đều là những người nổi tiếng giải và sáng tạo các bài toán, là George Szekeres và vợ ông. Đây là bài toán số học nên nó đã được gửi cho bốn nhà số học lớn nhất của Úc bấy giờ. Họ được yêu cầu giải bài toán trong sáu giờ và không có ai giải được sau đó. Hội đồng thẩm định nộp cho

[1]Đại học Khoa học Tự Nhiên

ban giám khảo IMO XXIX bài toán này với hai dấu hoa thị, để nói lên là nó rất khó, hoặc là quá khó để ra trong kì thi. Sau một hồi bàn bạc, hội đồng IMO XXIX quyết định chọn bài toán này làm bài cuối của kì thi. Có mười một học sinh cho lời giải hoàn chỉnh của bài toán."

Trong số 11 học sinh đó có Giáo sư Ngô Bảo Châu của chúng ta.

Lời giải nguyên thủy của bài toán và các vấn đề liên quan

Chúng ta bắt đầu với bài toán gốc:

Bài toán 1. Cho a, b là các số nguyên dương thỏa mãn $ab+1 \mid a^2+b^2$.
Chứng minh rằng

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

là số chính phương

Lời giải. Đặt $k = \frac{a^2+b^2}{ab+1}$. Cố định k và xét tất cả các cặp (a, b) nguyên dương thỏa mãn phương trình

$$k = \frac{a^2+b^2}{ab+1},$$

có nghĩa là xét tập

$$S = \left\{(a,b) \in \mathbb{N}^* \times \mathbb{N}^* | k = \frac{a^2+b^2}{ab+1}\right\}$$

Vì S là tập các cặp số nguyên dương nên luôn tồn tại một cặp (a_0, b_0) trong S mà $a_0 + b_0$ đạt giá trị nhỏ nhất và $a_0 \geqslant b_0$.
Xét phương trình

$$\frac{x^2+b_0^2}{xb_0+1} = k \Leftrightarrow x^2 - kx.b_0 + b_0^2 - k = 0$$

là một phương trình bậc hai ẩn x. Ta đã biết rằng phương trình trên có một nghiệm là a_0. Như vậy theo định lý Viete thì tồn tại nghiệm a_1 thỏa mãn phương trình bậc hai với ẩn x trên và

$$a_1 = kb_0 - a_0 = \frac{b_0^2 - k}{a_0}.$$

Từ đây ta có a_1 cũng là số nguyên. Ta chứng minh a_1 không âm. Thật vậy, nếu $a_1 < 0$ thì

$$a_1^2 - kb_0a_1 + b_0^2 - k \geqslant a_1^2 + k + b_0^2 - k > 0,$$

mâu thuẫn. Do đó ta có $a_1 \geqslant 0$. Từ đây ta có:
Nếu $a_1 > 0$ thì (a_1, b_0) là một cặp thuộc S. Theo định nghĩa của (a_0, b_0) ta có:

$$a_0 + b_0 \leqslant a_1 + b_0 \Rightarrow a_0 \leqslant a_1.$$

Do đó cũng theo Viete thì:

$$a_0^2 \leqslant a_0a_1 = b_0^2 - k < b_0^2 \Rightarrow a_0 < b_0,$$

trái với giả thiết ban đầu.
Do đó $a_1 = 0$, vì vậy suy ra $k = b_0^2$ là một số chính phương, ta có điều cần chứng minh. ❐

Từ bài toán này ta có thể thấy được các bước giải bài toán dùng phương pháp này như sau:

1. Nhận dạng bài toán thuộc lớp phương trình Diophante bậc hai (trở lên).
2. Cố định một giá trị nguyên mà đề bài cho, rồi giả sử tồn tại một cặp nghiệm thỏa mãn một vài điều kiện mà không làm mất tính tổng quát của bài toán.
3. Dựa vào định lý Viete để tìm các mối quan hệ và sự mâu thuẫn, từ đó tìm được kết luận của bài toán.

Điểm mấu chốt của các bài toán này là *nguyên lí cực hạn*: Trong tập hợp các số nguyên dương thì luôn tồn tại số nguyên dương nhỏ nhất. Mệnh đề trên không những hữu dụng trong các lớp bài toán này mà còn trong nhiều bài toán tổ hợp, tổ hợp số học và số học.
Từ những bài toán tiếp theo, tôi sẽ trình bày vắn tắt các bước làm và cách làm thay vì trình bày đầy đủ như bài toán trên, để các bạn có thể tự phát huy tính tự làm việc của mình. Phần gợi ý sẽ có ở cuối bài viết.

Bài toán 2. Tìm tất cả các số nguyên dương n sao cho phương trình sau có nghiệm nguyên dương :

$$x^2 + y^2 = n(x+1)(y+1).$$

Chứng minh. Chúng ta sẽ làm theo các bước như bài toán trên:

1. Cố định n, giả sử tồn tại cặp (x_0, y_0) mà tổng $x_0 + y_0$ min và $x_0 \geqslant y_0$.
2. Xét phương trình bậc 2 ẩn X như sau:

   $$X^2 - X.n(y+1) + y_0^2 - ny_0 - n = 0.$$

   Phương trình có nghiệm là x_0 nên có nghiệm x_1.
3. Áp dụng định lý Viete:

   $$x_0 + x_1 = n(y_0+1),\ x_0x_1 = y_0^2 - ny_0 - n.$$

4. Tương tự bài trước, các bạn chứng minh $x_1 \geqslant 0$ và từ đó sẽ chứng minh $x_1 = 0$ bằng cách chứng minh $x_1 > 0$ thì sẽ dẫn đến mâu thuẫn.
5. Từ đó đi đến kết luận bài toán: $x_1 = 0$ và $y_0^2 = n(y_0+1)$ suy ra $y_0 + 1 \mid y_0^2$, là điều không thể xảy ra khi y_0 nguyên dương.

Do đó không tồn tại số nguyên dương n thỏa mãn phương trình đầu tiên. ❐

Từ bài toán này, ta dẫn đến được bài toán thú vị sau:

Bài toán 3. Giả sử a, b nguyên dương thỏa mãn:

$$b+1 \mid a^2+1,\ a+1 \mid b^2+1.$$

Chứng minh rằng a, b đều là các số lẻ.

Chứng minh. Nhìn vào bài toán trên, từ giả thiết ta không nhìn thấy mối tương quan giữa a, b và tính chẵn lẻ của hai số đó. Vì vậy, nhờ bản năng và kinh nghiệm, cách làm tốt nhất để thêm dữ kiện là sử dụng phương pháp phản chứng.
Giả sử a, b đều là các số chẵn. Từ giả sử này, bạn đọc hãy chứng minh hai mấu chốt sau:

1. $a+1$ và $b+1$ nguyên tố cùng nhau.
2. $a+1 \mid a^2+b^2$, $b+1 \mid a^2+b^2$.

Từ đó suy ra tồn tại n nguyên dương sao cho $a^2+b^2 = n(a+1)(b+1)$ và theo bài toán trên ta có điều mâu thuẫn. Vì vậy a, b lẻ. ❐

Bài toán trên cũng là một bổ đề quan trọng của một bài toán trong IMO Shortlist 2009.

Bài toán 4. Tìm tất cả các số nguyên dương n sao cho tồn tại dãy số nguyên dương $a_1, a_2, ..., a_n$ thỏa mãn

$$a_{k+1} = \frac{a_k^2+1}{a_{k-1}+1} - 1$$

với mọi k thỏa mãn $2 \leqslant k \leqslant n-1$.

(Phần gợi ý sẽ có ở cuối bài viết).
Khi đã giải được hai bài toán trên thì đa số các bài toán với hai biến x, y sẽ thành chuyện "đơn giản". Xin mời bạn đọc thử sức với bài toán sau, và điều ẩn sau đó mới là điều thú vị:

Bài toán 5. Tìm tất cả các số n nguyên dương sao cho phương trình sau có nghiệm nguyên dương:

$$(x+y)^2 = n(4xy+1).$$

Chứng minh. Chúng ta tuần tự theo các bước ở trên. Đáp án là với n là số chính phương thì phương trình luôn có nghiệm nguyên dương. ❐

Đáng chú ý là bài toán đơn giản như vậy mà lại là một bổ đề cực kì quan trọng cho một bài toán khó sau:

Bài toán 6 (Taiwan MO 1998)**.** Cho m, n là hai số lẻ với $m > n > 1$ thỏa mãn

$$m^2-n^2+1 \mid n^2-1.$$

Chứng minh rằng m^2-n^2+1 là số chính phương.

Chứng minh. Nhìn vào bài toán này và bài toán trên, chúng ta không thể thấy ngay sự liên hệ. Gợi ý cho bài toán này là làm thế nào để chuyển về bài toán trước.
Từ giả thiết ta có $m^2-n^2+1 \mid n^2-1$, để cho tiện và gọn hơn, ta có $m^2-n^2+1 \mid m^2$. Từ đây ta có thể đặt $m^2 = k.(m^2-n^2+1)$ với k nguyên dương. Đến đây thì chắc không khó để nhìn ra mối liên hệ: Từ giả thiết m, n lẻ, tồn tại hai số nguyên dương a, b sao cho $m = a+b, n = a-b$. Do đó phương trình trên trở thành:

$$(a+b)^2 = k(4ab+1),$$

chúng ta quay về bài toán trên. Vậy k là số chính phương, do đó $4ab+1$ cũng là số chính phương hay m^2-n^2+1 là số chính phương. ❐

Nhìn bài toán trên, như một người làm toán, chúng ta không khỏi thắc mắc là: liệu có tồn tại hai số m, n như vậy không để thỏa mãn $m^2 - n^2 + 1 | n^2 - 1$ để rồi suy ra $m^2 - n^2 + 1$ là số chính phương? Bằng lối suy nghĩ đó chúng ta nên tìm thử một nghiệm của bài toán:

Bài toán 7. Tìm một cặp nghiệm (m, n) lẻ nguyên dương thỏa mãn điều kiện bài toán trên.

Chứng minh. Thử một vài giá trị, bài toán không hề dễ như các bạn tưởng: Chúng ta không thể "mò" nghiệm để rồi suy ra được. Chúng ta nên bắt đầu với cách làm tự nhiên nhất: đặt $m^2 = k(m^2 - n^2 + 1)$. Vì bài toán chỉ yêu cầu một nghiệm, ta bắt đầu với $k = 1$ là số chính phương đầu tiên:

$$m^2 = m^2 - n^2 + 1 \Leftrightarrow n = 1,$$

không thỏa mãn vì $m > n > 1$.
Tiếp tục với $k = 4$ là số chính phương tiếp theo:

$$m^2 = 4(m^2 - n^2 + 1) \Leftrightarrow 4n^2 - 3m^2 = 4.$$

Từ phương trình trên suy ra $2 \mid m$ hay đặt $m = 2t$. Từ đó phương trình tương đương với

$$n^2 - 3t^2 = 1,$$

trở về phương trình Pell quen thuộc và phương trình này chắc chắn có nghiệm vì 3 không phải là số chính phương. Tìm nghiệm của phương trình này không hề khó, các bạn có thể tự tìm bằng cách sử dụng công thức nghiệm tổng quát của phương trình Pell hoặc hệ phương trình. ❐

Vậy tất cả các bài toán trên đều có thể tìm được nghiệm thỏa mãn. Bài toán vừa xong chỉ là một nghiệm đơn giản. Câu hỏi là có thể tìm được nghiệm tổng quát không? Câu trả lời là có. Trong kì thi chọn học sinh giỏi Toán quốc gia năm 2012, bài toán cũng sử dụng phương pháp bước nhảy Viete để giải được bài toán. Xin trích dẫn đề bài, bài giải trong tài liệu "Nhận xét và đánh giá đề thi VMO 2012" của Thầy Trần Nam Dũng:

Bài toán 8. Xét các số tự nhiên lẻ a, b mà a là ước số của $b^2 + 2$ và b là ước số của $a^2 + 2$. Chứng minh rằng a và b là các số hạng của dãy số tự nhiên (v_n) xác định bởi

$$v_1 = v_2 = 1; v_n = 4v_{n-1} - v_{n-2}, \forall n \geqslant 2.$$

Chứng minh. Giả sử (a, b) là cặp số tự nhiên lẻ mà a là ước số của $b^2 + 2$ và b là ước số của $a^2 + 2$. Trước hết ta chứng minh $(a, b) = 1$. Thật vậy, đặt $d = (a, b)$ thì do $d \mid a \mid b^2 + 2$ nên $d \mid 2$. Mà a, b lẻ nên d lẻ, suy ra $d = 1$.
Xét số $N = a^2 + b^2 + 2$ thì do $a^2 + 2$ chia hết cho b nên N chia hết cho b. Tương tự, N chia hết cho a. Vì $(a, b) = 1$ nên từ đây suy ra N chia hết cho ab. Vậy tồn tại số nguyên dương k sao cho

$$a^2 + b^2 + 2 = kab \tag{1}$$

Tiếp theo, ta chứng minh $k = 4$. Thật vậy, đặt $A = \{a + b | (a, b) \in \mathbb{N}^* \times \mathbb{N}^*, a_2 + b_2 + 2 = kab\}$. Theo giả sử ở trên thì $A \neq \emptyset$. Do tính sắp thứ tự tốt của $\mathbb{N}$, A có phần tử nhỏ nhất. Giả sử

a_0, b_0 là cặp số thỏa mãn điều kiện (1) với $a_0 + b_0$ nhỏ nhất.
Không mất tính tổng quát, có thể giả sử $a_0 \geqslant b_0$. Xét phương trình $a^2 - kb_0a + b_0^2 + 2 = 0$ có nghiệm a_0. Theo định lý Viete thì phương trình trên còn có 1 nghiệm nữa là $a_1 = kb_0 - a_0 = \frac{b_0^2+2}{2}$. Theo công thức nghiệm thì rõ ràng a_1 nguyên dương. Như vậy (a_1, b_0) cũng là một nghiệm của (1). Do tính nhỏ nhất của $a_0 + b_0$, ta có $a_0 + b_0 \leqslant a_1 + b_0$, tức là $a_0 \leqslant kb_0 - a_0$ suy ra $\frac{a_0}{b_0} \leqslant \frac{k}{2}$.
Ta có $a_0^2 + b_0^2 + 2 = ka_0b_0$ suy ra

$$\frac{a_0}{b_0} + \frac{b_0}{a_0} + \frac{2}{a_0b_0} = k \tag{2}$$

Do $\frac{a_0}{b_0} \leqslant \frac{k}{2}$ nên từ (2) ta có $k \leqslant \frac{k}{2} + 2 + 1$ hay $k \leqslant 6$.
Mặt khác, áp dụng bất đẳng thức AM-GM ta có $a_0^2 + b_0^2 \geqslant 2a_0b_0$ nên $k > 2$.
Nếu $k \neq 4$ thì $(a_0, b_0) \neq (1, 1)$, do đó $a_0b_0 \geqslant 2$. Dùng (2) để đánh giá ta có $k \leqslant \frac{k}{2} + 1 + 1$ nên $k \leqslant 4$. Vậy các giá trị $k = 5, 6$ bị loại. Nếu $k = 3$ thì do $a_0^2 + b_0^2 + 2 = 3a_0b_0$ nên suy ra $a_0^2 + b_0^2 + 2$ chia hết cho 3, suy ra một trong hai số a_0, b_0 chia hết cho 3, số còn lại không chia hết cho 3. Nếu $b_0 = 1$ thì a_0 chia hết cho 3, khi đó vế trái không chia hết cho 9 còn vế phải chia hết cho 9, mâu thuẫn. Vậy $b_0 > 1$. Từ đó suy ra $a_0b_0 \geqslant 6$. Lại sử dụng (2) để đánh giá, ta suy ra

$$k \leqslant \frac{k}{2} + 1 + \frac{2}{6} \Rightarrow k < \frac{8}{3}.$$

Mà $k \in \mathbb{N}$ nên $k \leqslant 2$, mâu thuẫn.
Như vậy ta đã chứng minh được nếu a, b là các số tự nhiên lẻ thỏa mãn điều kiện đề bài thì

$$a^2 + b^2 + 2 = 4ab \tag{3}$$

Ta sẽ chứng minh trong trường hợp như vậy thì tồn tại số nguyên dương n sao cho $(a, b) = (v_n, v_{n+1})$ với v_n là dãy số được định nghĩa ở đề bài.
Trước hết, ta có nhận xét : Nếu a, b là nghiệm của (3) thì $(4a - b, a)$ và $(4b - a, b)$ cũng là nghiệm của (3). Từ đó, do (v_1, v_2) là nghiệm của (3) nên $(4v_2 - v_1, v_2)$ cũng là nghiệm của (3), tức là (v_2, v_3) cũng là nghiệm của (3). Từ đây bằng quy nạp suy ra (v_n, v_{n+1}) là nghiệm của (3).
Giả sử tồn tại cặp số (a, b) thỏa mãn (3) nhưng không tồn tại n sao cho $(a, b) = (v_n, v_{n+1})$. Trong các cặp số như thế, chọn (a, b) có tổng $a + b$ nhỏ nhất. Không mất tính tổng quát, giả sử $a > b$ (chú ý a không thể bằng b vì nếu $a = b$ suy ra $a = b = 1$, khi đó $(a, b) = (v_1, v_2)$. Theo nhận xét trên thì $4b - a, b$ cũng là nghiệm của (3). Nhưng do $4b - a = \frac{b^2+2}{a} < a$ (Vì $a > b$ nên $ab - b^2 = (a + b)(a - b) \geqslant 3$)), nên $4b - a + b < a + b$. Theo định nghĩa của (a, b) ở trên, phải tồn tại n sao cho $(4b - a, b) = (v_n, v_{n+1})$. Sử dụng đẳng thức $4b - a = \frac{b^2+2}{a}$ và $b > 1$, ta suy ra $4b - a \leqslant b$. Như vậy $4b - a = v_n, b = v_{n+1}$. Nhưng từ đây $a = 4v_{n+1} - v_n = v_{n+2}$, tức là $(a, b) = (v_{n+1}, v_{n+2})$ mâu thuẫn. Vậy điều giả sử là sai, tức là phải tồn tại số tự nhiên n sao cho $(a, b) = (v_n, v_{n+1})$ và như vậy a, b là số hạng của dãy (v_n). Bài toán được giải quyết hoàn toàn. ❐

Nhận xét:

- Bài toán này có 2 ý chính:

1. Chứng minh rằng nếu k là số nguyên dương sao cho tồn tại a, b nguyên dương thỏa mãn điều kiện $a^2 + b^2 + 2 = kab$ thì $k = 4$. Phần này khá quen thuộc với các bạn biết về phương pháp phương trình Markov hay "bước nhảy Viete".
2. Mô tả tất cả các nghiệm của phương trình $a^2 + b^2 + 2 = 4ab$ thông qua cặp số hạng liên tiếp của dãy v_n, cái này gọi là phương pháp gien.

- Phương trình (3) còn có thể giải thông qua phương trình Pell $z^2 - 3b^2 = -2$. Tuy nhiên cách giải này sẽ khá cồng kềnh vì đây không phải là phương trình Pell loại 1.

Như vậy qua nhận xét của bài toán trên, thầy Trần Nam Dũng đã tổng kết lại các bước làm chính: Đó là sử dụng bước nhảy Viete để tìm được k và sử dụng phương pháp Gien, phương pháp lùi vô hạn để tìm được điểm đặc biệt của nghiệm, đó là nếu (a, b) là nghiệm thì $(4b-a, b)$ cũng là nghiệm, dẫn đến tìm được nghiệm tổng quát của phương trình trên.
Ngoài ra thầy cũng đã đề cập tới *phương trình Markov*, là một phương trình rất nổi tiếng, có thể nói là "thủy tổ" của phương pháp bước nhảy Viete:

Bài toán 9 (Phương trình Markov)**.** Tìm tất cả các số nguyên dương k sao cho phương trình sau có nghiệm nguyên dương:

$$x^2 + y^2 + z^2 = kxyz.$$

Chứng minh. Chúng ta vừa giải quyết xong các lớp bài toán với hai ẩn, vậy bài toán ba ẩn thì lời giải có khác không? Và khác như thế nào? Liệu ta có thể tìm được cách giải tổng quát cho bài toán với ba ẩn như với hai ẩn không?
Cách giải bài toán này phụ thuộc vào cách giải bài toán đối với hai số, trước hết ta cần bổ đề sau:

Bổ đề 1. $k = 3$ là số nguyên dương duy nhất để phương trình sau luôn có nghiệm nguyên dương (x, y):

$$x^2 + y^2 + 1 = kxy.$$

Bổ đề trên là một bài toán sử dụng bước nhảy Viete quen thuộc, mời bạn đọc tự giải.
Trở lại bài toán:

1. Thấy $k = 1$ thì phương trình có nghiệm $(3, 3, 3)$ và $k = 3$ thì phương trình có nghiệm $(1, 1, 1)$.
2. Xét $k \neq 1, 3$. Giả sử phương trình có nghiệm (x_0, y_0, z_0). Không mất tính tổng quát, giả sử $x_0 \leqslant y_0 \leqslant z_0$ và $x_0 + y_0 + z_0$ nhỏ nhất trong tất cả các tổng $x + y + z$ với x, y, z là nghiệm của phương trình.

   - Nếu $y_0 < z_0$, xét phương trình bậc hai:

     $$Z^2 - k.x_0y_0.Z + x_0^2 + y_0^2 = 0.$$

     Phương trình trên có một nghiệm là z_0. Theo định lý Viete thì có nghiệm thứ hai z_1 thỏa mãn:

     $$z_1 = kx_0y_0 - z_0 = \frac{x_0^2 + y_0^2}{z_0}.$$

Từ đó suy ra z_1 nguyên dương và (x_0, y_0, z_1) là nghiệm thứ hai. Do đó theo giả thiết cực hạn ta có:

$$x_0 + y_0 + z_0 \leqslant x_0 + y_0 + z_1 \Rightarrow z_0 \leqslant z_1,$$

dẫn đến

$$x_0^2 + y_0^2 - kx_0y_0 = z_1z_0 - z_1 - z_0 = (z_1 - 1)(z_0 - 1) - 1 \geqslant y_0^2 - 1,$$

và suy ra

$$1 \geqslant x_0(ky_0 - x_0) \geqslant x_0(kx_0 - x_0) \geqslant x_0,$$

mà x_0 nguyên dương suy ra $x_0 = 1$. Ta trở về bài toán $y^2 + z^2 + 1 = kyz$, chính là bổ đề suy ra $k = 3$, trái giả thiết.

- Nếu $y_0 = z_0$. Ta có

$$2y_0^2 - py_0^2 + x_0^2 = 0 \Rightarrow x_0^2 = y_0^2(px_0 - 2) \geqslant x_0^2(px_0 - 2),$$

và từ đó dẫn đến $3 \geqslant px_0$, mà $px_0 > 2$ nên $px_0 = 3$ suy ra $p \in \{1, 3\}$, trái giả thiết

Vậy $k \in \{1, 3\}$ thì phương trình luôn có nghiệm nguyên dương. ❐

Trên đây là một số bài toán mà tôi muốn giới thiệu với bạn đọc, đó là các bài toán khá quen thuộc và được lặp lại trong nhiều kì thi. Tôi hi vọng qua bài viết này bạn đọc có thể nắm bắt phương pháp giải một lớp các bài toán về phương trình bậc hai Diophante nhiều ẩn.
Sau đây là gợi ý cho các bài toán và một số các bài toán thử sức.

Gợi ý cho một số bài toán

2. Chứng minh $x_1 \geqslant 0$:

$$x_1^2 - x_1n(y_0 + 1) - n(y_0 + 1) + y_0^2 = 0 \Leftrightarrow x_1 = \frac{x_0^2 + y_0^2}{n(y_0 + 1)} - 1 > -1,$$

mà x_1 nguyên nên $x_1 \geqslant 0$.

3. Với a, b chẵn: có $b + 1 \mid b^2 - 1$, $b + 1 \mid a^2 + 1$ nên $b + 1 \mid a^2 + b^2$. Tương tự $a + 1 \mid a^2 + b^2$. Gọi $d = (a + 1, b + 1$, hãy chứng minh $d \mid 2$ mà d lẻ do $a + 1, b + 1$ lẻ nên $d = 1$, từ đó suy ra $a^2 + b^2 = k(a + 1)(b + 1)$.

4. $n = 1, 2, 3, 4$. Dễ dàng chỉ ra dãy với $n = 1, 2, 3$. Dãy có độ dài 4: 4,33,27,1384.
Phản chứng tồn tại dãy độ dài 5: a_1, a_2, a_3, a_4, a_5. Từ đây chứng minh hai mệnh đề sau:

   (a) a_2, a_3 chẵn (sử dụng phản chứng)

   (b) $a_2 + 1 \mid a_3^2 + 1, a_3 + 1 \mid a_2^2 + 1$.

5. Chứng minh $x_1 \geqslant 0$: từ phương trình ta có

$$4x_1y_0 = \frac{(x_1 + y_0)^2}{n} - 1 > -1 \Leftrightarrow x_1 > -\frac{1}{4y_0}$$

mà x_1 nguyên nên $x_1 > 0$.

Các bài toán thử sức

Bài toán 10. Chứng minh rằng nếu a, b là các số nguyên dương sao cho $k = \frac{a^2+b^2+6}{ab}$ là số nguyên thì $k = 8$.

Bài toán 11. 1. Tìm n sao cho phương trình sau có nghệm nguyên dương:

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

2. Tìm n sao cho phương trình sau có nghệm nguyên dương:

$$(x + y + z + t)^2 = nxyzt$$

Bài toán 12 (Mở rộng phương trình Markov)**.** Cho a, b, c là ba số nguyên thỏa mãn

$$a^2 + b^2 + c^2 = kabc.$$

Chứng minh rằng hoặc $(a, b, c) = 1$ hoặc $(a, b, c) = 3$.

Bài toán 13. Chứng minh rằng phương trình

$$x^2 + y^2 + z^2 = n(xyz + 1)$$

có nghiệm nguyên dương khi và chỉ khi n được biểu diễn dưới dạng tổng của hai số chính phương.

Bài toán 14 (Adapted from Vietnam TST 1992)**.** Tìm tất cả các cặp số nguyên dương (a, b) thỏa mãn

$$a^2 + b^2 = k(ab - 1).$$

Bài toán 15 (Turkey TST 1994)**.** Tìm tất cả các cặp (a, b) mà $ab \mid a^2 + b^2 + 3$.

Bài toán 16. Cho a, b, c là ba số nguyên dương thỏa mãn

$$0 < a^2 + b^2 - abc \leqslant c,$$

chứng minh rằng $a^2 + b^2 - abc$ là số chính phương.

Bài toán 17. Chứng minh rằng tồn tại vô hạn các cặp (m, n) nguyên dương thỏa mãn

$$\frac{m+1}{n} + \frac{n+1}{m} = 4.$$

Bài toán 18 (IMO Shortlist 2003)**.** Tìm tất cả các cặp a, b thỏa mãn

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

Bài toán 19. Chứng minh rằng tất cả nghiệm nguyên dương của phương trình $x^2+y^2+1 = 3xy$ là $(x, y) = (F_{2k-1}, F_{2k+1})$ với F_n là số Fibonacci.

Bài toán 20 (IMO 2007, IMO shortlist)**.** Cho a, b nguyên dương. Chứng minh rằng nếu $4ab - 1 \mid (4a^2 - 1)^2$, thì $a = b$.

Gợi ý. Dùng phản chứng, giả sử $a > b$ với mọi a, b thỏa mãn. Từ giả thiết, hãy chứng minh:

1. $4ab - 1 \mid (a - b)^2$
2. $a_0 - b_0 \geqslant (a_0 + b_0)(4a_0b_0 - 1)$ với a_0, b_0 là nghiệm nhỏ nhất theo nghĩa $a_0 + b_0$ min, từ đó suy ra mâu thuẫn

❒

Bài toán 21 (**, Kiran Kedlaya)**.** Chứng minh rằng $(xy + 1)(yz + 1)(zx + 1)$ là số chính phương khi và chỉ khi $xy + 1, yz + 1, zx + 1$ là số chính phương.

Gợi ý.
1. Nếu $xy + 1, yz + 1, zx + 1$ là số chính phương thì hiển nhiên ta có tích ba số đó chính phương.
2. Nếu $(xy + 1)(yz + 1)(zx + 1)$ là số chính phương. Hãy chứng minh tồn tại t thỏa mãn hệ sau:
$$(x + y - z - t)^2 = 4(xy + 1)(zt + 1)$$
$$(x + z - y - t)^2 = 4(xz + 1)(yt + 1)$$
$$(x + t - y - z)^2 = 4(xt + 1)(yz + 1)$$
(t chính là nghiệm của phương trình $t^2 + x^2 + y^2 + z^2 - 2(xy + yz + zt + tx + zx + ty) - 4xyzt - 4 = 0$). Xét nghiệm t nhỏ nhất.
Sử dụng phản chứng: giả sử $xy + 1$ không chính phương. Từ đây, hãy chứng minh:
   (a) $t \geqslant \frac{-1}{\max\{x,y,z\}} > -1$ nên $t \geqslant 0$.
   (b) Xét hai trường hợp $t = 0$ và $t > 0$, dẫn đến mâu thuẫn.

❒

Tài liệu tham khảo

1. Đặng Hùng Thắng, Nguyễn Văn Ngọc, Vũ Kim Thủy, *Bài giảng số học.* NXB Giáo dục, 1996.
2. Kiran S. Kedlaya, *When Is* $(xy + 1)(yz + 1)(zx + 1)$ *a Square.* Mathematics Magazine, Vol. 17, No.1, Feb., 1998.
3. Authur Engel, *Problem Solving Strategies.* Spinger Verlag, 1998.
4. Trần Nam Dũng, *Lời giải và bình luận VMO 2012.* Diễn đàn Mathscope, 2012.
5. Site: http://www.artofproblemsolving.com/Forum

Chuyên đề 2:
Vận dụng phương pháp LTE
vào giải các bài toán số học

Phạm Quang Toàn [1]

Bổ đề về số mũ đúng (Lifting The Exponent Lemma) là một bổ đề rất hữu dụng trong việc giải các bài toán số học và rất được biết đến trong lịch sử Olympiad. Thực chất là nó được mở rộng ra từ bổ đề Hensel. Ta thường viết tắt tên của bổ đề là **LTE**, tên Tiếng Việt thì có thể gọi là *bổ đề về số mũ đúng*. Bài viết này xin được giới thiệu với bạn đọc về bổ đề và những ứng dụng đặc sắc của nó vào các bài toán lý thuyết số.

Bài viết chủ yếu dựa vào tài liệu của thành viên Amir Hossein bên trang mathlinks.ro (về mặt lý thuyết thì mình giữ nguyên bản bài viết của Amir Hossein sang bài viết này) và có kèm theo một số ví dụ được lấy từ các kì thi Olympic toán trên thế giới.

Một số khái niệm

Ở đây, thay vì kí hiệu $a \vdots b$ nghĩa là a chia hết cho b, ta sẽ kí hiệu $b|a$. Và $a \not\vdots b$ sẽ được thay bằng $b \nmid a$.

Định nghĩa 1. Cho p là số nguyên tố, a là số nguyên và α là số tự nhiên. Ta có p^α là lũy thừa đúng (exact power) của a và α là số mũ đúng (exact exponent) của p trong khai triển của α nếu $p^\alpha | a$ và $p^{\alpha+1} \nmid a$. Khi đó ta viết $p^\alpha \parallel a$ hay $v_p(a) = \alpha$.

Ví dụ. Ta có $v_5(5400) = 3$ hay $5^3 \parallel 5400$ vì $5400 = 5^3 \cdot 3^2 \cdot 2^2$.

Sau đây là một số tính chất. Chứng minh tính chất này không khó, xin dành cho bạn đọc.

Tính chất 1. Cho a, b, c là các số nguyên. Ta có

1. $v_p(ab) = v_p(a) + v_p(b)$
2. $v_p(a^n) = n \cdot v_p(a)$
3. $\min\{v_p(a), v_p(b)\} \leqslant v_p(a+b)$
   Dấu đẳng thức xảy ra khi $v_p(a) \neq v_p(b)$.
4. $v_p\left(\gcd(|a|, |b|, |c|)\right) = \min\{v_p(a), v_p(b), v_p(c)\}$
5. $v_p\left(\operatorname{lcm}(|a|, |b|, |c|)\right) = \max\{v_p(a), v_p(b), v_p(c)\}$

Chú ý. $v_p(0) = \infty$ với mọi số nguyên tố p.

[1]Lớp 9C THCS Đặng Thai Mai, Tp Vinh

Hai bổ đề

Đầu tiên, xin giới thiệu với bạn đọc hai bổ đề. Và hai bổ đề này sẽ giúp ta tìm cách chứng minh được các định lí khác của LTE.

Bổ đề 1. Cho x, y là hai số nguyên và cho n là số nguyên dương. Cho số nguyên tố p bất kì sao cho $p|x-y$ và $p \nmid x, p \nmid y$. Ta có

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

Chứng minh. Ta có $p|x-y$ nên

$$x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} \equiv nx^{n-1} \not\equiv 0 \pmod{p}$$

Mà $x^n - y^n = (x-y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)$ nên ta suy ra điều phải chứng minh. ❐

Bổ đề 2. Cho x, y là hai số nguyên và n là số nguyên dương lẻ. Cho số nguyên tố p bất kì thỏa mãn $p|x+y$ và $p \nmid x, p \nmid y$. Khi đó

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

Chứng minh. Áp dụng bổ đề 1 ta có $v_p(x^n - (-y)^n) = v_p(x-(-y))$ nên $v_p(x^n+y^n) = v_p(x+y)$. (vì n lẻ). Bổ đề được chứng minh. ❐

Lifting The Exponent Lemma (LTE)

Định lý 1. Cho x và y là các số nguyên (không nhất thiết phải nguyên dương), n là một số nguyên dương và p là một số nguyên tố lẻ thỏa mãn $p|x-y$ và $p \nmid x, p \nmid y$. Ta có

$$v_p\left(a^n - b^n\right) = v_p(a-b) + v_p(n)$$

Chứng minh. Ta sẽ đi chứng minh quy nạp theo $v_p(n)$. Trước hết, ta sẽ đi chứng minh khẳng định sau:

$$v_p(x^p - y^p) = v_p(x-y) + 1$$

Để chứng minh điều đó thì ta cần chỉ ra rằng

$$p|x^{p-1} + x^{p-2}y + \cdots + xy^{p-2} + y^{p-1} \tag{1}$$

và

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

Với **(1)**, nhờ áp dụng $x \equiv y \pmod{p}$ ta suy ra

$$x^{p-1} + \cdots + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}$$

Với **(2)**, ta đặt $y = x + kp$ với $k \in \mathbb{N}^*$. Khi đó với $1 \leqslant i \leqslant p-1$ ($i \in \mathbb{N}$) thì

$$\begin{aligned} y^i x^{p-1-i} &\equiv (x+kp)^i x^{p-1-i} \\ &\equiv x^{p-1-i}\left(x^i + i(kp)x^{i-1} + \frac{i(i-1)}{2}(kp)^2 x^{i-2} + \cdots\right) \\ &\equiv x^{p-1-i}\left(x^i + i(kp)x^{i-1}\right) \\ &\equiv x^{p-1} + ikpx^{p-2} \pmod{p^2}. \end{aligned}$$

Do đó,

$$\begin{aligned} x^{p-1} + x^{p-2}y + \cdots + y^{p-1} &\equiv x^{p-1} + (x^{p-1} + kpx^{p-2}) + (x^{p-1} + 2kpx^{p-2}) + \cdots + (x^{p-1} + (p-1)kpx^{p-2}) \\ &\equiv px^{p-1} + \frac{p-1}{2} \cdot kp^2 x^{p-2} \\ &\equiv px^{p-1} \not\equiv 0 \pmod{p^2} \end{aligned}$$

Như vậy $v_p(x^p - y^p) = v_P(x-y) + 1$.
Quay lại bài toán, đặt $n = p^k \cdot h$ với $b, k \in \mathbb{N},\ b \geqslant 1$ $\gcd(b,p) = 1$. Khi đó thì

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

Định lý được chứng minh. ❐

Định lý 2. Cho hai số nguyên x, y, n là số nguyên dương lẻ, và p là ước nguyên tố lẻ sao cho $p|x+y$ và $p \nmid x, p \nmid y$. Khi đó

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

Chứng minh. Áp dụng định lý 1 ta có

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

hay

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

❐

Định lý 3. *(cho trường hợp $p = 2$)* Cho x, y là hai số nguyên lẻ thỏa mãn $4|x-y$. Khi đó

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

Chứng minh. Theo bổ đề 1 thì nếu p nguyên tố, $\gcd(p,n) = 1, p|x-y$ và $p \nmid x, p \nmid y$ thì

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

Do đó ta chỉ cần xét tới trường hợp n là lũy thừa của 2, tức cần chứng minh

$$v_2(x^{2^n} - y^{2^n}) = v_2(x - y) + n$$

Thật vậy, ta có

$$x^{2^n} - y^{2^n} = (x^{2^{n-1}} + y^{2^{n-1}})(x^{2^{n-2}} + y^{2^{n-2}}) \cdots (x^2 + y^2)(x + y)(x - y)$$

Vì $x \equiv y \equiv \pm 1 \pmod 4$ nên $x^{2^k} \equiv y^{2^k} \equiv 1 \pmod 4$. Do đó

$$v_2(x^{2^{n-1}} + y^{2^{n-1}}) = v_2(x^{2^{n-2}} + y^{2^{n-2}}) = \cdots = v_2(x + y) = 1$$

Như vậy $v_2(x^{2^n} + y^{2^n}) = n + v_p(x - y)$, ta có điều phải chứng minh. ❐

Định lý 4. *(cho trường hợp $p = 2$)* Cho hai số nguyên lẻ x, y, n là số nguyên dương chẵn và $2|x - y$. Khi đó

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

Chứng minh. Ta có $4|x^2 - y^2$ nên đặt $n = 2^k \cdot h$ với $k, h \in \mathbb{N}^*$, $\gcd(h, 2) = 1$. Khi đó ta có

$$\begin{aligned} v_2(x^n - y^n) &= v_2(x^{h \cdot 2^k} - y^{h \cdot 2^k}) \\ &= v_2((x^2)^{2^{k-1}} - (y^2)^{2^{k-1}}) \\ &\vdots \\ &= v_2(x^2 - y^2) + k - 1 \\ &= v_2(x - y) + v_2(x + y) + v_2(n) - 1 \end{aligned}$$

❐

Ta có hệ quả sau:

Hệ quả. Cho a, n là hai số nguyên dương:

i) p là hai số nguyên tố lẻ sao cho $v_p(a - 1) = \alpha \in \mathbb{N}^*$, khi đó với mọi số tự nhiên β ta có $v_(a^n - 1) = \alpha + \beta \Leftrightarrow v_p(n) = \beta$.

ii) n chẵn sao cho $v_2(a^2 - 1) = \alpha \in \mathbb{N}^*$, khi đó với mọi số nguyên dương β thì $v_2(a^n - 1) = \alpha + \beta \Leftrightarrow v_2(n) = \beta + 1$.

Chú ý.

a) Nếu trong các bài toán đòi hỏi vận dụng phương pháp LTE, ta nên để ý tới các điều kiện đặt ra của n, x, y, lựa chọn định lý phù hợp đưa vào lời giải bài toán.

b) Nếu dữ liệu bài toán cho $a|b$ với $a, b \in \mathbb{N}$ thì với mọi p là ước nguyên tố của b, ta luôn có $v_p(b) \geqslant v_p(a)$. Ngược lại, nếu $v_p(b) \geqslant v_p(a)$ thì $a|b$. Như vậy

$$a|b \Leftrightarrow v_p(b) \geqslant v_p(a)$$

Đây là một tính chất rất thường được dùng trong các bài toán sử dụng phương pháp LTE.

Một số ví dụ

Sau đây mình xin đưa ra một số ví dụ về các ứng dụng của phương pháp này.
Ví dụ . Tìm số nguyên dương n nhỏ nhất thỏa mãn $2^{2013}|1999^n - 1$.
Lời giải. Áp dụng **Định lý 4** ta có

$$v_2(1999^n - 1) = v_2(n) + v_2(2000) + v_2(1998) = v_2(n) + 5$$

Để thỏa mãn $2^{2013}|1999^n - 1$ thì $v_2(n) + 5 \geqslant 2013$ hay $v_2(n) \geqslant 2008$.
Vậy số nguyên dương n nhỏ nhất thỏa mãn đề ra là 2^{2008}.
Ví dụ . *(IMO Shortlist 1991)* Tìm số nguyên dương k lớn nhất thỏa mãn 1991^k là ước của

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Lời giải. Đặt $a = 1991$ thì a là số nguyên tố lẻ. Do đó theo **Định lý 2** thì

$$\begin{aligned} v_a\left((a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}\right) &= v_a\left((a-1)^{a^2})^{a^{a-1}} + (a+1)^{a^{a-1}}\right) \\ &= v_a\left((a-1)^{a^2} + a + 1\right) + v_a(a^{a-1}) \\ &= a - 1 + v_a\left((a-1)^{a^2} + a + 1\right) \end{aligned}$$

Cũng theo Định lý 2 thì $v_a\left((a-1)^{a^2} + 1\right) = v_a(a) + v_a(a^2) = 3$ nên $v_a\left((a-1)^{a^2} + a + 1\right) = 1$.
Vậy, $v_a\left((a-1)^{a^{a+1}} + (a+1)^{a^{a-1}}\right) = a$. Ta thu được $\max k = a = \boxed{1991}$.
Ví dụ 1. *(Italy TST 2003)* Tìm bộ số nguyên nguyên (a, b, p) sao cho a, b là số nguyên dương, p là số nguyên tố thỏa mãn $2^a + p^b = 19^a$.
Lời giải. Vì a nguyên dương nên $17|19^a - 2^a$. Vậy $p = 17$. Áp dụng **Định lý 1** ta có

$$\begin{aligned} &v_{17}(19^a - 2^a) = v_{17}(17) + v_{17}(a) \\ &\Leftrightarrow b = 1 + v_{17}(a) \leqslant 1 + a \end{aligned}$$

1. Nếu $b < 1 + a$ hay $1 \leqslant b \leqslant a$. Dễ dàng chứng minh quy nạp rằng $19^a - 2^a \geqslant 17^a$ với $a \geqslant 1$. Mà $17^a \geqslant 17^b$. Vậy $a = b = 1$ ở trường hợp này.

2. Nếu $b = 1 + a$ thì dễ dàng chứng minh quy nạp $19^a - 2^a < 17^{a+1} = 17^b$, mâu thuẫn.

Vậy $(a, b, p) = (1, 1, 17)$ là đáp án duy nhất bài toán.
Ví dụ . *(IMO 1990)* Tìm số nguyên dương n sao cho $n^2|2^n + 1$.
Lời giải. Với $n = 1$ thỏa mãn. Với $n \geqslant 2$, nhận thấy n lẻ.
Gọi p là ước nguyên tố lẻ nhỏ nhất của n. Khi đó ta suy ra $2^{2n} \equiv 1 \pmod{p}$. Gọi k là số nguyên dương nhỏ nhất thỏa mãn $2^k \equiv 1 \pmod{p}$. Khi đó $k|2n$. Theo định lý Fermat nhỏ thì $2^{p-1} \equiv 1 \pmod{p}$ nên $k|p - 1$. Như vậy ta suy ra $\gcd(n, k) = 1$ nên $k|2$. Với $k = 1$ thì $p|1$, mâu thuẫn. Vậy $k = 2$. Do đó $p = 3$ hay $3|n$.
Đặt $v_3(n) = k$ ($k \in \mathbb{N}^*$). Áp dụng **Định lý 2** thì ta có

$$v_3(2^n + 1) = v_3(3) + v_3(n) = 1 + k$$

Lại có vì $n^2|2^n+1$ nên $v_3(2^n+1) \geqslant v_3(n^2) \Leftrightarrow k+1 \geqslant 2k$. Vậy $k=1$. Đặt $n=3m$ với $m \in \mathbb{N}^*$ và $\gcd(m,3)=1$.

Gọi p_1 là ước nguyên tố nhỏ nhất của m. Khi đó ta có $2^{6m} \equiv 1 \pmod{p_1}$. Gọi k_1 là số nguyên dương nhỏ nhất thỏa mãn $2^k \equiv 1 \pmod{p_1}$. Tương tự thì ta dễ dàng suy ra $k|6$. Vì $p_1 \geqslant 5$ nên $k=3$ hoặc $k=6$.

Với $k=3$ thì $p_1|7$ nên $p_1=7$. Với $k=6$ thì $p_1|63$ mà $p_1 \geqslant 5$ nên $p_1=7$. Tuy nhiên $2^n+1=2^{3m}+1=8^m+1 \equiv 2 \pmod 7$ mà $7|n^2$, mâu thuẫn.

Vậy ước nguyên tố duy nhất của n là 3 mà $3 \parallel n$ nên $n=3$.

Số nguyên dương n thỏa mãn đề bài là $n \in \{1;3\}$.

Ví dụ 2. *(European Mathematical Cup 2012, Senior Division)* Tìm số nguyên dương a,b,n và số nguyên tố p thỏa mãn

$$a^{2013}+b^{2013}=p^n$$

Lời giải. Đặt $a=p^x \cdot y, b=p^z \cdot t$ với $x,y,z,t \in \mathbb{N};\ t,y \geqslant 1$ và $\gcd(y,p)=1, \gcd(t,p)=1$.

Không làm mất tính tổng quát, giả sử rằng $x \geqslant z$. Dễ nhận thấy rằng $n \geqslant 2013x \geqslant 2013z$. Khi đó phương trình ban đầu tương đương với

$$t^{2013}+p^{2013(x-z)} \cdot y^{2013}=p^{n-2013z}$$

Nếu $x>z$ thì $p \nmid VT$. Do đó $p \nmid p^{n-2013z}$ suy ra $n=2013z$. Vậy ta được phương trình

$$t^{2013}+p^{2013(x-z)} \cdot y^{2013}=1,$$

mâu thuẫn vì $VT \geqslant 2$ (do $,ty \geqslant 1$). Vậy $x=z$. Phương trình trở thành

$$t^{2013}+y^{2013}=p^{n-2013z}=p^k\ (k=n-2013z \in \mathbb{N}^*) \tag{3}$$

Nếu $p|2013$ thì theo định lý Fermat nhỏ ta suy ra $t^{2013}+y^{2013} \equiv 2 \pmod p$, mâu thuẫn vì $p|p^k$. Vậy $\gcd(p,2013)=1$.

Dễ thấy theo (3) thì $p|t+y$. Do đó bằng việc áp dụng **Định lý 2** ta có

$$v_p\left(t^{2013}+y^{2013}\right)=v_p(t+y)$$

Ta lại có $t+y|t^{2013}+y^{2013}$ và (3) nên ta suy ra

$$\begin{aligned} p^k=t+y&=t^{2013}+y^{2013}\\ t^{2012}(t-1)+y^{2012}(y-1)&=0 \end{aligned}$$

Vì $t,y \geqslant 1$ nên từ phương trình ta suy ra $t=y=1$. Do đó $p=2$, từ đó suy ra $a=b=2^h, n=2013h+1$ với $h \in \mathbb{N}$.

Nhận xét. Ta có thể tổng quát bài toán lên thành: Giải phương trình nghiệm nguyên dương

$$a^n+b^n=p^k$$

với p nguyên tố.

Ví dụ 3. *(Romanian IMO TST 2005)* Giải phương trình nghiệm nguyên dương

$$3^x=2^x \cdot y+1$$

Lời giải. Ta xét hai trường hợp:

1. Nếu x lẻ thì áp dụng **Định lý 1** ta có $v_2(3^x-1)=v_2(3-1)=1$ hay $v_2(2^x\cdot y)=1$. Do đó $x=1$. Từ phương trình ta suy ra $y=1$.

2. Nếu x chẵn thì áp dụng **Định lý 1** ta có

$$\begin{aligned} &v_2(3^x-1)=v_2(3-1)+v_2(3+1)+v_2(x)-1=2+v_2(x)\\ \Leftrightarrow &v_2(2^x\cdot y)=2+v_2(x)\Leftrightarrow x+v_2(y)=v_2(x)+2 \qquad (1)\end{aligned}$$

   Đặt $x=2^m\cdot k$ với $m,n\in\mathbb{N}^*$. Ta dễ dàng chứng minh bằng quy nạp rằng $2^m\cdot k>m+2$ với $m\in\mathbb{N},\ m\geqslant 3$. Do đó $x>v_2(x)+2$ với $v_2(x)\geqslant 3$ hay với $x\geqslant 2^{v_2(x)}=8$. Như vậy $x\geqslant 8$ thì (1) không xảy ra. Vậy $x\leqslant 8$, x chẵn nên $x\in\{2;4;6\}$. Từ đây ta tìm được $(x,y)=(2;2),(4;5)$.

Vậy phương trình có nghiệm nguyên dương $(x,y)=(1;1),(2;2),(4;5)$.
Nhận xét. Qua bài toán trên, ta lưu ý một số ý tưởng được dùng trong phương pháp này: Với p là một ước nguyên tố của $a=p^m\cdot k$ với $m,k\in\mathbb{N}^*$ thì:

i) $a\geqslant p^{v_p(a)}$.

ii) $p^m\cdot k\geqslant m+\alpha$ với $m\geqslant\beta$. Từ đây suy ra $a\geqslant v_p(a)+\alpha$ với $v_p(a)\geqslant\beta$ hay $a\geqslant p^\beta$.

Các bài trên chủ yếu là các bài không khó để vận dụng bổ đề LTE vì ta đã xác định được các yếu tố p,a,b một cách dễ dàng. Tuy nhiên, vẫn có một số bài toán đòi hỏi ta phải đi tìm ra các yếu tố p,a,b ...
Ví dụ 4. *(IMO 1999)* Tìm tất cả các cặp (n,p) nguyên dương sao cho p là số nguyên tố và $(p-1)^n+1$ chia hết cho n^{p-1}.
Lời giải. Dễ thấy với $n=1$ thì p là số nguyên tố bất kì đều thỏa mãn đề ra. Với $n\geqslant 2$, ta có các trường hợp:
Trường hợp 1. Nếu $p=2$ thì $n|2$. Do đó $n=2$.
Trường hợp 2. Nếu p lẻ. Lấy q là ước nguyên tố nhỏ nhất của n, khi đó $(p-1)^n\equiv -1 \pmod q$ hay $(p-1)^{2n}\equiv 1 \pmod q$ và $\gcd(p-1,q)=1$. Ta lấy o là số nguyên dương nhỏ nhất thỏa mãn $(p-1)^o\equiv 1 \pmod q$. Khi đó thì ta suy ra $o|2n$. Áp dụng định lý Fermat nhỏ ta có $(p-1)^{q-1}\equiv 1 \pmod q$. Do đó $o|q-1$.
Như vậy, $o|2n$ và $o|q-1$. Nếu $\gcd(o,n)>1$ hay o,n chia hết cho số nguyên tố r, khi đó ta suy ra $r|n$ và $r\leqslant o$. Mà $o|q-1$ nên $o<q$, do đó $r<q$. Mà r và q đều là ước nguyên tố của n, mâu thuẫn với điều kiện nhỏ nhất của q. Vậy $\gcd(n,o)=1$. Do đó $2|o$. Vậy $(p-1)^2\equiv 1 \pmod q$ hay $q|p(p-2)$.

1. Nếu $q|p-2$ thì ta có $(p-1)^n+1\equiv 1^n+1\equiv 2 \pmod q$. Vậy $q=2$. Ta có $(p-1)^n+1$ chia hết cho 2 nên $p=2$, mâu thuẫn vì p lẻ.

2. Nếu $q|p$. Dễ nhận thấy n phải lẻ (vì nếu n chẵn thì $(p-1)^n+1\equiv 0 \pmod 4$, mâu thuẫn vì p lẻ). Ta áp dụng **Định lý 2** ta có

$$v_q\left((p-1)^n+1\right)=v_q(n)+v_q(p)\geqslant v_q(n)\cdot(p-1) \qquad (4)$$

Đặt $p = q^a \cdot b$ với $a, b \in \mathbb{N}^*$. Dễ dàng chứng minh bằng quy nạp $q^a \cdot b \geqslant a + 2$ (chú ý vì $q|p$ nên $q \geqslant 3$), dấu bằng xảy ra khi $a = b = 1, q = 3$. Do đó $p \geqslant v_q(p) + 2$. Kết hợp với (3) ta suy ra

$$p - 2 \geqslant v_q(p) \geqslant v_q(n)(p-2)$$

Vậy $q = p = 3$ và $v_3(n) = 1$. Đặt $n = 3k$ với $k \in \mathbb{N}^*,\ \gcd(k,3) = 1,\ \gcd(k,2) = 1$. Như vậy từ đề bài ta sẽ có $9k^2 | 8^k + 1$.

Hiển nhiên $9|8^k + 1$. Ta chỉ cần đi tìm k sao cho $k^2|8^k + 1$. Với $k = 1$ thì $n = 3$, thỏa mãn. Với $k \geqslant 2$, hoàn toàn tương tự, lấy r là ước nguyên tố nhỏ nhất của k và s là số nguyên dương nhỏ nhất sao cho $8^s \equiv 1 \pmod r$. Ta suy ra $s|2$ nên $s = 2$. Khi đó $r|8^2 - 1$ hay $r|7$, điều này mâu thuẫn vì $8^k + 1 \equiv 2 \pmod 7$.

Vậy, cặp số (n, p) thỏa mãn đề bài là $(1, p), (2, 2), (3, 3)$.

Ví dụ 5. *(Brazil XII Olympic Revenge 2013)* Tìm các bộ ba số (p, n, k) nguyên dương thỏa mãn p là số nguyên tố Fermat và

$$p^n + n = (n+1)^k \tag{5}$$

Số nguyên tố Fermat là số nguyên tố có dạng $2^{2^x} + 1$ với x tự nhiên.

Lời giải. Đặt $\alpha = 2^x$. Nếu $n = 1$ thì $(5) \Leftrightarrow p = 2^k - 1 = 2^\alpha + 1$. Do đó $k = 2, \alpha = 1$ nên $p = 3$. Nếu $n \geqslant 2$. Ta gọi r là một ước nguyên tố của n. Từ phương trình ta suy ra $p^n \equiv 1 \pmod n$ hay $p^n \equiv 1 \pmod r$. Do đó $\gcd(p, r) = 1$. Đặt k là số nguyên dương nhỏ nhất thỏa mãn $p^k \equiv 1 \pmod r$. Ta cũng có theo định lý Fermat nhỏ thì $p^{r-1} \equiv 1 \pmod r$. Vậy ta suy ra $k|r - 1$ và $k|n$. Vì $\gcd(r - 1, n) = 1$ nên $k = 1$. Ta có $r|p - 1$ hay $r|2^\alpha$. Vậy $r = 2$ hay $2|n$. Ta có

$$(5) \Leftrightarrow p^n - 1 = (n+1)\left[(n+1)^{k-1} - 1\right]$$

Từ phương trình dẫn đến $v_2(p^n - 1) = v_2\left((n+1)^{k-1} - 1\right)$.
Nếu $k - 1$ lẻ thì

$$v_2\left((n+1)^{k-1} - 1\right) = v_2(n) < v_2\left(p^2 - 1\right) + v_2(n) - 1 = v_2(p^n - 1),$$

mâu thuẫn. Vậy $k - 1$ chẵn. Áp dụng **Định lý 4** ta có

$$\begin{aligned} & v_2(p^n - 1) = v_2\left((n+1)^{k-1} - 1\right) \\ \Leftrightarrow & v_2(p^2 - 1) + v_2(n) - 1 = v_2(n) + v_2(n+2) + v_2(k-1) - 1 \\ \Leftrightarrow & v_2(p-1) + v_2(p+1) = v_2(n+2) + v_2(k-1) \end{aligned}$$

Nếu $v_2(k-1) \geqslant v_2(p-1)$ thì $p - 1|k$. Do đó $(n+1)^k \equiv n + 1 \pmod p$ theo định lý Fermat nhỏ. Tuy nhiên theo (5) thì $n \equiv (n+1)^k \pmod p$ nên $n \equiv n + 1 \pmod p$, mâu thuẫn. Vậy $v_2(k-1) < v_2(p-1)$. Khi đó theo phương trình ta có

$$1 \leqslant v_2(p+1) = v_2(2^\alpha + 2) < v_2(n+2)$$

Do đó $v_2(n+2) \geqslant 2$. Ta suy ra $n \equiv 2 \pmod 4$.

1. Nếu $p > 5$ thì $2^{2^x} + 1 > 5$ nên $x \geqslant 2$. Do đó $p \equiv 2 \pmod 5$. Áp dụng $n \equiv 2 \pmod 4$ thì ta suy ra $p^n \equiv 4 \pmod 5$. Do đó $4 + n \equiv (n+1)^k \pmod 5$. Vì $n + 4 \not\equiv n + 1 \pmod 5$ nên $k \not\equiv 1 \pmod 4$. Vì k lẻ nên $k \equiv 3 \pmod 4$. Vậy $4 + n \equiv (n+1)^3 \pmod 5$.

- Nếu $n \equiv 0 \pmod 5$ thì $4+n-(n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 1 \pmod 5$ thì $4+n-(n+1)^3 \equiv 2 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 2 \pmod 5$ thì $4+n-(n+1)^3 \equiv 4 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 3 \pmod 5$ thì $4+n-(n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.
- Nếu $n \equiv 4 \pmod 5$ thì $4+n-(n+1)^3 \equiv 3 \pmod 5$, mâu thuẫn.

Vậy với mọi $n \in \mathbb{N}^*$ thì $n+4 \not\equiv (n+1)^3 \pmod 5$. Ta loại trường hợp $p > 5$.

2. Nếu $p = 5$ thì $\alpha = 2$. Khi đó thì $3 = v_2(n+2) + v_2(k-1)$. Vì $v_2(n+2) \geqslant 2$ nên ta suy ra $v_2(n+2) = 2, v_2(k-1) = 1$. Ta cũng có $5^n + n = (n+1)^k$.

   - Với $n = 2$ thì $k = 3$.
   - Với $n \geqslant 3$. Gọi q là ước nguyên tố lẻ của n thì $q|5^{(n,q-1)} - 1 = 5^2 - 1 = 24$. Vậy $q|3$ nên $q = 3$. Do đó $n \equiv 0 \pmod 6$. Kết hợp với $n \equiv 2 \pmod 4$ ta suy ra $5^n \equiv -1 \pmod{13}$ nên $n - 1 \equiv (n+1)^k \pmod{13}$. Áp dụng **Định lý 1** ta có

   $$v_3(5^n - 1) = v_3\left((n+1)^{k-1} - 1\right) \Leftrightarrow 1 + v_3\left(\frac{n}{2}\right) = v_3(k-1) + v_3(n)$$

   Vậy $3|k-1$. Ta cũng có $k \equiv 3 \pmod 4$ nên $k \equiv 7 \pmod{12}$. Theo định lý Fermat nhỏ ta suy ra $(n+1)^k \equiv (n+1)^7 \equiv \pm(n+1) \pmod{13}$. Như vậy $n - 1 \equiv -n - 1 \pmod{13}$ dẫn đến $n \equiv 0 \pmod{13}$, vô lý. (vì với $13|n$ thì $5^n \equiv 1 \pmod{13}$, mâu thuẫn do $5^n \equiv 5 \pmod{13}$).

Vậy $(p, n, k) = (3, 1, 2), (5, 2, 3)$.

Ví dụ . Tìm bộ ba số nguyên dương (a, b, c) sao cho $a^b + 1 = (a+1)^c$.

Lời giải. Gọi p là một ước nguyên tố lẻ của a. Khi đó thì theo **Định lý 1** ta có

$$\begin{aligned} & v_p((a+1)^c - 1) = v_p(a) + v_p(c) \geqslant v_p(a) \cdot b \\ \Leftrightarrow & v_p(c) \geqslant v_p(a)(b-1) \qquad (6) \end{aligned}$$

1. Nếu c lẻ thì ta có $v_2\left((a+1)^c - 1\right) = v_2(a)$. Do đó $b = 1$. Như vậy thì ta có $a+1 = (a+1)^c$ suy ra $c = 1$.

2. Nếu c chẵn thì $v_2(c) \geqslant 1$ và $b \geqslant 2$. Theo **Định lý 4** thì

   $$v_2((a+1)^c - 1) = v_2(a) + v_2(a+2) + v_2(c) - 1 = v_2(a) \cdot b \qquad (7)$$

   - Nếu $v_2(a) = 1$ thì ta luôn có $v_2(c) \geqslant v_2(a)$. Kết hợp với (6) ta suy ra $c \geqslant a(b-1) > b$, mâu thuẫn vì lúc đó thì $(a+1)^c > a^b + 1$.
   - Nếu $v_2(a) \geqslant 2$ thì $(7) \Leftrightarrow v_2(c) = v_2(a) \cdot (b-1)$. Kết hợp với (6) ta dẫn đến $c \geqslant a(b-1) > b$, mâu thuẫn

Vậy phương trình có nghiệm $(a, b, c) = (k, 1, 1)$ với k là số nguyên dương tùy ý.

Nhận xét. Từ bài toán trên, ta có thêm một số mở rộng sau:

Mở rộng 1. Tìm các số nguyên dương m, l, n, k thỏa mãn $(1 + m^n)^l = 1 + m^k$.

Mở rộng 2. (IMO Shortlist 2000) Tìm bộ ba số nguyên dương (a, m, n) thỏa mãn $a^m+1|(a+1)^n$.

Ngoài việc phương pháp LTE được ứng dụng trực tiếp vào lời giải thì phương pháp này còn được dùng để tìm dạng vô hạn của bài toán chia hết.

Ví dụ 6. Chứng minh tồn tại vô hạn số tự nhiên n thỏa mãn $n|3^n + 1$.

Phân tích và định hướng lời giải. Điều bây giờ ta cần làm và đi tìm một trong các dạng của n thỏa mãn $n|3^n + 1$.

Trước hết, nhận thấy $5|3^2 + 1^2$. Bây giờ ta để ý đến các điều kiện a, b, p trong **Định lý 2**, áp dụng và ta sẽ được $5^{k+1}|3^{2\cdot5^k} + 1^{2\cdot5^k}$. Do đó $2 \cdot 5^k|3^{2\cdot5^k} + 1$. Vậy ta chỉ cần chứng minh $n = 2 \cdot 5^k$ với $k \in \mathbb{N}$ thì $n|3^n + 1$.

Lời giải. Trước hết, ta sẽ đi chứng minh $3^{4\cdot5^{k-1}} \equiv 1 \pmod{5^k}$. Áp dụng **Định lý 1** ta có

$$v_5\left(3^{4\cdot5^{k-1}} - 1\right) = v_5(3^4 - 1) + v_5(5^{k-1}) = k$$

Vậy $3^{4\cdot5^{k-1}} \equiv 1 \pmod{5^k}$ hay $5^k|\left(3^{2\cdot5^k} - 1\right)\left(3^{2\cdot5^k} + 1\right)$. Do đó $5^k|3^{2\cdot5^k} + 1$. Lại có $2|3^{2\cdot5^k} + 1$ nên $2 \cdot 5^k|3^{2\cdot5^k} + 1$.

Vì $k \in \mathbb{N}^*$ nên tồn tại vô hạn số tự nhiên $n = 2 \cdot 5^k$ sao cho $n|3^n + 1$.

Ví dụ 7. *(Romanian Master of Mathematics Competition 2012)* Chứng minh tồn tại vô hạn số nguyên dương n thỏa mãn $2^{2^n+1} + 1$ chia hết cho n.

Phân tích và định hướng lời giải. Ta sẽ tìm một số n thỏa mãn điều kiện trên. Dễ thấy $n = 3$ thỏa mãn. Ta mạnh dạn thử với $n = 9, 27 \cdots$ cũng đều thỏa mãn. Từ đây ta dễ dàng tìm được một dạng của nn là $n = 3^k$. Ở đây mình xin giới thiệu hai lời giải:

Lời giải 1. Ta sẽ đi chứng minh số nguyên dương $a_n = 3^n$ thỏa mãn yêu cầu bài toán. Thật vậy, theo **Định lý 2** ta có

$$v_3(2^{a_n} + 1) = v_3(3) + v_3(a_n) = k + 1$$

Và

$$v_3(2^{2^{a_n}+1} + 1) = v_3(3) + v_2(2^{a_n} + 1) = k + 2$$

Vậy $a_n|2^{2^{a_n}+1} + 1$.

Lời giải 2. Ta sẽ đi chứng minh số nguyên dương $a_n = \frac{2^{3^n}+1}{9}$ thỏa mãn yêu cầu đề ra.

Áp dụng **Định lý 2** ta có

$$v_3(a_n) = v_3(3) + v_3(3^n) - 2 = n - 1$$

Đặt $a_n = 3^{n-1}m$ với $m \in \mathbb{N}^*,\ \gcd(3, m) = 1$. Ta có

$$v_3(2^{2^{a_n}+1} + 1) > v_3(2^{a_n} + 1) > v_3(a_n) = n - 1.$$

Vậy $3^{n-1}|2^{2^{a_n}+1} + 1$. Mặt khác, tiếp tục áp dụng **Định lý 2** thì

$$v_3(2^{a_n} + 1) = v_3(3) + v_3(a_n) = n$$

Do đó $3^n|2^{a_n} + 1$. Vậy ta suy ra $2^{3^n} + 1|2^{2^{a_n}+1} + 1$. Mà $m|2^{a_n} + 1$ nên $m|2^{2^{a_n}+1} + 1$.

Vì $\gcd(m, 3) = 1$ nên $a_n|2^{2^{a_n}+1} + 1$.

Bài tập vận dụng

1. Chứng minh phương trình $x^7 + y^7 = 1998^z$ không có nghiệm nguyên dương.

2. Tìm tất cả số nguyên dương n thỏa mãn $7^{2013}|5^n + 1$.

3. Tìm số nguyên dương n lớn nhất sao cho $2^n|2011^{2013^{2016}-1} - 1$.

4. Chứng minh tồn tại vô hạn số nguyên dương $n \in \mathbb{N}$ thỏa mãn $n^2|2^n + 3^n + 6^n + 1$.

5. *(Japan MO Finals 2012)* Cho p là số nguyên tố. Tìm mọi số nguyên n thỏa mãn với mọi số nguyên x, nếu $p|x^n - 1$ thì $p^2|x^n - 1$.

6. Cho $a > b > 1$, b là một số lẻ, n là một số nguyên dương. Nếu $b^n|a^n - 1$. Chứng minh $a^b > \frac{3^n}{n}$.

7. Tìm số nguyên dương n thỏa mãn $9^n - 1$ chia hết cho 7^n.

8. *(IMO Shortlist 2007)* Tìm mọi hàm số toàn ánh $f : \mathbb{N} \to \mathbb{N}$ sao cho với mỗi $m, n \in \mathbb{N}$ và với mỗi p nguyên thố, $f(m+n)$ chia hết cho p khi và chỉ khi $f(m) + f(n)$ chia hết cho p.

9. *(IMO 2000)* Tồn tại hay không số nguyên n thỏa mãn n có đúng 2000 ước nguyên tố và $2^n + 1$ chia hết cho n ?

10. Với một số tự nhiên n, cho a là số tự nhiên lớn nhất thỏa mãn $5^n - 3^n$ chia hết cho 2^a. Lấy b là số tự nhiên lớn nhất thỏa mãn $2^b \leqslant n$. Chứng minh rằng $a \leqslant b + 3$.

11. Chứng minh rằng nếu $n \geqslant 2$ sao cho $n|7^n - 3^n$ thì n chẵn.

12. Tìm số nguyên dương n thỏa mãn

    i) $n|5^n + 1$.

    ii) $n^2|5^n + 1$.

    iii) $n^3|5^n + 1$.

13. Tìm mọi số nguyên dương k sao cho k số nguyên tố lẻ đầu tiên $p_1, p_2 \cdots, p_k$ đều tồn tại hai số nguyên dương a, n thỏa mãn

$$p_1 \cdot p_2 \cdots p_k - 1 = a^n$$

14. *(MOSP 2001)* Tìm các số nguyên dương (x, r, p, n) thỏa mãn $x^r - 1 = p^n$.

15. Tìm tất cả các bộ số (m, p, q) với p, q nguyên tố và m nguyên dương sao cho $2^m p^2 + 1 = q^5$.

16. *(Iran TST 2009)* Cho n là một số nguyên dương. Chứng minh rằng

$$3^{\frac{5^{2^n}-1}{2^{n+2}}} \equiv (-5)^{\frac{3^{2^n}-1}{2^{n+2}}} \pmod{2^{n+4}}$$

17. *(IMO Shortlist 2010)* Tìm các cặp số nguyên không âm (m, n) thỏa mãn

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

18. *(Iran Third Round 2011)* Cho số tự nhiên $k \geqslant 7$. Có bao nhiêu cặp nguyên dương (x, y) thỏa mãn

$$73^{73^x} \equiv 9^{9^y} \pmod{2^k}?$$

19. Giải phương trình nghiệm nguyên dương trong đó p là số nguyên tố:

$$p^a - 1 = 2^n(p - 1)$$

Tài liệu tham khảo

[1] Amir Hossein Parvardi, Lifting The Exponent Lemma: (tài liệu pdf)
[2] Các diễn đàn toán:
diendantoanhoc.net/forum
forum.mathscope.org
mathlinks.ro

Chuyên đề 3:
Các bài toán số học hoán vị vòng quanh

Nguyễn Anh Huy, Nguyễn Việt Tâm [1]

Sự bình đẳng và hoán vị giữa các ẩn số là một nép đẹp của Toán học, thường được gặp trong các bài toán hệ phương trình và bất đẳng thức. Tương tự, Số học cũng có những bài toán hoán vị vòng quanh mà các ẩn là số nguyên, số nguyên dương, tuy nhiên lời giải đa dạng và phức tạp hơn rất nhiều. Bài viết này sẽ đề cập đến hai hướng đi cụ thể để giải dạng bài trên, là đối xứng hóa và bất đẳng thức.

Trong bài viết có sử dụng một số kiến thức về bước nhảy Viete và hàm $v_p(n)$, bạn đọc có thể tham khảo ở hai chuyên đề trước.

Phương pháp đối xứng hóa

Phương pháp này thường được dùng trong các bài toán chia hết hoán vị vòng: $a \mid f(b);\ b \mid f(a)$.
Nếu có $(a;b)=1$ ta xây dựng hàm g thỏa $g(x) \vdots x\ \forall x \in \mathbb{Z}$ và h thỏa
$h(a;b)=f(a)+g(b)=f(b)+g(a)$ đối xứng theo a,b. Khi đó

$$a \mid h(a;b);\ b \mid h(a;b) \Rightarrow ab \mid h(a;b) \Rightarrow h(a;b)=kab$$

Đây là phương trình nghiệm nguyên với a,b đối xứng. Ta có thể dùng bất đẳng thức nếu $\deg h=1$ hoặc bước nhảy Viete nếu $\deg h=2$.
Nếu không có $(a;b)=1$ thì từ giả thiết ta suy ra $ab \mid f(a)f(b)$, sau đó khai triển vế phải và bỏ các hạng tử chia hết cho ab để được phương trình nghiệm nguyên có dạng tương tự.

Bài tập 3.1. Tìm các số nguyên tố $p \geqslant q$ thỏa

$$\begin{cases} q-1 \mid 3p-1 \\ p-1 \mid 3q-1 \end{cases}$$

Lời giải

Đặt $a=p-1,\ b=q-1\ (a \geqslant b \geqslant 1)$, ta có

$$\begin{cases} a \mid 3(b+1)-1 \\ b \mid 3(a+1)-1 \end{cases} \Rightarrow ab \mid (3a+2)(3b+2)\ \ (*) \Rightarrow 6a+6b+4 \vdots ab$$

[1]Lớp 12CT THPT chuyên Lê Hồng Phong

Từ đó ta có

$$6a + 6b + 4 \geqslant ab \Rightarrow \frac{6}{a} + \frac{6}{b} + \frac{4}{ab} \geqslant 1$$

Lại có

$$\frac{12}{b} + \frac{4}{b^2} \geqslant \frac{6}{a} + \frac{6}{b} + \frac{4}{ab}$$

Suy ra

$$\frac{12}{b} + \frac{4}{b^2} \geqslant 1 \Rightarrow b^2 - 12b - 4 \leqslant 0 \Rightarrow 1 \leqslant b \leqslant 12$$

Do $b + 1$ nguyên tố nên $b \in \{1; 2; 4; 6; 10; 12\}$. Xét các trường hợp sau, với lưu ý $a + 1$ nguyên tố:

* Nếu $b = 1 : (*) \Rightarrow 6a + 6 + 4 \vdots a \Rightarrow 10 \vdots a \Rightarrow a \in \{1; 2; 10\}$.

* Nếu $b = 2 : (*) \Rightarrow 6a + 12 + 4 \vdots 2a \Rightarrow 8 \vdots a \Rightarrow a \in \{2; 4\}$.

* Nếu $b = 4 : (*) \Rightarrow 6a + 24 + 4 \vdots 4a \Rightarrow a + 14 \vdots 2a \Rightarrow a \in \{6; 10\}$.

* Nếu $b = 6 : (*) \Rightarrow 6a + 36 + 4 \vdots 6a \Rightarrow 40 \vdots 6a$ (loại).

* Nếu $b = 10 : (*) \Rightarrow 6a + 60 + 4 \vdots 10a \Rightarrow 3a + 32 \vdots 5a \Rightarrow a = 16$.

* Nếu $b = 12 : (*) \Rightarrow 6a + 72 + 4 \vdots 12a$ (loại).

Từ đó ta tìm được cặp (p, q) nguyên tố thỏa bài toán là

$(2, 2), (3, 3), (5, 3), (7, 5), (17, 11)$. □

Bài tập 3.2. Tìm số bộ số nguyên dương $(a; b; c)$ đôi một nguyên tố cùng nhau thoả $a < b < c$ và

$$a \mid bc - 31;\ b \mid ca - 31;\ c \mid ab - 31$$

Lời giải

Do $a \mid bc - 31$ và $a \mid a(b + c)$ nên ta có

$$a \mid ab + bc + ca - 31.$$

Tương tự với b và c. Lại do $(a; b) = (b; c) = (c; a) = 1$ nên

$$abc \mid ab + bc + ca - 31 \quad (*)$$

Xét các trường hợp sau:

⊛ **Trường hợp 1:** $a \geqslant 3$

Suy ra $b \geqslant 4;\ c \geqslant 5$, do đó $ab + bc + ca > 31$. Ta cũng có

$$abc \geqslant 3bc > ab + bc + ca > ab + bc + ca - 31$$

Điều này mâu thuẫn với (*).

⊛ **Trường hợp 2:** $a = 2$

Suy ra $b \mid 2c - 31$ và $c \mid 2b - 31$, do đó

$$bc \mid 2b + 2c - 31$$

Chứng minh tương tự ta có $b = 3;\ c = 5$.

⊛ **Trường hợp 3:** $a = 1$

Suy ra $b \mid c - 31$ và $c \mid b - 31$. Nếu $b + c = 31$ thì hai điều kiện trên hiển nhiên thoả. Khi đó ta có $a = 1 < b < c$ và $b + c = 31$. Do $a < b < c$ nên $2 \leqslant b \leqslant 15$. Dễ thấy có 14 bộ số $(a; b; c)$ thoả.

Nếu $b + c \neq 31$ thì ta chứng minh $1 < b < c < 31$. Nếu ngược lại:

* Nếu $b > 31 \Rightarrow c > b > b - 31 > 0$. Do đó c không là ước của $b - 31$.
* Nếu $b = 31$ thì $31 \mid c - 31 \Rightarrow 31 \mid c$, loại do $(b; c) = (31; c) = 1$.
* Nếu $b < 31 < c$ thì $|c| > |31 - b| > 0$ do đó c không là ước của $b - 31$.

Như vậy $1 < b < c < 31$. Ngoài ra, từ $b \mid c - 31$ và $c \mid b - 31$ với $(b; c) = 1$ ta cũng có

$$bc \mid 31 - b - c.$$

* Nếu $b \geqslant 5 \Rightarrow c \geqslant 6 \Rightarrow bc \geqslant 30 > 11 \geqslant 31 - (b + c)$, vô lý.
* Nếu $b = 4$ thì $4 \mid c - 31$ và $c \mid 27 \Rightarrow c = 27$ (loại do $b + c \neq 31$).
* Nếu $b = 3$ thì $3 \mid c - 31$ và $c \mid 28$, suy ra $c \in \{4; 7\}$.

Vậy trường hợp 3 cho 16 bộ $(a; b; c)$ thoả bài toán.

Kết luận: Có 17 bộ số $(a; b; c)$ thoả bài toán. □

Bài tập 3.3. Tìm các số nguyên tố p, q thoả $p < q < 1000$ và

$$q \mid p^3 - 1;\ p \mid q^3 - 1$$

Lời giải

Ta có $q \mid p^3 - 1 = (p - 1)(q^2 + q + 1)$ mà $q > p - 1$ nên

$$q \mid p^2 + p + 1.$$

Và $p \mid q^3 - 1 = (q - 1)(q^2 + q + 1)$. Do đó ta xét 2 trường hợp:

⊛ **Trường hợp 1:** $p \mid q - 1$

Đặt $p^2 + p + 1 = nq \ \ (n \in \mathbb{N}^*)$. Do $p^2 + p + 1 \equiv q \equiv 1 \pmod{p}$ nên $n \equiv 1 \pmod{p}$.

Lại có

$$n = \frac{p^2 + p + 1}{q} \leqslant \left[\frac{p^2 + p + 1}{p + 1}\right] = \left[p + \frac{1}{p + 1}\right] = p \ \ (\text{do } q \geqslant p + 1)$$

Suy ra $n = 1$, vậy $q = p^2 + p + 1$. Do đó $p \leqslant 31$, vì $37^2 + 37 + 1 > 1000$.

Thử với tất cả số nguyên tố $p < 31$ ta tìm được các bộ số thoả bài toán là

$(p; q) = (2; 7), (3; 13), (5; 31), (17; 307)$.

⊛ **Trường hợp 2:** $p \mid q^2 + q + 1$

Do $p \mid q^2 + q + 1$ và $q \mid p^2 + p + 1$ nên ta có

$$p \mid q^2 + q + 1 + p^2 + p;\ q \mid p^2 + p + 1 + q^2 + q$$

hay

$$pq \mid p^2 + q^2 + p + q + 1$$

Như vậy ta xét phương trình nghiệm nguyên dương

$$a^2+b^2+a+b+1=mab \ \ (*) \ \ (m\in\mathbb{N}^*)$$

Viết lại (*) dưới dạng

$$a^2+(1-mb)a+b^2+b+1=0 \ \ (**)$$

Gọi S là tập các bộ số nguyên dương $(a;b)$ thoả (**). Theo nguyên lý cực hạn trong S tồn tại cặp số $(a_0;b_0)$ thoả a_0+b_0 nhỏ nhất. Không giảm tổng quát giả sử $a_0\geqslant b_0$.
Theo định lý Viete, (**) cũng có nghiệm $(a';b_0)$ trong đó a' thoả

$$\begin{cases} a_0+a'=mb_0-1 \\ a_0a'=b_0^2+b_0+1 \end{cases}$$

Từ phương trình đầu suy ra $a'\in\mathbb{Z}$. Từ phương trình sau suy ra $a'>0$. Vậy $(a';b_0)\in S$. Do đó

$$a_0+b_0\leqslant a'+b_0\Leftrightarrow a_0\leqslant a'=\frac{b_0^2+b_0+1}{a_0}\Leftrightarrow b_0^2+b_0+1\geqslant a_0^2$$

Nếu $a_0>b_0$ thì $a_0\geqslant b_0+1\Rightarrow a_0^2\geqslant(b_0+1)^2>b_0^2+b_0+1$, mâu thuẫn. Vậy $a_0=b_0$, suy ra

$$a_0^2+(1-a_0).a_0+a_0^2+a_0+1=0$$

Suy ra $1\vdots a_0\Rightarrow a_0=b_0=1$. Vậy ta có $m=5$.
Khi đó (*) trở thành

$$a^2+b^2+a+b+1=5ab \ \ (*)$$

Theo chứng minh trên, nếu $(a_0;b_0)$ là nghiệm của (*) thì $(5a_0-b_0-1;a_0)$ cũng là nghiệm của (*). Do đó từ nghiệm $(1;1)$ ta có nghiệm $(3;1)$, sau đó là $(13;3)$, ...
Tóm lại các nghiệm của (*) được cho bởi công thức

$$(a_i;b_i)=(x_{i+1};x_i) \text{ với } (x_n):\begin{cases} x_0=x_1=1 \\ x_{n+1}=5x_n-x_{n-1}-1 \ \forall n\geqslant 1 \end{cases}$$

Việc chứng minh điều trên hoàn toàn tương tự bài số học VMO 2012, và xin được dành cho bạn đọc.
Tiếp theo ta tìm các nghiệm là số nguyên tố nhỏ hơn 1000. Dễ thấy chỉ cần xét $i\leqslant 4$, do $x_6>1000$. Từ đó ta tìm được $(p;q)=(3;13),(13;61)$.
Kết luận: Các bộ số $(p;q)$ thoả bài toán là $(2;7),(3;13),(5;31),(13;61),(17;307)$. $\square$

Phương pháp dùng bất đẳng thức

Ta có thể sắp xếp các ẩn số đối xứng theo thứ tự hoặc chỉ ra một ẩn có một đại lượng nào đó lớn nhất hoặc bé nhất. Lưu ý việc sắp xếp ở đây không chỉ giới hạn ở $a\geqslant b\geqslant c$, mà cũng có thể là $f(a)\geqslant f(b)\geqslant f(c)$, trong đó f là một hàm số học.

Bài tập 3.4. Cho các số nguyên dương a, b, c. Chứng minh

$$\frac{(a;b).(b;c).(c;a)}{(a;b;c)^2} = \frac{[a;b].[b;c].[c;a]}{[a;b;c]^2}$$

Trong đó $(a;b)$ và $[a;b]$ lần lượt là là ước chung lớn nhất và bội chung nhỏ nhất của a, b.

Lời giải

Gọi p là số nguyên tố bất kì. Nếu p không là ước của $[a;b;c]$ thì dễ thấy $v_p(VT) = v_p(VP) = 0$. Nếu $p \mid [a;b;c]$ thì p là ước của a, b hoặc c. Đặt $a = p^x.a_1; b = p^y.b_1; c = p^z.c_1$ và không giảm tổng quát giả sử $x \geqslant y \geqslant z$. Khi đó ta có

$$v_p(VT) = y + z + z - 2z = y$$

và

$$v_p(VP) = x + y + x - 2x = y$$

Suy ra $v_p(VT) = v_p(VP)\ \forall p \in \mathbb{P}$. Do đó $VT = VP$. $\square$
Nhận xét là trong lời giải trên ta đã giả sử $v_p(a) \geqslant v_p(b) \geqslant v_p(c)$, và sử dụng định lý cơ bản của số học: Mọi số nguyên lớn hơn 1 đều có một và chỉ một cách phân tích ra thừa số nguyên tố.

Bài tập 3.5. Tìm các số nguyên tố p, q thỏa

$$(5^p - 2^p)(5^q - 2^q) \vdots pq \quad (*)$$

Lời giải

Giả sử $p \leqslant q$. Nhận xét $p = q = 3$ thỏa.
$\divideontimes$ Nếu $p = 3, q > 3$ thì ta có

$$117(5^q - 2^q) \vdots 3q \Leftrightarrow 39(5^q - 2^q) \vdots q$$

Do $5^q - 2^q \equiv 5 - 2 \equiv 3\ [q]$ theo Fermat nên $q \mid 39$, do đó $q = 13$.
$\divideontimes$ Nếu $5 < p < q$ (để ý $VT(*)$ không chia hết cho 5 nên $p, q \neq 5$) thì tương tự ta có
$5^p - 2^p \equiv 5 - 2 \equiv 3\ [p]$, do đó từ giả thiết suy ra

$$5^q - 2^q \vdots p$$

Lại có $5^{p-1} \equiv 2^{p-1} \equiv 1\ \ [p]$ nên $5^{p-1} - 2^{p-1} \vdots p$.
Do $q > p - 1$ nên $(q, p-1) = 1$. Theo định lý Bezout, tồn tại $m, n \in \mathbb{N}^*$ thỏa

$$mq - (p-1)n = 1 \text{ hoặc } m(p-1) - nq = 1 \quad (**)$$

Xét đồng dư mod p ta có

$$\begin{cases} 5^{p-1} & \equiv 2^{p-1} \\ 5^q & \equiv 2^q \end{cases} \Rightarrow \begin{cases} 5^{n(p-1)} & \equiv 2^{n(p-1)} \\ 5^{mq} & \equiv 2^{mq} \end{cases}$$

Suy ra

$$5^{n(p-1)}.2^{mq} \equiv 2^{n(p-1)}.5^{mq}$$

Kết hợp với (**), sau khi rút gọn hai vế ta được $5 \equiv 2 \ \ [p]$ hay $p = 3$ (loại vì đang xét $p > 5$).
Kết luận: $(p; q) = (3; 3), (3; 13), (13; 3)$. $\square$

Bài tập 3.6. Tìm các cặp số nguyên tố (p, q) thỏa

$$2^p + 2^q \vdots pq$$

Lời giải

Nhận xét là $(x - 1, x + 1) = (2, x + 1) \leqslant 2 \ \forall x \in \mathbb{Z}$.
* Nếu $p = q$ thì $2^{p+1} \vdots p^2 \Rightarrow p = q = 2$.
* Nếu $p > q$:
Xét $q = 2$ ta có $2^2 + 2^p \vdots 2p \Rightarrow 2 + 2^{p-1} \vdots p \Rightarrow p \in \{2; 3\}$.
Xét $q > 2$ thì do $2^p + 2^q = 2^q(2^{p-1} + 1) \vdots q$ nên

$$2^{p-1} + 1 \vdots q \ \ (1) \Rightarrow 2^{2(p-q)} \equiv 1 \ \ [q]$$

Gọi a là số nhỏ nhất thỏa $2^a \equiv 1 \ \ [q]$. Theo tính chất của ord suy ra $q - 1 \vdots a$ và $2(p - q) \vdots a$.
Đặt $p - q = 2^k.m; \ q - 1 = 2^l.n; \ a = 2^r.s \ (k + 1 \geqslant r; l \geqslant r; m \vdots s; n \vdots s; m, n, s$ lẻ).

⁎ **Trường hợp 1:** $r = k + 1$. Ta suy ra $l \geqslant k + 1$ và

$$\begin{cases} 2(p-q) & = 2^{k+1}.m \\ q-1 & = 2^l.n \end{cases} \Rightarrow \begin{cases} 2(p-q)s & = am \\ (q-1)m & = (p-q).n.2^{l-k-1} \end{cases}$$
$$\Rightarrow \frac{n.2^{l-k-1}}{2s} = \frac{(q-1).m}{2s(p-q)} = \frac{q-1}{a} = \frac{2^l.n}{2^r.s}$$
$$\Rightarrow 2^{l-k-2} = 2^{l-r} \Rightarrow r = k + 2 \text{ (mâu thuẫn)}$$

⁎ **Trường hợp 2:** $r \leqslant k$
Suy ra $p - q \vdots a \Rightarrow 2^{p-q} - 1 \vdots 2^a - 1 \vdots q \ \ (2)$
Từ (1) và (2) suy ra $q \mid (2^{p-q} - 1, 2^{p-q} + 1)$.
Mà $(2^{p-q} - 1, 2^{p-q} + 1) \leqslant 2$ theo chứng minh trên, do đó $q = 2$ (mâu thuẫn do đang xét $q > 2$).
Kết luận: $(p, q) = (2; 2), (2; 3), (3; 2)$. $\square$

Bài tập 3.7. Cho các số nguyên dương x, y, z thoả $(xy+1)(yz+1)(zx+1)$ là số chính phương. Chứng minh $xy + 1, yz + 1, zx + 1$ đều là số chính phương.

Lời giải

Trong các bộ số $(x;y;z)$ thoả bài toán, xét bộ $(x;y;z)$ có $x+y+z$ nhỏ nhất. (1)
Không giảm tổng quát giả sử $z=\max\{x;y;z\}$.
Gọi t là số thỏa phương trình bậc hai

$$\begin{aligned} &t^2+x^2+y^2+z^2-2(xy+yz+zt+tx+zx+ty)-4xyzt-4=0 \quad (*)\\ \Leftrightarrow &t^2-2t(x+y+z+2xyz)+x^2+y^2+z^2-2(xy+yz+zx)-4=0 \end{aligned}$$

Nhận xét rằng (*) tương đương với 3 phương trình sau:

$$\begin{aligned} (x+y-z-t)^2&=4(xy+1)(zt+1)\\ (x+z-y-t)^2&=4(xz+1)(yt+1)\\ (x+t-y-z)^2&=4(xt+1)(yz+1) \end{aligned}$$

Và t nguyên do (*) có 2 nghiệm nguyên

$$t_{1,2}=x+y+z+2xyz\pm 2\sqrt{(xy+1)(yz+1)(zx+1)}$$

Nên nhân cả 3 phương trình trên vế theo vế, ta suy ra $(xt+1)(yt+1)(zt+1)$ là số chính phương.
Ngoài ra ta cũng có

$$xt+1\geqslant 0;\ yt+1\geqslant 0;\ zt+1\geqslant 0$$

Suy ra

$$t\geqslant \frac{-1}{\max\{x;y;z\}}>-1 \quad (\text{do } x=y=z=1 \text{ không thoả})$$

* Nếu $t=0$ thì từ (*) ta suy ra

$$(x+y+z)^2=4(xy+yz+zx+1)\Leftrightarrow (x+y-z)^2=4(xy+1)$$

Suy ra $xy+1$ là số chính phương. Chứng minh tương tự ta cũng có $yz+1, zx+1$ là số chính phương. * Nếu $t>0$ thì từ (1) suy ra $t\geqslant z$ với mọi t thoả (*).
Nhưng t chỉ có thể bằng t_1 hoặc t_2, và ta lại có

$$t_1t_2=x^2+y^2+z^2-2(xy+yz+zx)-4\leqslant z^2-x(2z-x)-y(2z-y)<z^2$$

Suy ra điều mâu thuẫn. Vậy ta có đpcm. □

Bài tập 3.8. Tìm các bộ số nguyên $(a;b;c)$ thỏa

$$\begin{cases} a^2-bc=91\\ b^2-ca=91\\ c^2-ab=91 \end{cases}$$

Lời giải

Không giảm tổng quát giả sử $a \leqslant b \leqslant c$. Do 91 không là số chính phương nên $a, b, c \neq 0$.
Nếu $a \geqslant 0$ thì $b, c \geqslant 0$ do đó $a^2 - bc \leqslant 0 < 91$, vậy $a < 0$.
Nếu $(a; b; c)$ thỏa hệ thì $(-a; -b; -c)$ cũng thỏa hệ. Do đó ta xét các bộ số có $c > 0$.
Nếu $b = c$ thì ta có

$$a^2 - b^2 = 91 = b^2 - ab \Leftrightarrow \left[\begin{array}{l} a - b = 0 \\ a = -2b \end{array}\right.$$

Dễ thấy $a = b = c$ vô lý, và $a = -2b$ cũng dẫn đến $5b^2 = 91$, vô lý.
Do đó $b \neq c$. Tương tự ta có $a \neq b$.

⊛ **Trường hợp 1:** $b > 0$
Từ hệ ta có

$$\begin{aligned} & 91b = b(b^2 - ac);\ 91c = c(c^2 - ab) \\ \Rightarrow\ & 91b - 91c = b^3 - c^3 \\ \Rightarrow\ & 91 = b^2 + bc + c^2 \geqslant 3b^2 \\ \Rightarrow\ & b \in \{1; 2; 3; 4; 5\} \end{aligned}$$

Thay vào hệ ta tìm được các nghiệm $(a; b; c) = (-10; 1; 9), (-11; 5; 6)$.

⊛ **Trường hợp 2:** $b < 0$
Từ hệ ta có

$$\begin{aligned} & 91b = b(b^2 - ac);\ 91a = a(a^2 - bc) \\ \Rightarrow\ & 91(b - a) = b^3 - a^3 \\ \Rightarrow\ & 91 = a^2 + ab + b^2 \geqslant 3b^2 \\ \Rightarrow\ & b \in \{-1; -2; -3; -4; -5\} \end{aligned}$$

Thay vào hệ ta tìm được các nghiệm $(a; b; c) = (-9; -1; 10), (-6; -5; 11)$.
Tóm lại các bộ $(a; b; c)$ thỏa giả thiết là
$(-10; 1; 9), (10; -1; -9), (-11; 5; 6), (11; -5; -6), (-9; -1; 10), (9; 1; -10), (-6; -5; 11), (6; 5; -11)$
và các hoán vị. □

Bài tập tự luyện

Bài 1: (APMO 2002) Tìm các số nguyên dương a, b thoả

$$b^2 - a \mid a^2 + b;\ a^2 - b \mid b^2 + a$$

Bài 2: Chứng minh có vô hạn bộ số nguyên dương $(a; b; c)$ thoả $ab + 1,\ bc + 1,\ ca + 1$ đều là số chính phương.
Bài 3: Tìm các số nguyên dương x, y, z đôi một nguyên tố cùng nhau thoả

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \in \mathbb{N}^*$$

Bài 4: Tìm các bộ số nguyên $(x; y; z)$ thoả $2 \leqslant x \leqslant y \leqslant z$ và

$$z \mid xy - 1;\ y \mid zx - 1; x \mid yz - 1$$

Bài 5: Tìm các số nguyên dương $a, b, c > 1$ đôi một khác nhau thỏa

$$(a-1)(b-1)(c-1) \mid abc-1$$

Bài 6: Chứng minh với mọi số nguyên dương a, b, n thì

$$(36a+b)(36b+a) \neq 2^n$$

Bài 7*: (VMO 2013) Tìm số các bộ $(a; b; c; a'; b'; c')$ với $a, b, c, a', b', c' \in \{0; 1; 2; ...; 14\}$ và thoả

$$ab + a'b' \equiv bc + b'c' \equiv ca + c'a' \equiv 1(\text{ mod } 15)$$

Bài 8: (VMO 2012) Tìm các số nguyên dương lẻ a, b thoả

$$a \mid b^2+2;\ b \mid a^2+2$$

Bài 9: Cho $a, b, c \in \mathbb{Z}$ thỏa

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

Chứng minh abc là lập phương một số nguyên.

Tài liệu tham khảo

1. Trang web brilliant.org.
2. Các chuyên đề số học - Phan Huy Khải.
3. Các phương pháp giải toán qua các kỳ thi Olympic - Trần Nam Dũng (Chủ biên), Võ Quốc Bá Cẩn, Lê Phúc Lữ.
4. Problems in Elementary Number Theory - Peter Vandendriessche, Hojoo Lee

Chuyên đề 4:
DÃY SỐ SỐ HỌC

Ninh Văn Tú[1]

Dãy số là một vấn đề khá thiết yếu trong giải tích và được ứng dụng vào khá nhiều các lĩnh vực khác như phương trình hàm, tổ hợp, số học... Những bài toán về giới hạn dãy số dường như trở thành vấn đề khá quen thuộc và xuất hiện nhiều trong các kì thi học sinh giỏi cấp trường, cấp tỉnh, cấp thành phố cũng như các kì thi Olympic, VMO... Nhưng một mảng khá đặc biệt của dãy số trong việc ứng dụng số học cũng như các bài toán số học để giải các bài toán dãy số là một vấn để khá thú vị trong mảng dãy số. Hi vọng chuyên đề này sẽ giúp ích cho các bạn trong việc tiếp thêm kinh nghiệm về mảng thú vị này.

Dãy số nguyên và tính chất số học

Ta sẽ lần lượt xét tổng quan các bài toán với dạng tổng quát để có thể có cái nhìn bao quát hết về thế giới dãy nguyên phong phú, đa màu. Từ đó ta sẽ có được các ý tưởng khi gặp một bài toán chứng minh dãy nguyên hoặc các bài toán liên quan đến dạng ấy.

Bài tập 4.1. Cho $a, b, c \in \mathbb{Z}$ thỏa mãn $a^2 = b + 1$. Dãy số (u_n) được xác định

$$\begin{cases} u_0 = 0 \\ u_{n+1} = au_n + \sqrt{bu_n{}^2 + c^2}, \forall n \in \mathbb{N} \end{cases}$$

Chứng minh rằng mọi số hạng của dãy đều là số nguyên.

Lời giải

Cách giải bài toán này cũng tương tự như cách tìm công thức truy hồi đúng của một dạng công thức truy hồi căn thức để tìm công thức tổng quát của một dạng dãy này nhưng với điều kiện ngặt. Ta có:

$$\begin{aligned} & u_{n+1} - au_n = \sqrt{bu_n{}^2 + c^2} \\ \Rightarrow & u_{n+1}{}^2 - 2au_nu_{n+1} + a^2u_n{}^2 = bu_n{}^2 + c^2 \\ \Rightarrow & u_{n+1}{}^2 = 2au_nu_{n+1} - u_n{}^2 + c^2 \quad (1) \end{aligned}$$

[1]Học sinh THPT chuyên Trần Đại Nghĩa.

Giảm n xuống 1 đơn vị ta có:

$$u_n{}^2 = 2au_nu_{n-1} - u_{n-1}{}^2 + c^2 \quad (2)$$

Lấy (1) − (2), ta có:

$$u_{n+1}{}^2 - u_{n-1}{}^2 = 2au_n\left(u_{n+1} - u_{n-1}\right) \Rightarrow \left[\begin{array}{l} u_{n+1} = u_{n-1} \\ u_{n+1} = 2au_n - u_{n-1} \end{array}\right.$$

*Với $u_{n+1} = u_{n-1}$, $\forall n \geqslant 1$ thì dãy (u_n) là dãy tuần hoàn theo chu kì 2. Như thế , ta suy ra

$$\left\{\begin{array}{l} u_0 = u_2 = u_4 = ... = u_{2k} = 0 \\ u_1 = u_3 = u_5 = ... = u_{2k+1} = |c| \end{array}\right.$$

Nên (u_n) có các số hạng đều là số nguyên.
*Với (u_n) thỏa

$$\left\{\begin{array}{l} u_0 = 1;\ u_1 = |c| \\ u_{n+1} = 2au_n - u_{n-1},\ \forall n \geqslant 1 \end{array}\right.,$$

Ta có các hệ số trong hệ thức truy hồi đều là số nguyên và 2 số hạng đầu tiên của dãy cũng là số nguyên nên từ đó ta suy ra (u_n) có các số hạng đều là số nguyên.
Tóm lại, các số hạng của dãy trên đều là số nguyên. □

Bài tập 4.2. Cho dãy (a_n) thỏa mãn điều kiện

$$\left\{\begin{array}{l} a_0 = 2;\ a_1 = 5 \\ a_{n+1}a_{n-1} - a_n{}^2 = 6^{n-1},\ \forall n \geqslant 1 \end{array}\right.$$

Chứng minh rằng tồn tại duy nhất dãy số nguyên dương thỏa mãn điều kiện trên.

Lời giải

Ý tưởng của bài toán này là tìm một công thức truy hồi đúng cho dãy trên. Như vậy, ta sẽ dùng phương pháp quen thuộc để đánh giá bài toán, đó là phương pháp sai phân.
Ta có

$$\left\{\begin{array}{l} a_{n+1}a_{n-1} - a_n{}^2 = 6^{n-1} \\ a_na_{n+2} - a_{n+1}{}^2 = 6^n \end{array}\right.$$

$$\Rightarrow a_n\left(a_{n+2} + 6a_n\right) = a_{n+1}\left(a_{n+1} + 6a_{n-1}\right)$$

$$\Rightarrow \frac{\left(a_{n+2} + 6a_n\right)}{a_{n+1}} = \frac{\left(a_{n+1} + 6a_{n-1}\right)}{a_n}$$

Đặt $v_n = \frac{(a_{n+1}+6a_{n-1})}{a_n}$, ta được

$$v_{n+1} = v_n = v_{n-1} = ... = v_1 = 5 \Rightarrow a_{n+1} = 5a_n - 6a_{n-1},\ \forall n = 1, 2, 3...$$

Do các số hạng đầu của dãy là số nguyên: $a_0 = 2$, $a_1 = 5$ và công thức truy hồi đúng của dãy đều có các hệ số là số nguyên nên từ đó ta suy ra dãy trên là dãy số nguyên.

Để có thêm điều kiện dãy trên có mọi số hạng là số nguyên dương, ta cần phải có thêm yếu tố đơn điệu tăng. Việc chứng minh đơn điệu không thể sử dụng công thức truy hồi mà ta vừa tìm được vì ta chưa chứng minh được công thức ấy là duy nhất. Chính vì thế mà ta sẽ chứng minh trực tiếp bằng quy nạp thông qua cách diễn đạt của đề bài.
Ta thấy điều trên đúng với $n = 1 : a_1 > a_0$ $(5 > 2)$.
Giả sử điều này đúng đến $n = k : a_k > a_{k-1}$.
Xét $n = k + 1$, ta có:

$$a_{k+1}a_{k-1} - {a_k}^2 = 6^{k-1} \Rightarrow a_{k+1} = \frac{6^{k-1} + {a_k}^2}{a_{k-1}} > \frac{6^{k-1}}{a_k} + a_k > a_k \ (a_k > a_{k-1})$$

Vậy điều trên cũng đúng với $n = k + 1$ nên theo nguyên lý quy nạp ta suy ra (a_n) là dãy đơn điệu tăng với mọi $n \in \mathbb{N}$.
Bây giờ ta sẽ chứng minh dãy trên là dãy duy nhất thỏa mãn điều kiện đề bài:
Cách thông thường mà chúng ta sẽ nghĩ đến là dùng phản chứng để chứng minh tồn tại duy nhất.
Giả sử tồn tại dãy ${a_n}'$ sao cho với $n \geqslant 2$ tồn tại ${a_{n+2}}' : a_{n+2} > {a_{n+2}}'$ thỏa:

$$\begin{cases} a_n a_{n+2} - {a_{n+1}}^2 = 6^n \\ a_n {a_{n+2}}' - {a_{n+1}}^2 = 6^n \end{cases}$$

Suy ra

$$a_n \left(a_{n+2} - {a_{n+2}}'\right) = 0 \text{ (vô lý do } a_{n+2} > {a_{n+2}}')$$

Như vậy ta suy ra dãy trên là dãy duy nhất thỏa mãn điều kiện đề bài. □
Những bài toán tương tự dạng trên có thể tồn tại ở nhiều dạng khác nhau. Đôi lúc những cách diễn đạt bằng truy hồi khiến ta mất đi phương hướng sai phân. Nhưng ta cần phải hiểu mục đích của việc chứng minh dãy số nguyên là tìm được công thức truy hồi đúng của nó.

Bài tập 4.3. (GER 2003, Ngày 2) Cho dãy số (a_n) được xác định bởi

$$\begin{cases} a_1 = 1;\ a_2 = 1;\ a_3 = 2 \\ a_{n+3} = \dfrac{a_{n+2}a_{n+1} + 7}{a_n}, \forall n \in \mathbb{N} \end{cases}$$

Chứng minh mọi số hạng của dãy trên đều là số nguyên dương.

Lời giải

Ta có:

$$a_{n+3}a_n = a_{n+1}a_{n+2} + 7$$

Do độ lệch các thứ tự của phần tử trong dãy không đều nhau nên sẽ khó cho ta nghĩ đến việc dùng sai phân vì nếu dùng sai phân sẽ xuất hiện thêm phần tử thứ 5. Tuy vậy, nhưng việc áp dụng sai phân trong dãy số nguyên là một công cụ khá mạnh và ta không nên bỏ qua nó chớp

nhoáng trong ý nghĩ.
Hạ n xuống 1 bậc, ta có:

$$a_{n+2}a_{n-1} = a_n a_{n+1} + 7$$

Trừ 2 biểu thức trên cho nhau, ta được

$$\begin{aligned} &a_{n+3}a_n - a_{n+2}a_{n-1} = a_{n+1}a_{n+2} - a_n a_{n+1} \\ \Rightarrow &a_n\left(a_{n+3} + a_{n+1}\right) = a_{n+2}\left(a_{n+1} + a_{n-1}\right) \\ \Rightarrow &\frac{a_{n+3} + a_{n+1}}{a_{n+2}} = \frac{a_{n+1} + a_{n-1}}{a_n} \end{aligned}$$

Đặt $v_n = \frac{a_{n+1}+a_{n-1}}{a_n}$, ta có $v_{n+2} = v_n$.
Vậy dãy (v_n) tuần hoàn theo chu kì 2.
Như vậy ta cần xét thêm tính chẵn lẻ của dãy, điều này dẫn đến đây là dãy gồm 2 công thức truy hồi song song nhau.
*Với n chẵn ta suy ra:

$$v_{2k+2} = v_{2k} = ... = v_2 = 3 \Rightarrow a_{n+1} = 3a_n - a_{n-1}$$

*Với n lẻ ta suy ra:

$$v_{2k+3} = v_{2k+1} = ... = v_3 = 5 \Rightarrow a_{n+1} = 5a_n - a_{n-1}$$

Từ đó ta xác định được công thức truy hồi của dãy là:

$$\begin{cases} a_1 = a_2 = 1,\ a_3 = 2 \\ a_{n+1} = 3a_n - a_{n-1},\ n = 2k \qquad (k \in \mathbb{N}) \\ a_{n+1} = 5a_n - a_{n-1},\ n = 2k+1 \end{cases}$$

Do các số hạng đầu của dãy đều là số nguyên và hệ số của hệ thức truy hồi của dãy cũng là số nguyên nên ta suy ra mọi số hạng của (a_n) đều là số nguyên.
Để dãy trên là dãy số nguyên dương, ta cần chứng minh dãy trên là dãy tăng ngặt với mọi $n \geqslant 2$.
Dễ thấy: $a_3 > a_2$ nên điều trên đúng với $n = 2$.
Giả sử điều trên đúng với $n = k :\ a_k > a_{k-1}$
Xét $n = k + 1$, ta có:

$$a_{k+1} = \frac{a_k a_{k-1} + 7}{a_{k-2}} > \frac{a_k a_{k-1} + 7}{a_{k-1}} > a_k + \frac{7}{a_{k-1}} > a_k$$

Vậy điều này cũng đúng với $n = k + 1$ nên theo nguyên lý quy nạp ta suy ra (a_n) là dãy tăng ngặt.
Từ đó, ta chứng minh được dãy (a_n) có mọi số hạng đều là số nguyên dương. □

Bài tập 4.4. (Croatia TST 2011) Với a, b là 2 số nguyên tố phân biệt, cho dãy (x_n) thỏa mãn

$$\begin{cases} x_1 = a,\ x_2 = b \\ x_{n+2} = \dfrac{{x_{n+1}}^2 + {x_n}^2}{x_{n+1} + x_n},\ \forall n \in \mathbb{N} \end{cases}$$

Chứng minh rằng x_n không là số nguyên với mọi $n \geqslant 3$.

Lời giải

Ta dễ dàng chứng minh được $x_n > 0$, $\forall x \in \mathbb{N}$ theo quy nạp.
Ta sẽ chứng minh một bổ đề của dãy này:
Bổ đề: Nếu kể từ một phần tử n_0 sao cho x_{n_0} không là số nguyên của dãy mà có dạng phân thức, thì sẽ không tồn tại n để $x_n \in \mathbb{N}$, $\forall n \geqslant n_0$.
Giả sử x_3 là một số hữu tỉ.
Ta có:

$$\begin{cases} x_3 = \frac{a^2+b^2}{a+b} = \frac{c}{d} \ (c, d \in \mathbb{N};\ (c,d) = 1) \\ \\ x_4 = \frac{\left(\frac{c}{d}\right)^2+b^2}{\frac{c}{d}+b} = \frac{c^2+b^2d^2}{d(c+bd)} \end{cases}$$

Do $(c,d) = 1$ nên $x_4 \notin \mathbb{N}$, đặt

$$x_4 = \frac{e}{f} \left(e, f \in \mathbb{N};\ (e,f) = 1;\ f \vdots d\right)$$

Ta có: $f \vdots d \Rightarrow f \geqslant d$. Ta chia làm 2 trường hợp:

⁕ Trường hợp 1: $f > d \Rightarrow 1 > \frac{d}{f}$, ta có:

$$x_5 = \frac{\left(\frac{c}{d}\right)^2 + \left(\frac{e}{f}\right)^2}{\frac{c}{d} + \frac{e}{f}} = \frac{(cf)^2 + (ed)^2}{(cf+de)\,df}$$

Giả sử $x_5 \in \mathbb{N}$, suy ra

$$(cf)^2 + (de)^2 \vdots df \Rightarrow (de)^2 \vdots df \Rightarrow de^2 \vdots f \text{ (vô lý)}$$

Mặt khác tử số cũng không thể bằng mẫu số do $f < (cf)^2 + (de)^2$ nên f không thể chia hết cho $(cf)^2 + (de)^2$.
Điều này vô lý do $(e,d) = 1$ và $d < f$.
Vậy x_5 là số vô tỉ.

⁕ Trường hợp 2: $f = d$, ta có:

$$x_5 = \frac{\left(\frac{c}{d}\right)^2 + \left(\frac{e}{f}\right)^2}{\frac{c}{d} + \frac{e}{f}} = \frac{(cf)^2 + (ed)^2}{(cf+de)\,df} = \frac{c^2+e^2}{f\,(c+e)}$$

Giả sử $x_5 \in \mathbb{N}$, suy ra

$$c^2 + e^2 \vdots c + e \Rightarrow 2ce \vdots c + e$$

Điều này hiển nhiên vô lý.
Vậy tóm lại, ta đã chứng minh rằng, nếu xuất phát với x_3 là một số hữu tỉ thì ta sẽ thu được một dãy số hữu tỉ và không tồn tại bất kì số nguyên nào trong dãy đó với $n \geqslant 3$.
Bây giờ ta chỉ việc chứng minh x_3 không thể là số nguyên. Do công thức truy hồi có dạng phân

thức nên x_3 sẽ có dạng phân số tối giản.
Giả sử $x_3 \in \mathbb{N}$, suy ra

$$a^2 + b^2 \vdots a + b \Rightarrow 2ab \vdots a + b$$

Xét một trong hai số là số nguyên tố chẵn. Giả sử đó là a, suy ra

$$a = 2 \Rightarrow 4b \vdots b + 2 \Rightarrow 4 \vdots b + 2 \text{ (vô lý do } b > 2)$$

Suy ra $4b = b + 2$ (vô lý do b là số nguyên tố lẻ nên tính chẵn lẻ của 2 vế không đồng nhất).
Kí hiệu $\{a, b\}$ là ước của a hoặc b.
Vậy $a + b \mid \{a, b, 2\}$ do $(a, b, 2) = 1$.
Ta có nhận xét rằng nếu $a + b \mid \{a, b, 2\}$ do:
* $a + b \mid \{a, b\}$ thì

$$\begin{cases} a \geqslant a + b \\ b \geqslant a + b \end{cases} \Rightarrow \begin{cases} 0 \geqslant b \\ 0 \geqslant a \end{cases} \text{ (sai do } a, b > 0)$$

* $a + b \mid \{2\}$: Do a, b là số nguyên tố nên $a + b > 2$. Suy ra

$$\Rightarrow a + b = 2ab \Rightarrow \begin{cases} a + b \vdots a \\ a + b \vdots b \end{cases} \Rightarrow \begin{cases} cb \vdots a \\ a \vdots b \end{cases} \Rightarrow a = b \text{ (sai do } a \neq b)$$

Như vậy, ta kết luận rằng điều giả sử là sai nên x_3 không thể là số nguyên.
Vậy theo bổ đề trên ta suy ra x_n không thể là số nguyên với mọi $n \geqslant 3$. □

Bài tập 4.5. Cho một dãy số nguyên dương sao cho ta có thể chọn 1998 phần tử bất kì của dãy tạo thành một hệ thăng dư không đầy đủ và riêng biệt nhau khi xét modulo 1999. Liệu có tồn tại cách chia 1998 phần tử này thành 2 tập con A, B sao cho tích của các phần tử trong mỗi tập con bằng nhau không?

Lời giải

Một suy luận đơn giản cho bài này: **2 tích bằng nhau thì chúng phải có cùng số dư khi xét modulo với một số nguyên dương.**
Sử dụng bổ đề quen thuộc: Nếu $x^2 + y^2 \vdots p$ (p nguyên tố) thì $p = 4k + 3$ hoặc $p = 4k + 1$. Khi $p = 4k + 3$ thì $x, y \vdots p$.
Gọi 1998 phần tử bất kì của dãy thỏa điều kiện đề bài là $x_1; x_2; x_3; ...; x_{1998}$.
Ta có: $A \cup B = \{x_1; x_2; ...; x_{1998}\}$.
Giả sử $\exists x_i \equiv 0 \pmod{1999}$. Do 1998 phần tử này lập thành một hệ thăng dư không đầy đủ và riêng biệt nhau nên

$$x_j \equiv r \neq 0 \pmod{1999} \, \forall j \neq i$$

Vì vậy nếu $x_i \in A$ thì A chia hết cho 1999 và B không chia hết cho 1999. Tương tự nếu $x_i \in B$.
Vậy không có phần tử nào trong dãy chia hết cho 1999. Vậy hệ thăng dư của dãy: $\{1; 2; 3...; 1998\}$.
Ta có:

$$\left(\prod_{x_k \in A} {x_k}^2 \right) = \prod_{x_i \in A} x_i . \prod_{x_j \in B} x_j \equiv 1.2.3...1998 \pmod{1999}$$

Suy ra

$$\left(\prod_{x_k\in A} x_k\right)^2 \equiv 1998! \,(\mathrm{mod}\, 1999)$$

Mặt khác theo định lý Wilson ta có: $1998! \equiv -1 \,(\mathrm{mod}\, 1999)$, do đó

$$\left(\prod_{x_k\in A} x_k\right)^2 + 1 \equiv 0 \,(\mathrm{mod}\, 1999)$$

Áp dụng bổ đề trên ta suy ra điều vô lý do 1999 là số nguyên tố dạng $4k+3$ nên 1 không thể chia hết cho 1999.
Vậy không thể chia 1998 phần tử bất kì của dãy nguyên dương này thành 2 tập con có tích các phần tử trong tập bằng nhau. □

Bài tập 4.6. Cho dãy số (u_n) thỏa

$$\begin{cases} u_1 = 1,\ u_2 = 2 \\ u_{n+1} = \dfrac{u_n u_{n-1}(n+1)}{P_{n-1}} \end{cases}$$

a) Tìm số nguyên tố pđể $S = \frac{u_{p-2}-1}{p^{p-1}}$ là số nguyên.
b) Chứng minh $\left[\frac{u_{n-1}}{n}\right] \equiv 0 \,(\mathrm{mod}\, n-1)$.

Lời giải

Ý tưởng của bài này đơn giản là tìm $p$là số nguyên tố để $u_{p-2} - 1 \equiv 0 \,(\mathrm{mod}\, p^{p-1})$. Qua đó, ta dự đoán công thức tổng quát của u_n để có thể đưa về một bài toán số học đơn thuần.

⁎ Câu a:
Ta chứng minh theo qui nạp $u_n = n!\ \forall n \in 1, 2, 3....$
Thật vậy điều này đúng với $n = 1; 2$: $\begin{cases} u_1 = 1 = 1! \\ u_2 = 2.u_1 = 2! \end{cases}$
Giả sử điều này đúng đến $n = k$tức $u_k = k!$ Xét u_{k+1}, ta có:

$$u_{k+1} = \frac{(k+1)u_k u_{k-1}}{P_{k-1}} = \frac{(k+1)!(k-1)!}{(k-1)!} = (k+1)!$$

Vậy điều này đúng đến $n = k+1$nên theo nguyên lý quy nạp ta suy ra $u_n = n! \forall n = 1; 2; ....$
Vậy $S = \frac{(p-2)!-1}{p^{p-1}}$.Giả sử S là số nguyên, ta suy ra $S.p^{p-1} + 1 = (p-2)!$.
Xét $p > 5$. ta có:

$$(p-2)! \equiv 0 \,(\mathrm{mod}\, p-1) \Rightarrow S.p^{p-1} + 1 \equiv 0 \,(\mathrm{mod}\, p-1) \Rightarrow S + 2 \equiv 0 \,(\mathrm{mod} p-1)$$

Mặt khác: $S + 2 < p - 1 \Leftrightarrow (p-2)! < 1 + p^{p-2}(p-3)$ (đúng).
Từ đó ta suy ra điều vô lý. Vậy $p \leqslant 5$. Dễ thấy $p = 3$ thỏa mãn điều kiện đề bài.

⁎ Câu b:
+Trường hợp 1: n là số nguyên tố.

Theo định lý Wilson ta có:

$$(n-1)! \equiv -1 \,(\mathrm{mod}\, n) \Rightarrow \frac{(n-1)!+1}{n} \in N*$$

Lại có

$$\left[\frac{u_{n-1}}{n}\right] = \left[\frac{(n-1)!}{n}\right] = \left[\frac{(n-1)!+1}{n} - \frac{1}{n}\right] = \frac{(n-1)!+1}{n} - 1 \ \ (\text{do } 0 < \frac{1}{n} < 1)$$

Suy ra

$$\left[\frac{u_{n-1}}{n}\right] = \frac{(n-1)! - (n-1)}{n} = \frac{(n-1)\left[(n-2)!-1\right]}{n}$$

Mặt khác, do $(n; n-1) = 1 \Rightarrow \frac{(n-2)!-1}{n} \in \mathbb{N}^*$ nên ta suy ra

$$\left[\frac{u_{n-1}}{n}\right] \equiv 0 \,(\mathrm{mod}\, n-1)$$

+ Trường hợp 2: n không là bình phương của 1 số nguyên tố $\Rightarrow n = rs$ với $1 < r < s \leqslant n-1$. Do $r < s \leqslant n-1$ nên ta suy ra $r < s \leqslant n-2$ nên r, slà ước số của một trong các số $\{1; 2; 3...; n-2\}$.
Vậy

$$\frac{(n-2)!}{n} = \frac{(n-2)!}{rs} \in N* \Rightarrow \left[\frac{u_{n-1}}{n}\right] = \frac{(n-1).(n-2)!}{n} = (n-1).k \equiv 0 \,(\mathrm{mod}\, n-1)$$

+Trường hợp 3: n là bình phương của 1 số nguyên tố. Đặt $n = p^2$ với $3 \leqslant p < n-1$ vì nếu $p = 2$ thì hiển nhiên ta có điều phải chứng minh.
Lập luận tương tự như trường hợp 2, p là ước của một trong các số $\{1; 2; 3...; n-2\}$. Bây giờ ta xét xem liệu p còn là ước của số nào nữa không.
Thật vậy, ta có: $n - 1 = p^2 - 1 = (p-1)(p+1) > 2p > p$.
Vậy $2p$ còn là ước của một số bất kì trong các số $\{1; 2; 3...; n-2\}$. Chính vì thế mà

$$(n-1)! \equiv 0 \,(\mathrm{mod}\, 2p.p.(n-1)) \Rightarrow (n-1)! \equiv 0 \,(\mathrm{mod}\, 2n(n-1))$$
$$\Rightarrow \frac{(n-1)!}{n} \equiv 0 \,(\mathrm{mod}\, n-1) \Rightarrow \left[\frac{u_{n-1}}{n}\right] \equiv 0 \,(\mathrm{mod}\, n-1)$$

Từ các điều trên ta có đpcm. □

Bài tập 4.7. Cho dãy số xác định bởi:

$$a_{n+1} = \{a_n\}\,[a_n]\,,\ n \geqslant 0$$

Chứng minh rằng $a_n = a_{n+2}$ khi n đủ lớn.

Lời giải

⁕ Xét $0 < a_0 < 1$, ta có

$$[a_0] = 0 \Rightarrow a_n = [a_n]\{a_n\} = 0,\ \forall n = 1, 2, 3...$$

⁕ Xét $a_0 > 1$, ta có:

$$a_{n+1} = \{a_n\}[a_n] < [a_n] < a_n \Rightarrow 0 < [a_{n+1}] < [a_n] < ... < [a_1] \Rightarrow [a_{n_0}] = c_1 \text{ khi } n_0 \text{ đủ lớn}$$

⁕ Xét $a_0 < 0 \Rightarrow a_n < 0,\ \forall n = 1, 2, 3...$ ta có:

$$a_{n+1} = \{a_n\}[a_n] > a_n \Rightarrow 0 > [a_{n+1}] > [a_n] > ... > [a_1] \Rightarrow [a_{n_0}] = c_2 \text{ khi } n_0 \text{ đủ lớn}$$

Như vậy $[a_{n_0}] = k$ với n_0 đủ lớn.
Ta có:

$$a_{n+1} = \{a_n\}[a_n] = a_n[a_n] - ([a_n])^2 = ka_n - k^2,\ \forall n \geqslant n_0$$

Sử dụng phương pháp sai phân với từng hạng tử của dãy với hệ số tương ứng ta có:

$$\begin{cases} k^{n-1}a_{n+1} = k^n a_n - k^{n+1} \\ k^n a_{n+2} = k^{n-1}a_{n+1} - k^n \\ ... \\ ka_{i+n-1} = k^2 a_{i+n-2} - k^3 \\ a_{i+n} = ka_{i+n-1} - k^2 \end{cases} \Rightarrow a_{i+n} = k^n a_n - \frac{k^2(1-k^n)}{1-k} = k^n\left(a_n + \frac{k^2}{1-k}\right) - \frac{k^2}{1-k}$$

Nếu $|k| > 1$ thì

$$a_{n+i} = k^n\left(a_n + \frac{k^2}{1-k}\right) - \frac{k^2}{1-k} \to \infty \text{ (vô lý do dãy trên bị chặn)}$$

Suy ra $-1 \leqslant k \leqslant 1 \Rightarrow k \in \{-1; 0; 1\}$.
* Nếu $k = 0:\ a_n = 0,\ \forall n > n_0$
* Nếu $k = 1:\ a_{n+1} = a_n - 1,\ \forall n \geqslant n_0$ (vô lý do $[a_{n_0}] = k\ \forall n \geqslant n_0$ mà khoảng cách giữa 2 hạng tử liên tiếp của dãy là 1).
* Nếu $k = -1$ suy ra

$$a_{n+1} = 1 - a_n,\ \forall n \geqslant n_0 \Rightarrow \begin{cases} a_{n+1} = 1 - a_n \\ a_{n+2} = 1 - a_{n+1} \end{cases}$$

Trừ nhau ta có $a_n = a_{n+2},\ \forall n \geqslant n_0$ (đpcm). □

Dãy số nguyên và tính chính phương

Bài tập 4.8.
a) Chứng minh $\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n$ là số nguyên.
b) Chứng minh mọi số hạng lẻ của dãy $\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n - 2$ đều là số chính phương.

Lời giải

⁕ Câu a:

Xét dãy số sau:

$$\begin{cases} x_1 = 3;\ x_2 = 7 \\ x_{n+2} = 3x_{n+1} - x_n \forall n = 1; 2; .... \end{cases}$$

Ta chứng minh theo quy nạp

$$x_n = \left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n \forall n = 1; 2; ...$$

Thật vậy điều này đúng với $n = 1; 2$: $\begin{cases} x_1 = \left(\frac{3+\sqrt{5}}{2}\right) + \left(\frac{3-\sqrt{5}}{2}\right) = 3 \\ x_2 = \left(\frac{3+\sqrt{5}}{2}\right)^2 + \left(\frac{3-\sqrt{5}}{2}\right)^2 = 7 \end{cases}$

Giả sử điều này đúng đến $n = k$tức $x_k = \left(\frac{3+\sqrt{5}}{2}\right)^k + \left(\frac{3-\sqrt{5}}{2}\right)^k$.

Xét x_{k+1}, ta có:

$$x_{k+1} = 3x_k - x_{k-1} = 3\left[\left(\frac{3+\sqrt{5}}{2}\right)^k + \left(\frac{3-\sqrt{5}}{2}\right)^k\right] - \left[\left(\frac{3+\sqrt{5}}{2}\right)^{k-1} + \left(\frac{3-\sqrt{5}}{2}\right)^{k-1}\right]$$

$$\Leftrightarrow x_{k+1} = \left(\frac{3+\sqrt{5}}{2}\right)^{k-1}\left(\frac{7+3\sqrt{5}}{2}\right) + \left(\frac{3-\sqrt{5}}{2}\right)^{k-1}\left(\frac{7-3\sqrt{5}}{2}\right) = \left(\frac{3+\sqrt{5}}{2}\right)^{k+1} + \left(\frac{3-\sqrt{5}}{2}\right)^{k+1}$$

Vậy điều này đúng đến $n = k+1$ nên theo nguyên lý quy nạp ta suy ra

$$x_n = \left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n \forall n = 1; 2; ...$$

Do $x_n = \left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n \forall n = 1; 2; ...$ có công thức truy hồi với các hệ số nguyên và $x_1; x_2$ nguyên nên từ đó ta suy ra x_n nguyên. Vậy $\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n$ nguyên $\forall n = 1; 2; ....$

⁕ Câu b:

Tiếp tục với ý tưởng biện luận dãy nguyên theo công thức truy hồi và một chút biến đổi khéo léo để chứng minh số chính phương.

Ta có:

$$\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n - 2$$

$$= \left[\left(\frac{\sqrt{5}+1}{2}\right)^{2n} + \left(\frac{\sqrt{5}-1}{2}\right)^{2n} - 2\right]$$

$$= \left[\left(\frac{\sqrt{5}+1}{2}\right)^n - \left(\frac{\sqrt{5}-1}{2}\right)^n\right]^2$$

Vậy bài toán trở thành bài toán thứ nhất và ta chỉ việc chứng minh $x_n = \left(\frac{\sqrt{5}+1}{2}\right)^n - \left(\frac{\sqrt{5}-1}{2}\right)^n$ nguyên với mọi n lẻ.

Chứng minh theo quy nạp $x_n = \left(\frac{\sqrt{5}+1}{2}\right)^n - \left(\frac{\sqrt{5}-1}{2}\right)^n$ có công thức truy hồi là

$$\begin{cases} x_1 = 1;\ x_2 = \sqrt{5} \\ x_{n+2} = -\sqrt{5}x_{n+1} + 2x_n \ \forall n = 1; 2; ... \end{cases} \text{ và } x_{2n} = \alpha\sqrt{5}; x_{2n+1} = \gamma$$

Thật vậy điều này đúng với $n = 1; 2 :$ $\begin{cases} x_1 = \left(\frac{\sqrt{5}+1}{2}\right) - \left(\frac{\sqrt{5}-1}{2}\right) = 1 \\ x_2 = \left(\frac{\sqrt{5}+1}{2}\right)^2 - \left(\frac{\sqrt{5}-1}{2}\right)^2 = \frac{4\sqrt{5}}{4} = \sqrt{5} \end{cases}$

Giả sử điều này đúng đến $n = 2k$ tức $x_{2k+2} = \sqrt{5}x_{2k+1} - x_{2k}$và x_{2k+1} nguyên do $x_1; x_3; ...$ nguyên và $x_{2k} = \alpha\sqrt{5}$.

Vậy $x_{2k+2} = \beta\sqrt{5}\,(\beta = x_{2k+1} - \alpha)$

Xét $x_{2k+3}; x_{2k+4}$. Ta có:

$$\begin{aligned} & x_{2k+3} = \sqrt{5}x_{2k+2} - x_{2k+1} \\ =& \sqrt{5}\left[\left(\frac{\sqrt{5}+1}{2}\right)^{2k+2} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+2}\right] - \left[\left(\frac{\sqrt{5}+1}{2}\right)^{2k+1} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+1}\right] \\ \Rightarrow & x_{2k+3} = \left(\frac{\sqrt{5}+1}{2}\right)^{2k+1}\left(\frac{5+\sqrt{5}}{2} - 1\right) - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+1}\left(\frac{5-\sqrt{5}}{2} - 1\right) \\ \Rightarrow & x_{2k+3} = \left(\frac{\sqrt{5}+1}{2}\right)^{2k+1}\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+1}\left(\frac{3-\sqrt{5}}{2}\right) \\ =& \left(\frac{\sqrt{5}+1}{2}\right)^{2k+3} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+3} \quad (1) \end{aligned}$$

Và

$$\begin{aligned} & x_{2k+4} = \sqrt{5}x_{2k+3} - x_{2k+2} \\ =& \sqrt{5}\left[\left(\frac{\sqrt{5}+1}{2}\right)^{2k+3} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+3}\right] - \left[\left(\frac{\sqrt{5}+1}{2}\right)^{2k+2} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+2}\right] \\ \Rightarrow & x_{2k+4} = \left(\frac{\sqrt{5}+1}{2}\right)^{2k+2}\left(\frac{3+\sqrt{5}}{2}\right) - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+2}\left(\frac{3-\sqrt{5}}{2}\right) \\ =& \left(\frac{\sqrt{5}+1}{2}\right)^{2k+4} - \left(\frac{\sqrt{5}-1}{2}\right)^{2k+4} \quad (2) \end{aligned}$$

Lại có $x_{2k+3} = \sqrt{5}x_{2k+2} - x_{2k+1} = 5\beta - x_{2k+1}$ là số nguyên (3).

và $x_{2k+4} = \sqrt{5}x_{2k+3} - x_{2k+2} = \sqrt{5}(\lambda - \beta)$ không là số nguyên (4).

Từ (1);(2);(3);(4) ta suy ra những điều trên đúng với $n = k+1$ nên theo nguyên lý quy nạp ta chứng minh được

$$\begin{cases} x_1 = 1;\ x_2 = \sqrt{5} \\ x_{n+2} = -\sqrt{5}x_{n+1} + 2x_n\ \forall n = 1;2;... \end{cases} \text{ và } x_{2n} = \alpha\sqrt{5}; x_{2n+1} = \gamma$$

Do $x_{2n+1} = \gamma$ nên ta suy ra mọi số hạng lẻ của dãy trên đều là số chính phương. □
Dựa vào bài trên ta có thể xét thêm một bài thú vị sau:

Bài tập 4.9. Cho dãy số (x_n) thỏa mãn:

$$\begin{cases} x_0 = 1; x_1 = 3 \\ x_{n+2} = 6x_{n+1} - x_n \end{cases}$$

Chứng minh rằng với mọi $n \geqslant 1$ thì (x_n) không là số chính phương.

Lời giải

Tương tự ý tưởng của bài 2, ta sẽ biến đổi khéo léo để đưa về y như dạng của bài 2. Nhưng ở điều đặc biệt ở đây chính là ta cần 2 dãy chứng minh song song cùng nhau bằng quy nạp để củng cố cho lời giải của bài toán thêm chặt chẽ. (Lưu ý: Lời giải chỉ để bổ sung và cho ta thấy một ứng dụng khá mạnh của bài 2).
Dễ dàng chứng minh theo quy nạp:

$$x_n = \frac{\left(3+2\sqrt{2}\right)^n + \left(3-2\sqrt{2}\right)^n}{2}$$

Ta biến đổi x_n theo 2 hình thức sau:

$$\begin{cases} x_n = \dfrac{\left(\sqrt{2}+1\right)^{2n} + \left(\sqrt{2}-1\right)^{2n}}{2} = \dfrac{\left[\left(\sqrt{2}+1\right)^n + \left(\sqrt{2}-1\right)^n\right]^2}{2} - 1 \\ x_n = \dfrac{\left(\sqrt{2}+1\right)^{2n} + \left(\sqrt{2}-1\right)^{2n}}{2} = \dfrac{\left[\left(\sqrt{2}+1\right)^n - \left(\sqrt{2}-1\right)^n\right]^2}{2} + 1 \end{cases}$$

Và ta có thể dung phương pháp truy hồi để tìm công thức truy hồi của $\left(\sqrt{2}+1\right)^n \pm \left(\sqrt{2}-1\right)^n$ lần lượt có công thức truy hồi là:

$$\begin{cases} v_0 = 2; v_1 = 2\sqrt{2} \\ v_{n+2} = 2\sqrt{2}v_{n+1} - v_n \end{cases} \text{ và } \begin{cases} z_1 = 2; z_2 = 4\sqrt{2} \\ z_{n+2} = 2\sqrt{2}z_{n+1} - z_n \end{cases}$$

Theo như bài trên ta có thể chứng minh chúng lần lượt có tính chất

$$\begin{cases} v_{2n} = a \\ v_{2n+1} = b\sqrt{2} \end{cases} (a; b \in \mathbb{Z}) \text{ và } \begin{cases} z_{2n} = c\sqrt{2} \\ z_{2n+1} = d \end{cases} (c; d \in \mathbb{Z})$$

Từ đó ta rút ra được $x_n$có dạng $A^2 + 1$ hoặc $B^2 - 1$ nên rõ ràng x_n không thể là số chính phương với mọi $n \geqslant 1$. □

Một vấn đề thú vị rằng tại sao ta lại phải cần đến 2 dãy song song để chứng minh. Chính 2 dãy song song này đã tạo nên sự thú vị của bài toán, khiến nó trở nên chặt chẽ hơn trong lời giải. Vì khi xét n chẵn và lẻ ta có thể diễn đạt x_n theo 2 hình thức và do 2 hình thức trên đều có dạng $\frac{2x^2}{2} \pm 1$ nên hiển nhiên nó không thể là số chính phương với mọi $n \geqslant 1$.

Một lời giải khác chung ý tưởng nhưng lời giải ngắn gọn hơn:

Xét dãy số nguyên

$$\begin{cases} u_0 = 0;\ u_1 = 2 \\ u_{n+2} = 2u_{n+1} + u_n \end{cases}$$

Ta dễ dàng chứng minh theo quy nạp

$$u_n = \frac{\left(\sqrt{2}+1\right)^n - \left(1-\sqrt{2}\right)^n}{\sqrt{2}}$$

Mặt khác, dãy $\begin{cases} x_0 = 1; x_1 = 3 \\ x_{n+2} = 6x_{n+1} - x_n \end{cases}$ có công thức tổng quát là

$$x_n = \frac{\left(3+2\sqrt{2}\right)^n + \left(3-2\sqrt{2}\right)^n}{2} = \frac{\left(\sqrt{2}+1\right)^{2n} + \left(\sqrt{2}-1\right)^{2n}}{2}$$

Vậy $x_n + (-1)^{n+1} = {u_n}^2$. Từ đó ta kết luận rằng $x_n$không thể là số chính phương với mọi $n \geqslant 1$. $\square$

Bài tập 4.10. (CIS 1992)

Cho dãy số a_n xác định bởi

$$\begin{cases} a_1 = 1 \\ a_{n+1} = {a_1}^2 + {a_2}^2 + {a_3}^2 + ... + {a_n}^2 + n \ \forall n \geqslant 1 \end{cases}$$

Chứng minh rằng a_n không là số chính phương với mọi $n \geqslant 2$.

Lời giải

Với những bài toán có công thức truy hồi phức tạp như trên, việc đầu tiên ta cần nghĩ đến là sử dụng sai phân để đưa về một biểu thức ngắn gọn và đơn giản hơn để biện luận. Qua đó, ta vận dụng các tính chất của số chính phương để chứng minh. Cụ thể số chính phương chỉ có tận cùng là 0, 1, 4, 5, 6, 9.

Ta có: $a_2 = 2$

Với mọi $n \geqslant 2$; ta có:

$$\begin{cases} a_{n+1} = \sum\limits_{k=1}^{n} {a_k}^2 + n \\ a_n = \sum\limits_{k=1}^{n-1} {a_k}^2 + n - 1 \end{cases} \Rightarrow a_{n+1} - a_n = {a_n}^2 + 1 > 0$$

Ta suy ra dãy này là một dãy tăng ngặt.
Bây giờ ta có một dãy mới

$$\begin{cases} a_2 = 2 \\ a_{n+1} = {a_n}^2 + a_n + 1 \, \forall n \geqslant 2 \end{cases}$$

Vận dụng tính chất trên, ta sẽ chứng minh a_n không thể là số chính phương theo phương pháp quy nạp đơn thuần, vì nếu a_n là số chính phương thì nó phải có tận cùng là 1 trong các số 0, 1, 4, 5, 6, 9
Ta thấy rõ số hạng trong dãy có tận cùng là 7 xuất phát từ $n = 3$: $a_3 = 7; a_4 = 57$
Giả sử điều này đúng đến $n = k$; tức $a_k$có tận cùng là 7.
Xét $n = k + 1$, ta có: $a_{k+1} = {a_k}^2 + a_k + 1$
Do ta chỉ xét chữ số tận cùng của a_{k+1} nên ta sẽ xét chữ số tận cùng của từng số hạng trong biểu thức trên.
Ta có a_k có tận cùng là 7nên ${a_k}^2$có tận cùng là 9. Như vậy chữ số tận cùng của

$$a_{k+1} = \overline{.b_1 b_2 ... 9} + \overline{c_1 c_2 ... 7} + 1 = \overline{d_1 d_2 ... 7} \ \left(\overline{9} + \overline{7} + 1 = \overline{6} + 1 = \overline{7}\right)$$

Điều này cũng đúng với $n = k+1$, theo nguyên lý quy nạp ta suy ra a_n có tận cùng là$7 \, \forall n \geqslant 3$.
Áp dụng tính chất trên ta suy ra a_n không thể là số chính phương với mọi $n \geqslant 3$.
Mặt khác $a_2 = 2$ không là số chính phương.
Vậy ta suy ra a_n không là số chính phương với mọi $n \geqslant 2$. □

Bài tập 4.11. (Balkan 2002)
Cho dãy số a_n thỏa mãn

$$\begin{cases} a_1 = 20; \ a_2 = 30 \\ a_{n+2} = 3a_{n+1} - a_n \, \forall n \geqslant 1 \end{cases}$$

Tìm n để $A = 5a_{n+1}a_n + 1$ là số chính phương.

Lời giải

Tương tự, ta đi tìm công thức tổng quát của dãy số và biện luận. Đối với những bài tìm giá trị n để một biểu thức nào đó là số chính phương trong dãy số. Ta cần lưu ý đến những tính chất của dãy chính cũng như dãy con (nếu có) như đơn điệu, đồng dư...
Dễ dàng chứng minh theo quy nạp công thức tổng quát của a_n là

$$a_n = 10\left[\left(\frac{3+\sqrt{5}}{2}\right)^{n-1} + \left(\frac{3-\sqrt{5}}{2}\right)^{n-1}\right]$$

Suy ra

$$\begin{aligned}
&A = 5a_{n+1}a_n + 1\\
\Rightarrow &A = 5.10^2.\left[\left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n\right].\left[\left(\frac{3+\sqrt{5}}{2}\right)^{n-1} + \left(\frac{3-\sqrt{5}}{2}\right)^{n-1}\right] + 1\\
\Rightarrow &A = 500\left[\left(\frac{3+\sqrt{5}}{2}\right)^{2n-1} + \left(\frac{3-\sqrt{5}}{2}\right)^{2n-1} + 3\right] + 1\\
\Rightarrow &A = 500\left[\left(\frac{\sqrt{5}+1}{2}\right)^{4n-2} + \left(\frac{\sqrt{5}-1}{2}\right)^{4n-2} + 3\right] + 1\\
\Rightarrow &A = 500\left[\left(\frac{\sqrt{5}+1}{2}\right)^{2n-1} + \left(\frac{\sqrt{5}-1}{2}\right)^{2n-1}\right]^2 + 501
\end{aligned}$$

Xét dãy phụ sau:

$$\begin{cases} x_1 = \sqrt{5};\ x_2 = 6\\ x_{n+2} = \sqrt{5}x_{n+1} - x_n\ \forall n \geqslant 1 \end{cases}$$

Dãy trên có công thức tổng quát là

$$x_n = \left(\frac{\sqrt{5}+1}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2}\right)^n \forall n \in \mathbb{N}$$

Ta có:

$$\begin{aligned}
x_n - x_{n-1} &= \left(\frac{\sqrt{5}+1}{2}\right)^n + \left(\frac{\sqrt{5}-1}{2}\right)^n - \left(\frac{\sqrt{5}+1}{2}\right)^{n-1} - \left(\frac{\sqrt{5}-1}{2}\right)^{n-1}\\
&= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} + \left(\frac{\sqrt{5}-1}{2}\right)^{n-2} > 0
\end{aligned}$$

Suy ra $x_n > x_{n-1}\ \forall n \in \mathbb{N}$. Vậy x_n là dãy tăng ngặt.
Tương tự bài 2, dãy trên có một tính chất có thể chứng minh được bằng quy nạp theo 2 dãy song song là:

$$\begin{cases} x_{2n} = c\\ x_{2n-1} = d\sqrt{5} \end{cases} \quad (c; d \in \mathbb{N})$$

Chính vì thế mà ta suy ra: $A = 500\left(d\sqrt{5}\right)^2 + 501$.
Giả sử $\exists\, n_0 \in \mathbb{N} : A = 5a_{n_0+1}a_{n_0} + 1$ là số chính phương, ta có:

$$(50d)^2 + 501 = k^2\ (k \in \mathbb{N}) \Rightarrow 501 = (k - 50d)(k + 50d)$$

Mặt khác ta phân tích được $501 = 3.167$, mà

$$\begin{cases} k + 50d + k - 50d = 2k\\ k + 50d > k - 50d \end{cases}$$

nên ta suy ra

$$\begin{cases} k + 50d = 501 \\ k - 50d = 1 \end{cases} \Rightarrow d = 5$$

Vậy $\exists\, n_0 \in \mathbb{N} :\ x_{n_0} = 5\sqrt{5}$. Ta tính toán được $x_3 = 5\sqrt{5}$ và x_n là dãy tăng ngặt nên ta suy ra $n = 3$.
Vậy với $n = 3$ thì $A = 5a_{n+1}a_n + 1$ là số chính phương. $\square$

Bài tập 4.12. Cho dãy số t_n thỏa mãn:

$$\begin{cases} t_1 = 9; t_2 = 25;\ t_3 = 81 \\ t_{n+3} = 7t_{n+2} - 14t_{n+1} + 8t_n\ \forall n \geqslant 1 \end{cases}$$

a) Chứng minh rằng: $v_n = t_{n+1} - 2^{n+1}\sqrt{t_{n+1}} + 2^{2n}\ \forall n \geqslant 1$ là số chính phương.
b) Chứng minh rằng nếu $T = 2 + 2\sqrt{12t_n + 1} \in \mathbb{N}$ thì nó là số chính phương.
c) Giả sử tồn tại dãy số x_n sao cho $x_n.t_n$ có lẻ số ước. Chứng minh dãy x_n gồm toàn số chính phương.

Lời giải

⁎ Câu a:
Ta thấy biểu thức cần chứng minh có dạng căn thức. Điều này gợi cho ta việc chứng minh t_n là một dãy số chính phương.
Bằng việc thử lần lượt các số hạng đầu tiên của dãy, ta rút ra nhận xét rằng dãy t_n gồm toàn số chính phương. Bây giờ việc ta cần làm là chứng minh dãy t_n gồm toàn số chính phương.
Thông thường những bài toán chứng minh dãy là số chính phương hoặc không là số chính phương ta thường phải tìm ra công thức tổng quát của dãy để đưa về bài toán số học thông thường. Nhưng trong dãy số ta có thể chủ động biến đổi linh hoạt giữa chúng để tạo nên lời giải hợp lý. Điển hình với bài toán này ta thấy việc chứng minh $t_n = 2^{2^n} + 2^{n+1} + 1$ gồm toàn số chính phương rõ ràng là một công việc không khả thi.
Song ta có thể dựa vào phương pháp của dãy số và chứng minh thẳng để dự đoán và chứng minh t_n là bình phương của một đẳng thức nào đó.
Nhờ phương pháp sai phân ta có đánh giá như sau:

$$\begin{array}{ccccccccc} 3 & & 5 & & 9 & & 17 & & 33 \\ & 2^1 & & 2^2 & & 2^3 & & 2^4 & \end{array}$$

Hay

$$\begin{array}{ccccccccc} \sqrt{t_1} & & \sqrt{t_2} & & \sqrt{t_3} & & \sqrt{t_4} & & \sqrt{t_5} \\ & 2^1 & & 2^2 & & 2^3 & & 2^4 & \end{array}$$

Do đó, ta sẽ chứng minh theo quy nạp $t_{n+1} = \left(2^n + \sqrt{t_n}\right)^2$.
Do $t_1 = 9 = 3^2$ nên điều trên đúng với $n = 2 :\ t_2 = (2 + 3)^2 = 25$.

Giả sử điều này đúng với $n = k$; tức $t_k = \left(2^{k-1} + \sqrt{t_{k-1}}\right)^2$.
Ta xét $n = k + 1$; ta có:

$$t_{k+1} = 7t_k - 14t_{k-1} + 8t_{k-2} = 7t_k - 14t_{k-1} + 8\left(\sqrt{t_{k-1}} - 2^{k-2}\right)^2$$
$$\Rightarrow t_{k+1} = 7t_k - 6t_{k-1} - 8.2^{k-1}\sqrt{t_{k-1}} + 8.2^{2(k-2)} = 7t_k - 6\left(\sqrt{t_k} - 2^{k-1}\right)^2 - 8.2^{k-1}\left(\sqrt{t_k} - 2^{k-1}\right) + 8.2^{2(k-2)}$$
$$\Rightarrow t_{k+1} = t_k + 2.2^k\sqrt{t_k} + 2^{2k} = \left(\sqrt{t_k} + 2^k\right)^2$$

Vậy theo nguyên lý quy nạp ta suy ra

$$t_{n+1} = \left(2^n + \sqrt{t_n}\right)^2 \forall n \in \mathbb{N}$$

Mặt khác do $t_1 = 9$ là số chính phương nên từ đó ta suy ra mọi số hạng của dãy đều là số chính phương.
Vậy $v_n = t_{n+1} - 2^{n+1}\sqrt{t_{n+1}} + 2^{2n} = (\sqrt{t_{n+1}} - 2^n)^2$ là số chính phương.

⁎ Câu b:
Việc chứng minh số chính phương đã giúp ta đưa bài toán về một dạng quen thuộc hơn:
"Nếu $A = 2 + 2\sqrt{12a^2 + 1} \in \mathbb{N}$ thì nó là số chính phương".
Thật vậy, giả sử $A \in \mathbb{N} \Rightarrow \sqrt{12t_n + 1} = k\,(k \in \mathbb{N}) \Rightarrow 12t_n = (k-1)(k+1)$
Do k lẻ nên ta suy ra $k = 2l + 1\ \ (l \in \mathbb{N})$. Từ đó ta suy ra: $3t_n = l(l+1)$.
Do $(l; l+1) = 1$ và t_n là số chính phương nên ta suy ra

$$\begin{cases} l = 3a^2 \\ l + 1 = b^2 \end{cases} \text{ hoặc } \begin{cases} l = b^2 \\ l + 1 = 3a^2 \end{cases} (a; b \in \mathbb{N})$$

* Trường hợp 1: $\begin{cases} l = b^2 \\ l + 1 = 3a^2 \end{cases} \Rightarrow 3a^2 = 1 + b^2$

Mặt khác $3 = 4.0 + 3$ nên từ đó ta suy ra $b^2 + 1$ có ước dạng $4k + 3$ nên ta suy ra $1 \vdots 3$ (vô lý).
Vậy trường hợp này không thể xảy ra.

* Trường hợp 2: $\begin{cases} l = 3a^2 \\ l + 1 = b^2 \end{cases}$.
Ta có:

$$A = 2 + 2\sqrt{12t_n + 1} = 2 + 2k = 2\,(k+1) = 4(t+1) = 4b^2$$

Từ đó ta suy ra A là số chính phương.
Vậy nếu $A = 2 + 2\sqrt{12n^2 + 1} \in \mathbb{N}$ thì nó là số chính phương.

⁎ Câu c:
Một tính chất cơ bản của số chính phương: Nếu a là một số chính phương bất kì thì nó luôn có lẻ số ước và ngược lại. (tính chất được chứng minh nhờ việc sử dụng phép đếm).
Chứng minh: Giả sử a là số chính phương, ta viết dạng tổng quát của a là

$$a = {p_1}^{2\alpha_1}{p_2}^{2\alpha_2}{p_3}^{2\alpha_3}...{p_n}^{2\alpha_n}$$

Số ước của a chính là số tích số của các số nguyên tố với các lần thay đổi khác nhau của các số mũ α_i , $\forall\, i = \overline{1;n}$. Chính vì thế mà theo quy tắc nhân ta đếm được a có

$$(2\alpha_1 + 1)(2\alpha_2 + 1)(2\alpha_3 + 1)...(2\alpha_n + 1)$$

số ước và hiển nhiên tổng số ước trên là một số lẻ.
Ngược lại giả sử số a có lẻ số ước, ta có dạng tổng quát của a là

$$a = {p_1}^{r_1}{p_2}^{r_2}{p_3}^{r_3}...{p_n}^{r_n}$$

Theo quy tắc nhân ta đếm được $a$có

$$(r_1 + 1)(r_2 + 1)(r_3 + 1)...(r_n + 1)$$

Do a có lẻ số ước nên $r_i + 1,\ \forall i = \overline{1;n}$ đều phải là số lẻ, suy ra

$$r_i = 2k\ (k \in \mathbb{N})\,,\ \forall i = \overline{1;n}$$

Vậy a chính là số chính phương.
Tính chất đã được chứng minh hoàn tất. Quay lại bài toán trên và sử dụng tính chất này để tìm ra lời giải thích hợp cho bài toán.
Ta có: $x_n.t_n$ có lẻ số ước. Áp dụng tính chất trên ta suy ra $x_n.t_n$ là số chính phương. Mặt khác t_n là dãy các số chính phương $\Rightarrow x_n$ là dãy các số chính phương.

Bài tập 4.13. Cho dãy (u_n) thỏa mãn

$$\begin{cases} u_0 = 2;\ u_1 = 5 \\ u_{n+1} = 5u_n - 6u_{n-1},\ \forall n \geqslant 1 \end{cases}$$

Xét hàm số

$$f(x) = \frac{x^3}{3} - \frac{5x^2u_n}{2} + \left(6{u_n}^2 + 6^n\right)x + C\ (C \in \mathbb{R})$$

có đạo hàm tại $x_0 \in (a;b)$ với $a;b \in \mathbb{N}$.
Chứng minh rằng $f(x)$ có điểm cực đại và cực tiểu có hoành độ luôn là số nguyên.

Lời giải

Đầu tiên, ta có nhận xét sau: 2 điểm cực trị của hàm số trên thuộc phương trình

$$f'(x) = x^2 - 5xu_n + 6{u_n}^2 + 6^n = 0$$

Như thế điều kiện đầu tiên để nghiệm của phương trình trên là số nguyên thì $\Delta = {u_n}^2 - 4.6^n$ phải là số chính phương với mọi $n \geqslant 1$. Như vậy ta đưa bài toán về việc chứng minh $v_n = {u_n}^2 - 4.6^n$ là số chính phương với mọi $n \geqslant 1$.
Trong bài toán này, ta sẽ chứng minh bài này bằng phương pháp dùng tam thức bậc hai để giải quyết bài toán nhanh gọn hơn (nghĩa là ta sẽ đưa bài toán về dạng $X^2 + \alpha X u_n + \beta + 6^n = 0$ do số 6^n xuất hiện một cách không tự nhiên và mất cả số hạng u_n bậc nhất trong bài toán).

Như vậy dãy số sẽ có dạng ${u_{n+1}}^2 + \alpha u_n u_{n+2} + 6^n + \beta = 0$ (do ở dạng này ta có thể tách u_{n+2} theo công thức truy hồi và đưa phương trình trên về dạng đã nêu trên). Ngoài ra ta vẫn có thể chứng minh biểu thức trên thông thường theo quy nạp của một biểu thức đoán được.
Như đã diễn đạt ở trên, ta có:

$$ {u_{n+1}}^2 - 5\alpha u_{n+1} u_n + 6\alpha {u_n}^2 + 6^n + \beta = 0 $$

Xem biểu thức trên như phương trình bậc 2 theo tham số u_n ẩn u_{n+1}, ta được

$$ \Delta = 25\alpha^2 {u_n}^2 - 24\alpha {u_n}^2 - 4.6^n - 4\beta = \alpha^2 {u_n}^2 - 4.6^n - 4\beta $$

Đồng nhất hệ số với biểu thức cần chứng minh ta được $\alpha = 1$; $\beta = 0$.
Như vậy ta sẽ chứng minh theo quy nạp

$$ u_n u_{n+2} - {u_{n+1}}^2 = 6^n \, , \forall n \in \mathbb{N} $$

Thật vậy điều này đúng với $n = 0$ do $2.13 - 5^2 = 6^0 = 1$ và $n = 1$ do $5.35 - 13^2 = 6$.
Giả sử điều này đúng đến $n = k$, tức $u_k u_{k+2} - {u_{k+1}}^2 = 6^k$.
Xét $n = k + 1$, ta có:

$$ \begin{aligned} & u_{k+1} u_{k+3} - {u_{k+2}}^2 = u_{k+1} \left(5u_{k+2} - 6u_{k+1}\right) - {u_{k+2}}^2 = 5u_{k+1} u_{k+2} - 6{u_{k+1}}^2 - {u_{k+2}}^2 \\ \Rightarrow & u_{k+1} u_{k+3} - {u_{k+2}}^2 = 5u_{k+1} u_{k+2} + 6^{k+1} - 6u_k u_{k+2} - {u_{k+2}}^2 \\ = & u_{k+2} \left(5u_{k+1} - 6u_k\right) + 6^{k+1} - {u_{k+2}}^2 = 6^{k+1} \text{ (do } u_{k+2} = 5u_{k+1} - 6u_k) \end{aligned} $$

Vậy điều này đúng với $n = k + 1$, theo nguyên lý quy nạp ta chứng minh được

$$ u_n u_{n+2} - {u_{n+1}}^2 = 6^n \, , \forall n \in \mathbb{N} $$

Do đó, ta có:

$$ u_{n+1}^2 - u_n u_{n+2} + 6^n = 0 \Rightarrow u_{n+1}^2 - 5u_n u_{n+1} + 6u_n^2 + 6^n = 0 \quad (*) $$

Xem (*) như phương trình bậc 2 theo tham số u_n ẩn u_{n+1}, ta có:

$$ X^2 - 5u_n X + 6{u_n}^2 + 6^n = 0 $$

Do dãy số trên là dãy các số nguyên nên ta suy ra X cũng phải là số nguyên. Như vậy

$$ \Delta = 25{u_n}^2 - 24u_n^2 - 4.6^n = {u_n}^2 - 4.6^n = v_n $$

phải là số chính phương.
Xét phương trình tổng quát

$$ x^2 - 5u_n x + 6{u_n}^2 + 6^n = 0 \ (x \in \mathbb{R}) $$

Phương trình có nghiệm khi và chỉ khi $\Delta = v_n = {u_n}^2 - 4.6^n > 0$.
Mà v_n là số chính phương (chứng minh trên) nên phương trình này luôn có nghiệm và $\sqrt{\Delta} \in \mathbb{N}$.
Như vậy 2 nghiệm của phương trình trên lần lượt là

$$ x = \frac{5u_n \pm \sqrt{{u_n}^2 - 4.6^n}}{2} $$

+Với u_n lẻ cũng như u_n chẵn, thì $5u_n \pm \sqrt{{u_n}^2 - 4.6^n}$ luôn là một số chẵn nên hiển nhiên nó chia hết cho 2. Cho nên x luôn là một số nguyên.
Mặt khác

$$\int \left(x^2 - 5xu_n + 6^n + 6{u_n}^2\right) = \frac{x^3}{3} - \frac{5x^2u_n}{2} + \left(6{u_n}^2 + 6^n\right)x + C \ (C \in \mathbb{R}) = f(x)$$

Mặt khác hàm số chỉ có thể đạt cực đại hoặc cực tiểu tại a, b, x_0 nên từ đó ta suy ra điều phải chứng minh. □

Bài tập 4.14. Xét hàm số $f(t) = t + \left[\sqrt{t}\right]$. Dãy số (a_n) được xác định

$$\begin{cases} a_0 = m > 2, \ (m \in \mathbb{N}) \\ a_{n+1} = f(a_n), \ \forall n = 0, 1, 2... \end{cases}$$

và dãy $(t_b) : t_b = \left[b\sqrt{2}\right] \ \forall b \in \mathbb{N}$. Chứng minh rằng tồn tại $n_0; b_0 : \sqrt{a_{n_0}.t_{b_0}} \in \mathbb{Z}$.

Lời giải

Với điều kiện đề bài, ta có thể nhận ra rằng tích số trên phải là số chính phương. Như vậy hoặc $a_{n_0}; t_{b_0}$ đều là số chính phương, hoặc $a_{n_0} = t_{b_0}$, hoặc chỉ $a_{n_0}.t_{b_0}$ là số chính phương. Việc chỉ ra tồn tại hoặc $a_{n_0} = t_{b_0}$, hoặc chỉ $a_{n_0}.t_{b_0}$ là số chính phương là công đoạn tính toán vất vả nhất là đối với hàm phần nguyên. Như vậy ta sẽ chứng minh tồn tại vô số số hạng là số chính phương để khẳng định sự tồn tại của 2 biến độc lập mà không cần chỉ ra cụ thể điều kiện của 2 biến bằng việc tính toán. Ta sẽ tuần tự chứng minh bài toán theo tính chất của hàm phần nguyên áp dụng khai triển Newton trong dãy số cũng như độ lệch của các hạng tử trong dãy.
Xét dãy (a_n), ta có: $m < f(m) < f(f(m)) < ...$ nên dãy trên là dãy tăng ngặt. Vậy ta chia làm hai trường hợp sau:

⁎ Trường hợp 1: Nếu m không phải là số chính phương.
Gọi t^2 là số chính phương lớn nhất không vượt quá $m = a_0$. Theo cách xác định trên ta suy ra được $d = [\sqrt{m}]$.
Đặt $m = d^2 + k$. Ta có $d^2 < m \leqslant (d+1)^2 \Rightarrow 0 < k \leqslant 2d + 1$.

* a) Xét $0 < k < d + 1$.Theo cách xác định dãy ta có:

$$d^2 < a_1 = f(a_0) = m + \left[\sqrt{m}\right] = d^2 + k + d < (d+1)^2$$
$$\Rightarrow d < \sqrt{f(a_0)} < (d+1) \Rightarrow d = \left[\sqrt{f(a_0)}\right] = [\sqrt{a_1}]$$

Ta có:

$$a_2 = f(a_1) = a_1 + [\sqrt{a_1}] = m + \left[\sqrt{m}\right] + [\sqrt{a_1}] = m + 2d = (d+1)^2 + k - 1$$

Như vậy ta thấy số chính phương lớn nhất không vượt quá a_2 là $(d+1)^2$ và độ lệch của chúng giảm đi 1 sau 2 lần thực hiện quá trình trên.

Áp dụng tương tự với phần tử bắt đầu là a_1. Quá trình trên được lặp lại và độ lệch giảm dần về 0 nên sau hữu hạn bước ta sẽ gặp số chính phương.

* b) Xét $d+1 \leqslant k \leqslant 2d+1$ ta có:

$$a_1 = f(m) = m + \left[\sqrt{m}\right] = d^2 + k + d = (d+1)^2 + k - d - 1$$

Do $0 \leqslant k - d - 1 < d + 1$ nên ta có:

$$\sqrt{a_1} = \sqrt{f(m)} = \sqrt{(d+1)^2 + k - d - 1} \Rightarrow [\sqrt{a_1}] = \left[\sqrt{f(m)}\right] = d + 1$$

Mặt khác, ta lại có:

$$a_2 = f(a_1) = f(m) + \left[\sqrt{f(m)}\right] = d^2 + k + 2d + 1 = (d+1)^2 + k$$

Vậy $(d+1)^2$ là số chính phương lớn nhất không vượt quá a_2 và k chính là độ lệch của nó. Do $0 \leqslant k < d + 1$ nên ta quay lại trường hợp a) với phần tử bắt đầu của dãy này là a_2.
Như vậy, ta chứng minh được sau một hữu hạn bước thì dãy (a_n) sẽ gặp phần tử là số chính phương.

⁎ Trường hợp 2: Nếu m đã là số chính phương thì hoặc dãy (a_n) có vô hạn số chính phương hoặc tồn tại $n_0 \in \mathbb{N} : a_{n_0}$không là số chính phương. Khi ấy ta quay lại trường hợp 1 và sau hữu hạn bước ta sẽ gặp lại phần tử của dãy là số chính phương.
Do quá trình trên lặp lại vô hạn lần nên ta suy ra dãy trên có vô hạn số chính phương.
Xét dãy (t_b). Theo khai triển Newton, ta có:

$$\begin{cases} \left(\sqrt{2}+1\right)^l = z_l\sqrt{2} + y_l \\ \left(\sqrt{2}-1\right)^l = z_l\sqrt{2} - y_l \end{cases} \text{khi l lẻ}$$

$$\Rightarrow (2-1)^l = 2{z_l}^2 - {y_l}^2 \Rightarrow 1 + {y_l}^2 = 2{z_l}^2$$

$$\Rightarrow {y_l}^4 + {y_l}^2 = \left(y_l z_l \sqrt{2}\right)^2$$

$$\Rightarrow \sqrt{{y_l}^4 + {y_l}^2} = y_l z_l \sqrt{2}$$

Mặt khác:

$${y_l}^2 < \sqrt{{y_l}^4 + {y_l}^2} < \left({y_l}^2 + 1\right) \Rightarrow \left[\sqrt{{y_l}^4 + {y_l}^2}\right] = {y_l}^2$$

Lại có

$$\left[\sqrt{{y_l}^4 + {y_l}^2}\right] = \left[y_l z_l \sqrt{2}\right] \Rightarrow \left[y_l z_l \sqrt{2}\right] = {y_l}^2$$

Do $\left[y_l z_l \sqrt{2}\right]$ là một dãy con của dãy t_b nên ta suy ra dãy trên có vô hạn số chính phương.
Như vậy

$$\exists\, b_0, n_0 \in \mathbb{N} : \sqrt{a_{n_0}.t_{b_0}} \in \mathbb{Z} \Rightarrow a_{n_0+1} = f(a_{n_0}) = d^2 + d = d(d+1)$$

Vậy ta có đpcm. □

Chuyên đề 5:
Một số hàm số học và ứng dụng

Lê Phúc Lữ [1]

Hàm số học f là hàm nhận đối số và giá trị trên một tập rời rạc là tập con của số nguyên, thông thường thì ta xét $f : \mathbb{N} \to \mathbb{N}$. Các hàm số học quen thuộc và gặp nhiều ứng dụng như: hàm phần nguyên, hàm phần lẻ, hàm tổng các chữ số, hàm Euler... Còn các hàm tổng các ước và hàm số các ước rõ ràng là cũng được giới thiệu nhiều nhưng phần ứng dụng của nó khá ít. Bài viết dưới đây lược dịch từ một chương trong cuốn Elementary Number Theory and Its Application của tác giả Kenneth Rosen. Mong rằng với một số lượng bài tập khá phong phú, chúng ta sẽ được tiếp cận tốt hơn đối với hai hàm số học "quen mà cũng lạ" này.

Hàm tổng các ước số và số các ước số

Kiến thức cần nhớ

Định nghĩa và tính chất. Với mỗi số nguyên dương n, kí hiệu là tổng các ước dương của n (kể cả n) và $\tau(n)$ là số các ước dương của n (kể cả n).
Ta xét biểu diễn của n là

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_k^{a_k}$$

với $p_1, p_2, p_3, ..., p_k$ là các số nguyên tố còn $a_1, a_2, a_3, ..., a_k$ là các số nguyên dương. Từ đây ta quy ước biểu diễn của n dưới dạng này.
Khi đó ta có:

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \frac{p_3^{a_3+1} - 1}{p_3 - 1} ... \frac{p_k^{a_k+1} - 1}{p_k - 1}$$

và

$$\tau(n) = (a_1 + 1)(a_2 + 1)(a_3 + 1)...(a_k + 1)$$

Chú ý rằng ta cũng có thể kí hiệu $\sigma(n) = \sum_{d|n} d$ và $\tau(n) = \sum_{d|n} 1$.

Chứng minh.
Ta thấy rằng một số $d = p_1^{b_1} p_2^{b_2} p_3^{b_3} ... p_k^{b_k}$ là ước của n khi và chỉ khi $0 \leqslant b_i \leqslant a_i$ với $i = 1, 2, 3, ..., k$..
Như thế giá trị của b_i có thể có $a_i + 1$ cách chọn và như thế, theo nguyên lí nhân, số ước của

[1] Sinh viên Đại học FPT

n chính là . Tiếp theo, ta xét biểu diễn

$$\prod_{i=1}^{k}\left(\sum_{j=1}^{a_i} p_i^j\right) = \left(1+p_1+p_1^2+...+p_1^{a_1}\right)\left(1+p_2+p_2^2+...+p_2^{a_2}\right)...\left(1+p_k+p_k^2+...+p_k^{a_k}\right)$$

Dễ thấy khai triển này có tất cả $(a_1+1)(a_2+1)(a_3+1)...(a_k+1)$ và các số hạng đó là các ước phân biệt của n. Do đó, đại lượng trên chính là tổng các ước của n và có thể thu gọn thành

$$\sigma(n) = \frac{p_1^{a_1+1}-1}{p_1-1}\frac{p_2^{a_2+1}-1}{p_2-1}\frac{p_3^{a_3+1}-1}{p_3-1}...\frac{p_k^{a_k+1}-1}{p_k-1}$$

Nhận xét. Nếu f là hàm nhân tính, nghĩa là $f(m)f(n)=f(mn)$ với mọi $(m,n)=1$ thì ta có $F(n)=\sum\limits_{d|n} f(d)$ cũng là một hàm nhân tính.

Thật vậy, giả sử m,n là các số nguyên dương nguyên tố cùng nhau thì $F(mn)=\sum\limits_{d|(mn)} f(d)$. Rõ ràng ta có thể viết $d=d_1d_2$ một cách duy nhất sao cho d_1 là ước của m và d_2 là ước của n với $(d_1,d_2)=1$. Khi đó , ta có

$$F(mn)=\sum_{d|(mn)} f(d)=\sum_{d_1|m,\,d_2|n} f(d_1d_2)=\sum_{d_1|m,\,d_2|n} f(d_1)f(d_2)=\sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2)=F(m)F(n)$$

Nhận xét được chứng minh. Từ đây, lần lượt thay $f(x)=x$ và $f(x)=1$, ta suy ra được rằng các hàm $\sigma(n)$ và $\tau(n)$ đều là các hàm nhân tính.

Ví dụ áp dụng

Ví dụ 1.

1. Tìm tất cả các số nguyên dương n sao cho $\sigma(n)$ lần lượt bằng $12, 18, 24, 48, 52, 84$?
2. Tìm số nguyên dương n nhỏ nhất sao cho $\tau(n)$ lần lượt bằng $1, 2, 3, 6, 14, 100$?

Lời giải

1. Để làm các bài này, ta cần chọn các số nguyên tố và số mũ thích hợp sao cho

$$\left(1+p_1+p_1^2+...+p_1^{a_1}\right)\left(1+p_2+p_2^2+...+p_2^{a_2}\right)...\left(1+p_k+p_k^2+...+p_k^{a_k}\right)=\sigma(n)$$

Ta liệt kê các số có dạng $1+p_k+p_k^2+...+p_k^{a_k}$ từ nhỏ đến lớn:

$$1+2, 1+3, 1+5, 1+2+2^2, 1+7, 1+3+3^2, 1+2+2^2+2^3, ...$$

Với $\sigma(n)=12$, ta thấy chỉ có thể viết thành $12=(1+2)(1+3)$ và số cần tìm là $n=6$.
Các số còn lại thực hiện tương tự.

2. Ở bài này, ta cũng chọn các số mũ thích hợp trước rồi tiếp đến chọn các số nguyên tố nhỏ để cho giá trị của n càng nhỏ càng tốt. Chẳng hạn với $\tau(n)=14$, ta có thể chọn ngay số mũ là 13 ứng với ước nguyên tố 2, tức là $n=2^{13}$. Tuy nhiên, ta có thể làm cho giá trị này nhỏ hơn bằng cách viết $14=2\cdot 7$, ứng với 2 số mũ 1 và 6, ta chọn số $n=3\cdot 2^6$. Đây là số nhỏ nhất cần tìm.
Các số còn lại thực hiện tương tự.

Ví dụ 2.
1. Chứng minh rằng $\tau(n)$ là số lẻ khi và chỉ khi n là số chính phương.
2. Với các giá trị nào của n thì $\sigma(n)$ là số lẻ?

Lời giải

1. Ta thấy rằng $\tau(n) = (a_1 + 1)(a_2 + 1)(a_3 + 1)...(a_k + 1)$ nên nếu $\tau(n)$ lẻ khi và chỉ khi tất cả các số mũ đều phải là số chẵn, nghĩa là n là số chính phương.
2. Ta cần chọn các ước nguyên tố và số mũ thích hợp để $\sigma(n)$ là số lẻ. Ta có

$$\sigma(n) = \left(1 + p_1 + p_1^2 + ... + p_1^{a_1}\right)\left(1 + p_2 + p_2^2 + ... + p_2^{a_2}\right)...\left(1 + p_k + p_k^2 + ... + p_k^{a_k}\right)$$

nên nếu có ước nguyên tố nào đó là 2 thì vẫn thỏa mãn, nếu n có ước nguyên tố lẻ thì trong tổng trên, chúng phải xuất hiện chẵn lần. Do đó, số cần tìm có dạng $n = 2^k m^2$ với m là một số chính phương lẻ.

Ví dụ 3. Một mật khẩu hợp lệ có độ dài $n, n \geqslant 6$ gồm 2 phần: 4 kí tự đầu là 1 trong 2 chữ số 0 hoặc 1, $n - 4$ kí tự sau là 1 trong 26 kí tự của bảng chữ cái tiếng Anh nhưng không chứa toàn chữ 'A'. Chẳng hạn: 0100XYZ là một mật khẩu có 7 kí tự, hợp lệ nhưng 0111AAA hay 0123ABC là các mật khẩu có 7 kí tự nhưng không hợp lệ.
a. Hỏi tổng số mật khẩu hợp lệ là bao nhiêu? Đặt số lượng đó là s_n.
b. Gọi số tất cả các cách biểu diễn s_n thành tổng của các số nguyên dương bằng nhau (có lượng số hạng tùy ý và có thể chỉ gồm 1 số hạng) là t_n. Chứng minh rằng t_n chia hết cho 10.

Lời giải

Câu a:
Xét mật khẩu có dạng $X_1X_2X_3...X_n$ với

$$\begin{cases} X_i \in \{0; 1\}\ \forall i = \overline{1, 4} \\ X_k \in \{A, B, C, ..., Z\}\ \forall k > 4 \end{cases}$$

Mỗi số X_1, X_2, X_3, X_4 có 2 cách chọn nên có tất cả $2 \times 2 \times 2 \times 2 = 16$ cách chọn 4 kí tự đầu.
Mỗi số $X_k, 4 < k \leqslant n$ có 26 cách chọn nên có tất cả 26^{n-4} cách chọn nhưng trừ trường hợp toàn bộ là A đi nên có tổng cộng $26^{n-4} - 1$ cách chọn $n - 4$ kí tự sau.
Do đó, tổng số mật khẩu hợp lệ có thể có là $s_n = 16(26^{n-4} - 1)$.

Câu b:
Dễ dàng thấy rằng t_n chính là số ước của s_n. Ta cũng có $(16, 26^{n-4} - 1) = 1$ nên có thể viết s_n dưới dạng $s_n = 2^4 \times p$ với p là một số nguyên dương lẻ.
Do $n \geqslant 6$ nên $n - 4 \geqslant 2$ và 26^{n-4} chia hết cho 4, tức là $26^{n-4} - 1$ có dạng $4k + 3$, không thể là một số chính phương, tức là nó có số ước chẵn.
Thêm vào đó, $4 + 1 = 5$ nên theo công thức tính số ước của một số nguyên dương thì t_n vừa chia hết cho 5 và vừa chia hết cho 2 nên nó phải chia hết cho 10.
Ta có đpcm.

Ví dụ 4.

a) Cho n là một số tự nhiên thỏa mãn $n+1$ chia hết cho 24. Chứng minh rằng tổng các ước dương của n (kể của n) cũng chia hết cho 24.

b) Xét số nguyên

$$A = 2010^{2011} - 2011^{2010} - 2052^{1994}$$

Hãy chứng minh rằng A là một hợp số dương và tổng các ước số dương của A chia hết cho 24.

Lời giải

a) Gọi $d(n)$ là tổng các ước dương của n. Trước hết, ta sẽ chứng minh rằng $d(n)$ chia hết cho 3.

Thật vậy, gọi a là một ước nào đó của n thì $\frac{n}{a}$ cũng là ước của n và nếu xét $0 < a < \sqrt{n}$ thì các bộ $\left(a; \frac{n}{a}\right)$ đôi một khác nhau (do $n+1$ chia hết cho 24 nên n chia 3 dư 2 và nó không thể là số chính phương).

Vì n chia 3 dư 2 nên trong hai số $a, \frac{n}{a}$ có một số chia 3 dư 1 và một số chia 3 dư 2; suy ra tổng của chúng phải chia hết cho 3. Do đó

$$d(n) = \sum_{0<a<\sqrt{n}} \left(a + \frac{n}{a}\right) \vdots 3$$

Tương tự, ta thấy rằng $n+1$ chia hết cho 8 nên n chia 8 dư 7. Do n là số lẻ nên chia 8 có các số dư là $1, 3, 5, 7$; khi đó, dễ dàng thấy rằng trong hai số $a, \frac{n}{a}$ có một số chia 8 dư 1, một số chia 8 dư 7 hoặc một số chia 8 dư 3, một số chia 8 dư 5.

Dễ thấy khi đó tổng của hai ước này cũng chia hết cho 8.

Từ đó suy ra $d(n)$ chia hết cho 8.

Kết hợp hai điều trên lại, ta thấy rằng tổng các ước dương của n chia hết cho 24.

b) Trước hết, ta sẽ chứng minh rằng n là hợp số dương. Thật vậy, ta sẽ chứng minh rằng nếu $x > y \geqslant 3$ thì

$$y^x > x^y \quad (*)$$

Bất đẳng thức này tương đương với

$$x \ln y > y \ln x \Leftrightarrow \frac{\ln y}{y} > \frac{\ln x}{x}$$

Hàm số $f(t) = \frac{\ln t}{t}, t > 3$ có $f'(t) = \frac{1-\ln t}{t^2} < 0$ nên đây là hàm nghịch biến, suy ra $f(x) < f(y)$ hay (*) đúng.

Cũng bằng cách dùng hàm số, ta có thể chứng minh rằng với n đủ lớn và $0 < a < n$ thì có đánh giá

$$\frac{n^{n+a}}{(n+a)^n} > 2$$

Do đó $2010^{2011} > 2.2011^{2010} > 2011^{2010} + 2052^{1994}$ nên $A > 0$. Xét trong modun 5 thì

$$A \equiv -\left(1 + 2^{1994}\right) (\text{mod} 5)$$

Mà

$$2^4 \equiv 1(\text{mod}5) \Rightarrow 2^{1994} = 4\left(2^4\right)^{498} \equiv 4(\text{mod}5)$$

Suy ra A chia hết cho 5 hay A là một hợp số.
Tiếp theo, ta sẽ chứng minh rằng $A+1$ chia hết cho 24. Thật vậy, do $2010, 2052$ chia hết cho 3 nên

$$A+1 \equiv -\left((-1)^{2010}\right)+1 = 0(\text{mod}3)$$

Hơn nữa 2052 chia hết cho 8 và

$$A+1 \equiv -3^{2010}+1 \equiv -\left(3^2\right)^{1005}+1 \equiv -1^{1005}+1 = 0(\text{mod}8)$$

Suy ra $A+1$ chia hết cho 3 và chia hết cho 8 nên $A+1$ chia hết cho 24.
Theo kết quả ở câu a, ta có tổng các ước dương của A chia hết cho 24, suy ra đpcm.

Bài tập có hướng dẫn, gợi ý

Bài tập 5.1. Chứng minh rằng phương trình $\tau(n) = k$ có vô số nghiệm nguyên dương n với mọi k, còn phương trình $\sigma(n) = k$ thì có hữu hạn nghiệm nguyên dương n.

Gợi ý.
Ta thấy rằng giá trị của $\sigma(n)$ có sự tham gia của các số nguyên tố, còn giá trị của $\tau(n)$ thì không (điều này có nghĩa là ta có thể chọn giá trị của các ước nguyên tố của số n lớn tùy ý).

Bài tập 5.2. Tích của tất cả các ước của n bằng bao nhiêu? Chứng minh rằng hàm tích các ước của n là một đơn ánh trên tập hợp số nguyên dương.

Gợi ý.
Chú ý rằng các ước của n có thể chia thành từng cặp có dạng $\left(d; \frac{n}{d}\right)$ và như thế khi nhân chúng lại, ta sẽ được một giá trị n mới. Kết quả là $n^{\tau(n)/2}$.
Còn việc chứng minh tính đơn ánh thì có thể sử dụng phân tích thành thừa số nguyên tố.

Bài tập 5.3. Tìm tất cả các số nguyên dương n sao cho $\sigma(n) + \phi(n) = 2n$, trong đó kí hiệu $\phi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n.

Gợi ý.
Có thể sử dụng trực tiếp công thức của các hàm số trên rồi dùng bất đẳng thức chứng minh rằng $\sigma(n) + \phi(n) \geqslant 2n$ hoặc dùng lập luận trực tiếp dựa theo ý nghĩa của các hàm số.

Bài tập 5.4.
a. Chứng minh rằng số cặp có thứ tự các số có BCNN đúng bằng n là $\tau(n^2)$.
b. Chứng minh rằng với mọi số nguyên dương n thì

$$\tau(2^n - 1) \geqslant \tau(n).$$

c. Chứng minh rằng số nguyên dương n là hợp số khi và chỉ khi $\sigma(n) > n + \sqrt{n}$.

Gợi ý.

a. Ta tính số cách chọn bộ (a, b) mà $[a, b] = n$ là $(2a_1 + 1)(2a_2 + 1)...(2a_k + 1)$ bằng việc lập luận trên các số mũ tương tự như chứng minh công thức tính $\tau(n)$.

b. Chú ý rằng $(2^{ab} - 1) \vdots (2^a - 1)$ với $a, b \in \mathbb{Z}^+$ nên dễ thấy số ước của $2^n - 1$ nhiều hơn của n.

c. Giả sử $n = ab$ với $1 < a \leqslant b < n$ thì $\sigma(n) \geqslant 1 + a + b + n > 1 + \sqrt{n} + n > n + \sqrt{n}$. Chiều ngược lại chứng minh khá dễ dàng bằng việc kiểm tra các số nguyên tố.

Bài tập 5.5.

1. Chứng minh rằng

$$\sum_{i=1}^{n} \tau(i) = 2 \sum_{i=1}^{[\sqrt{n}]} \left[\frac{n}{i}\right] - \left[\sqrt{n}\right]^2$$

Từ đó tính tổng $\sum\limits_{i=1}^{100} \tau(i)$.

2. Cho a, b là các số nguyên dương. Chứng minh

$$\max\left\{\frac{\sigma(a)}{a}, \frac{\sigma(b)}{b}\right\} \leqslant \frac{\sigma(ab)}{ab} \leqslant \frac{\sigma(a)\sigma(b)}{ab}$$

3. Chứng minh rằng nếu a, b là các số nguyên dương thì $\sigma(a)\sigma(b) = \sum\limits_{d|(a,b)} d \cdot \sigma\left(\frac{ab}{d^2}\right)$.

Gợi ý.

a. Ta sử dụng phương pháp quy nạp. Chú ý rằng trong bước quy nạp, ta kiểm tra 2 trường hợp n là số chính phương hoặc không. Tổng $\sum\limits_{i=1}^{100} \tau(i) = 482$.

b. Ta chia thành 2 bất đẳng thức $b\sigma(a) \leqslant \sigma(ab)$ và $\sigma(ab) \leqslant \sigma(a)\sigma(b)$ rồi sử dụng trực tiếp công thức của hàm $\sigma(n)$.

c. Đặt $a = \prod p_i^{a_i}, b = \prod p_i^{b_i}$ và $c_i = \min(a_i, b_i)$ với $i = 1, 2, 3, ..., k$. Trước hết, ta chứng minh rằng

$$\prod_{p_i} \sum_{j=0}^{c_i} p_i^j \sigma(p_i^{a_i+b_i-2j}) = \sum_{d|(a,b)} d\sigma\left(\frac{ab}{d^2}\right)$$

Sau đó xem xét các tổng có dạng $\sum\limits_{j=0}^{c} (p^{a+b-j} + p^{a+b-j-1} + ... + p^j)$ với $c = \min(a, b)$ và chú ý số lần xuất hiện của các thừa số nguyên tố trong $\sigma(a)\sigma(b)$.

Bài tập tự giải

Bài tập 5.6.

a) Tìm tổng các ước dương của các số sau: $35, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11, 196, 2^5 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11, 1000, 10!, 2^{100}$.

b) Tìm số các ước của các số sau $36, 99, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 99, 144, 20!$.

Bài tập 5.7.
a. Hỏi các số nguyên dương nào có đúng 2 ước nguyên dương?
b. Hỏi các số nguyên dương nào có đúng 3 ước nguyên dương?
c. Hỏi các số nguyên dương nào có đúng 4 ước nguyên dương?

Bài tập 5.8. Cho số nguyên dương a. Xét dãy số (u_n) xác định bởi

$$\begin{cases} u_1 = a, \\ u_{n+1} = \tau(u_n), n = 1, 2, 3, ... \end{cases}$$

Chứng minh rằng với n đủ lớn thì $u_N = 2, \forall N \geqslant n$.

Bài tập 5.9. Số n được gọi là "highly composite" nếu $\tau(m) < \tau(n)$ với mọi $1 \leqslant m < n$.
1. Chứng minh rằng với mỗi $k \in \mathbb{Z}^+$, tồn tại số HC n thỏa mãn $k \leqslant n < 2k$. Từ đó suy ra có vô hạn số HC và đánh giá chặn trên cho số HC thứ k nào đó.
2. Chứng minh rằng nếu n là một số HC thì tồn tại số nguyên dương k nào đó sao cho ta có biểu diễn $n = 2^{a_1}3^{a_2}5^{a_3}...p_k^{a_k}$ với p_k là số nguyên tố thứ k và $a_1 \geqslant a_2 \geqslant ... \geqslant a_k \geqslant 1$.
3. Tìm tất cả các số HC có dạng $n = 2^a3^b$ với a, b là các số nguyên dương.

Biết số square-free là số có dạng $n = p_1p_2p_3...p_k$ với $p_1, p_2, p_3, ..., p_k$ là các số nguyên tố. Hãy trả lời các câu hỏi sau đây.

Bài tập 5.10.
a. Hỏi trong các số sau đây, số nào là số square-free?

$$A.44 \qquad B.50 \qquad C.10000000 \qquad D.95$$

b. Một số square-free nào đó có số các ước là A. Hỏi A có thể nhận giá trị nào?

$$A.25 \qquad B.30 \qquad C.1024 \qquad D.99$$

c. Cho tập hợp $B = \{2, 3, 5, 7\}$. Hỏi có tất cả bao nhiêu số square-free có các ước nguyên tố thuộc tập B?

$$A.15 \qquad B.16 \qquad C.17 \qquad D.14$$

Bài tập 5.11. Cho n là số nguyên dương. Chứng minh các đẳng thức sau:
a. $\left(\sum_{d|n} \tau(n)\right)^2 = \sum_{d|n} (\tau(d))^3$.
b. $\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$ với $\omega(n)$ là số các ước nguyên tố của n.
c. $\sum_{d|n} \frac{n\sigma(d)}{d} = \sum_{d|n} d\tau(d)$.

Bài tập 5.12. Chứng minh rằng tồn tại vô số cặp số (m, n) sao cho $\phi(m) = \sigma(n)$ nếu như tồn tại vô số cặp số nguyên tố Mersense (số nguyên tố dạng $2^n - 1$) hoặc tồn tại vô số cặp số nguyên tố sinh đôi.

Một số hàm số khác

Hàm phần nguyên

Các kiến thức cần nhớ

Các tính chất của phần nguyên:

- $[x] = x$ khi và chỉ khi x là số nguyên.
- $[x + n] = [x] + n$ với n là số nguyên.
- $[x + y] \leqslant [x] + [y]$ với mọi số thực x, y.
- $[x] + [y] = x + y - 1$ với x, y là các số không nguyên và $x + y$ nguyên.
- Số các số nguyên dương không vượt quá n và chia hết cho k là $\left[\frac{n}{k}\right]$.
- Khai triển Legendre: số mũ của số nguyên tố p trong khai triển của số nguyên dương $n!$ thành thừa số nguyên tố là

$$\sum_{i=1}^{+\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Các bài tập áp dụng

Bài tập 5.13. Hỏi có bao nhiêu số nguyên không vượt quá 2013 và chia hết cho 2 hoặc 3 hoặc 5?

Bài tập 5.14. Chứng minh rằng số các số nguyên không vượt quá n và không chia hết cho 2 hoặc 3 là

$$n + \left[\frac{n}{6}\right] - \left(\left[\frac{n}{2}\right] + \left[\frac{n}{3}\right]\right)$$

Bài tập 5.15. Chứng minh rằng với mọi số nguyên dương x, y thì $\frac{(x+y)!}{x!y!}$ là số nguyên.

Bài tập 5.16. . Phần lẻ $\{x\}$ chính là đại lượng tính bằng $x - [x]$. Chứng minh rằng $0 \leqslant \{x\} < 1$ và với mọi số thực x, y thì $\{x + y\} \leqslant \{x\} + \{y\}$.

Bài tập 5.17. Cho x, y, z là các số thực thỏa mãn $\{x\} + \{y\} + \{z\} = 2$. Tính giá trị của biểu thức

$$P = [x + y + z] - ([x] + [y] + [z])$$

Bài tập 5.18. Rút gọn biểu thức sau:

$$A = \left[\frac{2^1}{3}\right] + \left[\frac{2^2}{3}\right] + \left[\frac{2^3}{3}\right] + ... + \left[\frac{2^{100}}{3}\right]$$

Hàm tổng các chữ số

Các kiến thức cần nhớ

Kí hiệu $S(n)$ là tổng các chữ số của n. Ta có các tính chất:

- $n - S(n)$ chia hết cho 9.
- $S(m+n) \leqslant S(m) + S(n)$ với m, n là các số nguyên dương.
- $S(mn) \leqslant S(m)S(n)$ với m, n là các số nguyên dương.
- $S(n) = n - 9\sum_{k=1}^{+\infty} \left[\frac{n}{10^k}\right]$.

Bài tập áp dụng

Bài tập 5.19. Tìm số nguyên dương n nhỏ nhất sao cho $S(n), S(n+1)$ đều chia hết cho 7.

Bài tập 5.20. Khi viết 4444^{4444} trong hệ thập phân thì tổng các chữ số của nó là A. Gọi B là tổng các chữ số của A. Tính tổng các chữ số của B.

Bài tập 5.21. Chứng minh rằng với mọi số nguyên dương n thì ta có các bất đẳng thức:
a) $S(2n) \leqslant S(n) \leqslant 5S(2n)$.
b) $S(5n) \leqslant S(n) \leqslant 2S(5n)$.

Bài tập 5.22. Người ta gọi các số có thể biểu diễn thành tổng $a + b$ với $S(a) = S(b)$ là các số đẹp.
a. Chứng minh rằng các số $999, 2999$ không phải là số đẹp và tồn tại vô số số không là số đẹp.
b. Chứng minh rằng tất cả các số thỏa mãn $999 < k < 2999$ đều là số đẹp.

Hàm Euler

Kiến thức cần nhớ

Với mỗi số nguyên dương n, kí hiệu $\phi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Dây được gọi là hàm Euler.
Ta có các kết quả quen thuộc:

- $\phi(p) = p - 1$ với p là số nguyên tố.
- $\phi(p^k) = p^{k-1}(p-1)$ với p là số nguyên tố.
- $\phi(mn) = \phi(m)\phi(n)$ với $(m, n) = 1$.

Trong trường hợp tổng quát, ta có

$$\phi\left(p_1^{a_1}p_2^{a_2}p_3^{a_3}...p_k^{a_k}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)...\left(1 - \frac{1}{p_k}\right)$$

Bài tập tổng hợp

Bài tập 5.23.

1. Cho n là số nguyên dương lớn hơn 2. Chứng minh rằng $\phi(n)$ chẵn.
2. Với giá trị nào của n thì $\phi(n) = \frac{n}{2}$? $\phi(n) \,|n$? $\phi(3n) = 3\phi(n)$? $\phi(n)$ chia hết cho 4?
3. Chứng minh rằng nếu n có k ước nguyên tố lẻ phân biệt thì $\phi(n)$ chia hết cho 2^k.
4. Chứng minh rằng nếu $m, n \in \mathbb{Z}^+$ và $m|n$ thì $\phi(m)|\phi(n)$.
5. Chứng minh rằng hàm $f(n) = \frac{\phi(n)}{n}$ là hàm nhân tính đầy đủ.

Bài tập 5.24.

1. Giả sử $m, n \in \mathbb{Z}^+$ và $(m, n) = p$ với p nguyên tố . Chứng minh $\phi(mn) = p\frac{\phi(m)\phi(n)}{p-1}$.
2. Chứng minh rằng

$$\phi(m^k) = m^{k-1}\phi(m)$$

với mọi $m, k \in \mathbb{Z}^+$.

3. Cho $a, b \in \mathbb{Z}^+$, chứng minh rằng

$$\phi(ab) = (a, b)\frac{\phi(a)\phi(b)}{\phi\left((a, b)\right)},$$

từ đó suy ra $\phi(ab) = \phi(a)\phi(b)$ với $(a, b) > 1$.

Bài tập 5.25.

1. Chứng minh rằng nếu phương trình $\phi(n) = k$ với $k \in \mathbb{Z}^+$ có nghiệm duy nhất n thì n chia hết cho 36.
2. Chứng minh rằng phương trình $\phi(n) = k$ với $k \in \mathbb{Z}^+$ có hữu hạn nghiệm n.
3. Chứng minh rằng nếu p là số nguyên tố, $2^a p + 1$ là hợp số với $a = 1, 2, 3, ..., r$ và p không phải là số nguyên tố Fermat thì

$$\phi(n) = 2^r p$$

vô nghiệm.

4. Chứng minh rằng tồn tại vô hạn số nguyên dương k sao cho phương trình

$$\phi(n) = k$$

có đúng 2 nghiệm nguyên dương n.

Gợi ý: xét các số nguyên dương có dạng $k = 2 \cdot 3^{6j+1}, j = 1, 2, 3, ...$

Bài tập 5.26.

1. Chứng minh rằng nếu $n \neq 2, n \neq 6$ thì $\phi(n) \geqslant \sqrt{n}$.
2. Chứng minh rằng n là hợp số khi và chỉ khi $\phi(n) \leqslant n - \sqrt{n}$.
3. Tìm số nguyên dương n nhỏ nhất thỏa mãn $\phi(n) \geqslant 10^5$.

Bài tập 5.27. Chứng minh rằng nếu n là hợp số và $\phi(n) \,|(n-1)$ thì n là số square-free và nó là tích của ít nhất 3 ước nguyên tố phân biệt.

Bài tập 5.28. Cho số nguyên dương a. Xét dãy số (u_n) xác định bởi

$$\begin{cases} u_1 = a, \\ u_{n+1} = \phi(u_n), n = 1, 2, 3, ... \end{cases}$$

Chứng minh rằng với n đủ lớn thì $u_N = 1, \forall N \geqslant n$.

Bài tập 5.29.

1. Chứng minh rằng $\sum_{d|n} \phi(d) = n$ với mọi số nguyên dương n.

2. Chứng minh rằng $\sum_{1 \leqslant a \leqslant n, (a,n)=1} a = \frac{n\phi(n)}{2}$.

3. Giả sử $p > 4$ là một số nguyên dương và $p - 1, p + 1$ là hai số nguyên tố sinh đôi . Chứng minh rằng $3\phi(p) \leqslant p$.

4. Chứng minh rằng điều kiện cần và đủ để n là số nguyên tố là $\sigma(n) + \phi(n) = n\tau(n)$.

Chuyên đề 6:
Thặng dư bình phương

Nguyễn Huy Hoàng, Trần Hy Đông [1]

Thặng dư bình phương là một trong những công cụ mạnh để giải quyết các bài toán số học. Thặng dư bình phương rất đơn giản, dễ hiểu nhưng lại cực kì hữu dụng. Tuy vậy, độc giả cần có một nền tảng kiến thức tốt (như về cấp của 1 số, định lý Fermat,...) để có thể sử dụng thành thục.

Tính chất cơ bản của thặng dư bình phương và kí hiệu Legendre

Định nghĩa 6.0.1.

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

Ví dụ: -1 là số chính phương mod 5 (vì $7^2 \equiv -1(\mathrm{mod}5)$)

Định lý 6.0.1.

Nếu p là một số nguyên tố lẻ thì trong các số $1,2,3,\ldots,p-1$ có đúng $\frac{p-1}{2}$ số chính phương mod p.

Phần chứng minh hai định lý trên xin dành cho bạn đọc.

Định nghĩa 6.0.2.

Cho $a \in Z$, p là số nguyên tố lẻ . Ký hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau:
Nếu $(a,p)=1$ và a là số bình phương mod p thì

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \\ -1 \\ 0 \end{cases}$$

Nếu $(a,p)=1$ và a không là số bình phương mod p thì

$$(a,p) \neq 1$$

[1]Lớp chuyên Toán trường Phổ Thông Năng Khiếu và trường THPT Chuyên Lê Hồng Phong

Ví dụ: Ta thấy rằng:
$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$
$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$

Định lý 6.0.2.

Giả sử p là một số nguyên tố lẻ , $(a, p) = 1$. Khi đó :

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Chứng minh:

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

Khi đó phương trình đồng dư $x^2 \equiv a(\mathrm{mod} p)$ có nghiệm x_0 . Theo định lý Fermat nhỏ, ta có :

$$a^{\frac{p-1}{2}} \equiv \left(x_0^2\right)^{\frac{p-1}{2}} = x_0^{p-1} \equiv a\,(\mathrm{mod} p)\,(\text{đpcm})$$

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

Khi đó phương trình đồng dư $x^2 \equiv a(\mathrm{mod} p)$ vô nghiệm . Với mỗi i từ 1 đến $p-1$, tồn tại duy nhất j,$1 \leqslant j \leqslant p-1$ sao cho $i.j \equiv a(\mathrm{mod} p)$.

Rõ ràng là $i \neq j$ nên có thể nhóm các số từ 1 đến $p-1$thành $\frac{p-1}{2}$ cặp , sao cho tích trong mỗi cặp đều đồng dư a mod p . Nhân tất cả các số $1, 2, 3, \ldots, p-1$, ta được :

$$(p-1)! \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Theo định lý Wilson , $(p-1)! \equiv -1(\mathrm{mod} p)$, định lý được chứng minh .

Định lý 6.0.3.

Giả sử p là 1 số nguyên tố lẻ , a và b là những số nguyên không chia hết cho p. Khi đó:
1/ $a \equiv b(\mathrm{mod} p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2/ $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3 /$\left(\frac{a^2}{p}\right) = 1$.

Bạn đọc dễ chứng minh định lý 4 bằng định lý 3.

Định lý 6.0.4.

Với mỗi số nguyên $p > 2$, ta có

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$$

Từ đây suy ra phương trình đồng dư $x^2 \equiv -1(\mathrm{mod} p)$ có nghiệm khi và chỉ khi $p = 2$ hoặc $p \equiv 1(\mathrm{mod} 4)$

Ví dụ: Ta dễ thấy $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p - 1 \vdots 4$.

Định lý 6.0.5.

Giả sử $(x;y)=1$, a,b,c là các số nguyên p là 1 ước nguyên tố của $ax^2+bxy+cy^2$, p không là ước của abc thì $D=b^2-4ac$ là thặng dư bậc 2 mod p.
Đặc biệt nếu p là ước của x^2-Dy^2và $(x,y)=1$thì D là thặng dư bậc 2 mod p.

Chứng minh:

Dễ biến đổi

$$p\left|(2ax+by)^2-Dy^2\right.$$

Giả sử $p\left|y\right.$, khi đó $p\left|2ax+by\right.\Rightarrow p\left|2ax\right.$
Mà $(a,p)=1$ nên $p\left|x\right.$. Vậy $(x,y)>1$ (Vô lý)
Do đó $(p,y)=1$ nên tồn tại y'sao cho $yy'\equiv 1(\mathrm{mod}p)$.
Suy ra

$$(2axy'+byy')^2\equiv Dyy'\equiv D(\mathrm{mod}p)$$

Vậy D là thặng dư chính phương mod p.

Định lý 6.0.6. (Bổ đề Gauss)

Giả sử p là 1 số nguyên tố lẻ , a là số nguyên không chia hết cho p . Nếu trong số các thặng dư bé nhất của các số nguyên $a,2a,3a,...,\frac{p-1}{2}a$ có s thặng dư lớn hơn $\frac{p}{2}$ thì:

$$\left(\frac{a}{p}\right)=(-1)^s\text{hay}\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}\left[\frac{2ka}{p}\right]}$$

Chứng minh:

Cho a là 1 số nguyên , p là 1 số nguyên tố sao cho $(a,p)=1$. Với mỗi $k\in\left\{1;2;3;...;\frac{p-1}{2}\right\}$ đều tồn tại $r_k\in\left\{\pm1;\pm2;\pm3;...;\pm\frac{p-1}{2}\right\}$ sao cho

$$ka\equiv r_k(\mathrm{mod}p)$$

Dễ thấy không tồn tại hai r_k có cùng trị tuyệt đối , do đó

$$\left|r_1\right|,\left|r_2\right|,\left|r_3\right|,...,\left|r_{\frac{p-1}{2}}\right|$$

là 1 hoán vị của $\left\{1;2;3;...;\frac{p-1}{2}\right\}$.
Cho k chạy từ $1\rightarrow\frac{p-1}{2}$ rồi nhân tất cả các vế lại với nhau ta được :

$$a^{\frac{p-1}{2}}\equiv\frac{r_1r_2r_3...r_{\frac{p-1}{2}}}{1.2.3....(\frac{p-1}{2})}=\frac{r_1r_2r_3...r_{\frac{p-1}{2}}}{\left|r_1\right|\left|r_2\right|\left|r_3\right|...\left|r_{\frac{p-1}{2}}\right|}(\mathrm{mod}p)$$

Đặt $b_k=\frac{r_k}{|r_k|};b_k=\pm1$.Ta có

$$a^{\frac{p-1}{2}}\equiv b_1...b_k(\mathrm{mod}p)$$

$b_k=-1$ khi và chỉ khi phần dư khi lấy ka chia cho p lớn hơn p' tức là $ka=pq+r$.
$r>\frac{p-1}{2}$ khi và chỉ khi

$$\frac{2ka}{p}=2p+\frac{2r}{p}\Leftrightarrow\left[\frac{2ka}{p}\right]=2p+1=2\left[\frac{ka}{p}\right]+1\Leftrightarrow b_k=(-1)^{\left[\frac{2ka}{p}\right]}$$

Vậy $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} \left[\frac{2ka}{p}\right]}$ (đpcm).

Từ định lý trên ta có thể thu được các hệ quả sau.

Định lý 6.0.7.

a/$\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$

b/-2 là thặng dư bậc 2 mod p khi và chỉ khi $p \equiv 1; 3(\text{mod}8)$

c/ -3 là thặng dư bậc 2 mod p khi và chỉ khi $p \equiv 1(\text{mod}6)$

d/ 3 là thặng dư bậc 2 mod p khi và chỉ khi $p \equiv \pm 1(\text{mod}12)$

e/ 5 là thặng dư bậc 2 mod p khi và chỉ khi $p \equiv \pm 1(\text{mod}10)$

Định lý 6.0.8. Luật tương hỗ

Nếu p,q là các số nguyên tố lẻ và p khác q thì

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

Bài tập ví dụ

Bài tập 6.1. Chứng minh rằng với mọi số nguyên tố $p = 4k + 3$, nếu $x^2 + y^2 \vdots p$ thì $\begin{cases} x \vdots p \\ y \vdots p \end{cases}$

Lời giải

Giả sử $x, y \not\vdots p \Rightarrow \left(\frac{x}{p}\right), \left(\frac{y}{p}\right) \neq 0$, ta có $\left(\frac{-y^2}{p}\right) = 1$.

Nhưng theo định lý 4b, 4c và 5, ta có $\left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$(vô lí!)

Do đó ta có $\begin{cases} x \vdots p \\ y \vdots p \end{cases}$

Bài tập 6.2. Chứng minh rằng với mọi số nguyên tố $p = 3k+2$ thì $m^2+mn+n^2 \vdots p \Leftrightarrow \begin{cases} m \vdots p \\ n \vdots p \end{cases}$

Lời giải

Giả sử $m, n \not\vdots p \Rightarrow \left(\frac{m}{p}\right), \left(\frac{n}{p}\right) \neq 0$.

Ta có

$$m^2+mn+n^2 \vdots p \Rightarrow 4\left(m^2+mn+n^2\right) \vdots p \Rightarrow (2m+n)^2+3n^2 \vdots p \Rightarrow \left(\frac{-3n^2}{p}\right) = 1 \Rightarrow \left(\frac{-3}{p}\right) = 1$$

Theo định lý 8c, ta suy ra đây là điều vô lí, do đó $m^2 + mn + n^2 \vdots p \Leftrightarrow \begin{cases} m \vdots p \\ n \vdots p \end{cases}$

Nhận xét :Các tính chất này dễ dàng chứng minh được bằng định lý Fermat, nhưng đây chỉ là

một ứng dụng khá cơ bản của thặng dư bình phương.
Các định nghĩa của thặng dư bình phương đôi khi được sử dụng để chứng minh một số bài toán khá thú vị. Chúng ta chỉ cần áp dụng những tính chất cơ bản để lập luận nhưng nó vẫn thể hiện được sức mạnh của thặng dư bình phương.

Bài tập 6.3. Chứng minh rằng với mọi số nguyên tố lẻ p:

$$\exists a \in \mathbb{Z}^+ : \begin{cases} \left(\frac{a}{p}\right) = -1 \\ a < 1 + \sqrt{p} \end{cases}$$

Lời giải

Gọi a là số tự nhiên nhỏ nhất không là thặng dư bậc hai mod p.
Đặt $b = \left(\frac{p}{a}\right) + 1 \Rightarrow 0 < ab - p < a$ do đó hiệu $ab - p$ là thặng dư bậc 2 mod p. Vậy

$$1 = \left(\frac{ab-p}{p}\right) = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -\left(\frac{b}{p}\right)$$

Suy ra b không là thặng dư bậc 2 mod p.
Do đó

$$a \leqslant b < \frac{p}{a} + 1 \Rightarrow a < \sqrt{p} + 1$$

Bài tập 6.4. (Korea Final 2000) Cho số nguyên tố $p = 4k + 1$, hãy tính

$$\sum_{x=1}^{p-1} \left(\left[\frac{2x^2}{p}\right] - 2\left[\frac{x^2}{p}\right] \right)$$

Lời giải

Đầu tiên, ta có nhận xét:

$$[2x] - 2[x] \leqslant 1 \forall x \in \mathbb{R}$$

Đẳng thức xảy ra khi và chỉ khi $\{x\} \geqslant \frac{1}{2}$.
Thế nên, nhiệm vụ của chúng ta bây giờ là tìm số đồng dư của một số chính phương khi chia cho số nguyên tố $p = 4k + 1$ sao cho nó lớn hơn $\frac{p-1}{2}$.
Theo tính chất số 1 của thặng dư bình phương, ta có đúng $\frac{p-1}{2}$ số chính phương mod p.
Bởi vì $p = 4k + 1 \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow \left(\frac{-a^2}{p}\right) = 1 \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{p-a}{p}\right)$.
Như vậy ,ta sẽ có đúng $\frac{p-1}{4}$ số chính phương mod p không lớn hơn hơn $\frac{p-1}{2}$ và đúng $\frac{p-1}{4}$ số chính phương mod plớn hơn $\frac{p-1}{2}$.
Do đó

$$\sum_{x=1}^{p-1} \left(\left[\frac{2x^2}{p}\right] - 2\left[\frac{x^2}{p}\right] \right) = \frac{p-1}{2}$$

vì nếu $\begin{cases} \forall i,j \in \mathbb{N} \\ 1 \leqslant i,j \leqslant p-1 \text{ thì } i^2 \equiv j^2 \,(\mathrm{mod} p). \\ i+j=p \end{cases}$

Bài tập 6.5. (Iran TST 2004) Cho trước số nguyên tố p và số nguyên dương k, chứng minh rằng tồn tại số nguyên dương n sao cho

$$\left(\frac{n}{p}\right) = \left(\frac{n+k}{p}\right)$$

Lời giải

Bài toán tương đương với việc chứng minh tồn tại n sao cho $\left(\frac{n\,(n+k)}{p}\right) = 1$.
Ta giả sử điều ngược lại, tức là giả sử tồn tại $1 \leqslant k \leqslant p-1$ sao cho $\left(\frac{n\,(n+k)}{p}\right) = -1 \forall 1 \leqslant n \leqslant p-1$.
Vì với mỗi số nguyên tố p bất kì, có đúng $\frac{p-1}{2}$ số không chính phương mod p. Do đó nếu $f\,(n,k,p) = n\,(n+k) \bmod p$ nhận nhiều hơn $\frac{p-1}{2}$ giá trị phân biệt thì tồn tại ít nhất 1 số chính phương mod p.
Vậy tập giá trị của $f\,(n,k,p)$ nhận không quá $\frac{p-1}{2}$phần tử, do đó theo nguyên lý Dirichlet, ta có ít nhất ba số x,y,z nguyên phân biệt sao cho

$$\begin{cases} 1 \leqslant x,y,z \leqslant p-1 \\ f\,(x,k,p) = f\,(y,k,p) = f\,(z,k,p) \end{cases}$$

Tức là

$$x\,(x+k) \equiv y\,(y+k) \equiv z\,(z+k)\,(\mathrm{mod} p) \Leftrightarrow \begin{cases} p|x+y+k \\ p|y+z+k \\ p|z+x+k \end{cases} \Leftrightarrow x \equiv y \equiv z\,(\mathrm{mod} p)$$

Điều này vô lí vì x,y,z phân biệt và $1 \leqslant x,y,z \leqslant p-1$. Do đó ta có điều phải chứng minh.
Nhận xét: Rõ ràng là trong hai bài toán này, ta chủ yếu dùng định lý số 1 và định lý số 2 làm cơ sở lập luận.
Thặng dư bình phương cũng rất hữu dụng trong giải phương trình nghiệm nguyên, ta cùng xét đến ví dụ sau:

Bài tập 6.6. (Serbia-2008) Tìm tất cả nghiệm nguyên không âm của phương trình :

$$12^x + y^4 = 2008^z$$

Lời giải

Nếu $z > 0$ thì $y > 0$.
Nếu x chẵn thì VT có dạng $a^2 + b^2$, nếu x lẻ thì VT có dạng $a^2 + 3b^2$.

Dễ thấy 2008 có ước nguyên tố là 251 , a,b đều không chia hết cho 251 . Từ đây ta có -1 hoặc -3 sẽ là các số chình phương mod 251 .Tức là

$$\left(\frac{-1}{251}\right) = 1 \ \vee \left(\frac{-3}{251}\right) = 1$$

Mà

$$\begin{cases} \left(\frac{-1}{251}\right) = (-1)^{\frac{251-1}{2}} = -1 \\ \left(\frac{-3}{251}\right) = -\left(\frac{3}{251}\right) = -(-1)^{\frac{251-1}{2}} \left(\frac{251}{3}\right) = \left(\frac{2}{3}\right) = -1 \end{cases}$$

Suy ra $x = y = z = 0$.

Kí hiệu Jakobil

Không dừng lại ở tập số nguyên tố, các tính chất của thặng dư bình phương còn có thể mở rộng ra cho cả hợp số. Do không sợ nhầm lẫn nên tương tự như kí hiệu Legendre, kí hiệu Jakobil được viết dưới dạng $\left(\frac{a}{n}\right)$.
Một số tính chất của kí hiệu Jakobil:
Với n là số tự nhiên lẻ và a nguyên, $(a, n) = 1$ ta có các định lý sau:

Định lý 6.0.9.
Với mọi a, b: $a \equiv b \,(\mathrm{mod} n) \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

Định lý 6.0.10.
Đặt $n = \prod {p_i}^{a_i}$, với p_i là ước nguyên tố của n, ta có:

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{{p_i}^{a_i}}\right) = \prod \left(\frac{a}{p_i}\right)^{a_i}$$

Hay nói một cách khác

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right) \ \forall m, n \in \mathbb{Z}^+$$

Nhưng lưu ý: a là số chính phương mod n khi và chỉ khi a phải là số chính phương mod p_i với mọi p_i là ước nguyên tố của n. Ta sẽ tiến hành chứng minh hai bước:
1. $\left(\frac{a}{{p_i}^{a_i}}\right) = \left(\frac{a}{p_i}\right)^{a_i}$
2. $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$ khi $\gcd(p, q) = 1$

Định lý 6.0.11. Ta có kí hiệu Jakobil là một hàm nhân tính hoàn toàn, bởi vì:

$$\left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right) \forall a, b \in \mathbb{Z}$$

Hệ quả: $\left(\frac{a^2}{n}\right) = 1$

Định lý 6.0.12.

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

Định lý 6.0.13.

$$\left(\frac{2}{n}\right) = (-1)^{\frac{(n-1)(n+1)}{8}}$$

Định lý 6.0.14.

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\left(\frac{n-1}{2}\right)\left(\frac{m-1}{2}\right)}$$

Bài tập ví dụ

Bài tập 6.7. Cho $m, n \in \mathbb{Z}^+$ sao cho $n+1 \vdots 4m$, hãy chứng minh $\left(\frac{-m}{n}\right) = -1$.

Lời giải

Ta giả sử điều ngược lại là $\left(\frac{-m}{n}\right) = 1$.
Vì tính chẵn lẻ của m không quan trọng cho nên ta có thể coi như m là số lẻ.
Đầu tiên, ta có nhận xét: $\left(\frac{-1}{k}\right) = 1 \Leftrightarrow k - 1 \vdots 4$
Vì $n+1 \vdots 4m \Rightarrow \left(\frac{-1}{n}\right) = -1$ theo nhận xét trên.
Do đó $\left(\frac{m}{n}\right) = \left(\frac{-m}{n}\right)\left(\frac{-1}{n}\right) = -1$.
Vì $n+1 \vdots 4m \Rightarrow \gcd(m,n) = 1$ nên ta có thể áp dụng luật nghịch đảo bình phương, ta có:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)}{2}\cdot\frac{(n-1)}{2}} \Leftrightarrow \left(\frac{n}{m}\right) = \frac{(-1)^{\frac{(m-1)}{2}}}{-1} \text{ do } \left(\frac{-1}{n}\right) = -1$$

Nếu $m = 4t+1 \Rightarrow \left(\frac{-1}{m}\right) = 1 \Rightarrow \left(\frac{n}{m}\right) = -1 \Rightarrow \left(\frac{-n}{m}\right) = -1$.
Nhưng vì $n+1 = 1^2 + n \vdots 4m \Rightarrow \left(\frac{-n}{m}\right) = 1$, mâu thuẫn.
Với trường hợp còn lại, ta cũng dễ dàng suy ra được điều vô lí, do đó $\left(\frac{-m}{n}\right) = 1$ là không thể, suy ra đpcm.

Bài tập 6.8. (Korea 1999) Tìm mọi số nguyên dương n sao cho $2^n - 1 \vdots 3$ và tồn tại số nguyên m sao cho

$$2^n - 1 \mid 4m^2 + 1$$

Lời giải

Ta có nhận xét nếu $x^2 + 1 \vdots p \Leftrightarrow p = 4k+1$ vì $2^n - 1 \vdots 3 \Rightarrow n \vdots 2$.
• Điều kiện cần:
Ta sẽ chứng minh số nguyên dương cần tìm là một luỹ thừa của 2.
Giả sử $n \vdots q \left(q > 1, q \not\vdots 2\right)$, ta có: $2^n - 1 \vdots 2^q - 1$.
Nhưng $\begin{cases} 2^q - 1 \not\vdots 3 \\ 2^q + 1 \vdots 4 \end{cases}$, do đó $2^q - 1$ có ước nguyên tố dạng $4k+3$ khác 3, vô lý.
Vậy ta có nếu tồn tại số nguyên m sao cho $2^n - 1 | 4m^2 + 1$ thì n là một luỹ thừa của 2.
• Điều kiện đủ:
Theo chứng minh trên, ta có $2^{2^k} - 1$ không có ước nguyên tố dạng dạng $4k+3$ khác 3, hơn nữa

$2^{2^k}-1 \not\vdots 9$, ta phân tích thành các thừa số nguyên tố $\frac{2^n-1}{3}=\prod p_i^{a_i}$
Áp dụng kí hiệu Jakobil, ta có:

$$\left(\frac{-1}{\frac{2^n-1}{3}}\right)=\left(\frac{-1}{\prod p_i^{a_i}}\right)=\prod\left(\frac{-1}{p_i^{a_i}}\right)=\prod\left(\frac{-1}{p_i}\right)^{a_i}=1$$

Do đó, tồn tại số nguyên t sao cho

$$\begin{aligned}&t^2+1\vdots\frac{2^n-1}{3}\\&\Leftrightarrow 2^{2^k}t^2+1+2^{2^k}-1\vdots\frac{2^{2^k}-1}{3}\\&\Leftrightarrow 2^{2^k}t^2+1\vdots\frac{2^{2^k}-1}{3}\\&\Leftrightarrow 4u^2+1\vdots\frac{2^{2^k}-1}{3}\end{aligned}$$

Kết thúc chứng minh.
Bình luận: Trong cuốn sách số học của Titu Andreescu thì có lời giải liên quan đến số nguyên tố Fermat và định lý thặng dư Trung Hoa, nhưng ở đây khi sử dụng kí hiệu Jakobil, bài toán này trở nên đơn giản.

Khai thác một bổ đề

Bây giờ xin giới thiệu độc giả một bổ đề rất thú vị sau:

Chứng minh rằng với mọi số nguyên dương a không phải là số chính phương, tồn tại vô số số nguyên tố p sao cho

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

Chứng minh bổ đề

Phân tích a thành các thừa số nguyên tố, ta có $a=2^t\prod_{i=1}^{n}p_i^{a_i}$, để cho đơn giản, ta giả sử số đó là số square-free (tức là số không có ước là bình phương của một số nguyên tố) $\Rightarrow a_i=1, t\in\{0;1\}$.
Chọn s là số không chính phương modulo p_n.
Sử dụng định lý thặng dư Trung Hoa, ta dễ dàng tìm được một số nguyên v sao cho

$$\begin{cases}v\equiv 1\,(\mathrm{mod}8)\\v\equiv 1\,(\mathrm{mod}p_i)\,(1\leqslant i\leqslant n-1)\\v\equiv s\,(\mathrm{mod}p_n)\end{cases}$$

Đặt $v=\prod_{j=1}^{m}q_j$, với q_j là ước nguyên tố ta có:

$$\prod_{i=1}^{m}\left(\frac{2}{q_i}\right)=\left(\frac{2}{v}\right)=(-1)^{\frac{v^2-1}{8}}$$

Và theo định lý nghịch đảo bình phương, ta có:

$$\prod_{j=1}^{m}\left(\frac{p_i}{q_j}\right)=\prod_{j=1}^{m}(-1)^{\frac{(p_i-1)\left(q_j-1\right)}{2}}\left(\frac{q_j}{p_i}\right)=\left(\frac{v}{p_i}\right)\forall 1\leqslant i\leqslant n$$

Do đó

$$\prod_{j=1}^{m}\left(\frac{a}{q_j}\right)=\left[\prod_{j=1}^{m}\left(\frac{2}{q_j}\right)\right]^2\prod_{j=1}^{m}\prod_{i=1}^{n}\left(\frac{p_i}{q_j}\right)=\prod_{i=1}^{n}\left(\frac{v}{p_i}\right)=\left(\frac{v}{p_n}\right)=\left(\frac{s}{p_n}\right)=-1$$

Suy ra rằng phải có q_j sao cho $\left(\frac{a}{q_j}\right)=-1$, mà vì có vô số số như vậy nên ta có dpcm. Với trường hợp $a=2$ thì bài toán hiển nhiên đúng.
Bổ đề này lúc đầu nhìn vào thì ta tưởng như không có ứng dụng nhiều, nhưng trên thực tế nó có thể có những ứng dụng rất bất ngờ, điển hình là bài toán sau:

Bài tập 6.9. (CWMO 2011) Tìm mọi cặp số nguyên (a,b) sao cho với mọi số nguyên dương n, ta có

$$n\mid a^n+b^{n+1}$$

Lời giải

Chọn $n=p$ với p là số nguyên tố lẻ đủ lớn, ta có

$$a^p+b^{p+1}\equiv a+b^2\equiv 0\,(\mathrm{mod}p)\Rightarrow\left(\frac{-a}{p}\right)=1\ \forall p\geqslant p_0$$

Với p_0 là số nguyên tố lẻ đủ lớn thoả mãn $\gcd(a,p_0)=1$.
Mà theo bổ đề quen thuộc là nếu x không là số chính phương thì tồn tại vô số số nguyên tố lẻ p sao cho $\left(\frac{x}{p}\right)=-1$, do đó ta phải có $-a$ là một số chính phương.
Tương tự, chọn $n=2p$ với p là số nguyên tố lẻ đủ lớn thì ta có

$$\left(\frac{-b^{2p+1}}{p}\right)=1\ \forall p\geqslant p_0\Rightarrow\left(\frac{-b}{p}\right)=1\ \forall p\geqslant p_0$$

Từ đây suy ra $-b$là một số chính phương. Tiếp tục chọn $n=p$ với p là số nguyên tố lẻ, đặt $-a=k^2,-b=l^2$ ta có

$$\left(-k^2\right)^p+\left(-l^2\right)^{p+1}\vdots p\Leftrightarrow l^4-k^2\equiv 0\,(\mathrm{mod}p)\ \text{(theo định lý Fermat nhỏ)}$$

Do đó ta lại có $l^2\pm k\equiv 0\,(\mathrm{mod}p)$ với vô số số nguyên tố p, vì vậy ta lại suy ra tiếp $(\pm k)^2$ là một luỹ thừa bậc 4.
Tương tự, chọn $n=2p$ với p là số nguyên tố lẻ thì ta lại có tiếp $(\pm l)^2$ là một luỹ thừa bậc 4.
Lập lại quá trình này vô hạn lần, ta có $-a,-b$ là luỹ thừa bậc 2^t tuỳ ý, do đó $\left[\begin{array}{l}-a=-b=1\\-a=-b=0\end{array}\right.$.
Vậy ta có $(a,b)\in\{(0,0),(-1,-1)\}$.

Bài tập 6.10. (Mathlink contest 2004) Cho 2004 số nguyên không âm $a_1, ..., a_{2004}$ sao cho $\sum_{i=1}^{2004} a_i^n$ là số chính phương với mọi n. Tìm số số hạng nhỏ nhất bằng không.

Lời giải

Chọn số nguyên tố lẻ p sao cho p không là ước của bất kì số nào trong các số đã cho, áp dụng định lý Fermat nhỏ, ta có:

$$\sum_{i=1}^{2004} a_i^{p-1} \equiv k \,(\mathrm{mod} p) \Rightarrow \left(\frac{k}{p}\right) = 1$$

Do $\sum_{i=1}^{2004} a_i^n$ là số chính phương với mọi n.
Vì chỉ có hữu hạn p sao cho $\left(\frac{k}{p}\right) = -1$ nên theo bổ đề trên, ta có k là số chính phương, mà

$$k \leqslant 2004 < 2025 = 45^2 \Rightarrow k \leqslant 44^2$$

Do đó, số số hạng bằng không nhỏ nhất là $2004 - 1936 = 68$.
Ta chỉ ra rằng $a_1 = a_2 = ... = a_{1936} = t^2, a_{1937} = ... = a_{2004} = 0$ thoả mãn đề bài.

Bài tập đề nghị

1. **(Bulgaria NMO 1998)**Cho m, n là 2 số tự nhiên sao cho $A = \frac{(m+3)^n+1}{3m}$ là số nguyên. Chứng minh rằng A lẻ.

2. **(Poland 2013)** Cho các số nguyên a,b sao cho $3 + a + b^2$ chia hết cho $6a$. Chứng minh rằng a âm.

3. Chứng minh rằng $3^n + 1$không có ước nguyên tố có dạng $3k + 2$ nếu n là số nguyên dương lẻ.

4. Chứng minh rằng $2^n - 1$luôn có ước nguyên tố có dạng $8k + 7$ nếu n là số nguyên dương lẻ.

5. **(Vietnam TST 2003 P6)** Cho số nguyên dương n. Chứng minh rằng $2^n + 1$ không có ước nguyên tố dạng $8k - 1$.

6. Chứng minh rằng với mọi số nguyên tố p, tồn tại các số nguyên x, y sao cho $x^2 + y^2 + 1 \vdots p$.

7. **(Korea Final 2000 P1)** Chứng minh rằng với mọi số nguyên tố , tồn tại các số nguyên x, y, z và sao cho $x^2 + y^2 + z^2 = wp$và $0 < w < p$.

8. **(IMO Shortlist 1998 N5)**Tìm mọi số nguyên dương n sao cho tồn tại số nguyên m để $2^n - 1$ là ước của $m^2 + 9$.

9. **(Czech-Polish-Slovak MO 2008)** Chứng minh rằng tồn tại số nguyên dương n sao cho với mọi số nguyên dương k thì $k^2 + k + n$ không có ước nguyên tố nhỏ hơn 2008.

10. **(AMM)** Tìm mọi số nguyên dương n sao cho $2^n - 1 | 3^n - 1$.

11. Nếu $p = 2^n + 1\,(n \geqslant 2)$ là số nguyên tố thì chứng minh rằng

$$3^{\frac{p-1}{2}} + 1 \vdots p$$

12. **(Sierpinski)** Chứng minh rằng ta không thể tìm được số nguyên dương $n > 1$ sao cho $2^{n-1} + 1 \vdots n$.

13. **(AoPS)** Cho 3 số nguyên a, b, c, chứng minh rằng a, b, c, abc không là số chính phương khi và chỉ khi tồn tại vô số số nguyên tố p sao cho

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

14. **(Iran TST 2013)** Có tồn tại các số nguyên a,b,c sao cho

$$a^2 + b^2 + c^2 \vdots 2013(ab + bc + ca)$$

15. **(IMO Shortlist 2009 N7)** Cho a, b là hai số nguyên phân biệt, chứng minh rằng tồn tại số nguyên dương n sao cho $(a^n - 1)\,(b^n - 1)$ không là số chính phương.

Cấp và căn nguyên thủy

Phạm Tiến Kha [1]

Cấp và căn nguyên thủy là các công cụ hết sức hữu dụng trong việc giải các bài toán số học sơ cấp. Không những thế, chúng còn là cầu nối để ta bước lên các khái niệm, định lý cao cấp trong toán học. Bài viết này xin trình bày một số ứng dụng của cấp và căn nguyên thủy trong các bài toán Olympiad.

Cấp của một số nguyên dương

ĐỊNH NGHĨA: Cho $(a,n)=1$. Số $h \geqslant 1$ được gọi là cấp của a modulo n , kí hiệu $h = o_n(a)$, nếu h là số nguyên dương nhỏ nhất thoả mãn

$$a^h \equiv 1 \mod n$$

Từ định nghĩa về cấp, ta rút ra được tính chất quan trọng sau:

$$\text{Nếu } n|a^k - 1 \text{ thì } o_n(a)|k$$

Chứng minh tính chất trên đơn giản. Đặt $o_n(a) = h$, và giả sử $k = lh + r$. Chú ý rằng:

$$a^k \equiv a^{hl}.a^r \equiv a^r \equiv 1 \mod n$$

Do $r < h$ nên theo định nghĩa về cấp, suy ra $r = 0$, hay $h|k$.
Ta bắt đầu với một bài toán quen thuộc về cấp:

Bài 1. *Chứng minh rằng mọi ước nguyên tố lẻ p của số $a^{2^n}+1$, trong đó $a > 1$ là số tự nhiên bất kì, đều thoả mãn*

$$p \equiv 1 \mod 2^{n+1}$$

Giải. Từ giả thiết suy ra $p|a^{2^{n+1}} - 1$. Đặt $h = o_p(a)$ thì $h|2^{n+1}$, và theo định lý Fermat nhỏ thì $h|p-1$.
Giả sử $h < 2^{n+1}$, tức là $h|2^n$. Suy ra $p|a^{2^n} - 1$. Mặt khác, theo giả thiết thì $p|a^{2^n} + 1$. Suy ra $p|2$ (!). Do đó $h = 2^{n+1}$, hay

$$p \equiv 1 \mod 2^{n+1}.\square$$

Bài toán này quen thuộc đến nỗi nó trở thành một bổ đề cho rất nhiều bài toán khác về cấp. Ta lần lượt xét các bài toán như vậy.

[1]Lớp 12CT THPT chuyên Lê Hồng Phong

Bài 2. *Chứng minh rằng tồn tại vô hạn số nguyên tố có dạng $2^n k + 1$ với n cố định.*

Giải. Rõ ràng bài toán này có liên quan mật thiết, hay nói cách khác là một hệ quả trực tiếp của Bài 1. Việc còn lại của ta là cần tìm a để dãy $x_n = a^{2^n} + 1$ có các số hạng đôi một nguyên tố cùng nhau.
Xét dãy Fermat $F_n = 2^{2^n} + 1$. Ta chứng minh $(F_n, F_m) = 1$ với mọi $m \neq n$.
Thật vậy, chú ý đẳng thức sau:

$$F_n - 2 = F_{n-1} F_2 \cdots F_0$$

Từ đây dễ dàng suy ra với mọi $m \neq n$ thì $(F_n, F_m) = 1$, và bài toán cũng được giải quyết.□

Nhận xét: Dãy Fermat $F_n = 2^{2^n} + 1$ và đại lượng 2^{2^n} rất phổ biến trong các bài toán về cấp, và ta sẽ tiếp tục gặp dãy này trong lời giải các bài toán sau.

Bài 3. *Cho $n > 1$, a là số nguyên dương thoả mãn $n | a^n + 1$. Chứng minh rằng*

$$(a + 1, n) > 1$$

Giải. Gọi p là ước nguyên tố bé nhất của n, và đặt $o_n(a) = h$. Từ giả thiết suy ra $h | 2n$ và $h | p - 1$. Do tính bé nhất của p nên $(n, p - 1) = 1$. Do đó

$$h | (2n, p - 1) = (2, p - 1) = 1, 2$$

- Nếu $h = 1$ thì $p | a - 1$, mà $p | a^n + 1$ nên $p = 2$. Khi đó $2 | (a + 1, n)$.
- Nếu $h = 2$ thì $p | a^2 - 1$, lại theo định nghĩa của h nên suy ra $p | a + 1$. Khi đó $p | (a + 1, n)$.□-

Nhận xét: Nếu p là số nguyên tố và $n | (p - 1)^n + 1$ thì $p | n$.

Bài 4. *Tìm tất cả cặp số nguyên dương (m, n) thoả mãn*

$$\begin{cases} n | 2^{m-1} + 1 \\ m | 2^{n-1} + 1 \end{cases}$$

Giải. Với $m = 1$ thì $n = 1, 2$ và ngược lại. Ta xét trường hợp $m, n > 1$.
Đặt $m - 1 = 2^a.x, n - 1 = 2^b.y$, trong đó a, b, x, y nguyên dương và xy lẻ. Gọi p là một ước nguyên tố của n thì

$$p | 2^{m-1} + 1 = (2^x)^{2^a} + 1$$

Theo Bài 1 thì $p \equiv 1 \mod 2^{a+1}$. Suy ra n cũng có dạng $2^{a+1}.k + 1$, hay $n - 1 = 2^{a+1} k$. Suy ra $b \geqslant a + 1$.

Tương tự, ta cũng suy ra được $a \geqslant b+1$, và điều này mâu thuẫn với $b \geqslant a+1$.
Tóm lại, $(m,n) = (1,1),(1,2),(2,1)$.□

Bài 5. *Cho $(a,b) = 1$ là hai số nguyên dương không đồng thời bằng 1, và p là số nguyên tố lẻ thoả mãn $p|a^{2^n} + b^{2^n}$ thì*

$$p \equiv 1 \mod 2^{n+1}$$

Giải. Lại một bài toán với hình thức gần như tương tự với Bài 1. Ở đây ta chỉ cần một bước chuyển nhỏ: chú ý rằng $(b,p) = 1$ (nếu không thì $p|a$ và $p|(a,b)$, trái giả thiết) nên tồn tại b' thoả mãn

$$bb' \equiv 1 \mod p$$

Do đó từ giả thiết suy ra

$$p|(ab')^{2^n} + 1$$

Và ta bắt gặp lại Bài 1. Bài toán được giải quyết.□

Một khởi đầu nhẹ nhàng cho bài viết, và đã đến lúc đẩy độ khó của các bài toán lên một bậc. Những bài toán tiếp sau sẽ cần những suy luận dài hơi và tinh tế hơn.

Bài 6. (**Hàn Quốc 1999**) *Tìm tất cả số n nguyên dương sao cho tồn tại m thoả mãn*

$$\frac{2^n - 1}{3} | 4m^2 + 1$$

Giải. Rõ ràng với n lẻ thì $2^n - 1 \equiv -2 \mod 3$ nên $2^n - 1$ không chia hết cho 3. Do đó n chẵn. Ta có bổ đề quen thuộc sau:

Các số có dạng $x^2 + 1$ thì không có ước nguyên tố dạng $4k + 3$

Do n chẵn nên $2^n - 1 \equiv 3 \mod 4$. Nếu n có ước nguyên tố lẻ thì $2^n - 1$ có ước nguyên tố $p \neq 3$ dạng $4k + 3$. Khi đó $p|(2m)^2 + 1$, mâu thuẫn bổ đề.
Do đó $n = 2^k$. Ta chứng minh với mọi n như vậy luôn tồn tại m thoả mãn đề bài.
Chú ý kí hiệu về số Fermat $F_n = 2^{2^n} + 1$. Như vậy

$$\frac{2^n - 1}{3} = F_{k-1}F_{k-2}\cdots F_1$$

Lại do tính đôi một nguyên tố cùng nhau của các số Fermat nên theo định lý Thặng dư Trung Hoa, tồn tại c chẵn thoả

$$c^2 \equiv 2^{2^{i-1}} \mod 2^{2^i}, i = \overline{1, k-1}$$

Chọn $m = \frac{c}{2}$, ta có đpcm.□

Bạn đang thắc mắc về bài toán trên, vì nó không liên quan đến cấp? Hãy tiếp tục theo dõi bài toán sau.

Bài 7. *Cho n là số thoả mãn tồn tại m sao cho $\frac{2^n-1}{3}|4m^2+1$.*

Chứng minh rằng với mọi ước nguyên dương d của $\frac{2^n-1}{3}$, luôn tồn tại q nguyên dương sao cho

$$d \equiv 1 \mod 2^q$$

Giải. Rõ ràng với bổ đề là Bài 6, bài toán này đã trở nên đơn giản hơn rất nhiều. Theo kết quả Bài thì:

$$\frac{2^n-1}{3} = F_{k-1}F_{k-2}\cdots F_1$$

Theo Bài 1 thì với mọi i, mọi ước nguyên tố p_i của số F_i đều thoả mãn $p_i \equiv 1 \mod 2^{i+1}$. Do đó với một ước nguyên dương bất kì $d = p_{i_1}^{a_1}p_{i_2}^{a_2}\cdots p_{i_l}^{a_l}$, chọn $q = \min\{i_1, i_2, \cdots, i_l\}$, ta được:

$$d \equiv 1 \mod 2^q.\square$$

Ta tiếp tục với một kết quả của nhà toán học người Pháp Francois Édouard Anatole Lucas:

Bài 8. *Cho $n > 1$. Nếu p là số nguyên tố thoả $p|F_n = 2^{2^n}+1$ thì*

$$p \equiv 1 \mod 2^{n+2}$$

Giải. Đây là một mở rộng của Bài 1. Để giải bài toán này, trước hết ta cần một kiến thức về thặng dư chính phương:

Nếu p là số nguyên tố thoả $p \equiv 1 \mod 8$ thì tồn tại x để $x^2 \equiv 2 \mod p$

Đây là một kết quả cơ bản, và trong khuôn khổ bài viết này xin không nêu chứng minh ở đây. Trở lại bài toán của chúng ta. Do $n > 1$ và $p \equiv 1 \mod 2^{n+1}$ nên $p \equiv 1 \mod 8$. Do đó tồn tại x để

$$x^2 \equiv 2 \mod p$$

Luỹ thừa 2^n hai vế, ta được

$$x^{2^{n+1}} \equiv 2^{2^n} \equiv -1 \mod p$$

Suy ra

$$p|x^{2^{n+1}}+1$$

Sử dụng kết quả Bài một lần nữa, ta được đpcm.$\square$

Nhận xét: Mở rộng hơn nữa thì với mọi a thoả mãn tồn tại x mà $a \equiv x^2 \mod p$ (hay a thuộc hệ thặng dư chính phương của p), trong đó p là ước của $a^{2^n}+1$ thì

$$p \equiv 1 \mod 2^{n+2}$$

Ta tiếp tục đến với một kết quả hết sức thú vị trong kì thi chọn đội tuyển Trung Quốc:

Bài 9. (**Trung Quốc TST 2005**) *Chứng minh rằng với mọi $n > 2$, ước nguyên tố lớn nhất của số $2^{2^n}+1$ không bé hơn $(n+1)2^{n+2}+1$.*

Giải. Đặt $2^{2^n}+1 = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ với $p_1 < p_2 < \cdots p_r$.
Chú ý rằng $p_i \equiv 1 \mod 2^{n+1}$ nên tồn tại q_i sao cho

$$p_i = 1 + 2^{n+1}q_i$$

Viết lại hệ thức $2^{2^n}+1 = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ theo modulo 2^{2n+2}, ta có:

$$1 \equiv 1 + 2^{n+1}\sum_{i=1}^{r} k_i q_i \mod 2^{2n+2}$$

Suy ra

$$2^{n+1} \leqslant \sum_{i=1}^{r} k_i q_i \leqslant q_r \sum_{i=1}^{r} k_i$$

Mặt khác

$$2^{2^n}+1 > \left(1+2^{n+1}\right)^{k_1+k_2+\cdots+k_r} > 2^{(n+1)(k_1+k_2+\cdots k_r)}$$

Suy ra

$$\sum_{i=1}^{r} k_i < \frac{2^n}{n+1}$$

Do đó

$$q_r \geqslant \frac{2^{n+1}}{\sum_{i=1}^{r} k_i} \geqslant 2(n+1)$$

Vậy

$$p_r \geqslant (n+1)2^{n+2}+1.\square$$

Nhận xét: Với kết quả của Bài 8, ta được một phát biểu mạnh hơn:

Với mọi $n > 3$ thì ước nguyên tố lớn nhất của $2^{2^n}+1$ không bé hơn $(n+2)2^{n+4}+1$.

Một câu hỏi thú vị được đặt ra: giá trị bé nhất của ước nguyên tố bé nhất của các số dạng $2^{2^n}+1$ là bao nhiêu?

Tiếp theo, ta sẽ đi đến một định lý hết sức đẹp đẽ về số nguyên tố - Định lý Dirichlet:

Nếu a, b là hai số nguyên dương nguyên tố cùng nhau thì dãy $a+b, 2a+b, 3a+b, \ldots$ chứa vô hạn số nguyên tố.

Chứng minh định lý này hoàn toàn không dễ, và phải sử dụng đến các kiến thức của toán cao cấp. Trong khuôn khổ bài viết này, ta chỉ xét đến một trường hợp rất nhỏ của định lý Dirichlet, khi $b = 1$ và a là số nguyên tố.

Bài 10. (**Hàn Quốc TST 2003**) *Cho một số nguyên tố p bất kì, đặt*

$$f_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

a) Chứng minh rằng nếu $p|m$ thì mọi ước nguyên tố của $f_p(m)$ sẽ nguyên tố cùng nhau với $m(m-1)$.
b) Chứng minh rằng tồn tại vô hạn n nguyên dương để $pn + 1$ là số nguyên tố.

Giải. a) Gọi q là một ước nguyên tố của $f_p(m)$. Rõ ràng $(q, m) = 1$. Nếu $(q, m-1) \neq 1$ thì $q|m-1$. Khi đó $0 \equiv f_p(m) \equiv m \mod q$, suy ra $q|m$ (vô lí!).
b) Ta sẽ chứng minh tồn tại vô hạn số nguyên tố q mà $p|q-1$.
Gọi q là một ước nguyên tố bất kì của $f_p(m)$. Suy ra $q|m^p - 1$. Do p là số nguyên tố nên $o_q(m) = 1 \vee p$.
Nếu $o_q(m) = 1$ thì $q|m-1$, mâu thuẫn với kết quả câu a. Do đó $o_q(m) = p$, suy ra $p|q-1$.
Việc còn lại là xây dựng một dãy $\{m_k\}_{k\geqslant 1}$ để $f_p(m_k)$ chia hết cho vô hạn số nguyên tố.
Xét dãy $m_1 = p$, $m_k = pf_p(m_1)f_p(m_2)\cdots f_p(m_{k-1})$. Khi đó

$$f_p(m_1)f_p(m_2)\cdots f_p(m_{k-1})|f_p(m_k) - f_p(0) = f_p(m_k) - 1$$

Suy ra $f_p(m_k)$ nguyên tố cùng nhau với $f_p(m_1), f_p(m_2), \cdots, f_p(m_{k-1})$.□

Ta công nhận một mở rộng của bài toán trên:

Với mọi a nguyên dương thì dãy $a+1, 2a+1, \ldots$ chứa vô hạn số nguyên tố.

Sau đây ta sẽ xét đến một vài ứng dụng của định lý Dirichlet trong các bài toán Số học.

Bài 11. *Cho r là số nguyên tố. Đặt*

$$f_r(x) = x^{r-1} + x^{r-2} + \cdots + x + 1$$

Chứng minh rằng $f_r(x)$ chia hết cho vô hạn số nguyên tố với x là số nguyên tố.

Giải. Giả sử $f_r(p)$ chỉ chia hết cho hữu hạn số nguyên tố $q_1 < q_2 \cdots < q_k$
Theo định lý Dirichlet, tồn tại l sao cho $p = l.q_1q_2\cdots q_k + 1$là số nguyên tố. Suy ra

$$f_r(p) \equiv r \equiv 0 \mod q_i$$

với i bất kì thuộc $\{1, 2, \cdots k\}$.
Suy ra $r = q_i$. Hơn nữa, $f_r(p)$ chỉ chứa ước nguyên tố duy nhất q_i, vì nếu tồn tại $q_j \neq q_i$ mà $q_j|f_r(p)$ thì $r = q_j = q_i$, mâu thuẫn với sự phân biệt của q_i và q_j. Đặt $f_r(p) = q_i^s = r^s$. Chú ý $r|p-1$. Xét

$$v_r(f_r(p)) = v_r(p^r - 1) - v_r(p-1) = v_r(p-1) + v_r(r) - v_r(p-1) = 1$$

Suy ra $f_r(p) = r$. Tuy nhiên, chọn p đủ lớn thì $f_r(p) > r$, mâu thuẫn. Ta có đpcm.□

Nhận xét: Kết quả bài toán trên tổng quát hơn so với phần chứng minh trong Bài 11. Và ta cũng có thể kết luận hàm số $f_r(x)$ chia hết cho vô hạn số nguyên tố với mọi $x \in \mathbb{Z}$.

Bài 12. (**A.Makowski**) *Cho $k \geqslant 2$ là số nguyên dương. Chứng minh rằng tồn tại vô hạn hợp số n thoả mãn $n|a^{n-k} - 1$ với mọi a nguyên tố cùng nhau với n*

Giải. Chọn $n = kp$ với p là số nguyên tố. Ta cần $p|a^{n-k} - 1$ và $k|a^{n-k} - 1$. Chọn n sao cho $p - 1|n - k$, điều kiện đầu tiên được thoả mãn. Lại chọn n sao cho $\varphi(k)|n - k$, điều kiện thứ hai được thoả mãn. Tóm lại, ta cần chọn p sao cho $\varphi(k)|p - 1$, và chứng minh rằng tồn tại vô hạn p như vậy. Tuy nhiên đây lại là kết quả trực tiếp từ định lý Dirichlet, và bài toán được chứng minh hoàn toàn.□

Bài 13. *Cho $k \geqslant 1$ là số nguyên. Chứng minh rằng tồn tại số nguyên tố p và một dãy tăng nghiêm ngặt $a_1, a_2, \ldots$ thoả mãn $p + ka_1, p + ka_2, \ldots$ là số nguyên tố.*

Giải. Theo định lý Dirichlet thì tồn tại vô hạn số nguyên tố p thoả $p \equiv 1 \mod k$. Trước hết chọn một số nguyên tố p bất kì như vậy, và đặt $p = lk + 1$
Khi đó $p + ka_i = k(l + a_i) + 1$. Việc tồn tại một dãy tăng nghiêm ngặt $a_1, a_2, \ldots$ là hiển nhiên theo định lý Dirichlet.□

Bài 14. (**Định lý Hardy-Wright**) *Cho p là số nguyên tố lẻ. Chứng minh rằng luôn tồn tại x, y nguyên dương sao cho*

$$p|x^2 + y^2 + 1$$

Giải. • Nếu $p = 4k + 1$ thì -1 là số chính phương $\mod p$, tức tồn tại x sao cho $p|x^2 + 1$. Chọn $y = p$, ta có $p|x^2 + y^2 + 1$.
• Nếu $p = 4k + 3$:
Chú ý rằng $(4p, 2p - 1) = 1$. Xét dãy

$$1.4p + 2p - 1, 2.4p + 2p - 1, 3.4p + 2p - 1, \ldots$$

Theo định lý Dirichlet, tồn tại l sao cho $l.4p + 2p - 1$ là số nguyên tố. Khi đó

$$l.4p + 2p - 1 = (4l + 2)p - 1 \equiv 1 \mod 4$$

Theo một kết quả quen thuộc: mọi số nguyên tố dạng $4k + 1$ biểu diễn được dưới dạng tổng của hai số chính phương, suy ra tồn tại x, y để

$$l.4p + 2p - 1 = x^2 + y^2$$

Khi đó $p|x^2 + y^2 + 1$. Bài toán được chứng minh hoàn toàn.□

Bài 15. *Chứng minh rằng với mọi số nguyên tố p và a nguyên dương, số $a^p - 1$ luôn có ít nhất một ước nguyên tố q thoả mãn*

$$q \equiv 1 \mod p$$

Giải. Ta xét trường hợp $a > p$. Đặt $a^p - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k \alpha_k$. Ta có $o_{q_i}(a) = p \vee 1$ và $o_{q_i}(a) | q_i - 1$. Giả sử không tồn tại i sao cho $o_{q_i}(a) = p$. Khi đó với mọi $j = \overline{1,k}$ thì $q_j | a - 1$. Mặt khác:

$$a^{p-1} + a^{p-2} + \dots + a + 1 \equiv p \mod q_i, i = \overline{1,k}$$

Suy ra $(a^{p-1} + a^{p-2} + \dots + a + 1, q_i) = 1, \forall q_i \neq p$. Do đó $v_{q_i}(a^p - 1) = v_{q_i}(a - 1) = \alpha_i, \forall q_i \neq p$. Giả sử $p = q_j$. Suy ra $a^p - 1 | (a-1) q_j^{\alpha_j}$, hay $a^{p-1} + a^{p-2} + \dots + a + 1 \leqslant q_j^{\alpha_j} = p^{\alpha_j} \leqslant p^{p-1}$ (vô lí!). Trường hợp còn lại khi $a \leqslant p$ thì $(p, q_i) = 1, i = \overline{1,k}$. Từ đó tiếp tục giải như trên, ta cũng có đpcm.
Do đó, luôn tồn tại ước nguyên tố q của $a^p - 1$ thoả $q \equiv 1 \mod p$.□

Nhận xét: Với cách lí luận như trên, ta cũng có thể thay p bởi một luỹ thừa của p. Có thể thấy bài toán này gần giống với Bài 1, tuy nhiên thay vì "với mọi ước nguyên tố" như Bài 1 thì ở đây ta chỉ khẳng định "tồn tại một ước nguyên tố". Dạng tổng quát này có vẻ yếu hơn, nhưng đây lại là bắt nguồn để ta đi đến một định lý mạnh hơn rất nhiều-Định lý Zsigmondy:

Dạng 1:

> Với mọi $a > b \geqslant 1$ và $(a, b) = 1$ thì $a^n - b^n$ luôn có một ước nguyên tố p thoả mãn $p | a^n - b^n$, nhưng $p \nmid a^k - bk$ với mọi $1 \leqslant k < n$.
> (trừ các trường hợp $2^6 - 1^6$ và $a^2 - b^2$ với $a + b$ là một luỹ thừa của 2)

Dạng 2:

> Với mọi $a > b \geqslant 1$ thì $a^n + b^n$ luôn có một ước nguyên tố p thoả mãn $p | a^n + b^n$ nhưng $p \nmid a^k + b^k$ với mọi $1 \leqslant k < n$
> (trừ trường hợp $2^3 + 1^3$)

Ta sẽ không đề cập đến chứng minh khá dài của định lý này ở đây, mà chỉ xét một số ứng dụng của nó.

Bài 16. (Romanian TST) *Chứng minh rằng dãy $a_n = 3^n - 2^n$ không có ba số hạng nào lập thành một cấp số nhân.*

Giải. Giả sử tồn tại $x < y < z$ sao cho

$$(3^y - 2^y)^2 = (3^x - 2^x)(3^z - 2^z)$$

Từ đẳng thức trên suy ra mọi ước nguyên tố p của $3^x - 2^x$ đều chia hết $3^y - 2^y$. Tuy nhiên, do $x > y$ nên điều này mâu thuẫn định lý Zsigmondy. Ta có đpcm.□

Bài 17. (IMO SL 2000) *Tìm tất cả a, m, n nguyên dương thoả mãn*

$$a^m + 1 | (a+1)^n$$

Giải. Nếu $a \neq 3$ thì theo định lý Zsigmondy, $a^m + 1$ tồn tại một ước nguyên tố p mà $p \not| a+1$, mâu thuẫn với yêu cầu đề bài.
Nếu $m = 3, a = 2$. Khi đó mọi $n \geqslant 2$ đều thoả mãn

$$2^3 + 1 | (2+1)^n$$

Nếu $a = 1$ thì chọn m, n nguyên dương bất kì.
Vậy $(a, m, n) = (2, 3, x+2)$ với $x \in \mathbb{N}$ hay $(1, m, n)$. $\square$

Bài 18. (Nhật Bản 2011) *Tìm a, n, p, q, r nguyên dương thoả mãn*

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

Giải. Giả sử $p \geqslant q \geqslant r$, Nếu a, n không rơi vào các trường hợp ngoại lệ của định lý Zsigmondy, ta dễ dàng suy ra điều vô lí.
Nếu $a = 2, n = 6$, suy ra $p = 6, q = r = 1$.
Nếu $n = 2$ thì không tồn tại a, p, q, r.
Nếu $a = 1$ thì chọn n, p, q, r nguyên dương bất kì.
Tóm lại, $(a, n, p, q, r) = (1, n, p, q, r), (2, 6, 6, 1, 1), (2, 6, 1, 6, 1), (2, 6, 1, 1, 6)$.$\square$

Bài 19. (Iran) Cho A là một tập hữu hạn các số nguyên tố và $a > 1$ là số nguyên dương. Chứng minh rằng tồn tại hữu hạn n sao cho tất cả các ước nguyên tố của $a^n - 1$ đều thuộc A.

Giải. Giả sử $A = \{p_1, p_2, \cdots, p_k\}$. Ta xét $N = [p_1 - 1, p_2 - 1, \cdots, p_k - 1]$. Rõ ràng

$$p_i | a^N - 1, \forall i = \overline{1, k}$$

Khi đó, theo định lý Zsigmondy, với mọi $n_0 > N$, số $a^{n_0} - 1$ luôn có một ước nguyên tố q không phải là ước của $a^N - 1$, hay $q \notin A$.
Suy ra nếu n là số thoả điều kiện đề bài thì $n \leqslant N$, tức là chỉ có hữu hạn n như vậy.$\square$

Bài 20. (Ba Lan) *Cho $2 < q < p$ là hai số nguyên tố lẻ. Chứng minh rằng $2^{pq} - 1$ có ít nhất ba ước nguyên tố phân biệt.*

Giải. Theo định lý Zsigmondy, $2^{pq} - 1$ có ước nguyên tố r mà $r \not| 2^p - 1$ và $r \not| 2^q - 1$.
Lại theo định lý Zsigmondy, $2^p - 1$ có ước nguyên tố s mà $s \not| 2^q - 1$.
Hơn nữa, nếu tất cả các ước nguyên tố của $2^q - 1$ đều chia hết $2^p - 1$ thì $q | p$, vô lí vì p nguyên

tố. Do đó, $2^q - 1$ cũng có một ước nguyên tố t không chia hết $2^p - 1$.
Ba ước nguyên tố r, s, t chính là ba ước cần tìm.□

Bài 21. *Cho $a \in \mathbb{N}^*$. Gọi A là tập hợp các số tự nhiên n sao cho $n|a^n + 1$, và B là tập tất cả các ước nguyên tố của các phần tử trong A. Chứng minh rằng B hữu hạn.*

Giải. • Trường hợp n lẻ:
Gọi B_1 là tập hợp các ước nguyên tố của các phần tử lẻ trong A.
Từ giả thiết suy ra $n|a^{2n} - 1$. Gọi p là ước nguyên tố bé nhất của n và đặt $h = o_p(a)$. Khi đó $h|2n$ và $h|p - 1$. Suy ra $h|(2n, p - 1) = (2, p - 1) = 1 \vee 2$. Suy ra $p|a^2 - 1$, hay B_1 hữu hạn.
• Trường hợp n chẵn:
Gọi B_2 là tập hợp các ước nguyên tố của các phần tử chẵn trong A.
Đặt $n = 2n_1$ thì n_1 lẻ (nếu không thì $4|n| \left(a^{\frac{n}{2}}\right)^2 + 1$, vô lí). Từ đó lí luận tương tự trường hợp n lẻ, ta cũng suy ra B_2 hữu hạn.
Do B_1, B_2 hữu hạn nên $B = B_1 \cup B_2$ cũng hữu hạn.□

Nhận xét: Với cách lí luận tương tự, ta có bài toán quen thuộc (và cơ bản) sau đây:

$$\text{Nếu } n|2^n - 1 \text{ thì } n = 1$$

Tuy vậy, thật bất ngờ rằng bài toán đơn giản này cũng có một ứng dụng hết sức thú vị:

Bài 22. (Ba Lan) *Tìm tất cả đa thức với $f(n)$ có hệ số hữu tỉ thoả mãn*

$$f(n)|2^n - 1, \forall n \in \mathbb{N}$$

Giải. Chú ý rằng $f(n)|f(n + f(n))$ với mọi n. Suy ra

$$f(n)|f(n + f(n))|2^{n+f(n)} - 1$$

Suy ra

$$f(n)|2^{n+f(n)} - 2^n = 2^n \left(2^{f(n)} - 1\right)$$

Do $(2^n, f(n)) = 1$ với mọi n nên

$$f(n)|2^{(f(n)} - 1$$

Suy ra $f(n) = 1, \forall n \in \mathbb{N}$.□

Nhận xét: Một bài toán "có vẻ tương tự" dành cho bạn đọc:

$$\text{Tìm tất cả đa thức hệ số nguyên } f(n) \text{ thoả mãn } f(n)|2^n + 1, \forall n \in \mathbb{N}$$

Bài 23. *Tìm số nguyên tố p nhỏ nhất sao cho tồn tại a thoả mãn $p|a^{2^{21}} - a$ và $p \not| a^{2^k} - a$, $\forall 1 \leqslant k < 21$.*

Giải. Rõ ràng $(a,p)=1$ nên $p|a^{2^{21}-1}-1$. Đặt $h=o_p(a)$. Khi đó h thoả hệ điều kiện sau:

$$\begin{cases} h|2^{21}-1 \\ h \not| 2^k-1, \forall 1 \leqslant k < 21 \\ h|p-1 \end{cases}$$

Với mọi $1 \leqslant k < 21$, ta có một bổ đề quen thuộc

$$(2^{21}-1, 2^k-1) = 2^{(21,k)}-1 \leqslant 2^7-1 = 127$$

Do đó với mọi $p > 127$ thì điều kiện $h \not| 2^k-1, \forall 1 \leqslant k < 21$ được thoả mãn. Chọn $h=49$, khi đó giá trị nhỏ nhất của p là 197.
Tóm lại, giá trị nhỏ nhất của p là 197.□

Nhận xét: Bạn đọc hãy giải bài toán tương tự sau:

Tìm p nguyên tố nhỏ nhất sao cho tồn tại a thoả

$$\begin{cases} p|a^{2^{15}+1}-1 \\ p \not| a^{2^k+1}-1, \forall 1 \leqslant k < 15 \end{cases}$$

Bài 26. (**Fermat**) *Cho $p>3$ là số nguyên tố. Chứng minh rằng mọi ước dương của $\frac{2^p+1}{3}$ đều có dạng $2kp+1$.*
Giải. Trước hết nhận thấy rằng

$$v_3(2^p+1) = v_3(2+1)+v_3(p) = 1$$

nên mọi ước nguyên tố của số $\frac{2^p+1}{3}$ đều lớn hơn 3. Gọi q là ước nguyên tố bất kì của $\frac{2^p+1}{3}$. Khi đó $q|2^p+1$, suy ra $q|2^{2p}-1$. Gọi $h=o_q(2)$. Ta có $h|2p$, suy ra $h=1 \vee 2 \vee p \vee 2p$. Nếu $h=1$ thì $q|1$. Nếu $h=2$ thì $q|2^2-1=3$. Nếu $h=p$ thì $q|2^p-1$, suy ra $q|h$. Tất cả các trường hợp này đều vô lí. Do đó $h=2p$. Suy ra $h=2p|q-1$ hay $q \equiv 1 \mod 2p$. Từ đây dễ dàng kết luận rằng mọi ước dương của $\frac{2^p+1}{3}$ đều có dạng $2k+1$.□

Nhận xét: Bài toán có thể được tổng quát như sau:

- Cho $p,q>2$ là các số nguyên tố phân biệt. Khi đó tất cả ước dương của số $\frac{(q-1)^p+1}{q}$ đều có dạng $2kp+1$.

- Cho $p,q>2$ là các số nguyên tố phân biệt. Khi đó tất cả ước dương của số $\frac{(q+1)^p-1}{q}$ đều có dạng $2kp+1$.

Một số bài toán thú vị phát triển từ bài toán này:

★ Cho $p>2$ là số nguyên tố. Số nguyên dương a thoả ít nhất một trong hai điều kiện

sau:
i) a là bội số của 4;
ii) a lẻ và $(a,p)=1$.
Chứng minh rằng mọi ước dương của $\frac{(a-2)^p+2^p}{a}$ và $\frac{(a-1)^p+1}{a}$ đều có dạng $2kp+1$.

★ Cho số nguyên tố $p>3$. Chứng minh rằng mọi ước dương của $\frac{2^p+1}{3}$ đều có dạng $2kp+1$, và $k\equiv p \mod 4$ nếu ước đó là ước nguyên tố.

Bài 27. (**VN TST 1997**) *Chứng minh rằng tồn tại một hàm số f nhận giá trị nguyên thoả mãn*

$$2^n | 19^{f(n)} - 97$$

với mọi n nguyên dương.
Giải. Dễ thấy rằng

$$v_2(19^{2^{n-2}}-1) = v_2(19-1)+v_2(2^{n-2}) = n$$

nên $o_{2^n}(19)=2^{n-2}$.ngSuy ra 19^t chứa 2^{n-2} thặng dư phân biệt trong hệ thặng dư của 2^n.
Mặt khác, để ý rằng 19^t chỉ chứa các thặng dư lẻ, cụ thể $19^t \equiv 1,3 \mod 8$, mà 2^{n-2} là một nửa số thặng dư lẻ của 2^n, suy ra 19^t chứa tất cả thặng dư đồng dư với $1,3 \mod 8$ của 2^n.
Do $97\equiv 1 \mod 8$, suy ra tồn tại f để $19^{f(n)} \equiv 97 \mod 2^n$.□

Bài 28. (**Italian TST 2006**) *Cho số nguyên dương n. Gọi A_n là tập tất cả $a\in\mathbb{Z}, 1\leqslant a\leqslant n$ thoả mãn $n|a^n+1$*
a) Tìm tất cả n để $A_n\neq\varnothing$.
b) Tìm tất cả n để $|A_n|$ chẵn và khác không.
c) Liệu có tồn tại n để $|A_n|=130$ không?

Giải. a) Với n lẻ, ta chọn $a=n-1$.
Xét n chẵn, đặt $n=2n_1$. Khi đó $2n_1|(a^{n_1})^2+1$. Suy ra n_1 lẻ và n_1 chỉ có ước nguyên tố dạng $4k+1$. Tóm lại, $A_n\neq\varnothing$ khi n lẻ hoặc $n=2n_1$, trong đó n_1 lẻ và chỉ gồm các ước nguyên tố dạng $4k+1$.

b) Xét $n>2$ chẵn. Khi đó nếu $n|a^n+1$ thì $n|(n-a)^n+1$ (chú ý rằng $a\neq n_1$). Do đó nếu n chẵn thì $|A_n|$ chẵn.
Xét n lẻ. Chú ý rằng $\varphi(n)$ chẵn với mọi $n>2$, suy ra $\varphi(n)-2$ cũng chẵn.
Rõ ràng $(a,n)=1$. Xét $a\neq 1, n-1$ thoả $n|a^n+1$. Do $(a,n)=1$ nên tồn tại $2\leqslant b\leqslant n-2$ thoả $ab\equiv 1 \mod n$. Lại có $n|a^n+1$, suy ra $n|b^n+1$. Điều này có nghĩa là $|A_n\setminus\{n-1\}|$ chẵn, hay $|A_n|$ lẻ.
Tóm lại, $|A_n|$ chẵn khi n chẵn và $n>2$.

c) Giả sử tồn tại n thoả $|A_n|=130$. Theo câu b thì n chẵn. Đặt $n=2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, trong đó $p_i\equiv 1 \mod 4$ với mọi $i=\overline{1,k}$. Ta chứng minh bổ đề sau:

Cho số nguyên tố p. Phương trình $x^2\equiv -1 \mod p$ hoặc không có nghiệm, hoặc có

đúng 2 nghiệm modulo p.

Xét x thoả $x^2 \equiv -1 \mod p$. Giả sử tồn tại $y \neq x$ thoả mãn $y^2 \equiv 1 \mod p$. Khi đó $x^2 \equiv y^2 \mod p$, suy ra $x \equiv -y \mod p$, hay $y = p - x$.□
Trở lại bài toán. Do p_i đều có dạng $4l + 1$ nên -1 là số chính phương $\mod p_i^{\alpha_i}$. Theo bổ đề trên thì số nghiệm theo modulo n của phương trình $x^2 \equiv -1 \mod n$ là 2^k. Suy ra không tồn tại n để $|A_n| = 130$.□

Bài 29. (**IMO 2003**) *Chứng minh rằng với mọi số nguyên tố p, luôn tồn tại số nguyên tố q không phải là ước của $n^p - p$ với mọi $n \geqslant 1$.*

Giải. Với $p = 2$ thì $q = 5$. Xét p lẻ. Ta có

$$p^p - 1 = (p-1)(1 + p + p^2 + \cdots + p^{p-1})$$

Chú ý rằng $1 + p + p^2 + \cdots + p^{p-1}$ không đồng dư $1 \mod p^2$, nên sẽ có một ước nguyên tố q không có dạng $kp^2 + 1$. Ta chứng minh q thoả điều kiện đề bài.,, suy ra $q|p - 1$. Suy ra $0 \equiv 1 + p + p^2 + \cdots + p^{p-1} \equiv p \mod q$, hay $p = q$, vô lí.□

Bài 30. *Tìm các số nguyên $k, m, n > 0$ sao cho $k^m | m^n - 1$ và $k^n | n^m - 1$.*

Giải. Gọi $p \geqslant 3$ là ước nguyên tố của k. Giả sử $m > n$. Đặt $d = o_p(m)$. Suy ra

$$v_p(m^n - 1) = v_p(m^d - 1) + v_p\left(\frac{n}{d}\right) = o_p(m^d - 1)$$

Suy ra $p^m | m^d - 1$. Suy ra $p^m \leqslant m^d - 1 \leqslant m^{p-1} - 1 < m^p$. (1)
Mặt khác, $k^m \leqslant m^n - 1 < m^m - 1 < m^m$. Suy ra $p < k < m$.
Nếu $p \geqslant 3$ thì $m \geqslant 3$. Khi đó hàm số $f(x) = \frac{x}{\log x}$ đồng biến trên $[3, +\infty)$, suy ra $\frac{m}{\log m} > \frac{p}{\log p}$, hay $p^m > m^p$, mâu thuẫn (1).
Suy ra $p = 2$. Suy ra m, n lẻ.
Nếu $n = 1$ dễ dàng suy ra $m = 1$. Khi đó k bất kì.
Xét $m > n > 1$. Ta có $4|k^m|m^n - 1$, mà n lẻ nên $m \equiv 1 \mod 4$. Suy ra

$$v_2(m^n - 1) = v_2(m^d - 1)$$

Suy ra $2^m | m^d - 1$, suy ra $2^m \leqslant m^d - 1 = m - 1$, vô lí.
Tóm lại, $(m, n, k) = (1, 1, k), (m, n, 1)$.□

Căn nguyên thủy

ĐỊNH NGHĨA: Số nguyên dương a được gọi là căn nguyên thủy của n nếu $o_n(a) = \varphi(n)$.

Lưu ý rằng không phải số nguyên dương n nào cũng có căn nguyên thủy. Ta chứng minh được rằng n có căn nguyên thủy khi và chỉ khi $n = 2, 4, p^k, 2p^k$ với p là số nguyên tố lẻ. Sau

đây ta xét một số bài tập về căn nguyên thủy.

Bài 1. *Chứng minh rằng 2 là căn nguyên thủy của 3^n với mọi $n \geqslant 1$.*

Giải. Ta chứng minh bằng quy nạp. Dễ thấy khi $n = 1$, kết luận của bài toán là đúng. Giả sử kết luận trên đúng với $n = k$, tức là $2^{\varphi(3^k)} \equiv 2^{2.3^{k-1}} \equiv 1 \mod 3^k$. Gọi d là bậc của $2 \mod 3^{k+1}$. Do $2^d \equiv 1 \mod 3^{k+1}$ nên $2^d \equiv 1 \mod 3^k$, suy ra $2.3^{k-1}|d$. Mặt khác, $d|\varphi 3^{k+1} = 2.3^k$. Suy ra $d = 2.3^{k-1}$ hay $d = 2.3^k$. Ta chứng minh bổ đề sau bằng quy nạp:

$$2^{2.3^{n-1}} \equiv 1 + 3^n \mod 3^{n+1}$$

Bổ đề đúng với $n = 1$. Giả sử bổ đề đúng với $n = k$, suy ra

$$2^{2.3^{k-1}} = 1 + 3^k + 3^{k+1}.m$$

Lập phương hai vế

$$2^{3^k} = 1 + 3^{k+1} + 3^{k+2}.M$$

Suy ra

$$2^{2.3^k} \equiv 1 + 3^{k+1} \mod 3^{k+2}$$

Theo nguyên lý quy nạp, bổ đề được chứng minh. Suy ra $d = 2.3^k$. □

Nhận xét: Ta cũng chứng minh được bài toán sau: *2 là căn nguyên thủy của 5^n với mọi $n \geqslant 1$*

Bài 2. *Chứng minh rằng nếu $n = 3^{k-1}$ thì $2^n \equiv -1 \mod 3^k$.*

Giải. Theo Bài 1 thì 2 là căn nguyên thủy của 3^k, suy ra bậc của $2 \mod 3^k$ là $2n$. Suy ra $2^{2n} - 1 \equiv (2^n - 1)(2^n + 1) \equiv 1 \mod 3^k$. Mặt khác, $2^n - 1 \equiv (-1)^{3^{k-1}} - 1 \equiv 1 \mod 3$, suy ra $2^n + 1 \equiv 1 \mod 3^k$.□

Bài 3. *Cho $n \geqslant 2$ và $p = 2^n + 1$. Chứng minh rằng nếu $3^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$ thì p là số nguyên tố.*

Giải. Do $\frac{p-1}{2} = 2^{n-1}$ nên $3^{2^{n-1}} \equiv -1 \mod p$, suy ra $3^{2^n} \equiv 1 \mod p$, suy ra bậc của $3 \mod p$ là 2^n, hay $p-1$. Suy ra $p-1|\varphi(p)$, hay $p-1 \leqslant \varphi(p)$. Suy ra $\varphi(p) = p-1$, hay p là số nguyên tố. □

Bài 4. (**AMM**) *Xét $f(n)$ là ước chung lớn nhất của $2^n - 2, 3^n - 3, 4^n - 4, \ldots$ Xác định $f(n)$ và chứng minh rằng $f(2n) = 2$.*

Giải. Gọi p là một ước nguyên tố bất kì của $f(n)$. Dễ thấy $v_p(f(n)) = 1$, do $p||p^n - p$. Gọi a là căn nguyên thủy của p (do p nguyên tố nên tồn tại a như vậy). Do $(a, p) = 1$ và $p|a^n - a$, suy ra $p - 1|n - 1$. Với $p - 1|n - 1$ thì $p|m^n - k$ với mọi số nguyên dương m. Do đó hàm f được xác định như sau

$$f(n) = p_1p_2\cdots p_k \text{ với } p_i - 1|n-1,\ i = \overline{1,k}$$

Xét $f(2n)$. Theo cách xác định trên thì nếu $f(2n)$ có ước nguyên tố $q > 2$ thì $q-1$ là một ước chẵn của $2n-1$, vô lí. Do đó $f(2n) = 2$.□

Bài 5. *Cho $p \geqslant 2$ là số nguyên tố. Tìm tất cả số nguyên dương k sao cho*

$$p|1^k + 2^k + \cdots + (p-1)^k$$

Giải. Đặt $S_k = 1^k + 2^k + \cdots + (p-1)^k$. Với k là bội của $p-1$, ta có

$$S_k \equiv p - 1 \not\equiv 0 \mod p$$

Ta chứng minh rằng với mọi k không phải là bội của $p-1$ thì $p|S_k$.
Thật vậy, gọi a là căn nguyên thủy của p. Dễ dàng chứng minh rằng $\{0, a^1, a^2, \ldots, a^{p-1}\}$ là hệ thặng dư đầy đủ mod p. Suy ra $(a^1, a^2, \ldots, a^{p-1})$ là một hoán vị của $(1, 2, \ldots, p-1)$.
Suy ra

$$\begin{aligned} 1^k + 2^k + \cdots + (p-1)^k &\equiv \left(a^1\right)^k + \left(a^2\right)^k + \cdots \left(a^{p-1}\right)^k \\ &\equiv a^k\left(1 + a^k + \cdots a^{(p-2)k}\right) \\ &\equiv a^k.\frac{a^{(p-1)k} - 1}{a-1} \\ &\equiv 0 \mod p. \end{aligned}$$

Vậy với mọi k không phải là bội của $p-1$ thì $p|S_k$. □

Nhận xét: Bài toán trên có một ứng dụng đặc sắc như sau:
Cho a, b, c là các số nguyên và p là số nguyên tố. Chứng minh rằng tồn tại các số nguyên x, y, z không đồng thời chia hết cho p sao cho $p|ax^2 + by^2 + cz^2$.

TÀI LIỆU THAM KHẢO

1. Titu Andreescu, Gabriel Dospinescu, *Prolems from the book.*
2. Naoki Sato, *Number theory.*
3. Hà Duy Hưng, *Một số phương pháp giải toán số học sơ cấp.*
4. Các diễn đàn AoPS, MathScope.

Chuyên đề 8: Hàm phần nguyên và phần lẻ

Lưu Giang Nam [1]

Phần nguyên là một lĩnh vực hay và độc đáo của toán sơ cấp, cao cấp và ứng dụng.Có nhiều bài toán hay về phần nguyên đã được sử dụng làm đề thi học sinh giỏi các cấp, trong đó có rất nhiều các đề thi học sinh giỏi quốc gia và Olympic quốc tế. Mặt khác, hàm phần nguyên có những ứng dụng quan trọng không chỉ trong toán học phổ thông, mà còn trong nhiều vấn đề của toán ứng dụng và công nghệ thông tin (làm tròn số, tính gần đúng,...). Phần nguyên cũng thể hiện sự kết nối giữa tính liên tục và tính rời rạc, giữa toán giải tích và toán rời rạc nên khá thú vị. Tuy nhiên vì sự giới hạn của kiến thức nên trong bài viết này tác giả xin trình bày các tính chất, ứng dụng của phần nguyên trong phạm vi THPT.

Định nghĩa, tính chất và bài tập cơ bản

Định nghĩa

Phần nguyên của số thực x, kí hiệu $[x]$, là số nguyên lớn nhất không vượt quá x.
Phần lẻ của số thực x, kí hiệu $\{x\}$, là phần còn lại của x bỏ phần nguyên: $\{x\} = x - [x]$.
Giá trị nhỏ nhất giữa hai số $x - z$ và $x + 1 - z$ được gọi là khoảng cách từ x đến số nguyên gần nó nhất và được kí hiệu là]x[.
Số nguyên gần một số thực x nhất được kí hiệu là (x) và được gọi là số làm tròn của x

Các tính chất quen thuộc

1. $x = [x]$ nếu $x \in Z$
2. $x = \{x\}$ nếu $0 \leqslant x < 1$
3. $x - 1 < [x] \leqslant x$
4. Nếu $k \in Z$ thì $[x + k] = [x] + k, \{x + k\} = \{x\} + k$
5. $[x + y] - [x] - [y] \in \{0; 1\}$ suy ra $[x + y] \geqslant [x] + [y], \{x + y\} \leqslant \{x\} + \{y\}$
6. $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right], n \in N$

[1]Chuyên Phan Ngọc Hiển Cà Mau

7. Số các số nguyên dương chia hết cho n không vượt quá x là $\left[\frac{x}{n}\right]$

8. $\left[\frac{x+a}{b}\right] = \frac{x}{b}$, nếu $n \to +\infty$

9. $x \geqslant y \Leftrightarrow [x] \geqslant [y]$

10. Nếu $[x] = [y]$ thì $|x - y| \leqslant 1$

11. Trong hai số x và y có một số nguyên và một số không phải là số nguyên thì $0 < \{x\}+\{y\} < 1$

12. Với mọi x và y là các số thực ta có $[2x] + [2y] \geqslant [x] + [y] + [x + y] \geqslant 2([x] + [y])$

13. Nếu $\max\{\{x\}, \{y\}\} < \frac{1}{2}$ thì

$$[2\{x\}] + [2\{y\}] = 0 = [\{x\} + \{y\}] \text{ và } [2x] + [2y] + [x] + [y] + [x + y] = 2[x] + 2[y]$$

14. Nếu $\min\{\{x\}, \{y\}\} < \frac{1}{2} \leqslant max\{\{x\}, \{y\}\} \leqslant 2[x] + 2[y]$ thì

$[2\{x\}] + [2\{y\}] = 1 = [\{x\} + \{y\}] + 1$ và $[2x] + [2y] = [x] + [y] + [x + y] = 2[x] + 2[y] + 1$

15. Nếu $\frac{1}{2} \leqslant \min\{\{x\}, \{y\}\}$ thì

$[2\{x\}] + [2\{y\}] = 2 = [\{x\} + \{y\}] + 1$ và $[2x] + [2y] = [x] + [y] + [x + y] + 1 = 2[x] + 2[y] + 2$

16. Với $x \in R$ ta có

$$\left[\{x\} + \frac{1}{2}\right] = [2\{x\}] \text{ và } \left[x + \frac{1}{2}\right] = [2x]\text{-}[x]$$

Hệ quả : Với mọi số nguyên dương ta luôn có $\left[\frac{n}{2}\right] + \left[\frac{n+1}{2}\right] = n$

17. Với mọi số tự nhiên n và với mọi số thực $x \in R$ ta có $n[x] \leqslant [nx] \leqslant n[x] + n - 1$

18. Với mọi số thực x không phải là số nguyên và với mọi số nguyên n ta luôn có $[x]+[n-x] = n - 1$

19. Cho $k_1, k_2, ..., k_n,$ là bộ n số nguyên dương. Khi ấy

$$k_1 + k_2 + k_3 + ... + k_n \geqslant \left[\frac{k_1 + k_2 + ... + k_n}{n}\right] + n - 1$$

20. Cho a và $b \geqslant 2$ là các số tự nhiên bất kì . Khi ấy $[\log_b a] + 1$ chính là số các chữ số của một số a viết trong hệ đếm cơ số b.

21. Giả sử r là phần dư khi chia một số nguyên m cho một số nguyên dương n , $m = pn + r$ với $r \in \{0, 1, ..., n - 1\}$. Khi ấy

$$r = m - n\left[\frac{m}{n}\right]$$

22. Nếu p và q là những số nguyên dương sao cho $\frac{p}{q}$ không phải là số nguyên thì

$$\frac{p}{q} \geqslant \left[\frac{p}{q}\right] + \frac{1}{q}$$

23. Cho q là số tự nhiên, x là số thực dương bất kì. Có đúng $\left[\frac{x}{q}\right]$ số tự nhiên không vượt quá x và chia hết cho q .

24. Các qui tắc đổi chỗ (hoán vị), kết hợp của phép toán cộng và phép toán nhân; qui tắc kết hợp giữa phép toán nhân và phép toán cộng vẫn đúng cho phần nguyên và phần dư

25. Định lí Legendre: Số mũ của số nguyên tố p trong phân tích tiêu chuẩn của n! được tính theo công thức:

$$v_p(n) = \sum_{i=1}^{+\infty} \left[\frac{n}{p^i}\right]$$

26. Định lí Hermite : Với $n \in N^*$, x là số thực bất kì ta có :

$$[nx] = [x] + \left[x + \frac{1}{n}\right] + .. + \left[x + \frac{n-1}{n}\right]$$

Bài tập cơ bản

1. Phương trình $x^4 - 3x^3 - 6 = 0$ có đúng 2 nghiệm thực p và q . Tính $[p] + [q]$.

2. Giải phương trình $[x^2] = [x]^2$

3. Giải phương trình $\left[\frac{x}{2}\right] + \left[\frac{x}{3}\right] + \left[\frac{x}{5}\right] = x$

4. Giải bất phương trình $[x] + \{x\} < x - 1$

5. Cho x là số thực dương thỏa $\left[\sqrt{x} + \sqrt{x+1}\right] = \left[\sqrt{4x+2}\right]$. Chứng minh rằng

$$\exists n \in N^* : \frac{1}{n^2} + n^2 \leqslant 4n + 2 < (n+1)^2$$

6. (THTT số 408) Giải phương trình $x^2 - (1 - [x])x + 2011 = 0$

7. (THTT số 424) Giải phương trình $[x]^3 + 2x^2 = x^3 + 2[x]^2$

8. (THTT số 411) Tìm tất cả các hàm số liên tục $f : \mathbb{R} \to \mathbb{R}$ thỏa mãn $\{f(x+y)\} = \{f(x) + f(y)\}$ với mọi $x, y \in \mathbb{R}$

9. (APMO 1993) Tìm tất cả các giá trị khác nhau của hàm số

$$f(x) = [x] + [2x] + \left[\frac{5x}{3}\right] + [3x] + [4x]$$

10. (THTT số 416) Cho $n > 1$ số hữu tỉ $r_1, r_2, ..r_n$ thỏa mãn $0 < r_i \leqslant \frac{1}{2}, \sum_{i=1}^{n} r_i = 1$ và hàm số

$$f(x) = [x] + \left[x + \frac{1}{2}\right]$$

Hãy tìm giá trị lớn nhất của biểu thức $P(k) = 2k - \sum_{i=1}^{n} f(kr_i)$ khi k chạy trên tập các số nguyên.

11. (Romania MO 2003) Cho $A = \sqrt{4n^2 + n}$, $n \in \mathbb{N}$. Chứng minh rằng

$$\{A\} \leqslant \frac{1}{4}$$

12. (Austrian MO 1974, Hong Kong TST 1988) Chứng minh rằng

$$\left[\sqrt{n} + \sqrt{n+1}\right] = \left[\sqrt{4n+2}\right]$$

13. (Canada MO 1987) Cho n là số tự nhiên. Chứng minh rằng:

$$\left[\sqrt{n} + \sqrt{n+1}\right] = \left[\sqrt{4n+1}\right] = \left[\sqrt{4n+2}\right] + \left[\sqrt{4n+3}\right]$$

14. (Đề nghị Olympic 30/4, THPT Lê Quý Đôn Quảng Trị) Tìm tất cả các nghiệm không nguyên của phương trình

$$x + \frac{96}{x} = [x] + \frac{96}{[x]}$$

15. (Đề nghị Olympic 30/4, THPT Lê Quý Đôn Quảng Trị) Giải phương trình

$$\left[\frac{8x+1}{6}\right] + \left[\frac{4x-1}{3}\right] = \frac{16x-7}{9}$$

16. (Sweden MO 1982) Với mỗi $n \in \mathbb{N}$, hãy xác định xem phương trình $x^2 - [x^2] = \{x^2\}$ có bao nhiêu nghiệm trên đoạn [1;n]

17. (VMO 1979) Tìm tất cả những số α sao cho phương trình $x^2 - 2x[x] + x - \alpha = 0$ có hai nghiệm số phân biệt không âm.

18. (Olympic Czech and Slovak, 1998) Tìm tất cả các số thực x sao cho

$$x[x[x[x]]] = 88$$

19. (Belarusian Olympiad 1999) Chứng tỏ rằng phương trình $\{x^3\} + \{y^3\} = \{z^3\}$ có vô số nghiệm nguyên.

20. (Australian MO 1999) Giải hệ phương trình

$$\begin{cases} x + [y] + \{z\} = 200 \\ \{x\} + y + [z] = 190,1 \\ [x] + \{y\} + z = 178,8 \end{cases}$$

Ứng dụng định lý Hermite và định lý Legendre

Ứng dụng định lý Hermite qua một bài toán

Định lí Hermite : Với số tự nhiên n và số thực x ta luôn có :

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + ... + \left[x + \frac{n-1}{n}\right] = [nx]$$

hay

$$[nx] = \sum_{i=0}^{p-1} \left[x + \frac{i}{n}\right] \quad (*)$$

Hệ quả :

$$[x] + \left[x + \frac{1}{2}\right] = [2x] \text{ và } \sum_{0 \leqslant i \leqslant j \leqslant n} \left[\frac{x+i}{j}\right] = n\,[x]$$

Đẳng thức (*) là 1 đẳng thức đẹp trong số học và tổ hợp, nó được ứng dụng nhiều trong các bài toán tính tổng liên quan đến phần nguyên. Trước hết ta xét bài toán mở đầu:

Ví dụ 1: Cho $n \in \mathbb{R}, m \in \mathbb{N}, m \geqslant 2$, tính tổng

$$S = \sum_{i=0}^{\infty} \sum_{j=0}^{m-1} \left[\frac{n + jm^i}{m^{i+1}}\right]$$

Giải : Ta có

$$S = \sum_{i=0}^{\infty} \sum_{j=0}^{m-1} \left[\frac{n}{m^{i+1}} + \frac{j}{m}\right] = \sum_{i=0}^{\infty} \left(\left[\frac{n}{m^i}\right] - \left[\frac{n}{m^{i+1}}\right]\right) = [n]$$

Vậy $S = [n]$. Bài toán được chứng minh khá đơn giản nhưng có ứng dụng khá hay trong nhiều bài toán tính tổng, đặc biệt là các bài toán có nhiều dấu $\sum$. Ta sẽ xét 1 số bài toán ứng dụng cho bổ đề trên :

Bài toán 1: Chứng minh rằng

$$\sum_{k=0}^{n-1} \sum_{i=0}^{\infty} \sum_{j=1}^{m-1} \left[\frac{2^k + jm^i}{2^{i+1}}\right] = 2^n - 1$$

HD : Ứng dụng bổ đề trên ta có $VT = \sum_{k=0}^{n-1} 2^k = \frac{2^n - 1}{2 - 1} = 2^n - 1$ (ĐPCM)

Bài toán 2: Chứng minh rằng

$$\sum_{k=0}^{p-1} \sum_{i=0}^{\infty} \sum_{j=0}^{m-1} \left[\frac{x + \frac{k}{p} + jm^i}{m^{i+1}}\right] = [px]$$

HD: Ứng dụng bổ đề trên ta có $VT = \sum_{k=0}^{p-1} \left[x + \frac{k}{p}\right] = [px]$ (Áp dụng định lí Hermite 2 lần)

Bài toán 3: Tìm m để $y \vdots 2$ với

$$y = \sum_{k=0}^{p-1} \sum_{i=0}^{\infty} \sum_{j=0}^{m-1} \left[\frac{C_n^2 + \frac{k}{p} + jm^i}{m^{i+1}}\right] - \sum_{k=0}^{\left[\frac{p}{2}\right]} \sum_{j=0}^{\infty} \sum_{j=0}^{m-1} \left[\frac{C_p^{2k} + jm^i}{m^{i+1}}\right]$$

HD: Dễ thấy $y = \dfrac{p^2(p-1)}{2} - 2^{p-1}$. Để $y \vdots 2$ thì $p^2(p-1) \vdots 4$.
Điều này dẫn ta tới $p \equiv 0(\mod 2)$ hoặc $p \equiv 1(\mod 4)$.
Bài toán 4: (IMO 1968) Tính tổng

$$\sum_{k=0}^{\infty} \left[\frac{x+2^k}{2^{k+1}}\right]$$

HD: Áp dụng bổ đề với $j = 1, m = 2$ ta dễ dàng thu được $\sum_{k=0}^{\infty} \left[\frac{x+2^k}{2^{k+1}}\right] = [x]$.

Bài toán 5: Tính tổng

$$S = \sum_{i=0}^{m-1} \left\{\frac{ai+b}{am}\right\}$$

HD : Ta có

$$S = \sum_{i=0}^{m-1} \frac{ai+b}{am} - \sum_{i=0}^{m-1} \left[\frac{ai+b}{am}\right] = \sum_{i=0}^{m-1} \frac{ai+b}{am} - \sum_{i=0}^{m-1} \left[\frac{b}{am} + \frac{i}{m}\right],$$

đến đây áp dụng bổ đề trên ta được kết quả.

Ứng dụng của định lý Legendre về số mũ nguyên tố

Định lí Legendre: Số mũ của số nguyên tố p trong phân tích tiêu chuẩn của n! được tính theo công thức

$$v_p(n) = \sum_{i \geqslant 1} \left[\frac{n}{p^i}\right]$$

Chứng minh :
Ta có nhận xét $n < p^i$ thì $\left[\dfrac{n}{p^m}\right] = 0, m \geqslant i$. Trong phân tích chuẩn n có đúng $\left[\dfrac{n}{p}\right]$ bội số của p.
Do đó

$$n! = p^{\left[\frac{n}{p}\right]} \left[\frac{n}{p}\right]! A_1 \text{ , trong đó } (A_1, p) = 1$$

Tương tự

$$\left[\frac{n}{p}\right]! = p^{\left[\frac{\left[\frac{n}{p}\right]}{p}\right]} \left[\frac{\left[\frac{n}{p}\right]}{p}\right]! A_2 \text{ , trong đó } (A_2, p) = 1$$

Mà theo tính chất $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$ ta có

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right] \Rightarrow n! = p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right]} . \left[\frac{n}{p^2}\right]! A_2$$

Lí luận tương tự trên với $\left[\dfrac{n}{p^2}\right]!$ và tiếp tục cho tới khi $\left[\dfrac{n}{p^k}\right] < p$.
Cuối cùng ta thu được số mũ $v_p(n)$ của p trong phân tích chuẩn n! là :

$$v_p(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + ... + \left[\frac{n}{p^k}\right]$$

trong đó số k thỏa mãn $p^k \leqslant n < p^{k+1}$ (ĐPCM).
Vậy định lí được chứng minh.
Đây là một định lí có ứng dụng khá rộng trong các bài toán chứng minh chia hết và tính số mũ nguyên tố trong phân tích chuẩn của n!. Ta sẽ mở đầu bằng bài toán trong đề IMO 1972 :
Ví dụ 1: Cho các số tự nhiên m, n, chứng minh rằng

$$\frac{(2m)!(2n)!}{m!n!(m+n)!} \in \mathbb{N}^*$$

HD: Ta sẽ tìm số mũ của p bất kì trong phân tích chuẩn của $(2m)!(2n)!$ và $n!m!(m+n)!$, sau đó chứng minh $v_p((2m)!.(2n)!) \geqslant v_p(n!m!(m+n)!)$.
Giải :
Ta có

$$v_p((2m)!(2n)!) = \sum_{i=1}^{\infty} \left[\frac{2m}{p^i}\right] + \sum_{j=1}^{\infty} \left[\frac{2n}{p^j}\right]$$

$$v_p(n!m!(m+n)!) = \sum_{i=1}^{\infty} \left[\frac{m}{p^i}\right] + \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right] + \sum_{k=1}^{\infty} \left[\frac{m+n}{p^k}\right]$$

Ta cần chứng minh

$$\left[\frac{2m}{p^k}\right] + \left[\frac{2m}{p^k}\right] \geqslant \left[\frac{m}{p^k}\right] + \left[\frac{n}{p^k}\right] + \left[\frac{m+n}{p^k}\right]$$

Theo tính chất 12 ta thấy BĐT trên đúng => ĐPCM.
Vậy $\frac{(2m)!(2n)!}{m!n!(m+n)!} \in \mathbb{N}^*$. (đpcm)
Các bài tập tương tự :
Bài toán 1 : CMR với $m, n \in \mathbb{N}$ ta luôn có

$$\frac{(m+n)!}{m!n!} \in \mathbb{N}^*$$

HD: Áp dụng BĐT $[x+y] \geqslant [x] + [y]$
Bài toán 2 :(USMO 1975) CMR với $n \in \mathbb{N}$ ta có

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

là số tự nhiên
HD: Chứng mình và áp dụng BĐT $[5x] + [5y] \geqslant [3x+y] + [x+3y]$
Bài toán 3 : CMR với $n \in \mathbb{N}$ ta có

$$\frac{12(5n)!}{n!(n+1)!(n+2)!(n+3)!(n+4)!}$$

là số tự nhiên.

Tiếp theo ta sẽ đi qua một dạng mới là chứng minh chia hết, kết hợp với hệ đếm cơ số.

Ví dụ 2 : Cho số nguyên tố p. Tìm $n \in \mathbb{N}$ sao cho $n! \vdots p^{n-1}$.
Giải :

$\divideontimes p = 2$ ta cần chứng minh $n! \vdots 2^{n-1}$.
Với n lẻ tức $n = 2k + 1$ ta có :

$$v_2((2k+1)!) = v_2((2k)!) = \sum_{i=1}^{\infty} \left[\frac{2k}{2^i}\right] < \sum_{i=1}^{\infty} \frac{2k}{2^i} = \frac{2k}{2-1} = 2k = n-1$$

Suy ra số mũ của 2 trong phân tích n! là nhỏ hơn n-1, do đó $n!$ không chia hết cho 2^{n-1}.
Với $n = 2^k(2m+1)$ ta có :

$$\begin{aligned} v_2(n!) &= v_2((2^k(2m+1))!) = \sum_{i=1}^{\infty} \left[\frac{2^k(2m+1)}{2^i}\right] \\ &= \sum_{t=0}^{k-1} 2^i(2m+1) + \sum_{t=0}^{\infty} \frac{2m+1}{2^t} \\ &< (2m+1)(2^k-1) + 2m = 2^k(2m+1) - 1 = n-1 \end{aligned}$$

Suy ra $n!$ không chia hết cho 2^{n-1}
Với $n = 2^k$ ta có

$$v_2(n!) = v_2((2^k)!) = \sum_{i=1}^{\infty} \left[\frac{2^k}{2^i}\right] = \sum_{i=1}^{k-1} \left[2^i\right] = 2^k - 1 = n-1$$

Suy ra n! chia hết cho 2^{n-1}.
Vậy $n = 2^k$là giá trị cần tìm.
$\divideontimes p = 3$ làm tương tự ta thu được không có giá trị n nào thỏa mãn.
$\divideontimes p > 3$ ta cũng có kết quả là không có giá trị n nào thỏa mãn.
Vậy chỉ có giá trị $n = 2^k, k \in \mathbb{N}$ (ứng với p=2) thỏa đề.
Nhận xét : Từ đây ta có nhận xét là nếu $n = 2^k, k \in \mathbb{N}$ thì tất cả các ước nguyên tố của n! đều lớn hơn n-1.
Sau đây là 1 số bài toán sử dụng hệ đếm cơ số trong các bài toán phần nguyên.
Ví dụ 3: Giả sử $m! = 2^l(2k+1), m, k, p \in \mathbb{N}$, chúng minh rằng tồn tại vô hạn m sao cho:

$$2m - l = 1^1 + 2^2 + ... + 2014^{2014}$$

Giải:
Giả sử trong hệ đếm cơ số 2 , m được biểu diễn dưới dạng:

$$m = \overline{a_n a_{n-1} ... a_0} = \sum_{k=0}^{n} a_k 2^k$$

Khi đó

$$l = v_p(m!) = \sum_{i=0}^{\infty} \left[\frac{m}{2^i}\right] = \sum_{i=0}^{n} \left[\frac{m}{2^i}\right] = \sum_{i=0}^{n} \left[\sum_{k=0}^{n} a_k 2^{k-i}\right] = \sum_{k=0}^{n} \left[a_k \sum_{i=0}^{n} 2^{k-i}\right]$$

Mặc khác ta có $\left[a_i \sum_{i=k+1}^{n} 2^{k-i}\right] = 0$ chính vì thế ta có :

$$\begin{aligned} l &= \sum_{k=0}^{n} \left[a_k \sum_{i=0}^{k} 2^{k-i}\right] \\ &= \sum_{k=0}^{n} \left[a_k 2^k \sum_{i=0}^{k} \frac{1}{2^i}\right] \\ &= \sum_{k=0}^{n} \left[a_k.2^k \frac{1-\frac{1}{2^{k+1}}}{1-\frac{1}{2}}\right] \\ &= \sum_{k=0}^{n} \left[a_k.2^k.\left(2-\frac{1}{2^k}\right)\right] = 2m - \sum_{k=0}^{n} a_k \end{aligned}$$

Suy ra

$$2m - l = \sum_{k=0}^{n} a_k$$

Công việc cuối cùng là phải chứng minh tồn tại vô hạn bộ số $(a_k)_{i=0}^{n}$ sao cho

$$\sum_{k=0}^{n} a_k = 1^1 + 2^2 + ... + 2014^{2014}$$

Mà điều này là hiển nhiên. Vậy bài toán được chứng minh.
Ta cùng xét các ví dụ tương tự sau:
Bài toán 1: Giả sử $m! = 3^l(3k+1), m, k, p \in \mathbb{N}$, chúng minh rằng tồn tại vô hạn m sao cho:

$$m - 2l = 1! + 2! + ... + 30!$$

HD : Làm tương tự bài trên, giả sử $m = \overline{a_n a_{n-1}...a_0} = \sum_{k=0}^{n} a_k 3^k$, sau biến đổi ta được $m - 2l = \sum_{k=0}^{n} a_k$.

Hàm có chứa phần nguyên

Trong tổ hợp, các dạng bài toán tính tổng rất đa dạng và nhiều cách giải . Một trong những vấn đề hay gặp trong các bài toán tính tổng là tổng các hàm có chứa phần nguyên.. Sau đây tôi xin được giới thiệu 1 dạng toán khá đẹp về phần này với 2 bài toán mở đầu.

Ví dụ 1: Cho p là 1 số nguyên tố lẻ, q là 1 số nguyên không chia hết cho p, $f : \mathbb{N} \to \mathbb{R}$, thỏa
1) $f(x)$ không chia hết cho p , với mọi $x \in \mathbb{N}$
2) $f(x) + f(p-x)$ chia hết cho p với mọi $x \in \mathbb{N}$
Chứng minh rằng :

$$\sum_{k=1}^{p-1} \left[f(k).\frac{q}{p}\right] = \frac{q}{p} \sum_{k=1}^{p-1} f(k) - \frac{p-1}{2}$$

Giải :
Ta có $\frac{qf(k)}{p}+\frac{qf(p-k)}{p}\in\mathbb{Z}$, mà $\frac{qf(k)}{p}\notin\mathbb{Z}$ nên $\frac{qf(p-k)}{p}\notin\mathbb{Z}$ với mỗi $k=\overline{1,p-1}$.
Do vậy từ tính chất phần lẻ ta có

$$0\leqslant\left\{\frac{qf(k)}{p}\right\}+\left\{\frac{qf(p-k)}{p}\right\}<2$$

Suy ra

$$\left\{\frac{qf(k)}{p}\right\}+\left\{\frac{qf(p-k)}{p}\right\}=1$$

Lấy tổng các giá trị từ 1 đến p-1 ta có :

$$\sum_{k=1}^{p-1}\left\{\frac{qf(k)}{p}\right\}+\sum_{k=1}^{p-1}\left\{\frac{qf(p-k)}{p}\right\}=p-1$$

Suy ra

$$2\sum_{k=1}^{p-1}\left\{\frac{qf(k)}{p}\right\}=p-1\Leftrightarrow\sum_{k=1}^{p-1}\left\{\frac{qf(k)}{p}\right\}=\frac{p-1}{2}$$

Từ đó ta có

$$\sum_{k=1}^{p-1}\left[f(k)\frac{q}{p}\right]=\sum_{k=1}^{p-1}\frac{q}{p}f(k)-\sum_{k=1}^{p-1}\left\{\frac{q}{p}f(k)\right\}=\sum_{k=1}^{p-1}\frac{q}{p}f(k)-\frac{p-1}{2}$$

Suy ra đpcm.
Vậy $\sum_{k=1}^{p-1}\left[f(k)\frac{q}{p}\right]=\frac{q}{p}\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}$.
Việc áp dụng bài toán trên khá dễ vì chỉ cần thay$f(x)$ bằng 1 hàm hay 1 giá trị nào đó.
Bài toán áp dụng:
Bài toán 1: Cho p,q là 2 số nguyên dương và nguyên tố cùng nhau, chứng minh rằng :

$$\sum_{k=1}^{p-1}\left[\frac{kq}{p}\right]=\frac{(p-1)(q-1)}{2}$$

HD giải : Chọn $f(k)=k$, theo bài toán mở đầu ta có

$$\sum_{k=1}^{p-1}\left[\frac{kq}{p}\right]=\sum_{k=1}^{p-1}\left[\frac{f(k)q}{p}\right]=\frac{q}{p}\sum_{k=1}^{p-1}f(k)-\frac{p-1}{2}$$

Mà $\sum_{k=1}^{p-1}f(k)=\frac{p(p-1)}{2}$ nên dễ dàng có

$$\sum_{k=1}^{p-1}\left[\frac{kq}{p}\right]=\frac{(p-1)(q-1)}{2}$$

Bài toán 2 : Cho p là số nguyên tố lẻ, tính

$$\sum_{k=1}^{p-1}\left[\frac{k^3}{q}\right]$$

HD: Chọn $f(k) = k^3$, khi đó

$$\sum_{k=1}^{p-1} f(k) = \left(\frac{p(p-1)}{2}\right)^2$$

.

Bài toán 4: Cho p là số nguyên tố lẻ, tính

$$S = \sum_{k=1}^{p-1} \left[\frac{(-1)^{k+1}k^3}{p}\right]$$

Áp dụng giải phương trình $S = 0$.
HD : Chọn $f(k) = (-1)^{k+1}k^3$, khi đó

$$\sum_{k=1}^{n} f(k) = \frac{(n+1)^2(2n-1)}{4}$$

khi n chẵn và

$$\sum_{k=1}^{n} f(k) = \frac{-n^2(2n+3)}{4}$$

khi n lẻ.
Ta nhận thấy trong các bài trên, tất cả deg $f(k)$ đều lẻ (vì khi đó mới đáp ứng được điều kiện 2 của đề. Còn nếu deg $f(k)$ chẵn thì sao? Trường hợp này ta sẽ xét các ví dụ sau:
Bài toán 5 : Với p là số nguyên tố có dạng $4k + 1$, tính

$$S = \sum_{i=1}^{p-1} \left[\frac{i^2}{p}\right]$$

Nhận xét : Ta thử làm giống các bài trên. Chọn $f(k) = k^2$. Khi đó dễ thấy f(k) không chia hết cho p và $f(k) + f(p-k) = k^2 + (p-k)^2 = 2k^2 - 2pk + p^2$ cũng không chia hết cho p. Điều này mâu thuẫn với 2 điều kiện đề cho. Vậy ta không thể làm như các bài trên được.
Giải :
Trước hết chứng minh bổ đề.
Bổ đề : Với p là số nguyên tố thỏa $p \equiv 1(\text{mod}4)$ thì mỗi số tự nhiên a với $1 \leqslant a \leqslant \frac{p-1}{2}$ sẽ luôn tồn tại duy nhất số tự nhiên b thỏa mãn $\frac{p+1}{2} \leqslant b \leqslant p-1$ và $a^2 + b^2 \equiv 0(\mod p)$.
Chứng minh : Theo định lí Wilson ta có : $(p-1)! \equiv -1(\mod p)$.
Với mỗi $k = \overline{1, \frac{p-1}{2}}$ thì $p - k \equiv -k(\mod p) \Rightarrow k(p-k) \equiv -k^2(\mod p)$.
Kết hợp với giả thiết $p \equiv 1(\mod 4) \Rightarrow \frac{p-1}{2} \equiv 0(\mod 2)$, ta được:

$$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 = \left(\left(\frac{p-1}{2}\right)!\right)^2 (\text{mod}p)$$

Đặt $\varphi = \left(\frac{p-1}{2}\right)! \Rightarrow \varphi^2 \equiv -1(\text{mod}p)$
Với mỗi $1 \leqslant a \leqslant \frac{p-1}{2}$ ta chọn $\frac{p+1}{2} \leqslant b \leqslant p-1$ thỏa mãn $b^2 \equiv a^2\varphi^2(\text{mod}p)$, dễ thấy b tồn

tại và duy nhất.
Khi đó

$$a^2 + b^2 \equiv a^2(p^2+1) \equiv 0(\mathrm{mod}p)$$

Suy ra ĐPCM.
Vậy bổ đề được chứng minh.
Áp dụng với $1 \leqslant i \leqslant \dfrac{p-1}{2}$ và $\dfrac{p+1}{2} \leqslant j \leqslant p-1$ ta thấy :

$$S = \sum_{i=1}^{p-1} \left[\frac{i^2}{p}\right] = \sum_{i=1}^{\frac{p-1}{2}} \left(\left[\frac{i^2}{p}\right] + \left[\frac{i^2 j^2}{p}\right] \right) = \sum_{i=1}^{p-1} \frac{i^2}{p} - \frac{p-1}{2} = \frac{(p-1)(p-2)}{3}$$

.
Vậy

$$S = \frac{(p-1)(p-2)}{3}$$

Tiếp tục là bài 5 trong đề thi Chọn đội tuyển IMO Việt Nam năm 2005 (Vietnam TST 2005).
Bài toán 6 (Vietnam TST 2005) : Cho p là số nguyên tố ($p > 3$). Tính:
a) $S = \sum_{k=1}^{\frac{p-1}{2}} \left(\left[\frac{2k^2}{p}\right] - 2\left[\frac{k^2}{p}\right] \right)$ nếu $p \equiv 1(\mathrm{mod}4)$.
b) $P = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{k^2}{p}\right]$ nếu $p \equiv 1(\mathrm{mod}8)$.
Giải:
Trước hết ta chứng minh 2 bổ đề :
Bổ đề 1 : Với p là số nguyên tố thỏa $p \equiv 1(\mathrm{mod}4)$ thì mỗi số tự nhiên a với $1 \leqslant a \leqslant \dfrac{p-1}{2}$ sẽ luôn tồn tại duy nhất số tự nhiên b thỏa mãn $\dfrac{p+1}{2} \leqslant b \leqslant p-1$ và $a^2 + b^2 \equiv 0(\mathrm{mod}p)$.
Bổ đề 2 : Với x là số thực bất kì thì $[2x] - 2[x]$ bằng 1 nếu $\dfrac{1}{2} \leqslant \{x\} < 1$ và bằng 0 nếu $0 \leqslant x < \dfrac{1}{2}$.
Chứng mình :
Bổ đề 1 : Xem bổ đề của bài 5.
Bổ đề 2 : Ta có $x = [x] + \{x\}$. Suy ra

$$[2x] - 2[x] = [2[x] + 2\{x\}] - 2[[x] + \{x\}] = [2\{x\}] - 2[\{x\}] = [2\{x\}]$$

Khi đó:
+) nếu $\dfrac{1}{2} \leqslant \{x\} < 1$ thì $[2\{x\}] = 1 \Rightarrow [2x] - 2[x] = 1$
+) nếu $0 \leqslant x < \dfrac{1}{2}$ thì $[2\{x\}] = 0 \Rightarrow [2x] - 2[x] = 0$
Vậy bổ đề được chứng minh.
Quay trở lại bài toán :

a) Ta thấy S có tất cả $\dfrac{p-1}{2}$ số hạng.
Theo bổ đề 2 thì tất cả số hạng trên đều có giá trị là 0 hoặc 1.

Theo bổ đề 1 thì với mỗi số tự nhiên a với $1 \leqslant a \leqslant \dfrac{p-1}{2}$ sẽ luôn tồn tại duy nhất số tự nhiên b thỏa mãn

$$\frac{p+1}{2} \leqslant b \leqslant p-1 \text{ và } a^2+b^2 \equiv 0(\mathrm{mod} p)$$

Suy ra $a^2+(p-b)^2 \equiv 0(\mod p)$
Do đó tồn tại duy nhất $a' \in \left[1; \dfrac{p-1}{2}\right]$ thỏa $a^2+a'^2 \equiv 0(\mathrm{mod} p)$.
Gọi x,y lần lượt là số các số dư khi chia k^2 cho p $\left(1 \leqslant k \leqslant \frac{p-1}{2}\right)$ có giá trị lớn hơn và nhỏ hơn $\frac{p-1}{2}$. Theo nhận xét trên thì $x=y$, hơn nữa $x+y=\dfrac{p-1}{2} \Rightarrow x=y=\dfrac{p-1}{4}$.
Từ đó $S=x.1+y.0=\frac{p-1}{4}$.
Vậy $S=\dfrac{p-1}{4}$.

b) Do $p \equiv 1(\mod 8)$ nên tồn tại a sao cho $a^2 \equiv 2(\mod p)$ và $p \equiv 1(\mod 4)$.
Ta có :

$$P=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{k^2}{p}\right]=\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-\left[\frac{k^2}{p}\right]\right)-\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-2\left[\frac{k^2}{p}\right]\right)=\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-\left[\frac{k^2}{p}\right]\right)-S$$

Ta cần tính

$$\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-\left[\frac{k^2}{p}\right]\right)$$

Ta có :

$$\begin{aligned}&\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-\left[\frac{k^2}{p}\right]\right)\\&=\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{2k^2}{p}-\frac{k^2}{p}\right)-\sum_{k=1}^{\frac{p-1}{2}}\left(\left\{\frac{2k^2}{p}\right\}-\left\{\frac{k^2}{p}\right\}\right)\\&=\sum_{k=1}^{\frac{p-1}{2}}\frac{k^2}{p}-\sum_{k=1}^{\frac{p-1}{2}}\left(\left\{\frac{2k^2}{p}\right\}-\left\{\frac{k^2}{p}\right\}\right)\end{aligned}$$

Theo nhận xét trên thì tập hợp các số dư khi chia k^2, $1 \leqslant k \leqslant \dfrac{p-1}{2}$ cho p trùng với tập hợp các số dư khi chia $2k^2$,$1 \leqslant k \leqslant \dfrac{p-1}{2}$ cho p tức là

$$\sum_{k=1}^{\frac{p-1}{2}}\left(\left\{\frac{2k^2}{p}\right\}-\left\{\frac{k^2}{p}\right\}\right)=0$$

Suy ra

$$\sum_{k=1}^{\frac{p-1}{2}}\left(\left[\frac{2k^2}{p}\right]-\left[\frac{k^2}{p}\right]\right)=\sum_{k=1}^{\frac{p-1}{2}}\left(\frac{k^2}{p}\right)=\frac{p^2-1}{24}$$

Vậy $P=\dfrac{p^2-1}{24}-\dfrac{p-1}{2}=\dfrac{(p-1)(p-5)}{24}$.
Từ 2 nhận xét trên ta thấy bổ đề 1 khá quan trọng, và được sử dụng thường xuyên trong các

bài toán tính tổng dạng này. Sau đây là các bài toán tương tự :

Bài toán 7: Cho $p \equiv 1(\mod 3)$, m không chia hết cho p, tính

$$\sum_{i=1}^{p-1}\left(\left[\frac{3mi^2}{p}\right]-m\left[\frac{3i^2}{p}\right]\right)$$

HD : Làm tương tự ta được kết quả $\frac{(m-1)(p-1)}{2}$.

Bài toán 8: (THTT số 430) Cho p là số nguyên tố có dạng $4k+1$, tính tổng

$$\sum_{k=1}^{p-1}\left(\left[\frac{2k^2}{p}\right]-2\left[\frac{k^2}{p}\right]\right)$$

HD: Giải tương tự như câu a bài toán 6 và cho kết quả là $\frac{p-1}{2}$.

Bài toán 9: Cho p là số nguyên tố có dạng $4k+1$, tính tổng

$$\sum_{k=1}^{p-1}\left(\left[\frac{2k^3}{p}\right]-2\left[\frac{k^3}{p}\right]\right)$$

HD : Bài này ta sử dụng kết quả của bài toán mở đầu 1 , và cũng cho kết quả là $\frac{p-1}{2}$.

Nhận xét : Bài toán 8 và 9 đã cho ta nhận xét về bài toán tổng quát là tính tổng $S=\sum_{k=1}^{p-1}\left(\left[\frac{2k^n}{p}\right]-2\left[\frac{k^n}{p}\right]\right)$ với $n=2$ và $n=3$ thì $S=\frac{p-1}{2}$, với n=1 thì cũng làm như trường hợp n=3 ta cũng có kết quả tương tự. Vậy $\forall n \in \mathbb{N}$thi kết quả trên có đúng không? Đáp án là đúng, và phần chứng minh xin dành cho bạn đọc.

Ví dụ 2: Chứng minh rằng với p là số nguyên tố thỏa $p \equiv 1(\mod 4)$, với hai hàm số $f(x)$ và $g(x)$ thỏa mãn

$$\begin{cases}(f(x),p))=1\\(g(x),p))=1\end{cases}\ \forall x$$

Khi đó chứng minh rằng

$$\sum_{i=1}^{p-1}\left(\left[\frac{g(x)f(x)i^2}{p}\right]-g(x)\left[\frac{f(x)i^2}{p}\right]\right)=\frac{(g(x)-1)(p-1)}{2}$$

Chứng minh: Bài này dễ dàng chứng minh bằng bài toán mở đầu 1 và theo cách của Bài toán 6 câu a.

Áp dụng bài toán trên khá hay khi chỉ cần chọn 2 hàm thỏa mãn là có thể sử dụng. Ví dụ như bài 8 : Chọn $f(x)=1, g(x)=2$, khi đó

$$\sum_{i=1}^{p-1}\left(\left[\frac{2i^2}{p}\right]-2\left[\frac{i^2}{p}\right]\right)=\frac{(2-1)(p-1)}{2}=\frac{p-1}{2}$$

Bài tập tương tự:

Bài toán 10: Cho p là số nguyên tố có dạng $4k+1$, chứng minh rằng

$$2\sum_{i=1}^{p-1}\left(\left[\frac{(p+1)i^2}{p}\right]-(p+1)\left[\frac{i^2}{p}\right]\right)\equiv 0(\mod 2)$$

Bài toán 11: Cho p là số nguyên tố có dạng $4k+1$, chứng minh rằng

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

không là số nguyên tố với mọi p.

Bài toán 12: Cho p là số nguyên tố có dạng $4k+1$. Tìm p để

$$S=\sum_{i=1}^{p-1}\left(\left[\frac{(2p+3).i^2}{p}\right]-(2p+3)\left[\frac{i^2}{p}\right]\right)-25$$

là số chính phương.

Hàm phần nguyên trong việc tính tổng các chữ số

Định nghĩa

Giả sử n là 1 số tự nhiên. Ta định nghĩa $S(n)$ là tổng của các chữ số của n khi biểu diễn trong hệ thập phân.

Tính chất

1. Với n là số nguyên dương ta có

$$S(n)=n-9\sum_{k=1}^{\infty}\left[\frac{n}{10^k}\right]$$

CM: Trong hệ thập phân ta biểu diễn

$$n=\overline{a_ma_{m-1}...a_0}=10^ma_m+10^{m-1}a_{m-1}+...+a_1.10+a_0$$

Khi đó

$$n-9\sum_{k=1}^{\infty}\left[\frac{n}{10^k}\right]=\overline{a_ma_{m-1}...a_0|}10-9\left(\overline{a_ma_{m-1}...a_1|}10+\overline{a_ma_{m-1}...a_2|}10+...a_m\right)$$

Suy ra $n-9\sum\limits_{k=1}^{\infty}\left[\frac{n}{10^k}\right]=\sum\limits_{i=0}^{m}a_i(10^i-9(10^{i-1}+10^{i-2}+...+1)=\sum\limits_{i=1}^{m}a_i=S(n)$.
Từ đó có đpcm.

2. $S(n)\equiv n(\text{mod}9)$
CM: Ta nhận thấy $\sum\limits_{k=1}^{\infty}\left[\frac{n}{10^k}\right]$ là số nguyên nên $9\sum\limits_{k=1}^{\infty}\left[\frac{n}{10^k}\right]\vdots 9$
Suy ra đpcm.

3. $0 \leqslant S(n) \leqslant n$
   CM : Dễ thấy $S(n) \geqslant 0$, và từ

$$S(n) = n - 9\sum_{k=1}^{\infty}\left[\frac{n}{10^k}\right]$$

   Suy ra $S(n) \leqslant n$ (dấu "=" xảy ra khi $0 \leqslant n \leqslant 9$)

4. $S(m+n) \leqslant S(m) + S(n)$
   CM : Ta có : $S(m) + S(n) = m + n - 9\left(\sum_{k=1}^{\infty}\left[\frac{m}{10^k}\right] + \sum_{k=1}^{\infty}\left[\frac{n}{10^k}\right]\right)$.
   Áp dụng BĐT $[a] + [b] \leqslant [a+b]$ ta được

$$S(m) + S(n) \geqslant m + n - 9\left(\sum_{k=1}^{\infty}\left[\frac{m+n}{10^k}\right]\right) = S(m+n) \text{ (đpcm)}$$

   Dấu bằng xảy ra khi và chỉ khi phép cộng $m + n$ không có nhớ.

5. $S(m.n) \leqslant S(m).S(n)$
   Bạn đọc có thể chứng minh thông qua biểu diễn của m, n và mn trong hệ thập phân.
   Từ đó ta có tổng quát :

6. $S(\sum_{i=1} a_i) \leqslant \sum_{i=1} S(a_i)$

7. $S(\prod_{i=1} a_i) \leqslant \prod_{i=1} S(a_i)$

Bài tập ví dụ

Ví dụ 1: Tìm n sao cho

$$S(n) = n^2 - 2014n + 5$$

Giải :
Ta có $0 \leqslant S(n) \leqslant n \Leftrightarrow 0 \leqslant n^2 - 2014n + 5 \leqslant n$.
Giải hệ bất phương trình, kết hợp $n \in \mathbb{N}$ ta được $n = 2014$.
Vậy $n = 2014$.

Ví dụ 2: Tìm n sao cho: $n + S(n) + S(S(n)) = 2001$.
Giải :
Ta có $n \leqslant 2000 \Rightarrow S(n) \leqslant S(1999) = 28 \Rightarrow S(S(n)) \leqslant 10 \Rightarrow n \geqslant 1972$.
Mà

$$3n \equiv n + S(n) + S(S(n)) \equiv 2001 \equiv 3(\text{mod}9) \Rightarrow n \equiv 1(\text{mod}9)$$

$$\Rightarrow n \in \{1963, 1966, 1969, 1972, 1975, 1978, 1981\}$$

Bằng cách thử trực tiếp ta thấy các giá trị n cần tìm là $n \in \{1969, 1972, 1975\}$.

Ví dụ 3: Tìm n thỏa $n + S(S(n)) = 2014$.
Bài toán này xin dành cho bạn đọc.

Ví dụ 4 : (PTNK 2008) Với mỗi số nguyên dương n, gọi $S(n)$ là tổng các chữ số của n.
a) Chứng minh rằng các số n = 999 và n = 2999 không thể biểu diễn được dưới dạng $a + b$ với $S(a) = S(b)$.
b) Chứng minh rằng mọi số $n, 999 < n < 2999$ đều biểu diễn được dưới dạng $a + b$ với $S(a) = S(b)$.
Giải :

a) Giả sử có thể biểu diễn được.
$*n = 999$: Ta có : $a + b = 999$, mà phép cộng trên không có nhớ nên $S(a) + S(b) = S(a + b) = S(999) = 27$
Mà $S(a) = S(b)$ nên $2S(a) = 27$ (vô lý)
$*n = 2999$:
Tương tự vì phép cộng a+b=2999 không có nhớ nên ta có ĐPCM.

b) Trước hết ta chứng minh rằng nếu $999 < n < 2999$ thì tồn tại số tự nhiên k sao cho $S(k) + S(n \breve{} k)$ là một số chẵn. Thật vậy, nếu $S(n)$ là số chẵn thì ta chọn $k = 0$. Nếu $S(n)$ lẻ, giả sử $n = \overline{ba_2a_1a_0}$, trong đó $b \in \{1; 2\}$. Do $999 < n < 2999$ và $n \neq 1999$ (do $S(n)$ lẻ) nên tồn tại i sao cho$a_i < 9$. Chọn i lớn nhất thoả mãn điều kiện này. Khi đó chọn $k = 10i.(a_i + 1)$ thì $S(k) = a_i + 1$ còn $S(n - k) = S(n) \breve{} ai \breve{} 1 + 9$ (phép trừ có nhớ tạo ra số 9 ở vị trí ai và giảm đi 1 đơn vị ở vị trí trước đó). Từ đó suy ra $S(k) + S(n - k) = ai + 1 + S(n) \breve{} ai \breve{} 1 + 9 = S(n) + 9$ chẵn do $S(n)$ lẻ. Bây giờ giả sử ta đã tìm được k sao cho $S(k) + S(n - k)$ là số chẵn. Khi đó nếu đặt

$$k = \overline{a_3a_2a_1a_0} \text{ và } n - k = \overline{b_3b_2b_1b_0}$$

Do $S(k) + S(n - k)$ chẵn nên số các chỉ số i sao cho $a_i + b_i$ lẻ là chẵn. Với 1 cặp chỉ số (i, j) sao cho $a_i + b_i = 2j_i + 1, a_j + b_j = 2k_i + 1$ lẻ, ta đổi $a_i \to a'_i = k_i + 1, b'_i = k_i, a'_j = k_j, b'_j = k_j + 1$. Với các chỉ số i sao cho $a_1 + b_1 = 2k_i$, ta đổi $a_i \to a'_i = b'_i = k_i$. Khi đó dễ dàng nhận thấy rằng

$$\overline{a'_3a'_2a'_1a'_0} + \overline{b'_3b'_2b'_1b'_0} = \overline{a_3a_2a_1a_0} + \overline{b_3b_2b_1b_0} = n$$

và

$$S\left(\overline{a'_3a'_2a'_1a'_0}\right) = S\left(\overline{b'_3b'_2b'_1b'_0}\right)$$

Từ đó ta có điều phải chứng minh.

Ví dụ 5: (IMO 1975) Đặt $A = S(4444^{4444})$ và $B = S(A)$. Tìm $S(B)$.
Giải :
Đặt $N = 4444^{4444}$. Do $N < 10000^{4444}$ nên N không quá $4444.4 < 20000$ số .
Từ đó

$$A < 9.20000 = 180000 \Rightarrow B \leqslant S(9999) = 45 \Rightarrow S(B) \leqslant 39 = 12 \quad (1)$$

Mặt khác

$$4444 \equiv (-2)(\text{mod}9) \Rightarrow N \equiv 2^{4444} = 8^{1431}.2 \equiv (-2)(\text{mod}9)$$

Do đó $S(B) \equiv 7(\mod 9)$ (2) Từ (1) và (2) ta có $S(B) = 7$.
Bài tập tương tự:

Ví dụ 6: Đặt $A = S(30.4^{2012})$, và $B = S(A)$. Tính $S(B)$.

Ví dụ 7: (VMO 20004) Tìm giá trị nhỏ nhất của $S(n)$ khi n chạy trên tập các bội của 2003.
HD : Sử dụng 3 bổ đề :

- 1001 là số nguyên dương nhỏ nhất trong số các số nguyên dương $m$mà $10^m \equiv 1(\text{mod } 2003)$.
- Không tồn tại bội dương của 2003 có dạng $10^k + 1$ với $k \in \mathbb{N}$.
- Tồn tại bội dương của 2003 có dạng $10^k + 10^h + 1$, với $k, h \in \mathbb{N}$.

Và sử dụng thêm các tính chất của $S(n)$ ta được đáp án $\min S(n) = 3$.
Bài tập tự luyện :

Bài toán 1 : Cho số tự nhiên N thỏa $S(N) = 100, S(5N) = 50$. Chứng minh rằng N chẵn.
Hướng dẫn: Đặt $M = 5N$ thì $S(M) = 50$ và $S(2M) = S(10N) = S(N) = 100$. Suy ra phép cộng $M + M = 2M$ là phép cộng không nhớ.

Bài toán 2: Tìm n nhỏ nhất sao cho trong n số tự nhiên liên tiếp tùy ý luôn chọn được một số N mà $S(N)$ $vdots$ 13.
Đáp án : 79.

Bài toán 3: Đặt $a = S((2^9)^{1999}); b = S(a); c = S(b)$. Tìm c.
Đáp án : c=8.

Bài toán 4: CMR với n là số tự nhiên bất kì ta luôn có

$$\frac{S(8n)}{S(n)} \geqslant \frac{1}{8}$$

Bài toán 5: Cho a là số chẵn nhưng không chia hết cho 5. Chứng minh rằng

$$\lim_{n \to +\infty} S(a^n) = +\infty$$

Bài tập tổng hợp

Bài toán 1 : Cho n là số nguyên dương thỏa mãn $n!$ có đúng 2002 chữ số 0 tận cùng. Chứng minh rằng $n \leqslant 8024$.

Bài toán 2 : Với n là số nguyên , chứng minh rằng

$$\left[\frac{n+2}{4}\right] + \left[\frac{n+4}{4}\right] + \left[\frac{n-1}{2}\right] = n$$

Bài toán 3 : (Đài Loan 1998) Chứng minh rằng với mọi số nguyên dương m và n, ta luôn có:

$$(m,n) = 2\sum_{k=0}^{m-1}\left[\frac{kn}{m}\right] + m + n - mn$$

Bài toán 4 : Tìm $\min\{x_n | 1 \leqslant n \leqslant M\}$ với $M = 20142014$ và

$$(x_n): \begin{cases} x_1 = M \\ x_{n+1} = \left[\frac{x + \left[\frac{M}{x_n}\right]}{2}\right] \ \forall n \geqslant 1 \end{cases}$$

Bài toán 5 : Tìm số nguyên dương n lớn nhất sao cho 2014! chia hết cho 7^n.

Bài toán 6: (Canada 1998) Tim số các số a thỏa mãn

$$\left[\frac{a}{2}\right] + \left[\frac{a}{3}\right] + \left[\frac{a}{5}\right] = a$$

Bài toán 7: (Hàn Quốc 1997)Tính tổng $\sum_{k=1}^{n}\left[\sqrt{k}\right]$ theo n và $a = \sqrt{n}$.

Bài toán 8 : Cho $(m,n) = 1$ với m chẵn. Tính tổng

$$S = \frac{1}{2n} + \sum_{k=1}^{n-1}(-1)^{\left[\frac{km}{n}\right]}\left\{\frac{km}{n}\right\}$$

Bài toán 9 : (Balkan 1998) Tính các số hạng khác nhau trong dãy

$$\left\{\left[\frac{k^2}{1998}\right] : k = 1, 2, ..., 1997\right\}$$

Bài toán 10 : Chứng minh rằng tích của n số nguyên liên tiếp luôn chia hết cho $n!$.

Bài toán 11 : (APMO 2001) Tìm số nguyên N lớn nhất sao cho số các số thuộc tập hợp $\{1, 2, \ldots, N\}$ và chia hết cho 3 bằng số các số thuộc tập đó và chia hết cho 5 hoặc 7.

Bài toán 12 : Chứng minh rằng với mọi số nguyên dương $n \geqslant 3$ thì

$$(2n-1)(2n-2)(2n\breve{}4)\ldots(2n-2n-1) \vdots n!$$

Bài toán 13 : Chứng minh rằng

$$C_n^k \equiv 1 \ (\mod 2) \ \ \forall k = \overline{0,n} \Leftrightarrow n \equiv 1 \ (\mod 2)$$

Bài toán 14 : Cho $n \geqslant 2$ là số nguyên dương. Chứng minh rằng:

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

.

Bài toán 15 : Tính

$$\lim_{n\to+\infty} \left(\frac{1}{n}\sum_{k=1}^{n}\left(\left[\frac{2n}{k}\right] - 2\left[\frac{n}{k}\right]\right)\right)$$

Bài toán 16 : (Định lý LTE) Gọi $v_p(n)$ là số mũ của p trong khai triển ra thừa số nguyên tố của n. Cho p là số nguyên tố lẻ, x, y là các số nguyên sao cho x, y không chia hết cho p nhưng x – y chia hết cho p, n là số nguyên dương. Chứng minh

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

Tài liệu tham khảo

1. Phần nguyên- Bài tập và ứng dụng : Hoàng Xuân Thanh.
2. Vẻ đẹp phần nguyên từ tính chất cơ bản : Nhóm học sinh chuyên toán trường KHTN Hà Nội.
3. Hàm phần nguyên và ứng dụng: Luận văn thạc sĩ toán học của Tạ Duy Phượng.
4. Số học qua các định lý và bài toán : Trần Nam Dũng.
5. Các hàm số học và ứng dụng : Luận văn thạc sĩ Toán học, Đỗ Cao Sơn.
6. Các diễn đàn : mathscope.org , diendantoanhoc.net/forum, artofproblemsolving.com/Forum.

Ngoài ra tác giả còn nhận được sự ủng hộ và giúp sức của Tiến sĩ Trần Nam Dũng, xin trân thành cảm ơn sự giúp đỡ của thầy. Chúc các bạn sẽ hiểu sâu hơn, chắc hơn về Phần nguyên sau khi đọc bài viết này.