

DOÃN QUANG TIẾN

HUỖNH KIM LINH

TÔN NGỌC MINH QUÂN

NGUYỄN MINH TUẤN

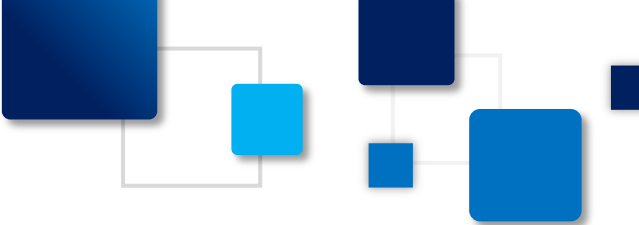
# CHINH PHỤC OLYMPIC TOÁN

$$x^n + y^n = z^n$$

## *Chuyên đề* ĐA THỨC VÀ SỐ HỌC

TẠP CHÍ VÀ TƯ LIỆU TOÁN HỌC

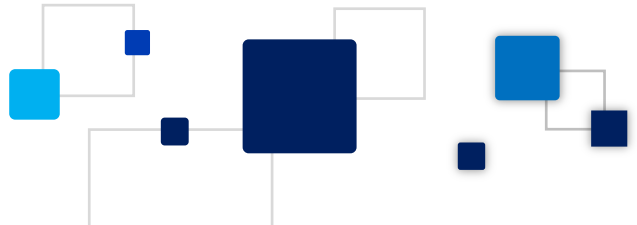




# LỜI GIỚI THIỆU

Số học hay đa thức đều là các chủ đề thường xuyên xuất hiện trong các đề thi học sinh giỏi cấp quốc gia, các kì thi khu vực cũng như quốc tế với các bài toán khó tới rất khó được các nước cũng như các thầy cô phát triển rất nhiều. Đa thức là mảng mà chứa đựng trong nó các yếu tố về đại số, giải tích, hình học và cả các tính chất về số học. Chính vì thế ta có thể xem đa thức có thể xem như là các bài toán tổ hợp giữa các mảng khác của Toán học cũng như đóng vai trò liên kết các mảng đó lại với nhau thành một thể thống nhất. Và chúng ta cũng biết rằng số học không phải tự nhiên rất nhiều nhà toán học, những người làm toán gọi nó với cái tên mỹ miều là **Bà chúa của toán học**. Thế giới các con số rất quen thuộc với chúng ta trong cuộc sống thường ngày, là một thế giới hết sức kì lạ đầy bí ẩn: loài người đã phát hiện trong đó bao nhiêu tính chất rất hay, bao nhiêu quy luật rất đẹp và bất ngờ đồng thời cũng đang chịu "bó tay" trước nhiều sự kiện, nhiều dự đoán. Điều lí thú là nhiều mệnh đề khó nhất của số học được phát biểu rất đơn giản, ai cũng hiểu được ; nhiều bài toán khó nhưng có thể giải rất sáng tạo với những kiến thức số học phổ thông đơn giản. Không ở đâu như trong số học, chúng ta lại có thể lần theo được dấu vết của những bài toán cổ xưa để đến được với những vấn đề mới đang còn chờ đợi người giải – *Trích từ cuốn sách Số học – Bà chúa của toán học – Hoàng Chúng*. Chính vì thế sự kết hợp của 2 mảng kiến thức này sẽ mang tới cho chúng ta những bài toán đẹp nhưng vẻ đẹp thì không bao giờ là dễ để chúng ta chinh phục cả, nó luôn ẩn chứa những điều khó khăn và “nguy hiểm”. Trong chủ đề của bài viết này, chúng ta sẽ đi khám phá cũng như chinh phục phần nào vẻ đẹp của sự kết hợp đó.

*Nhóm tác giả*



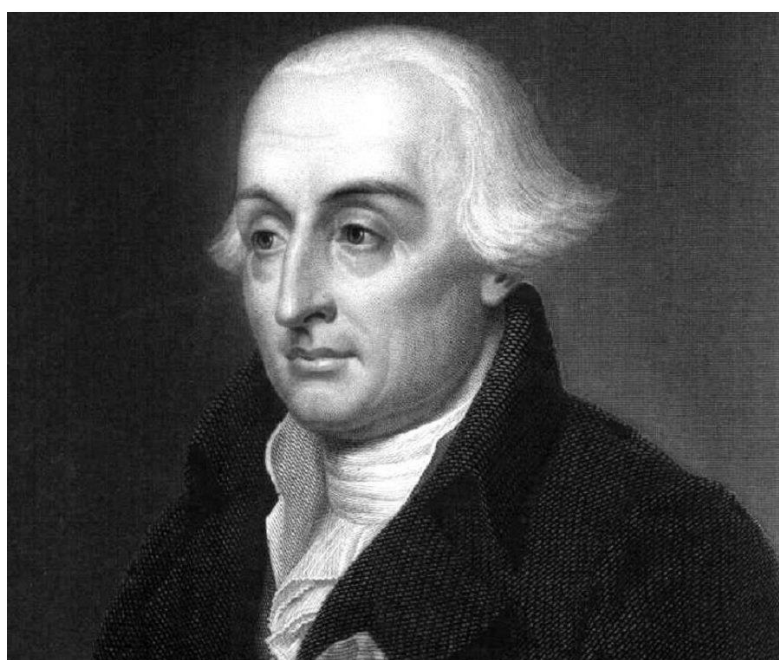




## CÂU CHUYỆN TOÁN HỌC

### *Joseph – Louis Lagrange*

Nếu nhạc sĩ người Áo *Wolfgang Amadeus Mozart* (1756 – 1791) đã để lại cho đời sau những bản nhạc tuyệt vời thì hơn hai trăm năm sau, trong những năm đầu tiên của thế kỷ 21, với lòng tôn sùng một bậc tài danh, những người yêu âm nhạc cổ điển chỉ còn biết lắng nghe để thưởng thức âm điệu mà thôi. Nhưng cùng thời với ông, ở Âu châu còn có một thiên tài khác cũng lừng danh, nhưng tiếng tăm không vang ra ngoài nhân thế vì ở trong bộ môn hạn hẹp là toán học. Tuy vậy công trình của ông để lại, không những được người đời sau ghi chú học hỏi, mà còn được áp dụng trong nhiều bộ môn khoa học thực dụng cho đời sống hàng ngày, và cả trong những chương trình thám hiểm không gian và vũ trụ để tìm hiểu về nguồn gốc đời sống của con người và tương lai về sau. Người được nhắc đến trong bài này là *Joseph – Louis Lagrange* (1736 – 1813), một nhà toán học lỗi lạc nhất, mà cũng là người thật khiêm tốn, đã được nhiều bậc vương giả Âu châu trọng vọng vào cuối thế kỷ 18 và đầu thế kỷ 19. Để phê bình về danh nhân này, *Đại đế Napoléon* đã từng nói rằng: "*Lagrange thật là một kim tự tháp cao vời trong bộ môn toán học*". Lời nói của Hoàng đế thường đi đôi với việc làm và ông đã phong cho *Lagrange* làm Bá tước, cử ông làm Thượng Nghị sĩ và còn vinh tặng ông *Đệ Nhất Đẳng Bắc Đẩu Bội Tinh*. Nhiều bậc vương giả khác ở Âu châu như Quốc vương xứ Sardinia và Hoàng đế *Frederick* của Đức quốc cũng đã hết mực tôn vinh *Lagrange*.



*Joseph – Louis Lagrange (1736 – 1813)*



*Lagrange* sinh ngày 25 – 1 – 1736 tại Turin (Italia), mất ngày 10 – 4 – 1813 tại Paris (Pháp). Ông được xem là một trong những thiên tài toán học lớn nhất trong lịch sử toán học, đồng thời cũng là một nhân vật đặc sắc trong thời đại ông – một thời đại đầy xáo động về mọi mặt: chính trị, văn hóa, xã hội.

Ông là người Pháp, nhưng có pha dòng máu Ý. Tổ phụ của *Lagrange* là một đại úy kỵ binh Pháp, đã tới phục vụ dưới trướng của Quốc vương đảo Sardinia là *Charles Emmanuel II*. Sau đó vị sĩ quan kỵ binh điển trai và anh dũng này tới định cư ở tỉnh Turin và được nhận vào làm rể của dòng họ quyền quý Conti của nước Ý. Thân phụ của *Lagrange* cũng được hưởng cái may mắn trong hôn ước như thế và đã kết duyên cùng cô *Marie – Thérèse Gros* là ái nữ độc nhất của một bác sĩ giàu có ở tỉnh Cambiano. Cặp tài tử và giai nhân này sống vui hạnh phúc và hai ông bà có đến mười người con nhưng tất cả đều mệnh yếu khi còn tuổi ấu thơ và chỉ về sau mới may mắn được thêm cậu út là *Joseph – Louis* ra đời ngày 25 tháng Giêng năm 1736 để rồi lớn lên và trở thành một nhà bác học danh tiếng lẫy lừng. Thân phụ của *Lagrange* cũng là người có tài trí, và đã có thời làm Tổng Giám Đốc ngân sách binh bị cho đảo quốc Sardinia. Ông xây dựng nên một tài sản khá lớn, lại cộng thêm với của hồi môn của bà vợ nên gia đình được vào hạng giàu có lớn trong tỉnh. Nhưng ông lại ham mê đầu tư nên theo với nền kinh tế đương thời ở Châu Âu, tài sản của gia đình bị giảm sút dần dần đến khánh kiệt khi *Lagrange* bước vào tuổi trưởng thành. Cậu con út được cưng chiều nay lại không được thừa kế chút di sản nào của cha mẹ, vì thật ra không còn gì đáng giá để lại. Trong cuộc đời sau này của *Lagrange*, ông thường cho sự phá sản đó lại là một điều may cho mình và đã nói rằng: "*Nếu tôi được hưởng một gia tài lớn thì chắc tôi đã không dựa vào Toán Học để xây dựng đời mình*".

## Sự Nghiệp Toán Học

Vào đầu thế kỷ 18, nền khoa học nói chung, và toán học nói riêng, chưa phải là một môn học chính cho sĩ tử, nên lúc mới đầu *Lagrange* theo về văn học cổ điển. Nhưng trong khi nghiên cứu về văn hoá Hy Lạp, chàng thanh niên được biết đến những công trình về Hình Học của những vĩ nhân toán học đời trước như *Euclid* (330 – 275 tr. CN) và *Archimedes* (287 – 212 tr. CN). Tuy vậy chàng cũng không chú ý lắm về những môn này. Nhưng sau đó *Lagrange* được đọc một bài tham luận của nhà thiên văn học *Edmund Halley* (1656 – 1742) ca tụng môn Giải Tích Học mới được xây dựng và hoàn bị bởi nhà bác học *Isaac Newton* (1642 – 1727) và cho rằng môn toán học này vượt trội hơn môn Hình Học. Bài này gợi trí tò mò của chàng thanh niên và anh đã dồn hết tâm trí vào để trong một thời gian ngắn học được hết những gì đã được công bố trên sách vở về những phép tính vi phân và tích phân trong môn giải tích học. Sự hiểu biết về toán học cao cấp này đã làm



cho *Lagrange* được bổ nhiệm làm giáo sư toán học tại *Trường Pháo binh Hoàng gia* ở tỉnh Turin khi chàng mới 16 tuổi. Nơi đây, hàng ngày *Lagrange* giảng bài cho lớp sinh viên mà người nào cũng lớn tuổi hơn mình. Tuy vậy chàng cũng thừa uy tín để chinh phục được mọi người và có nhiều năng lực để tổ chức được một *Hội Nghiên cứu Khoa học* là khởi thủy của một Trung tâm để sau này trở thành *Viện Hàn lâm Khoa học Turin*. Chỉ mấy năm sau, vào năm 1759, khi *Lagrange* mới 23 tuổi, mà *Hội Nghiên cứu* do chàng sáng lập đã xuất bản được *Tập san* đầu tiên. Nhưng ta phải nói rằng với một tâm địa tốt, luôn luôn nâng đỡ các bạn đồng nghiệp mà nhiều bài khảo cứu toán học đăng trên những số đầu tiên của tập san nghiên cứu, tuy ký tên những tác giả khác, mà thực ra là công trình của *Lagrange* vì đã được chàng sửa chữa và viết lại hoàn toàn. Trong những trường hợp này, có một tác giả của một bài viết thật đặc sắc – sau khi đã được *Lagrange* sửa lại – được mọi người chú ý và ngợi khen, và khi chuyển tới tai quốc vương Sardinia, tác giả được vời tới và giao cho giữ *Bộ Hải quân* là một chức vụ thật quan trọng vì Sardinia là một đảo quốc. Chỉ có một điều là trong lịch sử môn toán học, người ta thấy ông này chỉ viết ra được một bài độc nhất là bài mà do sự nâng đỡ của *Lagrange* đã giúp cho ông được địa vị trong triều. Cũng trong thời gian sáng tác phong phú này mà *Lagrange* đã tạo dựng nên lý thuyết cho môn *Cơ học Giải tích*.

Một bài toán được biết từ thời thượng cổ là *bài toán đẳng chu* (*isoperimetric problem*) khi người ta tìm một hình phẳng có một diện tích cực đại cho một chu vi cho sẵn. Lời giải tất nhiên là hình tròn nhưng phải đợi đến thế kỷ 17 mọi người mới chú ý đến những bài toán cực đại hay cực tiểu khi hai anh em toán gia *Bernouilli*, người Thụy Sĩ, ông anh tên là *James* (1654 – 1706) và người em là *John* (1667 – 1748) thách thức nhau giải bài toán sau đây:

"Từ một điểm khởi đầu *O*, thả trôi một cái vòng theo một đường giây nhẵn thín nằm trong mặt phẳng thẳng đứng, để cho tuột xuống một điểm *A* ở dưới. Phải uốn đường giây theo hình nào để cho thời gian tuột được ngắn nhất."

Dĩ nhiên hai anh em nhà *Bernouilli* không những đưa ra nhiều lời giải, nhưng lại còn đề ra nhiều bài toán khác nữa thuộc loại này. Những bài viết của anh em nhà *Bernouilli* đã gây phấn khởi cho một thiên tài toán học khác người Thụy Sĩ là *Leonhard Euler* (1707 – 1783) là học trò của *John Bernouilli*, và *Euler* đã đưa ra phương pháp tổng quát để giải những bài toán mà *James Bernouilli* đã đề nghị khi xưa. Ông cũng đặt tên cho phép tính này là *Phép tính biến thiên* (*Calculus of Variations*). Nhưng người thực sự đã đưa phép giải những bài toán để tìm ra những trường hợp tối ưu lại là *Lagrange*, lúc đó vẫn chỉ còn là một giáo sư ở Turin. Tuy chàng thanh niên, mới ở tuổi 19 và ở thế hệ sau, chỉ nghiên cứu bài toán đẳng



chu sau những bậc tiền bối danh tiếng vang lừng, nhưng *Lagrange* đã có những nhận xét tân kỳ để giải bài toán, và đã có can đảm viết một bức thư cho *Euler*, đang là Chủ tịch Ủy ban Toán học của Viện Hàn lâm Khoa học Vương quốc Phổ ở Berlin, để đưa ra một lời giải mà chàng cho là có tính cách tổng quát. Cũng may là *Euler* tuy là một thiên tài toán học thời ấy, danh tiếng vang lừng, nhưng cũng là người rộng lượng, ông nhận ngay ra rằng phương pháp của *Lagrange* đã giải toả được một vài thắc mắc của chính ông khi tìm phương pháp giải bài toán và *Euler* đã nhường cho *Lagrange* công bố kết quả ra trước. Hơn hai trăm năm sau, những khoa học gia không gian, khi tìm những quỹ đạo tối ưu để đưa những vệ tinh thám sát lên những hành tinh xa vời trong Thái dương hệ, đều phải viết những phương trình có tên chung là phương trình *Euler – Lagrange*. Không mấy người, dù chỉ trong một khoảnh khắc, đã nghĩ đến tài trí siêu việt của *Lagrange* và đức tính cao thượng của *Euler*, là những người đầu tiên đã khai phá ra môn toán học này. Trong những năm đầu tiên của một cuộc đời nghiên cứu và sáng tác toán học của *Lagrange*, những bài viết đều được đăng trong những tập san đề là *Miscellanea Taurinensia* tất cả tổng cộng có 5 Tập. Những bài viết này dù là để tên những học sinh hay những người cộng sự đều là do chàng giáo sư tuổi mới ngoài hai mươi đưa ra ý kiến và duyệt xét cùng sửa đổi lại. Tuy là ở một thị thành hẻo lánh nơi có hội toán học mà *Lagrange* sáng lập mà sau này trở thành Viện Hàn lâm Khoa học Turin, nhưng những tập san toán học phát xuất từ nơi đây, mà ngay ở số đầu tiên đã nói về *Phép tính biến thiên*, đã được toàn thế giới khoa học ở Âu châu chú ý tới và làm cho *Lagrange* đương nhiên trở thành một toán gia hàng đầu được mọi người ngưỡng mộ.

Ngoài toán gia *Euler*, *Lagrange* còn được một trưởng bối người Pháp là *D'Alembert* (1717 – 1783) nhiệt tình ủng hộ. Những người bạn tốt này đều nghĩ rằng chỉ khi nào chàng tới một thủ đô văn học và tiếp xúc với những toán gia hàng đầu của thế kỷ thì tài năng của *Lagrange* mới được nẩy nở toàn diện. Trước đó *Lagrange* đã được mời tới London, nhưng đi được nửa đường khi vừa tới Paris thì bị ốm. Nơi đây ông được tiếp đón trọng vọng và vì sức khoẻ chưa hồi phục được nên đành phải trở về Turin một thời gian để chờ cơ hội khác. Mấy năm sau thì dịp may đó tới khi đại toán gia *Euler* nhận lời mời của Viện Hàn lâm Khoa học St Petersburg để chuyển cư tới đó. Do đề nghị của 2 nhà toán học *D'Alembert* và *Euler*, Hoàng đế *Frederick* của Phổ Quốc đã viết cho *Lagrange* một bức thư đại để nói là Hoàng đế *Frederick* vĩ đại nhất châu Âu muốn được toán gia lừng danh nhất của thế kỷ tới vương triều để hàng ngày cùng nhau bàn luận. *Lagrange* đã nhận lời để tới Berlin thế vào chỗ trống của *Euler* và trong khoảng 20 năm khi cư ngụ ở Phổ Quốc ông đã viết hơn một trăm bài khảo luận toán học để đăng trên các tập san ở Turin và ở Berlin. Cũng trong thời gian này mà *Lagrange* hoàn tất tác phẩm vĩ đại nhất của đời ông về môn *Cơ học Giải tích*.





Khi mất ông được chôn cất trong điện Panthéon tại Paris.

*Nguồn nội dung: Diễn đàn toán học Việt Nam – VMF*

*Nguồn ảnh: Wikipedia*

## Chuyên đề

# ĐA THỨC VÀ SỐ HỌC

Tạp chí và tư liệu toán học

Trong chủ đề này, thay vì việc phân chia các dạng toán cụ thể kèm lời phân tích chi tiết từng dạng thì mình sẽ mang tới cho bạn đọc một tuyển tập các bài toán hay và khó để ôn tập và nâng cao kiến thức chuẩn bị cho kì thi học sinh giỏi cũng như các kì thi khác mà các bạn tham gia. Nào chúng ta cùng bắt đầu nhé!

## CÁC KIẾN THỨC CƠ BẢN

### 1. ĐA THỨC.

Đơn thức theo biến  $x$  là biểu thức có dạng  $m.x^n$  trong đó  $m$  là hằng số và  $n$  là số nguyên không âm.

Đa thức là tổng hữu hạn của nhiều đơn thức hay đa thức là biểu thức có dạng

$$P(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0 \quad (a_k \neq 0).$$

Khi đó

- $a_i$  được gọi là các hệ số của đa thức.

Nếu  $a_i \in \mathbb{Z}, \forall i$  thì ta gọi đa thức  $P \in \mathbb{Z}[x]$  tức tập các đa thức hệ số nguyên.

- $n$  được gọi là bậc của đa thức, ký hiệu là  $\deg P = n$ .

### 2. MỘT SỐ TÍNH CHẤT CẦN NẮM.

**Tính chất 1.** Với hai số nguyên  $a, b$  trong đó  $b \neq 0$ , nếu tồn tại số nguyên  $c$  sao cho  $a = bc$  thì ta gọi  $a$  chia hết cho  $b$  hoặc  $b$  chia hết  $a$  hoặc  $b$  là ước của  $a$  hoặc cũng hay gọi  $a$  là bội của  $b$ .

**Ký hiệu.**  $a:b$  hoặc  $b|a$ .

**Tính chất 2.** Với  $P \in \mathbb{Z}[x]$  và  $a, b$  là hai số nguyên khác nhau, ta luôn có

$$P(a) - P(b) : (a - b).$$

**Chứng minh.** Giả sử  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (a_n \neq 0)$ .

Sử dụng hằng đẳng thức  $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$  với  $k \geq 1$  là số nguyên.

Khi đó  $P(a) - P(b) = (a - b) \left[ a_n (a^{n-1} + a^{n-2}b + \dots + b^{n-1}) + a_{n-1} (a^{n-2} + a^{n-3}b + \dots + b^{n-2}) + \dots + a_1 \right]$ .



Từ đó bài toán được chứng minh.

**Tính chất 3.** Cho đa thức  $P(x)$  với hệ số nguyên.

Khi đó không tồn tại ba số phân biệt  $a, b, c$  sao cho  $P(a) = b, P(b) = c, P(c) = a$ .

### 3. NHỮNG ĐỊNH LÝ QUAN TRỌNG.

Hai đa thức  $f(x), g(x)$  được gọi là nguyên tố cùng nhau nếu ước chung lớn nhất của hai đa thức đó là một hằng số.

Nhưng vì ước chung lớn nhất của hai đa thức chỉ khác nhau hằng số nên nếu hai đa thức nguyên tố cùng nhau thì ta có thể xem ước chung lớn nhất của chúng là 1. Nên ta ký hiệu  $(f(x), g(x)) = 1$ .

**Định lý Bézout.** Cho hai đa thức  $P(x), Q(x) \in \mathbb{Q}[x]$ . Gọi  $d(x)$  là ước chung lớn nhất của hai đa thức  $P(x), Q(x)$ .

- Khi đó tồn tại hai đa thức  $U(x), V(x)$  sao cho  $d(x) = U(x).P(x) + V(x).Q(x)$ .
- Nếu  $(P(x), Q(x)) = 1$  thì tồn tại các đa thức  $U(x), V(x)$  sao cho

$$U(x).P(x) + V(x).Q(x) = 1.$$

**Định lý Schur.** Cho  $P(x) \in \mathbb{Z}[x]$  là đa thức khác đa thức hằng. Khi đó có vô hạn các số nguyên tố  $p$  thỏa mãn tính chất: Ứng với số nguyên tố  $p$  tồn tại số nguyên  $m$  sao cho  $p \mid P(m)$ .

**Chứng minh.**

Ta xét các trường hợp sau

**Trường hợp 1.** Hệ số tự do bằng 0. Khi đó  $p \mid P(p)$  với mọi số nguyên tố  $p$ .

**Trường hợp 2.** Hệ số tự do bằng 1. Tức là  $P(0) = 1$ .

Ta giả sử tập các số nguyên tố thỏa mãn bài toán là hữu hạn. Gọi  $p$  là số nguyên tố lớn nhất trong các số đó. Ta xét  $P(p!) \equiv 1 \pmod{p!}$ . Ta gọi  $q > 1$  là số nguyên tố khác mà thỏa mãn  $p \mid P(p!)$  thì  $q > p$  vì nếu  $q < p$  thì do  $q \mid (p!)$  nên từ  $q \mid P(p!)$  ta suy ra  $q \mid 1$  là vô lí. Nhưng  $q > p$  thì lại mâu thuẫn với chuyện  $p$  là số nguyên tố lớn nhất.

Trường hợp nếu  $P(0) = a \neq 1$ .

Ta xét đa thức  $Q(x) = \frac{1}{a}P(ax)$  thì  $Q(x) \in \mathbb{Z}[x]$  và  $Q(0) = 1$ . Theo trên tồn tại vô hạn các số nguyên tố  $p$  sao cho ứng với mỗi số  $p$  thì luôn tồn tại số nguyên  $m$  để cho  $p \mid Q(m)$ .

Nhưng nếu  $p \mid Q(x) \Rightarrow p \mid P(ax)$ . Định lý được chứng minh.

**Định lý Dirichlet về số nguyên tố.** Cho  $a, b$  là các số tự nhiên với  $a \neq 0, (a, b) = 1$ . Khi đó tập hợp  $\{an + b, n \in \mathbb{N}\}$  chứa vô hạn số nguyên tố.



**Định lý về dãy tuần hoàn.** Cho  $f, g$  là hai đa thức hệ số nguyên và nguyên tố cùng nhau. Đặt  $a_n = \gcd(f(n), g(n)), n = 1, 2, 3, \dots$ . Khi đó dãy  $(a_n)$  tuần hoàn.

**Chứng minh – Nguyễn Hữu Điển.**

Do  $f, g$  là hai đa thức hệ số nguyên và nguyên tố cùng nhau nên tồn tại hai đa thức  $F, G$  và số nguyên dương  $a$  sao cho  $f.F + g.G = a$ . Khi đó do chia hết cho cả  $f(n), g(n)$  nên ta có  $f(n) | a, \forall n$ . Ta sẽ chứng minh  $a_n$  tuần hoàn theo chu kỳ  $a$ .

Ta chứng minh rằng  $a_n | a_{n+a}$ .

Thật vậy ta có  $f(n) \equiv f(n+a) \pmod{a}$  mà  $a_n | a, a_n | f(n) \Rightarrow a_n | f(n+a)$ .

Tương tự ta có  $a_n | g(n+a)$ . Như vậy ta có  $a_n | a_{n+a}$ .

Lập luận tương tự ta có  $a_n | a_{n+a}$ . Vậy  $a_n = a_{n+a}$ .

**Chú ý.** Hai đa thức nguyên tố cùng nhau khi ước chung lớn nhất của chúng là một đa thức hằng.

**Bổ đề Hensel.** Cho đa thức  $f(x)$  hệ số nguyên và số nguyên tố  $p$ . Nếu phương trình đồng dư  $f(x) \equiv 0 \pmod{p}$  có đúng  $r$  nghiệm phân biệt  $x_1^{(1)}, x_2^{(1)}, \dots, x_r^{(1)}$  thuộc đoạn  $[1; p]$  sao cho  $f'(x_i^{(1)}) \not\equiv 0 \pmod{p}, i = \overline{1, r}$  thì phương trình đồng dư  $f(x) \equiv 0 \pmod{p^k}$  có đúng  $r$  nghiệm nguyên phân biệt thuộc đoạn  $[1, p^k]$ .

**Chứng minh.**

Với  $k = 1$  hiển nhiên đúng.

Giả sử khẳng định đúng với  $k \geq 1$ . Điều đó có nghĩa là trên đoạn  $[1, p^k]$ , phương trình  $f(x) \equiv 0 \pmod{p^k}$  có đúng  $r$  nghiệm  $x_1^{(k)}, x_2^{(k)}, \dots, x_r^{(k)}$  và  $f'(x_i^{(k)}) \not\equiv 0 \pmod{p}, i = \overline{1, r}$ .

Ta cần chứng minh  $f(x) \equiv 0 \pmod{p^{k+1}}$  có đúng  $r$  nghiệm thuộc  $[1, p^{k+1}]$ .

Gọi  $x_0$  là một nghiệm của phương trình  $f(x) \equiv 0 \pmod{p}$  (1).

Xét số  $x_1 = x_0 + p^k t, t \in [0; p-1]$  với  $t$  là nghiệm duy nhất của phương trình

$$\frac{f(x_0)}{p^k} + f'(x_0)t \equiv 0 \pmod{p}$$

Ta sẽ chứng minh  $x_1$  là nghiệm của  $f(x) \equiv 0 \pmod{p^{k+1}}$  (2).

Ta có  $f(x_1) = f(x_0) + \frac{f'(x_0)}{1!}(x_1 - x_0) + \frac{f''(x_0)}{2!}(x_1 - x_0)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(x_1 - x_0)^n$

$$f(x_1) = f(x_0) + \frac{f'(x_0)}{1!}p^k t + \frac{f''(x_0)}{2!}(p^k t)^2 + \dots + \frac{f^{(n)}(x_0)}{n!}(p^k t)^n$$

Suy ra  $f(x_1) \equiv f(x_0) + f'(x_0)p^k t \pmod{p^{k+1}}$  vì  $\frac{f^{(i)}(x_0)}{i!} \in \mathbb{Z}$



$$\Rightarrow f(x_1) \equiv p^k \left[ \frac{f(x_0)}{p^k} + f'(x_0)t \right] \pmod{p^{k+1}} \equiv 0 \pmod{p^{k+1}}$$

Vậy phương trình (2) có ít nhất  $r$  nghiệm.

Thật vậy, giả sử  $x$  là nghiệm của (2), gọi  $x_0$  là nghiệm của (1). Ta có

$$f(x) \equiv 0 \pmod{p^{k+1}} \Rightarrow f(x) \equiv f(x_0) \pmod{p^k} \Rightarrow x \equiv x_0 \pmod{p^k} \Rightarrow x = x_0 + p^k t$$

Theo chứng minh trên thì  $t$  là nghiệm của phương trình  $\frac{f(x_0)}{p^k} + f'(x_0)t \equiv 0 \pmod{p}$ .

Vậy phương trình  $f(x) \equiv 0 \pmod{p^{k+1}}$  có đúng  $r$  nghiệm.

Từ cách chứng minh trên ta rút ra được nhận xét sau.

**Nhận xét.**  $f(x_0 + p^k t) \equiv f(x_0) + f'(x_0)p^k t \pmod{p^{k+1}}$

**Công thức nội suy Lagrange.**

Cho đa thức  $P(x)$  có bậc nhỏ hơn  $(n+1)$  và  $(n+1)$  số thực phân biệt  $x_i, i = \overline{1, n+1}$ .

Khi đó  $P(x)$  được xác định duy nhất như sau:  $P(x) = \sum_{i=1}^{n+1} P(x_i) \cdot \prod_{\substack{j=1 \\ j \neq i}}^{n+1} \frac{x - x_j}{x_i - x_j}$ .



## ĐỀ BÀI

**Câu 1.** Tìm các đa thức  $P(x)$  có hệ số nguyên, không âm, bậc không lớn hơn 6 thỏa  $P(7) = 102013$ .

**Câu 2.** Cho  $a, b, c \in \mathbb{Z}$  thỏa mãn các đa thức  $f(x) = ax^2 + bx + c$  và  $g(x) = (a-b)x^2 + (c-a)x + a+b$  có nghiệm chung. Chứng minh rằng  $a+b+2c \vdots 3$ .

**Câu 3.** Tồn tại hay không đa thức  $f(x) = x^2 + ax + b$  với  $a, b$  nguyên thỏa mãn  $a^2 - 4b \neq 0$  và nhận giá trị chính phương tại 2010 điểm phân biệt.

**Câu 4.** Chứng minh rằng không tồn tại đa thức  $P$  với hệ số nguyên, khác đa thức hằng có bậc không quá 4 thỏa mãn: tồn tại 5 số nguyên  $x_1, x_2, \dots, x_5$  khác nhau sao cho

$$P(x_1)P(x_2)P(x_3)P(x_4)P(x_5) = -1.$$

**Câu 5.** Chứng minh  $x^n - x - 1$  bất khả quy trên  $\mathbb{Z}[x]$ ,  $\forall n \geq 2$

**Câu 6.** Cho đa thức  $P$  là đa thức hệ số và tồn tại số nguyên dương  $m$  sao cho  $P(1); P(2); \dots; P(m)$  không chia hết cho  $m$ . Chứng minh rằng  $P(a) \neq 0$  với mọi  $a \in \mathbb{Z}$ .

**Câu 7.** Cho  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  là đa thức với  $a_0, a_1, \dots, a_n$  là các số nguyên dương. Đặt  $P_1(x) = P(x)$  và  $P_k(x) = P(P_{k-1}(x))$  với  $k > 1$ . Tồn tại hay không  $M > 0$  sao cho với  $m \geq M$  ta có  $m \mid P_{P(m)}(m)$

**Câu 8.** Cho đa thức  $P(x)$  là đa thức hệ số nguyên với bậc  $n \geq 2$ . Chứng minh rằng đa thức  $P(P(x)) - x$  có nhiều nhất  $n$  nghiệm.

**Câu 9.** Tìm tất cả các đa thức  $P$  hệ số nguyên sao cho  $P(n) \mid 2^n - 1$  với mọi số nguyên dương  $n$ .

**Câu 10.** Gọi  $x_0, x_1, \dots, x_n$  là các số nguyên thỏa mãn  $x_0 > x_1 > \dots > x_n$ . Chứng minh rằng một trong các số  $|P(x_0)|, |P(x_1)|, \dots, |P(x_n)|$  không nhỏ hơn  $\frac{n!}{2^n}$  với  $P(x)$  là đa thức bậc  $n$ .

**Câu 11.** Giả sử các đa thức  $P(x), Q(x), R(x)$  và  $S(x)$  thỏa mãn:

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x)$$

Chứng minh rằng khi đó đa thức  $P(x)$  chia hết cho  $x-1$ .

**Câu 12.** Tìm tất cả các đa thức  $P$  có hệ số nguyên sao cho với mọi số nguyên tố  $p$  và mọi cặp số tự nhiên  $(u, v)$  thỏa mãn  $P \mid (uv-1)$  thì ta có  $P \mid (P(u)P(v)-1)$ .

**Câu 13.** Tìm tất cả các đa thức  $P$  hệ số nguyên sao cho với mọi số tự nhiên  $a, b, c$  ta luôn có  $a+b+c \mid P(a)+P(b)+P(c)$ .

**Câu 14.** Cho  $m, n$  là các số nguyên dương. Chứng minh rằng  $n \vdots m$  khi và chỉ khi  $P(x) \vdots Q(x)$ , trong đó  $P(x); Q(x)$  là các đa thức hệ số nguyên được xác định:



$$P(x) = x^{n-1} + C_n^1 x^{n-2} + \dots + C_n^{n-1}$$

$$Q(x) = x^{m-1} + C_m^1 x^{m-2} + \dots + C_m^{m-1}$$

**Câu 15.** Tìm tất cả các đa thức  $P$  hệ số nguyên thỏa mãn tính chất: Với  $m, n$  là hai số nguyên tố cùng nhau thì hai số  $P(m); P(n)$  cũng là hai số nguyên tố cùng nhau.

**Câu 16.** Cho  $P(x), Q(x) \in \mathbb{Z}[x]$  là hai đa thức *monic* bất khả quy thỏa mãn với  $n$  đủ lớn thì  $P(n), Q(n)$  có cùng tập ước nguyên tố. Chứng minh rằng  $P = Q$ .

**Câu 17.** Gọi đa thức  $P(x) \in \mathbb{Z}[x]$  khác đa thức hằng và gọi  $n, k$  là hai số nguyên dương. Chứng minh rằng tồn tại số nguyên dương  $a$  sao cho mỗi  $f(a), f(a+1), \dots, f(a+n-1)$  có ít nhất  $k$  ước nguyên tố phân biệt.

**Câu 18.** Cho đa thức  $P(x), Q(x)$  là hai đa thức có hệ số nguyên nguyên tố cùng nhau. Đặt  $a_n = (P(n), Q(n))$ . Chứng minh dãy  $\{a_n\}$  tuần hoàn.

**Câu 19.** Với hai đa thức có hệ số nguyên  $p(x), q(x)$  ta viết  $p(x) \equiv q(x) \pmod{2}$  nếu  $p(x) - q(x)$  có tất cả các hệ số đều chia hết cho 2. Cho dãy đa thức  $p_n(x)$  thỏa mãn  $p_1(x) = p_2(x) = 1$  và  $p_{n+2}(x) = p_{n+1}(x) + xp_n(x)(1)$ , với mọi  $n$  là số tự nhiên. Chứng minh rằng  $p_{2^n}(x) \equiv 1 \pmod{2}$ .

**Câu 20.** Giả sử  $p_{2^n}(x) \equiv 1$  là hai số tự nhiên lớn hơn 1 và  $p_n(x) = p_n$ .

Dãy số vô hạn  $n = 1, 2, 3, \dots$  được xác định như sau

$$p_{n+4} = p_{n+3} + xp_{n+2} = (p_{n+2} + xp_{n+1}) + xp_{n+2} = (x+1)p_{n+2} + xp_{n+1}$$

Chứng minh rằng trong dãy số nói trên chứa vô hạn số đôi một nguyên tố cùng nhau.

**Câu 21.** Với mỗi số tự nhiên  $n$ , ta kí hiệu  $f(n)$  là tổng các chữ số của nó biểu diễn trong hệ thập phân. Ta xây dựng dãy số như sau

$$u_1(n) = f(n); u_2(n) = f(f(n)); \dots; u_k(n) = \underbrace{f(f(\dots f(n)\dots))}_k$$

Chứng minh rằng với mọi số tự nhiên  $n$ , tồn tại số tự nhiên  $d$  sao cho

$$u_k(n) = u_d(n), \forall k \geq d(1).$$

**Câu 22.** Cho  $\overline{abc}$  là một số nguyên tố.

Chứng minh rằng phương trình  $ax^2 + bx + c = 0$  (1) không có nghiệm hữu tỉ.

**Câu 23.** Cho đa thức  $P(x) = (x^2 - 2)(x^2 - 3)(x^2 - 6)$ . Chứng minh rằng với mọi số nguyên tố  $p$  đều tìm được số nguyên dương  $n$  sao cho  $P(n) \vdots p$ .

**Câu 24.** Chứng minh rằng với mọi số nguyên  $p$  ta có thể tìm được số nguyên dương  $f(x)$  sao cho  $n$  không phải là số chính phương.



**Câu 25.** Cho đa thức  $P(x) = x^{2017} - x^{1000} + 1$ . Tồn tại hay không các số tự nhiên  $a_1, a_2, \dots, a_{2018}$  sao cho tích  $P(a_i) \cdot P(a_j) : a_i a_j$  với mọi  $i \neq j$ .

**Câu 26.** Với mọi số tự nhiên  $m, n$ , chứng minh rằng  $(n!)$  chia hết cho  $m$  khi và chỉ khi tồn tại đa thức hệ số nguyên  $f(x) = \sum_{k=0}^n a_k x^k$  thỏa mãn  $(a_0, a_1, \dots, a_n, m) = 1, m \mid f(j)$  với mọi  $j$  nguyên dương.

**Câu 27.** Cho đa thức  $f(x) = 2009x^5 - x^4 - x^3 - x^2 - 2006x + 1$ . Chứng minh rằng với  $n$  là số nguyên tùy ý thì các số  $f(n), f(f(n)), \dots, f(\dots f(n) \dots)$  đôi một nguyên tố cùng nhau.

**Câu 28.** Gọi  $P(x)$  là đa thức bậc  $n$  thỏa mãn với  $k = 0, 1, \dots, n$  thì  $P(k) = \binom{n+1}{k}^{-1}$

Định đa thức  $P(n+1)$ .

**Câu 29.** Cho dãy  $\{u_n\}$  được xác định như sau  $\begin{cases} u_1 = 1990, u_2 = 1989, u_3 = 2000 \\ u_{n+3} = 19u_{n+2} + 9u_{n+1} + u_n + 1991, n = 1, 2, \dots \end{cases}$

a) Với mọi  $n$  gọi  $r_n$  là số dư của phép chia  $u_n$  cho 1992. Chứng minh rằng dãy  $\{r_n\}$  là một dãy tuần hoàn.

b) Chứng minh rằng tồn tại vô số số  $x$  của dãy  $\{u_n\}$  sao cho

$$5x^{1992} + 5x^{1994} + 4x^{1975} + 8x^{1945} + 2x^{1990} + 11x^2 + 48$$

chia hết cho 1992.

**Câu 30.** Chứng minh rằng tồn tại hằng số dương  $c$  sao cho với mọi số nguyên dương  $n$  và các số thực  $a_1, a_2, \dots, a_n$ , nếu  $P(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$  thì

$$\max_{x \in [0, 2]} |P(x)| \leq c^n \max_{x \in [0, 1]} |P(x)|$$

**Câu 31.** Tìm tất cả các đa thức  $P(x) \in \mathbb{Z}[x]$  và  $m \in \mathbb{Z}^+$  sao cho  $m + 2^n P(n)$  là số chính phương với mọi số nguyên dương  $n$ .

**Câu 32.** Cho  $P(x) \in \mathbb{Z}[x]$ ,  $p$  là số nguyên tố và  $x \equiv a \pmod{p}$ . Chứng minh rằng

$$P(x) \equiv P(a) + (x - a)P'(a) \pmod{p^2}$$

**Câu 33.** Với  $p$  là số nguyên tố, đặt  $h(x)$  là đa thức có hệ số nguyên sao cho  $h(0), h(1), \dots, h(p^2 - 1)$  là một hệ thặng dư đầy đủ modulo  $p^2$ . Chứng minh rằng  $h(0), h(1), \dots, h(p^3 - 1)$  là một hệ thặng dư đầy đủ modulo  $p^3$ .

**Câu 34.** Với số nguyên  $n \geq 3$ , đặt  $f(x), g(x)$  là đa thức với hệ số thực sao cho các điểm  $(f(1), g(1)), (f(2), g(2)), \dots, (f(n), g(n))$  trong tập  $\mathbb{R}^2$  là các đỉnh của đa giác  $n$  cạnh theo thứ tự ngược chiều kim đồng hồ. Chứng minh rằng ít nhất một trong các đa thức  $f, g$  có bậc không nhỏ hơn  $n - 1$ .





**Câu 35.** Cho  $p$  là một số nguyên tố lẻ. Chứng minh rằng có ít nhất  $\frac{p+1}{2}$  giá trị

$n \in \{0, 1, 2, \dots, p-1\}$  sao cho  $\sum_{k=0}^{p-1} k!n^k$  không chia hết cho  $p$ .

**Câu 36.** Có tồn tại hay không một dãy số thực và khác 0 là  $a_1; a_2; \dots, a_n$  thỏa với mỗi  $n \in \mathbb{N}$  thì đa thức  $a_0 + a_1x + \dots + a_nx^n$  có đúng  $n$  nghiệm trên  $\mathbb{R}$ .

**Câu 37.** Cho  $P(x) \in \mathbb{Z}[x]$  thỏa mãn  $P(x)$  là số chính phương với mọi  $x$  nguyên thì  $P(x) = Q^2(x)$  với  $Q(x) \in \mathbb{Z}[x]$ .

**Câu 38.** Tìm tất cả các đa thức số hệ số nguyên thỏa mãn  $a+b$  là số chính phương thì  $P(a)+P(b)$  cũng là số chính phương, trong đó  $a, b$  là các số tự nhiên.

**Câu 39.** Giả sử  $m, p$  là các số nguyên tố khác nhau. Chứng minh rằng nếu có một số tự nhiên  $x$  nào đó mà  $p$  là ước của  $P(x) = (x^{m-1} + x^{m-2} + \dots + 1)$  thì ta có  $p \equiv 1 \pmod{m}$ .

**Câu 40.** Cho đa thức  $P(x)$  có bậc  $n$  và có  $n$  nghiệm phân biệt  $x_1, x_2, \dots, x_n$ .

Chứng minh rằng:

$$a) \frac{P''(x_1)}{P'(x_1)} + \frac{P''(x_2)}{P'(x_2)} + \dots + \frac{P''(x_n)}{P'(x_n)} = 0$$

$$b) \frac{1}{P'(x_1)} + \frac{1}{P'(x_2)} + \dots + \frac{1}{P'(x_n)} = 0$$

**Câu 41.** Cho  $f$  là một đa thức có hệ số hữu tỉ và bậc không nhỏ hơn 2, và dãy  $(a_n)$  chỉ gồm các số hữu tỉ thỏa mãn  $f(a_{n+1}) = a_n$  với mọi số nguyên dương  $n$ . Chứng minh rằng dãy  $(a_n)$  tuần hoàn.

**Câu 42.** Cho  $P(x)$  là đa thức bậc  $n$  với hệ số thực sao cho  $P(-1)$  khác 0 và  $-\frac{P'(-1)}{P(-1)} \leq \frac{n}{2}$

Chứng minh rằng  $P(x)$  luôn có ít nhất một nghiệm  $x_0$  sao cho  $|x_0| > 1$ .

**Câu 43.** Giả sử tồn tại đa thức hệ phức  $P, Q, R$  thỏa mãn  $P^a + Q^b = R^c$  ( $a, b, c \in \mathbb{N}$ ).

Chứng minh rằng  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$

**Câu 44.** Cho đa thức  $P(x)$  và  $Q(x)$  với số thực  $k$  bất kì thỏa mãn  $P_k = \{z \in \mathbb{C} | P(z) = k\}$  và  $Q_k = \{z \in \mathbb{C} | Q(z) = k\}$ . Chứng minh rằng  $P_0 = Q_0$  và  $P_1 = Q_1$  suy ra được  $P(x) = Q(x)$ .

**Câu 45.** Cho đa thức  $P(x) \in \mathbb{Z}[x], \deg P \geq 2$ . Chứng minh rằng tồn tại  $m \in \mathbb{Z}^+$  để  $P(m!)$  là hợp số.



**Câu 46.** Cho  $f(x)$  là đa thức với hệ số hữu tỉ bậc lớn hơn hoặc bằng 2. Xét dãy  $\{a_n\}$  các số hữu tỉ thỏa mãn điều kiện  $f(a_{n+1}) = a_n, n \geq 1$ . Chứng minh rằng tồn tại  $k \geq 1$  để  $a_{n+k} = a_n (n \geq 1)$ .

**Câu 47.** Tìm tất cả đa thức  $P \in \mathbb{Z}[x]$  sao cho  $P(p) \mid 2^p - p, \forall p$  là số nguyên tố

**Câu 48.** Xét đa thức  $T(x) = x^3 + 17x^2 - 1239x + 2001$ . Đặt

$$T_1(x) = T(x), T_2(x) = T(T_1(x)), \dots, T_{n+1}(x) = T(T_n(x)) \text{ với mọi } n = 1, 2, 3, \dots$$

Chứng minh rằng tồn tại số nguyên  $n > 1$  sao cho  $T_n(x) - x$  chia hết cho 2003 với mọi số nguyên  $x$ .

**Câu 49.** Tìm tất cả các cặp số nguyên  $a, b$  sao cho tồn tại đa thức  $P(x) \in \mathbb{Z}[x]$  sao cho tích  $(x^2 + ax + b) \cdot P(x)$  là đa thức được viết dưới dạng:

$$x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 \text{ với } c_0, c_1, \dots, c_{n-1} \text{ bằng } 1 \text{ hoặc } -1$$

**Câu 50.** Cho hai đa thức hệ số nguyên

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

Biết rằng  $a_n - b_n$  là một số nguyên tố và  $a_{n-1} = b_{n-1}$ . Gọi  $m$  là một nghiệm hữu tỷ chung của hai đa thức. Chứng minh rằng  $m$  là một số nguyên.

**Câu 51.** Hỏi có tất cả bao nhiêu đa thức  $P_n(x)$  bậc  $n$  chẵn thỏa mãn các điều kiện

- Các hệ số của  $P_n(x)$  thuộc tập  $M = \{0; -1; 1\}$  và  $P_n(0) \neq 0$ .
- Tồn tại đa thức  $Q(x)$  có các hệ số thuộc  $M$  sao cho  $P_n(x) \equiv (x^2 - 1) \cdot Q(x)$ .

**Câu 52.** Cho dãy số nguyên  $(a_n)_{n=1}^{\infty}$  thỏa mãn  $m - n \mid a_m - a_n$  với mọi số tự nhiên  $m, n$  phân biệt. Giả sử tồn tại đa thức  $P(x)$  sao cho  $|a_n| < P(n), \forall n$ . Chứng minh rằng tồn tại đa thức  $Q(x)$  sao cho  $a_n = Q(n), \forall n$ .

**Câu 53.** Cho  $n$  là số nguyên dương và  $a_1, a_2, \dots, a_n$  là các số thực dương.

Ta đặt  $g(x) = (x + a_1)(x + a_2) \dots (x + a_n)$ .

Gọi  $a_0$  là một số thực bất kỳ và đặt  $f(x) = (x - a_0)g(x) = x^{n+1} + b_1 x^n + \dots + b_n x + b_{n+1}$ .

Chứng minh rằng  $b_1, b_2, \dots, b_{n+1}$  đều là số âm khi và chỉ khi  $a_0 > a_1 + a_2 + \dots + a_n$ .

**Câu 54.** Cho  $F$  là tập các đa thức  $\Gamma$  có hệ số nguyên và phương trình  $\Gamma(x) = 1$  có nghiệm nguyên. Cho trước một số nguyên dương  $k$ , tìm giá trị nhỏ nhất của  $m > 1$  theo  $k$  thỏa mãn tồn tại  $\Gamma \in F$  sao cho  $\Gamma(x) = m$  có đúng  $k$  nghiệm nguyên phân biệt.



**Câu 55.** Cho hai đa thức  $P(x), Q(x) \in \mathbb{R}[x]$  nguyên tố cùng nhau và khác đa thức hằng. Chứng minh rằng không có quá ba số thực  $\lambda$  thỏa mãn  $P(x) + \lambda Q(x)$  là bình phương của một đa thức.

**Câu 56.** Chứng minh rằng nếu đa thức  $f(x) \in \mathbb{R}[x]$  có bậc  $n$  và nhận giá trị nguyên tại  $n+1$  giá trị nguyên liên tiếp từ  $a \rightarrow a+n, a \in \mathbb{Z}$  thì  $f(x) \in \mathbb{Z}, \forall x \in \mathbb{Z}$ .

**Câu 57.** Tìm tất cả các đa thức  $P(x) \in \mathbb{Z}[x]$  sao cho với mọi  $a, b$  mà  $a$  không là nghiệm của  $P(x)$  thì  $P(a) \mid P(a+b) - P(b)$ .

**Câu 58.** Xét đa thức  $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  với  $n \geq 2, n \in \mathbb{N}$ . Giả sử  $P(x)$  có  $n$  nghiệm là  $x_1, x_2, \dots, x_n$ . Kí hiệu  $\max(x_i)$  là số lớn nhất trong các số  $x_1, x_2, \dots, x_n$ . Chứng minh rằng  $P(x+\delta) \sum_{i=1}^n \frac{1}{x-x_i} \geq 2n^2\delta^{n-1}, \forall x > \max(x_i)$  với  $\delta > 0$ .

**Câu 59.** Giả sử  $R$  là nghiệm của phương trình  $x^n - a_1x^{n-1} - \dots - a_{n-1}x - a_n = 0$  và đặt

$$A = \sum_{j=1}^n a_j, B = \sum_{j=1}^n ja_j. \text{ Khi đó thì ta có } A^A \leq R^B.$$

**Câu 60.** Cho đa thức  $P(x)$  là đa thức monic bậc  $n > 1$  có  $n$  nghiệm thực là  $x_1, x_2, \dots, x_n$  phân biệt và khác 0. Chứng minh rằng:

$$\frac{1}{x_1 P'(x_1)} + \frac{1}{x_2 P'(x_2)} + \dots + \frac{1}{x_n P'(x_n)} = \frac{(-1)^{n+1}}{x_1 x_2 \dots x_n}$$

**Câu 61.** Cho  $n \geq 2$  và đa thức  $P(x)$  xác định bởi  $P(x) = \sum_{k=0}^n \frac{x^k}{k!}$ . Chứng minh rằng phương trình  $P(x) = 0$  không có nghiệm hữu tỉ.

**Câu 62.** Cho  $p$  là một số nguyên tố. Tìm tất cả các đa thức  $f(x)$  với hệ số nguyên sao cho với mọi số nguyên dương  $n$ ,  $f(x)$  là ước của  $p^n - 1$ .

**Câu 63.** Cho số nguyên dương  $n$  và số nguyên tố  $p$  lớn hơn  $n+1$ . Chứng minh rằng đa thức  $P(x) = 1 + \frac{x}{n+1} + \frac{x^2}{2n+1} + \dots + \frac{x^p}{pn+1}$  không có nghiệm nguyên.

**Câu 64.** Cho đa thức  $P(x) = x^3 - 11x^2 - 87x + m (m \in \mathbb{Z})$ . Chứng minh rằng với mọi  $m$  tồn tại số nguyên  $n$  sao cho  $P(n) \vdots 191$ .

**Câu 65.** Cho  $m$  là số nguyên dương, tìm số nghiệm của phương trình  $x^2 \equiv x \pmod{m}$ .

**Câu 66.** Cho  $p$  là số nguyên tố ( $p \geq 3$ ). Xét đa thức

$$f(x) = (p-1)x^{p-2} + (p-2)x^{p-3} + 3x^2 + 2x + 1.$$



Biết rằng hệ  $A = \{a_1, a_2, \dots, a_p\}$  là một hệ thặng dư đầy đủ modulo  $p$ . Chứng minh rằng khi đó hệ  $B = \{f(a_1), f(a_2), \dots, f(a_p)\}$  cũng là một hệ thặng dư đầy đủ modulo  $p$ .

**Câu 67.** Xét đa thức  $P(x) = x^3 + 14x^2 - 2x + 1$ . Chứng minh rằng tồn tại số nguyên dương  $n$  sao cho với mọi số nguyên  $x$  ta có  $101 \mid P(P \dots P(x) \dots) - x$ .

**Câu 68.** Cho tập  $S = \{p_1, p_2, \dots, p_k\}$  là tập hợp  $k$  số nguyên tố phân biệt và  $P(x)$  là đa thức với hệ số nguyên sao cho với mọi số nguyên dương  $n$  đều tồn tại  $p_i$  trong  $S$  sao cho  $p_i \mid P(n)$ . Chứng minh rằng tồn tại  $i$  sao cho  $p_i \mid P(n), \forall n \in \mathbb{N}^*$ .

**Câu 69.** Cho đa thức  $P(x) = x^3 + 153x^2 - 111x + 38$ .

a) Chứng minh rằng trong đoạn  $[0; 3^{2000}]$  tồn tại ít nhất một số nguyên dương  $a$  sao cho  $P(a) \vdots 3^{2000}$ .

b) Hỏi trong đoạn  $[0; 3^{2000}]$  có tất cả bao nhiêu số nguyên dương  $a$  sao cho  $P(a)$  chia hết cho  $3^{2000}$ .

**Câu 70.** Tìm tất cả các đa thức  $f$  với hệ số nguyên sao cho  $f(n) \mid f(m) \Rightarrow n \mid m$ .

**Câu 71.** Cho  $a, b, c, d, e, f$  là các số nguyên dương. Giả sử rằng  $S = a + b + c + d + e + f$  là ước của các số  $abc + def$  và  $ab + bc + ca - de - ef - fd$ . Chứng minh rằng  $S$  là hợp số.

**Câu 72.** Tìm tất cả các đa thức  $P$  với hệ số nguyên thỏa mãn

$$P(n) \mid 2557^n + 213.2014, \forall n \in \mathbb{N}^*$$

**Câu 73.** Cho  $P$  là đa thức hệ số nguyên, có bậc  $n > 1$  và  $k$  là số nguyên dương bất kỳ. Xét đa thức  $Q(x) = P^k(x)$  với  $P$  được tác động  $k$  lần. Chứng minh rằng có nhiều nhất  $n$  số nguyên  $t$  sao cho  $Q(t) = t$ .

**Câu 74.** Cho  $A$  là tập vô hạn các số nguyên dương. Tìm tất cả các số nguyên dương  $n$  thỏa mãn với mọi  $a$  là phần tử của  $A$  thì

$$1 + a + a^2 + \dots + a^n \mid 1 + a^{1!} + a^{2!} + \dots + a^{n!}$$

**Câu 75.** Cho  $P, Q$  là hai đa thức hệ số nguyên không âm, khác đa thức hằng. Xét dãy số  $x_n = 2016^{P(n)} + Q(n), n \geq 1$ . Chứng minh rằng tồn tại vô hạn số nguyên tố  $p$  thỏa mãn: ứng với mỗi  $p$ , tồn tại số nguyên dương  $m$  sao cho  $p \mid x_m$ .

**Câu 76.** Tìm tất cả các đa thức  $P$  hệ số nguyên thỏa mãn  $P(p) \mid 2^p - p$ , với mọi số nguyên tố  $p$ .

**Câu 77.** Cho  $P(x), Q(x)$  là các đa thức hệ số nguyên khác đa thức hằng. Giả sử rằng đa thức  $P(x).Q(x) - 2009$  có ít nhất 25 nghiệm nguyên phân biệt. Chứng minh rằng bậc của mỗi đa thức  $P(x), Q(x)$  đều không nhỏ hơn 3.



**Câu 78.** Gọi  $d(n)$  là ước nguyên tố nhỏ nhất của số nguyên  $n$ , với  $n \neq \{-1, 0, 1\}$  và ta kí hiệu  $d(-1) = d(0), d(1) = 0$ .

Tìm tất cả các đa thức  $P(x)$  với hệ số nguyên thỏa mãn  $P(n + d(n)) = n + d(P(n))$ .

**Câu 79.** Tìm tất cả các số nguyên dương  $k$  thỏa mãn tồn tại đa thức  $f(x)$  với các hệ số đều nguyên, có bậc lớn hơn 1 sao cho với mọi số nguyên tố  $p$  và mọi số tự nhiên  $a, b$  mà  $p | ab - k$  thì  $p | f(a)f(b) - k$ .

**Câu 80.** Cho  $P$  là đa thức hệ số nguyên thỏa mãn  $P(0) = 0$  và  $(P(0), P(1), \dots) = 1$ . Chứng minh rằng có vô hạn số  $n$  sao cho  $(P(n) - P(0), P(n+1) - P(1), \dots) = n$ .

**Câu 81.** Cho  $p$  là số nguyên tố và  $P(x)$  là các đa thức bậc  $d$  hệ số nguyên thỏa mãn

- $P(0) = 0, P(1) = 1$
- Với mọi số nguyên dương  $n$  thì số dư trong phép chia  $P(n)$  cho  $p$  là 0 hoặc 1.

Chứng minh rằng  $d \geq p - 1$ .

**Câu 82.** Chứng minh rằng không tồn tại đa thức  $P$  hệ số thực  $\deg P = n \geq 1$  sao cho  $P(m)$  là số nguyên tố với mọi số nguyên dương  $m$ .

**Câu 83.** Cho  $n \in \mathbb{N}, n > 3$  và đa thức  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$  thỏa mãn  $a_0$  chẵn,  $a_k + a_{n-k}$  chẵn với mọi  $k = \overline{1, n-1}$ .

Giả sử thêm rằng tồn tại hai đa thức  $g(x), h(x) \in \mathbb{Z}[x]$  thỏa mãn  $\deg g \leq \deg h$ , mọi hệ số của  $h(x)$  đều lẻ và  $f(x) = g(x)h(x), \forall x$ .

Chứng minh rằng  $f(x)$  có ít nhất một nghiệm nguyên.

**Câu 84.** Cho đa thức  $f(x)$  monic, hệ số nguyên, bất khả quy và  $f(0)$  không phải là số chính phương. Chứng minh rằng  $g(x) = f(x^2)$  cũng là đa thức bất khả quy.

**Câu 85.** Cho đa thức hệ số nguyên  $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  thỏa mãn điều kiện  $|a_0| > |a_1| + |a_2| + \dots + |a_n|$  và  $|a_0|$  là số nguyên tố thì  $f(x)$  bất khả quy.

**Câu 86.** Tìm tất cả các đa thức  $P(x), Q(x)$  hệ số nguyên thỏa mãn với dãy số  $(x_n)$  xác định bởi  $x_0 = 2014, x_{2n+1} = P(x_{2n}), x_{2n+2} = Q(x_{2n+1}), \forall n \in \mathbb{N}$  thì mỗi số nguyên dương  $m$  là ước của một số hạng khác 0 nào đó của  $(x_n)$ .

**Câu 87.** Chứng minh rằng không tồn tại đa thức

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x] \text{ bậc } n \geq 1$$

sao cho  $P(0), P(1), \dots$  đều là số nguyên tố.

**Câu 88.** Cho đa thức  $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, P(x) \in \mathbb{Z}[x]$  với  $a_0$  chẵn và  $a_{n-k} + a_k$  chẵn, với mọi  $k = \overline{1, n-1}$ . Giả sử  $P(x) = Q(x)R(x)$ , với  $Q(x), R(x)$  là các đa thức hệ số



nguyên khác hằng,  $\deg(Q(x)) \leq \deg(R(x))$  và tất cả các hệ số của  $R(x)$  đều lẻ. Chứng minh rằng, đa thức  $P(x)$  có nghiệm nguyên.

**Câu 89.** Chứng minh rằng với mọi số nguyên dương  $n$  thì đa thức  $P(x) = (x^2 + x)^{2^n} + 1$  là đa thức bất khả quy trên  $\mathbb{Z}$ .

**Câu 90.** Giả sử  $n$  là số tự nhiên lớn hơn hoặc bằng 2 và  $P(x) = x^n - a_{n-1}x^{n-1} + \dots + a_1x + 1$  là đa thức hệ số nguyên dương. Giả sử  $a_k = a_{n-k}$  với mọi  $k = \overline{1, n-1}$ . Chứng minh rằng tồn tại

vô hạn cặp số nguyên dương  $(x, y)$  sao cho:  $\begin{cases} y | P(x) \\ x | P(y) \end{cases} (*)$ .

**Câu 91.** Chứng minh rằng, với mỗi số nguyên dương  $n$  tồn tại đa thức  $P(x) \in \mathbb{Z}[x]$  bậc  $n$  sao cho  $P(0), P(1), \dots, P(n)$  phân biệt và tất cả các số đó đều có dạng  $2 \cdot 2019^k + 3, k \in \mathbb{Z}^+$ .

**Câu 92.** Chứng minh rằng tồn tại tập vô hạn các điểm

$$\{\dots, P_{-3}, P_{-2}, P_{-1}, P_0, P_1, P_2, P_3, \dots\}$$

trong mặt phẳng thỏa mãn tính chất: Với ba số nguyên  $a, b, c$  phân biệt thì các điểm  $P_a, P_b, P_c$  thẳng hàng khi và chỉ khi  $a + b + c = 2014$ .

**Câu 93.** Cho  $x_1 < x_2 < \dots < x_n$  là  $n, n \geq 3$  số thực thỏa mãn:

$$x_2 - x_1 < x_3 - x_2 < x_4 - x_3 < \dots < x_n - x_{n-1}$$

Giả sử đa thức  $P(x)$  có  $n$  nghiệm thực là các giá trị  $x_1, x_2, \dots, x_n$ . Chứng minh rằng giá trị lớn nhất của  $|P(x)|$  đạt được tại một điểm  $x_0 \in [x_{n-1}, x_n]$ .

**Câu 94.** Cho  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  là đa thức hệ số nguyên thỏa mãn điều kiện  $P(r) = P(s) = 0$  trong đó  $r, s$  là các số nguyên thỏa mãn điều kiện  $0 < r < s$ . Chứng minh rằng tồn tại  $k \in \{0, 1, 2, \dots, n\}$  sao cho  $a_k \leq -s$ .

**Câu 95.** Cho  $P(x), Q(x)$  là các đa thức hệ số nguyên. Đặt  $a_n = n! + n$ . Chứng minh rằng nếu

$$\frac{P(a_n)}{Q(a_n)} \in \mathbb{Z}, \forall n \text{ thì } \frac{P(n)}{Q(n)} \in \mathbb{Z}, \forall n \text{ và } Q(n) \neq 0.$$

**Câu 96.** Cho  $P(x)$  là đa thức bậc  $n \geq 5$  với hệ số nguyên và

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Giả sử  $P(x)$  có  $n$  nghiệm nguyên phân biệt là  $0, \alpha_2, \dots, \alpha_n$ . Tìm tất cả các số nguyên  $k$  sao cho thỏa mãn  $P(P(k)) = 0$ .

**Câu 97.** Tìm số nguyên dương  $n$  nhỏ nhất sao cho tồn tại đa thức  $P(x)$  bậc  $n$  có hệ số nguyên thỏa mãn:  $P(0) = 0, P(1) = 1$  và với mọi  $\lambda \in \mathbb{N}^*$  thì

$$(P(\lambda) - 2)(P(\lambda) - 1)P(\lambda) \text{ là bội của } p \text{ với } p \text{ là số nguyên tố}$$



**Câu 98.** Chứng minh rằng với mọi  $m \in \mathbb{N}$  tồn tại đa thức  $P_m(x)$  có hệ số hữu tỉ thỏa mãn với mọi  $n \in \mathbb{N}^*$  thì  $1^{2m+1} + 2^{2m+1} + \dots + n^{2m+1} = P_m(n(n+1))$

**Câu 99.** Cho  $P(x), Q(x), R(x)$  là ba đa thức hệ số thực thỏa mãn:

$$P(Q(x)) + P(R(x)) = c, \forall x \in \mathbb{R} \text{ với } c = \text{const} \in \mathbb{R}$$

Chứng minh rằng:  $P(x)$  là hằng số hoặc  $(Q(x) + R(x))$  là hằng số.

**Câu 100.** Chứng minh rằng tồn tại các đa thức hệ số nguyên  $S_1, S_2, \dots$  tương ứng với các biến  $x_1, x_2, \dots, y_1, y_2, \dots$  thỏa mãn với mọi số nguyên  $n \geq 1$

$$\sum_{d|n} d \cdot S_d^{\frac{n}{d}} = \sum_{d|n} d \cdot \left( x_d^{\frac{n}{d}} + y_d^{\frac{n}{d}} \right) \quad (*)$$

Với hàm tổng chạy qua các ước nguyên dương  $d$  của  $n$ .

**Chú ý.** Lưu ý rằng ta chỉ xét đến các đa thức trong trường  $\mathbb{Z}[x]$ . Ví dụ, xét hàm  $S_1 = x_1 + y_1$

và  $S_2 = x_2 + y_2 - x_1 y_1$  trong trường hợp  $n = 2$  ta được

$S_1^2 + 2S_2 = (x_1^2 + y_1^2) + 2 \cdot (x_2 + y_2)$  là hàm  $(*)$  thỏa mãn yêu cầu bài toán.





## HƯỚNG DẪN GIẢI

**Câu 1.** Tìm các đa thức  $P(x)$  có hệ số nguyên, không âm, bậc không lớn hơn 6 thỏa  $P(7) = 102013$ .

*Đề chọn đội tuyển DakLak 2014*

*Lời giải*

Ta có  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$$\Rightarrow P(7) = a_n 7^n + a_{n-1} 7^{n-1} + \dots + a_1 7 + a_0 \Rightarrow P(7) = \overline{a_n a_{n-1} \dots a_0}_{(7)}$$

Lại có  $102013 = 6 \cdot 7^5 + 3 \cdot 7^3 + 2 \cdot 7^2 + 6 \cdot 7 + 2 \cdot 7^0 = \overline{603262}_{(7)} \Rightarrow P(x) = 6x^5 + 3x^3 + 2x^2 + 6x + 2$ .

**Nhận xét.** Ý tưởng các dạng bài toán này là ta đưa về việc xử lý dữ kiện đề bài dưới dạng chuyển đổi linh hoạt các hệ cơ số để đơn giản hóa cách làm cho bài toán.

**Câu 2.** Cho  $a, b, c \in \mathbb{Z}$  thỏa mãn các đa thức  $f(x) = ax^2 + bx + c$  và  $g(x) = (a-b)x^2(c-a)x + a+b$  có nghiệm chung. Chứng minh rằng  $a+b+2c \equiv 3$ .

*Lời giải*

Ta có  $f(x) - g(x) = (a+b-c)(x^2 + x - 1)$ . Giả sử  $x_0$  là nghiệm chung của 2 phương trình  $f(x) = 0$  và  $g(x) = 0$ . Khi đó

- Nếu  $a+b-c = 0$  thì do  $a+b+2c \equiv a+b-c \pmod{3}$  nên  $a+b+2c \equiv 3$
- Nếu  $a+b-c \neq 0$ , thì do  $x_0$  là nghiệm chung của  $f(x)$  và  $g(x)$  nên  $x_0$  là nghiệm của phương trình  $(x^2 + x - 1) = 0$ . Theo định lý về phép chia với số dư, ta có

$$f(x) = a(x^2 + x - 1) + r(x) \quad (*)$$

trong đó  $r \in \mathbb{Z}[x], \deg r < 2$ . Trong  $(*)$ , thay  $x = x_0$  ta được

$$0 = f(x_0) = a(x_0^2 + x_0 - 1) + r(x_0) \Rightarrow x_0 = \frac{-1 \pm \sqrt{5}}{2}, r(x_0) = 0$$

Từ đó, do  $r \in \mathbb{Z}[x], \deg r \leq 1, r(x_0) = 0$  và  $x_0 \notin \mathbb{Q}$  nên  $r(x) \equiv 0 \forall x \in \mathbb{R}$  suy ra

$$f(x) = a(x^2 + x - 1)$$

Và do đó  $b = a, c = -a$  suy ra  $a+b+2c = 0 \equiv 3$ .

**Câu 3.** Tồn tại hay không đa thức  $f(x) = x^2 + ax + b$  với  $a, b$  nguyên thỏa mãn  $a^2 - 4b \neq 0$  và nhận giá trị chính phương tại 2010 điểm phân biệt.

*Lời giải*

Tồn tại đa thức bậc hai có tính chất như vậy. Thật vậy:





Xét  $f(x) = x^2 + ax + b$ , ta có  $4f(x) = 4x^2 + 4ax + 4b = (2x + a)^2 + 4b - a^2$

Giả sử tồn tại  $x_1, x_2, \dots, x_{2010}, y_1, y_2, \dots, y_{2010}$  ( $x_i \neq x_j, \forall 1 \leq i \neq j \leq 2010$ ) là các số nguyên thỏa

$$\text{mãn } \begin{cases} 4f(x_i) = (2x_i + a)^2 + 4b - a^2 \\ 4f(x_i) = 4y_i^2 \end{cases} \quad \forall i = \overline{1, 2010}$$

Suy ra  $4b - a^2 = (2y_i - 2x_i - a)(2y_i + 2x_i + a) \quad \forall i = 1, 2, \dots, 2010$

Chọn  $a, b$  thỏa mãn  $\begin{cases} a \vdots 4 \\ 4b - a^2 = 16P_1 \cdot P_2 \cdot \dots \cdot P_{2010} \end{cases}$  ( $P_i$  là các số nguyên tố phân biệt)

Xét hệ phương trình  $\begin{cases} 2y_i - 2x_i - a = 4P_i \\ 2y_i + 2x_i + a = \frac{4P_1 P_2 \dots P_{2010}}{P_i} \end{cases}, \forall i = 1, 2, \dots, 2010$

Giải hệ, thu được  $\begin{cases} y_i = P_i + \frac{P_1 P_2 \dots P_{2010}}{P_i} \in \mathbb{Z}^+ \\ x_i = \frac{P_1 P_2 \dots P_{2010}}{P_i} - P_i - \frac{a}{2} \in \mathbb{Z} \end{cases}, \text{ thỏa mãn.}$

Rõ ràng  $x_i \neq x_j (\forall 1 \leq i \neq j)$

Vậy tồn tại đa thức thỏa mãn yêu cầu.

**Câu 4.** Chứng minh rằng không tồn tại đa thức  $P$  với hệ số nguyên, khác đa thức hằng có bậc không quá 4 thỏa mãn: tồn tại 5 số nguyên  $x_1, x_2, \dots, x_5$  khác nhau sao cho

$$P(x_1)P(x_2)P(x_3)P(x_4)P(x_5) = -1.$$

**Lời giải**

Không mất tính tổng quát, ta chỉ xét ba trường hợp sau:

- **Trường hợp 1.** Với  $P(x_1) = P(x_2) = P(x_3) = P(x_4) = P(x_5) = -1$ .

Khi đó đa thức  $P(x) + 1$  có bậc không quá 4 mà có đến 5 nghiệm nguyên khác nhau. Điều đó dẫn đến:  $P(x) \equiv -1$  (loại vì đa thức  $P$  cần tìm khác đa thức hằng).

- **Trường hợp 2.** Với  $P(x_1) = P(x_2) = P(x_3) = -1; P(x_4) = P(x_5) = 1$ . Khi đó:

$$\begin{cases} 2 = P(x_4) - P(x_1) = P(x_4) - P(x_2) = P(x_4) - P(x_3) \\ 2 = P(x_5) - P(x_1) = P(x_5) - P(x_2) = P(x_5) - P(x_3) \end{cases}$$

Ta có 2 là bội của các số  $x_4 - x_1; x_4 - x_2; x_4 - x_3; x_5 - x_1; x_5 - x_2; x_5 - x_3$ .

Điều này là không thể.

- **Trường hợp 3.** Với  $P(x_1) = P(x_2) = P(x_3) = P(x_4) = 1; P(x_5) = -1$ .

Khi đó đa thức  $P(x) - 1$  có bốn nghiệm là  $x_1; x_2; x_3; x_4$  phân biệt.

Do đó  $P(x) - 1 = K \cdot (x - x_1)(x - x_2)(x - x_3)(x - x_4)$  với  $K$  là một hằng số nguyên.



Điều này dẫn đến  $-2 = P(x_5) - 1 = K.(x_5 - x_1)(x_5 - x_2)(x_5 - x_3)(x_5 - x_4)$ .

Điều này lại không thể. Như vậy không tồn tại đa thức thỏa yêu cầu bài toán.

**Câu 5.** Chứng minh  $x^n - x - 1$  bất khả quy trên  $\mathbb{Z}[x]$ ,  $\forall n \geq 2$

*Lời giải*

**Bổ đề.** Với mọi nghiệm phức  $z$  của đa thức  $P(x) = x^n - x - 1$  chúng ta có bất đẳng thức sau.

$$2\operatorname{Re}\left(z - \frac{1}{z}\right) > \frac{1}{|z|^2} - 1$$

**Chứng minh.** Ta đặt  $z = r.e^{it}$ , bất đẳng thức tương đương  $(1 + 2r \cos t)(r^2 - 1) > 0$  và do nó là nghiệm của  $P(x)$  nên  $r^{2n} = |z|^{2n} = |z + 1|^2 = 1 + 2r \cos t + r^2 \Rightarrow 1 + 2r \cos t = r^{2n} - r^2$

Bất đẳng thức trở thành  $(r^{2n} - r^2)(r^2 - 1) > 0$  (đúng)

Giả sử  $P(x) = f(x)g(x)$  trong đó  $\deg f \geq 1$  và  $f, g \in \mathbb{Z}[x]$ , gọi các nghiệm phức của  $P(x)$

là  $z_1, z_2, \dots, z_n$ , sử dụng bổ đề, ta có  $2\sum_{i=1}^k \left(z_i - \frac{1}{z_i}\right) > \sum_{i=1}^k \frac{1}{|z_i|^2} - k$

Trong đó ta đã giả sử  $f(x) = \prod_{i=1}^k (x - z_i)$ .

Lại theo Viète ta có  $\prod_{i=1}^k |z_i| = |f(0)| = 1$ .

Theo bất đẳng thức AM - GM ta có  $\sum_{i=1}^k \frac{1}{|z_i|^2} - k \geq 0$ .

Từ đó kéo theo  $\sum_{i=1}^k \operatorname{Re}\left(z_i - \frac{1}{z_i}\right) > 0$ .

Mặt khác  $f$  monic và hệ số nguyên nên  $\sum_{i=1}^k \operatorname{Re}\left(z_i - \frac{1}{z_i}\right) \geq 1$ .

Lý luận tương tự với  $g$ , cộng lại thu được  $\operatorname{Re}\left(\sum_{i=1}^n \left(z_i - \frac{1}{z_i}\right)\right) \geq 2$ .

Theo Viète, ta lại có  $\sum_{i=1}^n \left(z_i - \frac{1}{z_i}\right) = 1$

Từ đây suy ra mâu thuẫn, vậy ta có  $P$  bất khả quy trên  $\mathbb{Z}[x]$ .

**Câu 6.** Cho đa thức  $P$  là đa thức hệ số và tồn tại số nguyên dương  $m$  sao cho  $P(1); P(2); \dots; P(m)$  không chia hết cho  $m$ . Chứng minh rằng  $P(a) \neq 0$  với mọi  $a \in \mathbb{Z}$ .

Beijing 1967

*Lời giải*



Giả sử tồn tại  $a \in \mathbb{Z}$  sao cho  $P(a) = 0$ .

Ta viết  $a$  dưới dạng  $a = qm + n$  với  $q, n$  là các số nguyên và  $0 \leq n < m$ .

- **Trường hợp 1.** Với  $n = 0$ . Khi đó  $qm - P(m) = P(a) - P(m) : (qm - m) : m$ .

Điều này dẫn đến  $P(m)$  chia hết cho  $m$  (mâu thuẫn).

- **Trường hợp 2.** Với  $1 \leq n < m$ . Hiển nhiên  $a \notin \{1; 2; \dots; m\}$  nên  $q \neq 0$ .

Khi đó  $P(n) = P(a - qm) - P(a) : qm$ .

Điều này dẫn đến  $P(n) : m$  (mâu thuẫn giả thiết).

Vậy bài toán được chứng minh.

**Câu 7.** Cho  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  là đa thức với  $a_0, a_1, \dots, a_n$  là các số nguyên dương. Đặt  $P_1(x) = P(x)$  và  $P_k(x) = P(P_{k-1}(x))$  với  $k > 1$ . Tồn tại hay không  $M > 0$  sao cho với  $m \geq M$  ta có  $m \mid P_{P(m)}(m)$

S.T.E.M.S Cat A/B P4

### Lời giải – AoPS

**Bổ đề.** Nếu  $Q(x)$  là đa thức với hệ số thực thì khi đó:

$$x \equiv y \pmod{m} \Rightarrow Q(x) \equiv Q(y) \pmod{m}$$

Ta sẽ chứng minh  $M$  không tồn tại. Giả sử điều ngược lại rằng  $M$  tồn tại.

Do  $m \equiv 0 \pmod{m}$ , áp dụng bổ đề trên ta được  $P_{P(m)}(m) \equiv P_{P(m)}(0) \pmod{m}$ .

Vì vậy  $\forall m > M, m \mid P_{P(m)}(0)$ .

Gọi  $q$  là số nguyên tố lớn hơn  $\max\{M, a_0\}$ .

Đặt  $t_q$  là số nguyên dương nhỏ nhất sao cho  $q \mid P_{t_q}(0)$ , như vậy  $t_q$  tồn tại và  $t_q \leq P(q)$  vì các điều kiện ở trên.

**Yêu cầu 1.** Nếu  $q \mid P_r(0)$  thì  $t_q \mid r$

Chứng minh. Ta dùng chung ý tưởng trong việc chứng minh  $\text{ord}_n(x) \mid \phi(n)$

**Chứng minh phản chứng.** Đặt  $r = t_q x + y$  với  $0 < y < t_q$ , khi đó:

$$0 \equiv P_r(0) = P_{r-t_q}(P_{t_q}(0)) \equiv P_{r-t_q}(0) \pmod{q}$$

Lặp lại các thao tác trên, ta thu được  $P_y(0) \equiv 0 \pmod{q}$ , mâu thuẫn với điều tối thiểu của  $t_q$

**Yêu cầu 2.**  $t_q \mid P(1)$

Chứng minh. Từ các điều kiện đã cho và từ yêu cầu 1,  $t_q \mid P(q)$  suy ra được  $q \nmid t_q$ .

Mặt khác  $q \mid a_0$  – vô lý vì  $q > a_0 > 0$ .

Vậy  $\gcd(t_q, q) = 1$  dẫn đến tồn tại số tự nhiên  $k$  sao cho  $qk \equiv 1 \pmod{t_q}$

Từ những điều kiện trên ta có  $q \mid qk \mid P_{P(qk)}(0)$



Từ yêu cầu 1 suy ra được rằng  $t_q \mid P(qk)$ , nhưng theo bổ đề ta có  $P(1) \equiv P(qk) \pmod{t_q}$

Vậy  $t_q \mid P(1)$ .

Quay trở lại bài toán

Xét các số  $P_1(0), P_2(0), \dots, P_{p(1)}(0)$ . Ta chọn số nguyên tố  $p$  đủ lớn sao cho  $p$  không chia hết cho tất cả các số trên và  $p > \max\{M, P(1)\}$

Khi đó, theo cách chọn  $p$ ,  $t_p > P(1)$ .

Nhưng theo yêu cầu 2 thì  $t_q \mid P(1)$ , điều này dẫn tới  $P(1) = 0$ , vô lý vì tất cả các hệ số đều dương.

Vậy  $M$  không tồn tại.

**Câu 8.** Cho đa thức  $P(x)$  là đa thức hệ số nguyên với bậc  $n \geq 2$ . Chứng minh rằng đa thức  $P(P(x)) - x$  có nhiều nhất  $n$  nghiệm.

*Romani TST – Gh. Eckstein*

*Lời giải*

Ta chứng minh bằng phản chứng.

Giả sử tồn tại các số nguyên  $a_1 < a_2 < \dots < a_{n+1}$  sao cho  $P(P(a_i)) = a_i$  với mọi  $i$ .

Theo tính chất trên ta có:

$$a_j - a_i \mid |P(a_j) - P(a_i)| \mid |P(P(a_j)) - P(P(a_i))| = a_j - a_i; \forall 1 \leq i < j \leq n+1$$

Điều đó kéo theo  $|P(a_j) - P(a_i)| = a_j - a_i$ . Từ đó ta được:

$$\left| \sum_{i=1}^n [P(a_{i+1}) - P(a_i)] \right| = |P(a_{n+1}) - P(a_1)| = a_{n+1} - a_1 = \sum_{i=1}^n (a_{i+1} - a_i) = \sum_{i=1}^n |P(a_{i+1}) - P(a_i)|$$

Như vậy tất cả các giá trị  $P(a_{i+1}) - P(a_i)$  có cùng dấu, nên tồn tại  $A, B$  sao cho:

$$P(a_i) - a_i = A; \forall i = 1, 2, \dots, n+1 \quad \text{hoặc} \quad P(a_i) + a_i = B; \forall i = 1, 2, \dots, n+1.$$

Tuy nhiên điều trên là không thể vì  $\deg(P(x) \pm x) = n$  không thể nhận cùng một giá trị nào đó với  $n+1$  giá trị khác nhau của  $x$ . Bài toán được chứng minh.

**Nhận xét.** Với  $P(x)$  là đa thức có bậc là  $n > 1$ .

Chứng minh rằng phương trình  $\underbrace{P(P(\dots(P(x))))}_k = x$  có nhiều nhất  $n$  nghiệm.

*IMO – 2006*

**Câu 9.** Tìm tất cả các đa thức  $P$  hệ số nguyên sao cho  $P(n) \mid 2^n - 1$  với mọi số nguyên dương  $n$ .

*Polish Olympiad*

*Lời giải*



Dễ dàng kiểm tra được rằng nếu  $P$  là đa thức hằng thì  $P \equiv 1; -1$ .

Ta giả sử  $P$  khác đa thức hằng. Không mất tính tổng quát, ta có thể giả sử hệ số cao nhất của đa thức  $P(x)$  là số nguyên dương.

Xét  $n$  sao cho  $P(n) > 1$  và xét  $p$  là số nguyên tố trong phân tích của  $P(n)$ .

Khi đó  $p \mid P(n) \mid 2^n - 1$  và theo tính chất bên trên, ta được:

$$p = ((n+p) - n) \mid P(n+p) - P(n) \Rightarrow p \mid P(n+p) \mid 2^{n+p} - 1$$

Điều đó ta có  $p \mid (2^n \cdot 2^p - 2^p + 2^p - 1) = [2^p (2^n - 1) + 2^p - 1] \Rightarrow p \mid 2^p - 1$

Điều trên là trái với định lý Fermat.

**Câu 10.** Gọi  $x_0, x_1, \dots, x_n$  là các số nguyên thỏa mãn  $x_0 > x_1 > \dots > x_n$ . Chứng minh rằng một trong các số  $|P(x_0)|, |P(x_1)|, \dots, |P(x_n)|$  không nhỏ hơn  $\frac{n!}{2^n}$  với  $P(x)$  là đa thức bậc  $n$ .

Đề xuất 1977 IMO – Vietnam

*Lời giải*

Định  $f_0, f_1, \dots, f_n$  bằng  $x_0, x_1, \dots, x_n$ .

Theo **công thức nội suy Lagrange** ta có  $P(x) = \sum_{i=0}^n P(x_i) \frac{f_i(x)}{f_i(x_i)}$

Vì cả hai vế là đa thức bậc  $n$  và bằng nhau tại các giá trị  $x_0, x_1, \dots, x_n$ .

So sánh các hệ số của  $x^n$  ta được  $1 = \sum_{i=0}^n \frac{P(x_i)}{f_i(x_i)}$

Do  $x_0, x_1, \dots, x_n$  là các số nguyên, giảm nghiêm ngặt, ta có

$$|f_i(x_i)| = \prod_{j=0}^{i-1} |x_j - x_i| \prod_{j=i+1}^n |x_j - x_i| \geq i!(n-i)! = \frac{1}{n!} \binom{n}{i}$$

Đặt giá trị lớn nhất của  $|P(x_0)|, |P(x_1)|, \dots, |P(x_n)|$  là  $|P(x_k)|$ .

Theo bất đẳng thức tam giác ta được  $1 \leq \sum_{i=0}^n \frac{|P(x_i)|}{|f_i(x_i)|} \leq \frac{|P(x_k)|}{n!} \sum_{i=0}^n \binom{n}{i} = \frac{2^n |P(x_k)|}{n!}$

Vậy  $|P(x_k)| \geq \frac{n!}{2^n}$ .

**Câu 11.** Giả sử các đa thức  $P(x), Q(x), R(x)$  và  $S(x)$  thỏa mãn:

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x)$$

Chứng minh rằng khi đó đa thức  $P(x)$  chia hết cho  $x-1$ .

USAMO – 1976

*Lời giải*



Giả sử  $S(x) = s_n x^n + s_{n-1} x^{n-1} + \dots + s_1 x + s_0$ . Khi đó:

$$\begin{aligned} (x-1)P(x^5) + x(x-1)Q(x^5) + x^2(x-1)R(x^5) &= (x^5-1)S(x) \\ \Leftrightarrow (x-1)P(x^5) + x(x-1)Q(x^5) + x^2(x-1)R(x^5) &= (x^5-1)[S_1(x) + S_2(x)] \end{aligned}$$

với  $S_1(x) = s_0 + s_5 x^5 + \dots + s_{5m} x^{5m}$ ;  $m = \left\lfloor \frac{n}{5} \right\rfloor$  và  $S_2(x) = S(x) - S_1(x)$ . Khi đó ta được:

$$xP(x^5) + x(x-1)Q(x^5) + x^2(x-1)R(x^5) - (x^5-1)S_2(x) = (x^5-1)S_1(x) + P(x^5)$$

Vì vế phải của đẳng thức trên là đa thức mũ bội 5 trong khi vế trái thì không.

Điều này xảy ra khi và chỉ khi cả hai vế là hai đa thức có tất cả các hệ số là 0.

Điều đó dẫn đến  $P(x^5) = -(x^5-1)S_1(x) \Rightarrow P(1) = 0$ . Do đó  $P(x) = (x-1).G(x)$  với  $G(x)$  là một đa thức nào đó.

**Câu 12.** Tìm tất cả các đa thức  $P$  có hệ số nguyên sao cho với mọi số nguyên tố  $p$  và mọi cặp số tự nhiên  $(u, v)$  thỏa mãn  $p \mid (uv-1)$  thì ta có  $p \mid (P(u)P(v)-1)$ .

*Iran TST 2009*

#### Lời giải

Ta xét các trường hợp sau.

- **Trường hợp 1.** Với  $P$  là đa thức hằng. Dễ dàng kiểm tra được  $P(x) \equiv 1$ ;  $P(x) \equiv -1$ .
- **Trường hợp 2.** Gọi  $n = \deg P \geq 1$ . Ta đặt  $G(x) = x^n P\left(\frac{1}{x}\right)$  thì  $G(x)$  cũng là đa thức hệ số nguyên.

Từ giả thiết bài toán, ta có được  $p \mid (P(u)P(u^{-1})-1)$  với mọi số nguyên dương  $u$  sao cho  $(u, p) = 1$  và trong đó  $u^{-1}$  là chỉ số nguyên dương  $v$  sao cho  $uv \equiv 1 \pmod{p}$ .

Từ đó ta được  $p \mid (u^n P(u)P(u^{-1}) - u^n)$  hay nói cách khác  $p \mid P(u)G(u) - u^n$  với mọi số nguyên dương  $u$  sao cho  $(u, p) = 1$ .

Ta cố định  $u$  và lấy  $p$  đủ lớn, thì tính chất trên chỉ đúng khi và chỉ khi  $P(u)G(u) = u^n$ . Hơn nữa  $G(x)P(x)$  là các đa thức nên điều đó kéo theo  $G(x)H(x) = x^n$ . Mà  $\deg P = n$  nên  $G$  là đa thức hằng. Tức là  $P(x) = ax^n$ , bằng cách thử lại ta được  $a = 1$ ;  $a = -1$ .

Vậy ta có bốn hàm đa thức thỏa mãn  $P(x) = 1$ ;  $P(x) = -1$ ;  $P(x) = x^n$ ;  $P(x) = -x^n$ .

**Câu 13.** Tìm tất cả các đa thức  $P$  hệ số nguyên sao cho với mọi số tự nhiên  $a, b, c$  ta luôn có  $a+b+c \mid P(a)+P(b)+P(c)$ .

#### Lời giải



Giả sử  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  với  $a_i \in \mathbb{Z}$ .

Với ba số tự nhiên  $a, b, c > 1$  tùy ý, ta có  $2P(0) + P(c) \equiv 3a_0 \pmod{c}$

Tức  $c \mid 3a_0$ , mà  $c$  là số tự nhiên tùy ý nên điều trên đúng khi và chỉ khi  $a_0 = 0$ . Từ đó bằng cách cho  $c = 0$  ta được tính chất  $a + b \mid P(a) + P(b)$  đúng với mọi  $a, b \in \mathbb{N}$ .

Để dàng chứng minh được tất cả các hệ số của đơn thức bậc chẵn đều bằng 0. Do đó:

$$(a+b+c) \mid [P(c) + P(a+b)]$$

Kết hợp với giả thiết của bài toán, ta được  $P(a) + P(b) - P(a+b) \equiv 0 \pmod{a+b+c}$

Mà  $P$  là đa thức và  $a, b, c$  là các số tự nhiên tùy ý nên  $P(a) + P(b) = P(a+b)$ .

Tức  $P$  cộng tính, một lần nữa vì  $P$  là đa thức nên ta được  $P(x) = kx$ . Thử lại ta được kết luận cho bài toán.

**Câu 14.** Cho  $m, n$  là các số nguyên dương. Chứng minh rằng  $n \mid m$  khi và chỉ khi  $P(x) \mid Q(x)$ , trong đó  $P(x); Q(x)$  là các đa thức hệ số nguyên được xác định:

$$\begin{aligned} P(x) &= x^{n-1} + C_n^1 x^{n-2} + \dots + C_n^{n-1} \\ Q(x) &= x^{m-1} + C_m^1 x^{m-2} + \dots + C_m^{m-1} \end{aligned}$$

*Lời giải*

Theo các định nghĩa của hai đa thức ta được:

$$xP(x) = (x+1)^n - 1; xQ(x) = (x+1)^m - 1$$

Do đó  $P(x) \mid Q(x) \Leftrightarrow [(x+1)^n - 1] \mid [(x+1)^m - 1] \Leftrightarrow ((x+1)^n - 1, (x+1)^m - 1) \equiv (x+1)^m - 1$

$$\Leftrightarrow (x+1)^{(m,n)} - 1 \equiv (x+1)^m - 1 \Leftrightarrow (m, n) = m \Leftrightarrow n \mid m$$

Bài toán được chứng minh.

**Câu 15.** Tìm tất cả các đa thức  $P$  hệ số nguyên thỏa mãn tính chất: Với  $m, n$  là hai số nguyên tố cùng nhau thì hai số  $P(m); P(n)$  cũng là hai số nguyên tố cùng nhau.

*Iran TST*

*Lời giải*

Để thấy  $P$  không thể là đa thức hằng.

Giả sử với  $p$  là số nguyên tố đủ lớn sao cho  $p$  không là ước của  $P(p)$ .

Khi đó  $(p, p + P(p)) = 1$  do đó  $P(p)$  và  $P(p + P(p))$  là hai số nguyên tố cùng nhau.

Tuy nhiên ta thấy  $P(p) = [P(p) + p - p] \mid [P(p + P(p)) - P(p)] \Rightarrow P(p) \mid P(p + P(p))$

Như vậy, để đúng với giả sử bên trên ta cần  $|P(p)| = 1$  hoặc  $P(p) = 0$ .

Điều này là không thể vì  $P$  là đa thức khác đa thức hằng và  $p$  là số nguyên tố đủ lớn.

Tóm lại, với  $p$  là số nguyên tố đủ lớn thì  $p \mid P(p)$ , theo tính chất bên trên, ta lại có:



$$p = p - 0 \mid P(p) - P(0) \Rightarrow p \mid P(0)$$

Mặt khác  $p$  là số nguyên tố đủ lớn tùy ý nên  $P(0) = 0$ .

Từ đó ta được  $P(x) = x.G(x)$  với  $G(x)$  là đa thức hệ số nguyên thỏa mãn tính chất giống như  $P(x)$  nhưng có bậc nhỏ hơn.

Thực hiện tương tự như vậy kết hợp với phương pháp quy nạp theo bậc của đa thức ta được:  $P(x) = \pm x^n$  với  $n \in \mathbb{N}^*$ .

**Câu 16.** Cho  $P(x), Q(x) \in \mathbb{Z}[x]$  là hai đa thức *monic* bất khả quy thỏa mãn với  $n$  đủ lớn thì  $P(n), Q(n)$  có cùng tập ước nguyên tố. Chứng minh rằng  $P = Q$ .

#### Lời giải

Ta chứng minh bằng phản chứng bằng cách giả sử  $P \neq Q$ . Khi đó  $P, Q$  là hai đa thức nguyên tố cùng nhau do chúng đều bất khả quy và là đa thức *monic*.

Theo định lý Bézout thì tồn tại hai đa thức  $f, g$  có hệ số nguyên và số nguyên dương  $a$  sao cho  $P(x).f(x) + Q(x).g(x) = a$ . Lại theo định lý Schur thì tồn tại vô hạn số nguyên tố  $p$  sao cho ứng với mỗi số  $p$  đang xét thì ta có tồn tại số nguyên  $n$  sao cho  $p \mid P(n)$ . Nhưng vì  $P(n), Q(n)$  có cùng tập ước nguyên tố nên ta có  $p \mid a$ . Như vậy số  $a$  có chứa vô hạn các ước nguyên tố của nó là điều vô lý. Vậy  $Q = P$ .

**Câu 17.** Gọi đa thức  $P(x) \in \mathbb{Z}[x]$  khác đa thức hằng và gọi  $n, k$  là hai số nguyên dương. Chứng minh rằng tồn tại số nguyên dương  $a$  sao cho mỗi  $f(a), f(a+1), \dots, f(a+n-1)$  có ít nhất  $k$  ước nguyên tố phân biệt.

*Bulgaria Olympiad*

#### Lời giải

Bài này gọi ta nghĩ đến **định lý thặng dư Trung hoa**.

Theo định lý Schur tồn tại vô hạn số nguyên tố  $p$  sao cho ứng với mỗi  $p$  sẽ tồn tại số nguyên  $m$  sao cho  $p \mid P(m)$ . Ta gọi  $A$  là tập số nguyên tố đó thì  $|A| = +\infty$ .

Gọi  $p_{ij} (1 \leq i \leq n, 1 \leq j \leq k)$  là các số nguyên tố thuộc tập  $A$ .

Ta cố định mỗi  $i$ . Theo **định lý Schur** thì tồn tại số  $x_{ij} \in \mathbb{Z}$  sao cho  $P(x_{ij}) \equiv 0 \pmod{p_{ij}}$ .

Theo định lý thặng dư Trung Hoa thì cứ mỗi  $i$  cố định sẽ tồn tại số  $a$  sao cho

$$a + i - 1 \equiv x_{ij} \pmod{p_{ij}} \text{ với } j = \overline{1; k}. \text{ Khi đó với mỗi } i \text{ cố định thì ta đều có}$$

$$f(a + i - 1) \equiv f(x_{ij}) \equiv 0 \pmod{p_{ij}} \text{ với } j = \overline{1; k}.$$

Nên  $f(a + i - 1)$  chia hết cho tất cả các số nguyên tố  $p_{ij} (j = \overline{1; k})$  với mọi số  $i = \overline{1; n}$ .





**Câu 18.** Cho đa thức  $P(x), Q(x)$  là hai đa thức có hệ số nguyên nguyên tố cùng nhau. Đặt  $a_n = (P(n), Q(n))$ . Chứng minh dãy  $\{a_n\}$  tuần hoàn.

**Lời giải**

Theo định lý Bézout tồn tại hai đa thức  $R(x), S(x)$  và hằng số  $a$  nguyên thỏa mãn  $P(x).R(x) + Q(x).S(x) = a, \forall x \in \mathbb{R}$ . Suy ra  $P(n).R(n) + Q(n).S(n) = a, \forall n \in \mathbb{Z}$ .

Từ giả thiết  $a_n = (P(n), Q(n))$ , ta suy ra  $a_n | a, \forall n$ . Do tập các ước là hữu hạn nên các số  $a_n$  lặp lại. Ta cần chứng minh là  $a_{n+a} = a_n$ .

Ta có  $P(a_n + a) \equiv P(a_n) \pmod{a}$ . Mà  $a_n | P(n), a_n | a \Rightarrow a_n | P(n+a)$ .

Hoàn toàn tương tự ta có  $a_n | Q(n+a) \Rightarrow a_n | a_{n+a}$ .

Mặt khác ta lại có  $P(a_n + a) \equiv P(a_n) \pmod{a}$ . Mà  $a_{n+a} | P(n+a), a_{n+a} | a \Rightarrow a_{n+a} | P(n)$ .

Lập luận tương tự ta có  $a_{n+a} | Q(n)$ . Do đó  $a_{n+a} | a_n$ . Từ đó ta có  $a_{n+a} = a_n$ .

**Câu 19.** Với hai đa thức có hệ số nguyên  $p(x), q(x)$  ta viết  $p(x) \equiv q(x) \pmod{2}$  nếu  $p(x) - q(x)$  có tất cả các hệ số đều chia hết cho 2. Cho dãy đa thức  $p_n(x)$  thỏa mãn  $p_1(x) = p_2(x) = 1$  và  $p_{n+2}(x) = p_{n+1}(x) + xp_n(x)$  (1), với mọi  $n$  là số tự nhiên. Chứng minh rằng  $p_{2^n}(x) \equiv 1 \pmod{2}$ .

**Lời giải**

Ta quy ước viết  $p_n(x) = p_n, n = 1, 2, 3, \dots$

Trước hết ta xét  $p_{n+4} = p_{n+3} + xp_{n+2} = (p_{n+2} + xp_{n+1}) + xp_{n+2} = (x+1)p_{n+2} + xp_{n+1}$   
 $= (x+1)p_{n+2} + x(p_{n+2} - xp_n) = (2x+1)p_{n+2} - x^2p_n \equiv p_{n+2} + x^2p_n \pmod{2} (*)$

Phần tiếp theo ta chứng minh  $p_{2^n} \equiv p_n^2 \pmod{2}$  với mọi  $n$ .

Thật vậy với  $n = 1$  ta có  $p_2 = p_1 = 1$  nên khẳng định đúng.

Giả sử khẳng định đúng với  $n = k \geq 1$ .

Khi đó kết hợp với (\*) ta có  $p_{2k+2} \equiv p_{2k} + x^2p_{2k-2} \pmod{2}$   
 $\equiv p_k^2 + x^2p_{k-1}^2 \pmod{2} \equiv p_k^2 + x^2p_{k-1}^2 + 2p_kxp_{k-1} \pmod{2} \equiv (p_k + xp_k)^2 \equiv p_{k+1}^2 \pmod{2}$

Như vậy  $p_{2^n} = p_{2.2^{n-1}} \equiv p_{2^{n-1}}^2 \equiv p_{2^{n-2}}^4 \equiv p_1^{2^n} \equiv 1 \pmod{2}$ .

**Câu 20.** Giả sử  $p_{2^n}(x) \equiv 1$  là hai số tự nhiên lớn hơn 1 và  $p_n(x) = p_n$ .

Dãy số vô hạn  $n = 1, 2, 3, \dots$  được xác định như sau

$$p_{n+4} = p_{n+3} + xp_{n+2} = (p_{n+2} + xp_{n+1}) + xp_{n+2} = (x+1)p_{n+2} + xp_{n+1}$$

Chứng minh rằng trong dãy số nói trên chứa vô hạn số đôi một nguyên tố cùng nhau.

**Lời giải**



Để ý là  $a > 1$  nên  $(a, a-1) = d > 1$ .

Giả sử từ dãy  $(x+1)p_{n+2} + x(p_{n+2} - xp_n)$  ta trích ra dãy con hữu hạn

$$(2x+1)p_{n+2} - x^2p_n \equiv p_{n+2} + x^2p_n \pmod{2}$$

Mà hai số bất kì trong dãy này thì nguyên tố cùng nhau, do dãy ban đầu vô hạn nên luôn trích được như vậy.

Đặt  $p_{2n} \equiv p_n^2$ . Xét  $n$  số sau  $n=1$ . Khi đó luôn tồn tại hai số đồng dư modulo  $q$ .

Tức là tồn tại hai số  $n=k \geq 1$  sao cho  $p_{2k+2} \equiv p_{2k} + x^2p_{2k-2}$ . Do đó  $\equiv p_k^2 + x^2p_{k-1}^2$ .

Do  $\equiv p_k^2 + x^2p_{k-1}^2 + 2p_kxp_{k-1}$  nên ta suy ra  $\equiv (p_k + xp_k)^2 = p_{k+1}^2$ , nên ta cũng suy ra

$$(ax^t, q) = 1 \quad (3)$$

Từ (1), (3) ta có  $x^{s-t} \equiv 1 \pmod{q} \Rightarrow x^{s-t} = lq + 1, \forall l \in \mathbb{N}$ .

Xét số  $u_{i_{k+1}} = a(lq+1) - a + 1 = alq + 1 \quad (4)$ .

Vì  $u_{i_{k+1}} = alq + 1 = al \cdot \prod_{j=1}^k u_{i_j} + 1$  nên  $(u_{i_{k+1}}, u_{i_j}) = 1, \forall j = 1, 2, \dots, k$ .

Hệ thức (5) chứng tỏ ta có thể bổ sung vào dãy  $u_{i_1}, u_{i_2}, \dots, u_{i_k}$  các bộ số mới mà bộ số này vẫn thỏa mãn hai số bất kì nguyên tố cùng nhau. Chứng tỏ có vô hạn số như vậy.

**Câu 21.** Với mỗi số tự nhiên  $n$ , ta kí hiệu  $f(n)$  là tổng các chữ số của nó biểu diễn trong hệ thập phân. Ta xây dựng dãy số như sau

$$u_1(n) = f(n); u_2(n) = f(f(n)); \dots; u_k(n) = \underbrace{f(f(\dots f(n)\dots))}_k$$

Chứng minh rằng với mọi số tự nhiên  $n$ , tồn tại số tự nhiên  $d$  sao cho

$$u_k(n) = u_d(n), \forall k \geq d \quad (1).$$

#### Lời giải

a) Giả sử rằng  $n = \overline{a_1a_2\dots a_n}$  là số được biểu diễn trong hệ thập phân với  $a_1 \neq 0$ .

Khi đó ta có biểu diễn  $n = a_1 \cdot 10^{p-1} + a_2 \cdot 10^{p-2} + \dots + a_{p-1} \cdot 10 + a_p$ .

Ta luôn có bất đẳng thức  $n \geq a_1 + a_2 + \dots + a_n = f(n)$ .

Dấu đẳng thức xảy ra khi và chỉ khi số có 1 chữ số.

Ta thấy rằng dãy  $\{u_n\}$  là dãy giảm thực sự cho đến khi ta thu được số có 1 chữ số thì dãy trở thành dãy dừng bởi vì  $f(n) \geq f(f(n)) \geq \dots \geq f(f\dots f(n))$ . Gọi  $d$  là số có một chữ số ấy.

Khi đó ta có  $u_k(n) = u_d(n), \forall k \geq d \quad (1)$ .



b) Kí hiệu  $S_k = \{x : f(x) = k\}$  là tập hợp các số  $x$  mà trong biểu diễn thập phân thì tập  $S_k \neq \emptyset$  vì chẳng hạn số  $11\dots1$  thuộc  $S_k$ . Với mỗi số tự nhiên  $k$  thì tập  $S_k$  là hữu hạn nên trong mỗi tập  $S_k$  đều tồn tại số bé nhất.

**Câu 22.** Cho  $\overline{abc}$  là một số nguyên tố.

Chứng minh rằng phương trình  $ax^2 + bx + c = 0$  (1) không có nghiệm hữu tỉ.

**Lời giải**

Do  $\overline{abc}$  là nguyên tố nên  $a \neq 0, c \neq 0$ . Ta chứng minh bằng *phản chứng*.

Giả sử phương trình có nghiệm hữu tỉ nên  $\Delta = b^2 - 4ac = d^2, d \in \mathbb{N}$ .

Do đó  $b^2 - d^2 = 4ac > 0 \Rightarrow b > d$ .

Mặt khác ta có  $4a.\overline{abc} = 4a(100a + 10b + c) = (20a + b)^2 - (b^2 - 4ac) = (20a + b)^2 - d^2$   
 $= (20a + b + d)(20a + b - d)$ .

Vì  $\overline{abc}$  là số nguyên tố nên suy ra  $\overline{abc}$  là ước của  $(20a + b + d)$  hoặc  $(20a + b - d)$ .

Tuy nhiên ta có  $(20a + b + d) < 100a + b + d < 100a + 10b + d = \overline{abc}$ .

Tương tự  $(20a + b - d) < 100a + b - d < 100a + 10b + d = \overline{abc}$ .

Như vậy ta suy ra điều vô lí.

Vậy phương trình không thể có nghiệm hữu tỉ.

**Câu 23.** Cho đa thức  $P(x) = (x^2 - 2)(x^2 - 3)(x^2 - 6)$ . Chứng minh rằng với mọi số nguyên tố  $p$  đều tìm được số nguyên dương  $n$  sao cho  $P(n) \vdots p$ .

**Lời giải**

Rõ ràng với  $p = 2$  thì ta tìm được  $n = 2$  thỏa mãn bài toán.

Với  $p = 3$  ta tìm được  $n = 3$  cũng thỏa mãn.

Bây giờ ta xét các số nguyên tố  $p > 3$ .

Trước hết ta có nhận xét là nếu  $(a, p) = 1$  và  $n^2 \not\equiv a \pmod{p}, \forall n$ . thì  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

**Chứng minh.**

Với mỗi  $k \in \{1, 2, \dots, p-1\}$  thì tồn tại duy nhất một số  $k' \in \{1, 2, \dots, p-1\}$  sao cho

$k.k' \equiv a \pmod{p}$ .

Vì  $n^2 \not\equiv a \pmod{p}, \forall n$  nên  $k \neq k'$ . Ta để ý là  $p-1$  là số chẵn nên ta sẽ có được  $\frac{p-1}{2}$  cặp tương ứng giữa  $k$  với  $k'$ .

Từ đó ta suy ra  $(p-1)! = (1.1')(2.2')\dots(k.k') \equiv a^{\frac{p-1}{2}} \pmod{p}$ . Ở đây ta hiểu  $1'$  là số tương ứng với  $1$  để  $1.1' \equiv a \pmod{p}$ .



Mặt khác theo **định lí Wilson** ta có  $(p-1)! \equiv -1 \pmod{p}$ . Vậy nên ta có  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

Nhận xét được chứng minh.

Trở lại với bài toán. Giả sử  $P(n)$  không chia hết cho  $p$  với mọi  $n$ .

Vì  $P(n) = (n^2 - 2)(n^2 - 3)(n^2 - 6)$  nên  $n^2$  không chia hết cho  $2; 3; 6$ .

Theo nhận xét ở trên ta suy ra  $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}; 3^{\frac{p-1}{2}} \equiv -1 \pmod{p}; 6^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

Nhưng vì  $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}; 3^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Rightarrow 6^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  là điều mâu thuẫn.

Chúng tỏ rằng giả thiết phản chứng là sai.

**Câu 24.** Chứng minh rằng với mọi số nguyên  $p$  ta có thể tìm được số nguyên dương  $f(x)$  sao cho  $n$  không phải là số chính phương.

**Lời giải**

Đặt  $f(n)$ . Nếu  $p^n - 1$  là số chính phương thì  $p-1$  hoặc  $f(x) \equiv b, b \in A$ .

Giả sử tồn tại bộ số nguyên  $\forall n \in \mathbb{N}^*, (p^n - 1) : (p-1) : b$  sao cho với mọi số nguyên dương  $f(x)$  thì  $n \in \mathbb{N}^*$  đều là số chính phương. Khi đó  $q$  đều là các số chính phương. Ta có

$$f(n); f(n+q) - f(n) : (n+q-n) = q \Rightarrow f(n) : q \quad (1)$$

Mặt khác do tính chất của số chính phương nên ta suy ra  $f(n+q) : q$ .

Kết hợp với (1) ta suy ra  $f(2) - f(4) \equiv 0 \pmod{4}$ .

Suy ra  $p \neq q, (p^q - 1) : q \quad (2)$ .

Bây giờ ta lại xét  $p^q \equiv p \pmod{q}$ .

Lập luận như trên ta suy ra  $p^q - 1 - (p^q - p) = p - 1 : q \quad (3)$ .

Kết hợp (2), (3) ta suy ra  $n \in \mathbb{N}^*$  là điều vô lí.

Chúng tỏ giả thiết phản chứng là sai.

**Câu 25.** Cho đa thức  $P(x) = x^{2017} - x^{1000} + 1$ . Tồn tại hay không các số tự nhiên  $a_1, a_2, \dots, a_{2018}$  sao cho tích  $P(a_i) \cdot P(a_j) : a_i a_j$  với mọi  $i \neq j$ .

**Lời giải**

Giả sử tồn tại các số  $a_1, a_2, \dots, a_{2018}$  sao cho với mọi  $i \neq j$  ta có  $P(a_i) \cdot P(a_j) : a_i a_j$ .

Dễ thấy rằng  $(a_i, P(a_i)) = 1$ . Từ đó suy ra  $P(a_i) : a_j$  và với mọi  $i \neq j$ .

Ta suy ra  $(a_i^{2017} - a_i^{1000} + 1) : a_j$ , từ đó suy ra  $(a_i, a_j) = 1$  với mọi  $i \neq j$ .

Không mất tính tổng quát ta có thể giả sử rằng  $a_1 < a_2 < \dots < a_{2018}$ .



Từ  $P(a_i):a_j$  ta suy ra rằng  $P(a_1):a_2.a_3...a_{2018} > a_1^{2017}$ .

Nhưng từ  $P(x)$  ta suy ra  $P(a_1) < a_1^{2017}$  là điều mâu thuẫn.

**Câu 26.** Với mọi số tự nhiên  $m, n$ , chứng minh rằng  $(n!)$  chia hết cho  $m$  khi và chỉ khi tồn tại đa thức hệ số nguyên  $f(x) = \sum_{k=0}^n a_k x^k$  thỏa mãn  $(a_0, a_1, \dots, a_n, m) = 1, m \mid f(j)$  với mọi  $j$  nguyên dương.

### Lời giải

Ta chứng minh tính hai chiều

Giả sử ta có  $m \mid (n!)$ . Ta xét đa thức sau  $f(x) = (x+1)(x+2)\dots(x+n)$  thì  $f$  là đa thức với hệ số nguyên. Ta cũng có  $f(j) = n!C_{n+j}^n$ . Do  $m \mid (n!)$  nên ta có  $f(j) \equiv 0 \pmod{m}$ . Mặt khác do hệ số bậc cao nhất của  $f$  là 1 nên ta có điều kiện  $(a_0, a_1, \dots, a_n, m) = 1$  được thỏa mãn. Như vậy tồn tại đa thức  $f(x) = (x+1)(x+2)\dots(x+n)$ .

Ngược lại giả sử ta có tồn tại đa thức  $f(x) = \sum_{k=0}^n a_k x^k$  hệ số nguyên thỏa mãn điều kiện là

$$(a_0, a_1, \dots, a_n, m) = 1, m \mid f(j).$$

Ta xét dạng của  $f$  là  $f(x) = b_0 + b_1x + b_2x(x-1) + \dots + b_nx(x-1)(x-2)\dots(x-n+1)$

$$= b_0 + \sum_{k=1}^n b_k x(x-1)\dots(x-k+1).$$

Với mỗi đa thức  $f$  hoàn toàn xác định thì các số  $b_k$  xác định duy nhất với mọi số  $k = \overline{0, n}$ .

Tiếp theo ta có nhận xét là  $(b_0, b_1, \dots, b_n) = (a_0, a_1, \dots, a_n)$ .

Thật vậy. Ta giả  $p$  là một ước của  $(b_0, b_1, \dots, b_n)$ , thì khi đó  $p$  là ước của  $f(j)$  với mọi số nguyên  $j$ . Do đó khi và chỉ khi  $p$  là một ước của  $(a_0, a_1, \dots, a_n)$ . Do đó ta có

$$(b_0, b_1, \dots, b_n) = (a_0, a_1, \dots, a_n).$$

Do  $m \mid f(j)$  nên  $f(j) \equiv 0 \pmod{m}$  với mọi  $j = 0, 1, 2, \dots, n$ . Nên đặc biệt ta có

$$b_0 = f(0) \equiv 0 \pmod{m}; \quad b_0 + b_1 = f(1) \equiv 0 \pmod{m} \Rightarrow b_1 \equiv 0 \pmod{m}.$$

Tương tự  $f(2) = b_0 + 2b_1 + 2b_2 \equiv 0 \pmod{m} \Rightarrow 2b_2 \equiv 0 \pmod{m}$ .

Bằng cách tương tự ta có khẳng định là  $j!.b_j \equiv 0 \pmod{m}$ .

Do  $(b_0, b_1, \dots, b_n, m) = (a_0, a_1, \dots, a_n, m) = 1$  nên tồn tại các số nguyên  $c_0, c_1, \dots, c_n, D$  sao cho

$$c_0b_0 + c_1b_1 + \dots + c_nb_n + Dm = 1 \Rightarrow n!(c_0b_0 + c_1b_1 + \dots + c_nb_n) + n!Dm = n! \quad (1).$$

Nhưng do  $j!.b_j \equiv 0 \pmod{m}$  nên từ (1) ta suy ra  $n! \equiv 0 \pmod{m}$  (ở bên vế phải).



**Câu 27.** Cho đa thức  $f(x) = 2009x^5 - x^4 - x^3 - x^2 - 2006x + 1$ . Chứng minh rằng với  $n$  là số nguyên tùy ý thì các số  $f(n), f(f(n)), \dots, f(\dots f(n) \dots)$  đôi một nguyên tố cùng nhau.

**Lời giải**

**Nhận xét.** Nếu  $a \equiv b \pmod{q}$  thì  $h(a) \equiv h(b) \pmod{q}$ .

Đặt  $f_k(x) = f(f \dots f(x) \dots)$  với  $f$  có mặt  $k$  lần với  $k \geq 1$ .

Gọi  $p_k$  là một ước nguyên tố tùy ý của  $(P_n(x))$  thì ta có  $f_k(n) \equiv 0 \pmod{p_k}$

Ta có  $(P_n(x)); f_{k+2}(n) = f(f_{k+1}(n)) \equiv f(1) \equiv 1 \pmod{p}$

Bằng quy nạp ta chứng minh được  $f_m(n) \equiv 1 \pmod{p}$  với mọi  $(P_n(x))$ , tức là  $f_k(n)$  và  $f_m(n)$  nguyên tố cùng nhau với mọi số  $m > k$ . Vì nếu không như thế thì  $(f_k(n), f_m(n)) = d$ .

Gọi  $p$  là một ước nguyên tố của  $d$  thì  $p$  là ước chung của cả  $f_k(n), f_m(n)$  là mâu thuẫn với chứng minh nêu trên. Ta hiểu là khi mà  $k$  thay đổi thì số nguyên tố  $p$  được điều chỉnh

thay đổi theo chỉ số  $k$ . Do  $k$  là số tùy nên ta có  $P(x) = \prod_{i=1}^{2015} (x - x_i) - 1$  đôi một nguyên tố cùng nhau.

**Câu 28.** Gọi  $P(x)$  là đa thức bậc  $n$  thỏa mãn với  $k = 0, 1, \dots, n$  thì  $P(k) = \binom{n+1}{k}^{-1}$

Định đa thức  $P(n+1)$ .

**Đề xuất 1981 IMO – Romanian**

**Lời giải**

Với  $k = 0, 1, \dots, n$ , đặt  $w_k = k$  và  $c_k = \binom{n+1}{k}^{-1} = \frac{k!(n+1-k)!}{(n+1)!}$

Định các giá trị cho  $f_0, f_1, \dots, f_n$ , ta được  $f_k(k) = (-1)^{n-k} k!(n-k)!$  và  $f_k(n+1) = \frac{(n+1)!}{(n+1-k)}$

Theo **công thức nội suy Lagrange** ta có  $P(n+1) = \sum_{k=0}^n c_k \frac{f_k(n+1)}{f_k(k)} = \sum_{k=0}^n (-1)^{n-k}$

Bằng 0 nếu  $n$  lẻ và bằng 1 nếu  $n$  chẵn.

**Nhận xét.** Trong một số bài toán về đa thức, ta đôi lúc sẽ bắt gặp một số công thức như nội suy Lagrange, khai triển Taylor, ... việc hiểu và vận dụng linh hoạt các công thức trên sẽ giúp bài toán trở nên gọn gàng và ít rườm rà hơn.



**Câu 29.** Cho dãy  $\{u_n\}$  được xác định như sau  $\begin{cases} u_1 = 1990, u_2 = 1989, u_3 = 2000 \\ u_{n+3} = 19u_{n+2} + 9u_{n+1} + u_n + 1991, n = 1, 2, \dots \end{cases}$

a) Với mọi  $n$  gọi  $r_n$  là số dư của phép chia  $u_n$  cho 1992. Chứng minh rằng dãy  $\{r_n\}$  là một dãy tuần hoàn.

b) Chứng minh rằng tồn tại vô số số  $x$  của dãy  $\{u_n\}$  sao cho

$$5x^{1992} + 5x^{1994} + 4x^{1975} + 8x^{1945} + 2x^{1990} + 11x^2 + 48$$

chia hết cho 1992.

### Lời giải

a) Đây là dãy truy hồi tuyến tính cấp ba. Gọi  $r_n$  là số dư khi chia  $u_n$  cho 1992. Ta thấy chỉ có tối đa 1992 số dư khác nhau. Số bộ ba các số dư có kể thứ tự khác nhau có thể là  $A_{1992}^3$ .

Xét các bộ ba số dư của phép chia  $u_n$  cho 1992 là ( vì ta cần truy hồi tới ba số hạng phía trước nên ta xét các bộ ba số  $(r_1, r_2, r_3); (r_2, r_3, r_4); \dots; (r_i, r_{i+1}, r_{i+2}); (r_{i+1}, r_{i+2}, r_{i+3}); \dots$  số các bộ số lập theo cách trên là vô hạn. Tuy nhiên chỉ có hữu hạn số dư ( tối đa là 1992 số) trong phép chia  $u_n$  cho 1992 nên chỉ có hữu hạn các bộ ba khác nhau. Tối đa là  $A_{1992}^3$  bộ. Do đó luôn tồn tại các số nguyên dương  $m, s$  sao cho

$$(r_m, r_{m+1}, r_{m+2}) = (r_{m+s}, r_{m+s+1}, r_{m+s+2}), \text{ tức là } \begin{cases} r_m = r_{m+s} \\ r_{m+1} = r_{m+s+1} \\ r_{m+2} = r_{m+s+2} \end{cases} \quad (1).$$

Như vậy có nghĩa là tồn tại  $k = m, m+1, m+2$  sao cho ta có  $r_k = r_{k+s} \quad (2), \forall k \geq 1$

Ta sẽ chứng minh bằng quy nạp rằng  $r_k = r_{k+s} \quad (2), \forall k \geq 1$ .

Ta đã có  $r_k = r_{k+s}$  với  $k = m, k = m+1, k = m+2$ .

Giả sử ta có (2) đúng với  $m \leq k \leq p$  trong đó  $p \geq m+2$ . Ta xét  $k = p+1$ .

$$\begin{aligned} \text{Ta có } u_{p+1+s} - u_{p+1} &= 19(u_{p+s} - u_p) + 9(u_{p+s-1} - u_{p-1}) + (u_{p+s-2} - u_{p-2}) \\ &\equiv 19(r_{p+s} - r_p) + 9(r_{p+s-1} - r_{p-1}) + (r_{p+s-2} - r_{p-2}) \equiv 0 \pmod{1992}. \end{aligned}$$

Như vậy ta có  $r_{p+1+s} = r_{p+1}$ .

Vậy ta có  $r_k = r_{k+s}, \forall k \geq m$

Cuối cùng ta phải chứng minh khẳng định  $r_k = r_{k+s}, \forall k \geq 1$ .

Nếu  $m = 1$  thì ta có  $r_1 = r_{1+s}$ .

Nếu  $m > 1$ , ta phải chứng minh  $r_k = r_{k+s}, 1 \leq k < m-1$ .

Từ cách xác định dãy ta truy ngược có  $u_{n+3} - 19u_{n+2} - 9u_{n+1} - 1991 = u_n$ .

$$\begin{aligned} \text{Cho nên ta có } u_{m-1+s} - u_{m-1} &= (u_{m+2+s} - u_{m+2}) - 19(u_{m+1+s} - u_{m+1}) - 9(u_{m+s} - u_m) \\ &\quad (r_{m+2+s} - r_{m+2}) - 19(r_{m+1+s} - r_{m+1}) - 9(r_{m+s} - r_m) \equiv 0. \end{aligned}$$

Cứ thế sau  $m-1$  bước lùi chỉ số ta thu được  $r_k = r_{k+s}, 1 \leq k < m-1$ .



Kết hợp lại ta có  $r_k = r_{k+s} (2), \forall k \geq 1$ .

Như vậy dãy  $\{r_n\}$  là dãy tuần hoàn với chu kỳ  $s > 1$  ( tại vì  $r_1 = -2 \neq r_2 = -3$  )

b) Đặt  $P(x) = 5x^{1992} + 5x^{1994} + 4x^{1975} + 8x^{1945} + 2x^{1990} + 11x^2 + 48$ .

Ta thấy dãy  $\{u_n\}$  là dãy tăng khi  $n \geq 2$ .

Do đó ta cũng suy ra với chu kỳ  $s > 1$  ở trên thì ta có ( chu kỳ  $s > 1$  vì  $r_2 \neq r_1$  ).

$$u_s < u_{2s} < \dots < u_{ks} < u_{(k+1)s} < \dots$$

Đây là dãy tăng thực sự nên có vô hạn phần tử.

Ta chỉ cần chứng minh  $P(u_{ks}) = 1992, \forall k \geq 1$ .

Ta có từ cách xác định dãy ta suy ra  $p(x)q(x)$ .

Do đó  $p(x) \equiv q(x)$  ( do  $p(x) - q(x)$  ) mà  $p_n(x)$ , lại do  $p_1(x) = p_2(x) = 1$  nên suy ra

$$p_{n+2}(x) = p_{n+1}(x) + xp_n(x).$$

Vậy ta có điều phải chứng minh!

**Câu 30.** Chứng minh rằng tồn tại hằng số dương  $c$  sao cho với mọi số nguyên dương  $n$  và các số thực  $a_1, a_2, \dots, a_n$ , nếu  $P(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$  thì

$$\max_{x \in [0, 2]} |P(x)| \leq c^n \max_{x \in [0, 1]} |P(x)|$$

*Lời giải – Lee Kai Seng*

Đặt  $S$  là giá trị lớn nhất của  $|P(x)| \forall x \in [0, 1]$ . Với  $i = 0, 1, 2, \dots, n$ , đặt  $b_i = \frac{i}{n}$  và

$$f_i(x) = (x - b_0) \cdots (x - b_{i-1})(x - b_{i+1}) \cdots (x - b_n)$$

Bằng **công thức nội suy Lagrange**, với mọi số thực  $x$  ta có  $P(x) = \sum_{i=0}^n P(b_i) \frac{f_i(x)}{f_i(b_i)}$

Với các giá trị  $w \in [0, 2], |w - b_k| \leq |2 - b_k| \forall k = 0, 1, 2, \dots, n$  nên

$$|f_i(w)| \leq |f_i(2)| = \prod_{i=0}^n \left(2 - \frac{i}{n}\right) = \frac{2n(2n-1)(2n-2) \cdots (n+1)}{n^n} = \frac{(2n)!}{n!n^n}$$

Lại có  $|P(b_i)| \leq S$  và  $|f_i(b_i)| = \frac{i!(n-i)!}{n^n}$ .

Theo bất đẳng thức tam giác ta có  $|P(w)| \leq \sum_{i=0}^n |P(b_i)| \frac{|f_i(w)|}{|f_i(b_i)|} \leq S \sum_{i=0}^n \binom{2n}{i} \binom{2n-i}{n}$

Suy ra  $\sum_{i=0}^n \binom{2n}{i} \binom{2n-i}{n} \leq \sum_{i=0}^n \binom{2n}{i} \binom{2n}{n} = 2^{2n} \binom{2n}{n} \leq 2^{4n}$

Vậy  $\max_{w \in [0, 2]} |P(w)| \leq 2^{4n} S = 16^n \max_{x \in [0, 1]} |P(x)|$ .





**Câu 31.** Tìm tất cả các đa thức  $P(x) \in \mathbb{Z}[x]$  và  $m \in \mathbb{Z}^+$  sao cho  $m + 2^n P(n)$  là số chính phương với mọi số nguyên dương  $n$ .

Nguyễn Song Minh

### Lời giải

Lời giải sau đây của thầy Nguyễn Song Minh – Admin Mathscope.

Giả sử  $P(x)$  và  $m$  là đa thức và số nguyên dương thỏa mãn, ta có 2 nhận xét sau:

**Nhận xét 1.** Nếu  $p$  là ước nguyên tố lẻ của  $m + 2^n P(n)$  thì  $p \mid P'(n)$

**Chứng minh.** Ta có  $v_p(m + 2^n P(n)) \geq 2$ , theo bổ đề Fermat bé thì:

$$m + 2^n P(n) \equiv m + 2^{n+p(p-1)} P(n + p(p-1)) \pmod{p}$$

Vì thế ta lại có  $v_p(m + 2^{n+p(p-1)} P(n + p(p-1))) \geq 2$ , theo **bổ đề tiếp tuyến** và **định lý Euler** ta có  $0 \equiv m + 2^{n+p(p-1)} P(n + p(p-1)) \equiv m + 2^n P(n) + 2^n p(p-1) P'(n) \pmod{p^2}$ .

Từ đây có  $p \mid P'(n)$ .

**Nhận xét 2.** Nếu  $p$  là ước nguyên tố lẻ của  $m + 2^K P(n)$  với  $K \in \mathbb{Z}^+$  thì  $p \mid P'(n)$ .

**Chứng minh.** Theo định lý thặng dư Trung Hoa, sẽ tồn tại số nguyên dương  $N$  sao cho  $N \equiv K \pmod{p-1}$  và  $N \equiv n \pmod{p}$ , từ đây có  $p \mid (m + 2^N P(N))$ .

Do đó theo nhận xét 1 thì  $p \mid P'(N)$  nhưng  $P'(x) \in \mathbb{Z}[x]$  nên từ  $N \equiv n \pmod{p}$  ta có:

$$p \mid P'(n)$$

Quay lại bài toán, với mỗi  $n \in \mathbb{Z}^+$  đủ lớn, sẽ có vô số số nguyên tố  $p$  có dạng  $8k+3$  đồng

thời  $p > \max\{m, P(n)\}$ . Lúc này ta để ý rằng  $\left(\frac{2}{p}\right) = -1$  nên 2 là căn nguyên thủy modulo  $p$

khi đó sẽ tồn tại  $K$  sao cho  $p \mid (m + 2^K P(n))$  (ta chọn  $K = \text{ind}_2(-m\bar{P})$  với  $\bar{P}$  là nghịch đảo của  $P(n)$  theo mod  $p$ , theo nhận xét 2 thì  $p \mid P'(n)$ .

Do đó có vô số số nguyên tố  $p$  như thế, và giá trị của chúng có thể lớn tùy ý nên  $P'(n) = 0$

Từ đây ta thấy rằng phương trình  $P'(x) = 0$  có vô số nghiệm, nên  $P(x) = C$  (với  $C$  là hằng số), từ đây ta dễ dàng chứng minh được  $P(x) = 0$  còn  $m$  là số chính phương.

**Nhận xét.** Bài toán trên yêu cầu ta phải vận dụng linh hoạt các tính chất số học của đa thức, ngoài ra có một số bổ đề nhỏ ta cần phải quan tâm như **bổ đề tiếp tuyến** được phát biểu và chứng minh ngắn gọn như sau.

**Câu 32.** Cho  $P(x) \in \mathbb{Z}[x]$ ,  $p$  là số nguyên tố và  $x \equiv a \pmod{p}$ . Chứng minh rằng

$$P(x) \equiv P(a) + (x-a)P'(a) \pmod{p^2}$$

Bổ đề tiếp tuyến

### Lời giải



Với mọi đa thức  $P(x)$  và  $a \neq b$  nguyên thì  $a - b \mid P(a) - P(b)$

Nếu  $P(x) \in \mathbb{Z}[x]$  và  $k \in \mathbb{Z}^+$  thì  $\frac{P^{(k)}(x_0)}{k!} \in \mathbb{Z} \forall x_0 \in \mathbb{Z}$ , do tích của  $k$  số nguyên liên tiếp chia hết cho  $k!$ , mà đạo hàm cấp  $k$  thì chứa các tích đó.

Khai triển Taylor của đa thức tại  $x = x_0$ :

$$P(x) = P(x_0) + \frac{P'(x_0)}{1!}(x - x_0) + \frac{P''(x_0)}{2!}(x - x_0)^2 + \cdots + \frac{P^{(n)}(x_0)}{n!}(x - x_0)^n$$

Từ những điều trên, xét  $x = a + pt$  với  $t \in \mathbb{Z}$  thì dễ dàng có:

$$P(x) \equiv P(x_0) + P'(x_0)pt + \underbrace{P''(x_0)(pt)^2}_{:p^2} + \cdots \equiv P(x_0) + P'(x_0)pt \pmod{p^2}$$

**Nhận xét.** Bổ đề trên là cơ sở cho **bổ đề Hensel (Hensel lifting lemma)** dùng để chứng minh tồn tại hoặc đếm số nghiệm của phương trình đồng dư với modulo là lũy thừa của số nguyên tố.

**Câu 33.** Với  $p$  là số nguyên tố, đặt  $h(x)$  là đa thức có hệ số nguyên sao cho  $h(0), h(1), \dots, h(p^2 - 1)$  là một hệ thặng dư đầy đủ modulo  $p^2$ . Chứng minh rằng  $h(0), h(1), \dots, h(p^3 - 1)$  là một hệ thặng dư đầy đủ modulo  $p^3$ .

*Putnam 2008 B4*

### Lời giải

Dưới đây xin giới thiệu với bạn đọc **lời giải** chính thức của cuộc thi.

Ta xác định đa thức với khai triển Taylor  $h(x + y) = \sum_{i=0}^{\deg(h)} \frac{h^{(i)}(x)}{i!} y^i$

Trong khai triển này,  $\frac{h^{(i)}(x)}{i!}$  là đa thức theo biến  $x$  với hệ số nguyên.

Với  $x = 0, \dots, p - 1$ , ta suy ra được  $h(x + p) \equiv h(x) + ph'(x) \pmod{p^2}$

Điều này có thể suy ra được trực tiếp bằng cách sử dụng khai triển Nhị thức Newton

Vì thế ta giả sử  $h(x)$  và  $h(x + p)$  phân biệt với modulo  $p^2$ , ta kết luận được

$h'(x) \not\equiv 0 \pmod{p}$ . Do  $h'$  là đa thức với hệ số nguyên, ta có  $h'(x) \equiv h'(x + mp) \pmod{p}$  với mọi số nguyên  $m$ , vì thế  $h'(x) \not\equiv 0 \pmod{p}$  với mọi số nguyên  $x$ .

Với  $x = 0, \dots, p^2 - 1$  và  $y = 0, \dots, p - 1$ , ta viết được đa thức  $h$  dưới dạng:

$$h(x + yp^2) \equiv h(x) + p^2 y h'(x) \pmod{p^3}$$

Do đó  $h(x), h(x + p^2), \dots, h(x + (p - 1)p^2)$  chạy qua tất cả các lớp giá trị dư của modulo  $p^3$ , đồng dạng với  $h(x)$  theo modulo  $p^2$ .



Vì đa thức  $h(x)$  đã chạy qua các lớp giá trị dư theo modulo  $p^2$ , chứng minh này đã dẫn tới  $h(0), h(1), \dots, h(p^3 - 1)$  phân biệt với modulo  $p^3$ .

### Cách 2.

Trước hết ta chứng minh  $P'(x)$  không chia hết cho  $p$  với mọi  $x$  nguyên.

Thật vậy giả sử tồn tại  $x$  mà  $P'(x) \equiv 0 \pmod{p}$ , khi đó ta chọn  $y$  sao  $0 \leq y < p$  và  $y \equiv x \pmod{p}$ . Theo cách chứng minh định lý Hensel ta có

$$P'(y) \equiv P'(x) \pmod{p} \Rightarrow P(x+p) \equiv P(y) + pP'(y) \pmod{p^2} \equiv P(y) \pmod{p^2}.$$

Mà ta lại có  $0 \leq y < y+p \leq p^2 - 1$ . Điều này mâu thuẫn với hệ  $\{P(0), P(1), \dots, P(p^2 - 1)\}$  là hệ thặng dư đầy đủ modulo  $p$ .

Phần tiếp theo ta chứng minh hệ  $\{P(0), P(1), \dots, P(p^3 - 1)\}$  là một hệ thặng dư đầy đủ modulo  $p^3$ .

Giả sử tồn tại hai số  $0 \leq a \leq b < p^3$  và  $P(a) \equiv P(b) \pmod{p^3}$ .

Ta đặt  $a = a_0 + p^2 a_1; b = b_0 + p^2 b_1$  với  $(0 \leq a_0, b_0, a_1, b_1 < p^2; 0 \leq a, b < p)$ .

Ta cần chứng minh khi đó  $a = b$ .

Từ cách đặt và giả sử ta có các điều kiện ta suy ra

$$P(a) \equiv P(a_0) \pmod{p^2}, P(b) \equiv P(b_0) \pmod{p^2}; P(a) \equiv P(b) \pmod{p^2}$$

Ta suy ra  $P(a_0) \equiv P(b_0) \pmod{p^2}$ . Từ đó suy ra  $a_0 = b_0$ .

Lại theo phần chứng minh trong định lý Hensel ta có

$$0 \equiv P(a) - P(b) \equiv P(a_0) + p^2 a_1 P'(a_0) - [P(b_0) + p^2 b_1 P'(b_0)] \equiv p^2 P'(a_0)(a_1 - b_1) \pmod{p^3}$$

$\Rightarrow a_1 - b_1 \equiv 0 \pmod{p}$ , do ta đã chứng minh  $P'(x) \not\equiv 0 \pmod{p}$ .

Từ đó ta có  $a = b \Rightarrow P(a) \equiv P(b) \pmod{p^3} \Leftrightarrow a = b$ . Ta có điều cần chứng minh.

### Nhận xét.

- Một cách tổng quát hơn, bằng cách chứng minh tương tự như trên ta có thể chỉ ra rằng với số nguyên  $d, e > 1$  bất kỳ, đa thức  $h$  hoán vị cho các lớp giá trị dư modulo  $p^d$  khi và chỉ khi nó hoán vị cho các lớp giá trị dư modulo  $p^e$ . Lập luận trên được thể hiện quen thuộc trong kết quả chứng minh của **bổ đề Hensel**.
- Khái niệm về lớp giá trị dư – **Residue class** – AoPS: Trong các bài toán số học về modulo, phần còn lại của một số nguyên  $a$  theo modulo  $n$  là giá trị duy nhất của  $0 \leq r \leq n-1$ , vậy  $a = kn + r$ . Lớp giá trị dư là tập các số nguyên đồng dạng theo modulo  $n$  với một vài giá trị nguyên dương  $n$ . Trong modulo  $n$ , có chính xác  $n$  lớp giá trị dư phân biệt, tương ứng với  $n$  giá trị còn lại  $\{0, 1, 2, 3, \dots, n-2, n-1\}$ . Mỗi lớp giá trị dư chứa tất cả các số nguyên dạng  $kn + r$  với  $r$  là phần dư tương ứng.



**Câu 34.** Với số nguyên  $n \geq 3$ , đặt  $f(x), g(x)$  là đa thức với hệ số thực sao cho các điểm  $(f(1), g(1)), (f(2), g(2)), \dots, (f(n), g(n))$  trong tập  $\mathbb{R}^2$  là các đỉnh của đa giác  $n$  cạnh theo thứ tự ngược chiều kim đồng hồ. Chứng minh rằng ít nhất một trong các đa thức  $f, g$  có bậc không nhỏ hơn  $n-1$ .

Putnam 2008 A5

**Lời giải**

Ta biểu diễn các điểm trên dưới dạng đa thức hệ số phức  $P(z) = f(z) + ig(z)$ . Không khó để chứng minh rằng  $\deg P \geq n-1$ , khi đó một trong các hàm  $f, g$  phải có bậc không nhỏ hơn  $n-1$ .

Thay  $P(z)$  bằng  $aP(z) + b$  với các số  $a, b \in \mathbb{C}$  thích hợp, ta biến đổi các đỉnh của đa giác  $n$  cạnh trên thành dạng  $\zeta_n, \zeta_n^2, \dots, \zeta_n^n$  với  $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$ . Dễ kiểm tra rằng không tồn tại đa thức  $P(z)$  có bậc không vượt quá  $n-2$  sao cho  $P(i) = \zeta_n^i$  với  $i = 1, \dots, n$ .

Ta chứng minh rằng với mọi số phức  $t \notin \{0, 1\}$ , với mọi số nguyên  $m \geq 1$ , mọi đa thức  $Q(z)$  sao cho  $Q(i) = t^i$  với  $i = 1, \dots, m$  có bậc không bé hơn  $m-1$ .

Nếu  $\deg Q = d$  và có hệ số cao nhất là  $c$ , khi đó  $R(z) = Q(z+1) - tQ(z)$  có  $\deg R = d$  và có hệ số cao nhất là  $(1-t)c$ . Tuy nhiên, theo giả thiết trên,  $R(z)$  có các nghiệm phân biệt  $1, 2, \dots, m-1$  nên  $d \geq m-1$ .

**Nhận xét.** Ta có thể giải bài toán trên bằng cách sử dụng *ma trận Vandermonde* hoặc công thức *nội suy Lagrange* để tính toán hệ số cao nhất của  $Q$ .

**Câu 35.** Cho  $p$  là một số nguyên tố lẻ. Chứng minh rằng có ít nhất  $\frac{p+1}{2}$  giá trị  $n \in \{0, 1, 2, \dots, p-1\}$  sao cho  $\sum_{k=0}^{p-1} k! n^k$  không chia hết cho  $p$ .

Putnam 2011

**Lời giải**

Đặt  $f(x) = \sum_{k=0}^{p-1} k! x^k \in F_p[x]$  là tập hợp các đa thức bậc  $p$  có hệ số thuộc trường  $F_p$ .

Ta phân hoạch  $F_p = Z \cup Z'$ , trong đó  $Z = \{a \in F_p; f(a) = 0\}; Z' = \{a \in F_p; f(a) \neq 0\}$

Ta thấy  $f(0) = 1 \Rightarrow 0 \in Z' \Rightarrow |Z| \geq 1$ . Đặt  $|Z| = p-r, |Z'| = r \geq 1$

Xét đa thức  $s(x) = \prod_{a \in Z'} (x-a) \Rightarrow \deg s(x) = r$ .

Dưa vào cách ta định nghĩa thì đa thức  $s(x)f(x)$  triệt tiêu (luôn bằng 0) tại mọi điểm của trường  $F_p$ .



Do đó  $s(x)f(x) = (x^p - x)h(x)$  trong đó  $\deg h = r - 1$  và thuộc  $F_p[x]$ , lưu ý đến bậc của hai vế + **định lý Fermat** nhỏ. Trong những tính toán tiếp theo có sử dụng đến đạo hàm hình thức. Ta có

$$\begin{aligned} x \frac{d}{dx}(xf(x)) &= x \frac{d}{dx} \sum_{k=0}^{p-1} k! x^{k+1} = x \sum_{k=0}^{p-2} (k+1)! x^k = \sum_{k=1}^{p-1} k! x^k = f(x) - 1 \\ \Rightarrow x^2 f'(x) + xf(x) &= f(x) - 1 \Rightarrow x^2 f'(x) + (x-1)f(x) + 1 = 0 \end{aligned}$$

Lấy đạo hàm hình thức  $s(x)f(x) = (x^p - x)h(x)$  ta được:

$$s'(x)f(x) + s(x)f'(x) = (x^p - x)h'(x) - h(x)$$

**Chú ý.** Loại bỏ các số hạng triệt tiêu trên trường  $F_p$

Từ các kết luận trên ta thấy

$$\begin{aligned} x^2 s'(x)f(x) &= (x^p - x)x^2 h'(x) - x^2 h(x) - s(x)x^2 f'(x) \\ &= (x^p - x)x^2 h'(x) - x^2 h(x) + s(x)((x-1)f(x) + 1) \\ &= (x^p - x)x^2 h'(x) - x^2 h(x) + (x-1)(x^p - x)h(x) + s(x) \\ &= (x^p - x)(x^2 h'(x) - (x-1)h(x)) - x^2 h(x) + s(x) \end{aligned}$$

Ta thấy vế trái triệt tiêu trên  $Z \cup \{0\}$ ,  $x^p - x$  triệt tiêu trên  $F_p$  nên đa thức  $-x^2 h(x) + s(x)$  triệt tiêu trên  $z \cup \{0\}$ .

Ta thấy  $r + 1 = \deg(-x^2 h(x) + s(x)) \geq |Z| + 1 = p - r + 1 \Rightarrow r \geq \frac{p+1}{2}$ .

**Câu 36.** Có tồn tại hay không một dãy số thực và khác 0 là  $a_1; a_2; \dots, a_n$  thỏa với mỗi  $n \in \mathbb{N}$  thì đa thức  $a_0 + a_1 x + \dots + a_n x^n$  có đúng  $n$  nghiệm trên  $\mathbb{R}$ .

**Lời giải – Dark Templar – VMF. Diễn đàn toán học Việt Nam**

Ta chứng minh dãy trên tồn tại bằng cách xây dựng nó bằng quy nạp.

Chọn  $a_0 = -1, a_1 = 1$  sao cho thỏa mãn tính chất trên với  $n = 1$ .

Đặt  $P_n(x) = \sum_{k=0}^n a_k x^k$  với  $n$  nghiệm phân biệt là  $r_1 < r_2 < \dots < r_n$ .

Chọn  $x_0 < r_1$ . Cho  $x_k \in (r_k; r_{k+1}); \forall k \in [1; n-1]$  là giá trị mà  $|P_n(x)|$  đạt giá trị lớn nhất.

Cho  $x_n > r_n$ , có  $P_n(x_k) \neq 0; \forall k \in [0; n]$  và ta có thể chọn  $a > 0$  sao cho

$$a|x_k|^{n+1} < |P_n(x_k)|; \forall k \in [0; n].$$

Nếu  $P_n(x_n) > 0$ , đặt  $a_{n+1} = -a$

Nếu  $P_n(x_n) < 0$ , đặt  $a_{n+1} = a$ , có  $a|x_k|^{n+1} < |P_n(x_k)|$  chứng tỏ rằng  $P_{n+1}(x_k) = P_n(x_k) + a_{n+1}x_k^{n+1}$  luôn khác không và có cùng dấu với  $P_n(x_k)$  và  $\lim_{x \rightarrow +\infty} P_{n+1}(x)$  có dấu khác  $P_{n+1}(x_n)$ .

Do đó  $P_{n+1}(x)$  có 1 nghiệm thuộc  $(x_k; x_{k+1}); \forall k \in [0; n-1]$  và 1 nghiệm lớn hơn  $x_n$ .



**Câu 37.** Cho  $P(x) \in \mathbb{Z}[x]$  thỏa mãn  $P(x)$  là số chính phương với mọi  $x$  nguyên thì  $P(x) = Q^2(x)$  với  $Q(x) \in \mathbb{Z}[x]$ .

**Lời giải**

Ta chứng minh bằng phản chứng. Giả sử  $P(x) = Q(x)^2 \cdot p_1(x) \cdot p_2(x) \dots p_k(x)$  với  $p_i(x)$  là các đa thức bất khả quy bậc lớn hơn 1

Do  $p_i(x)$  bất khả quy nên  $p_1(x)$  và  $p_1'(x) \cdot p_2(x) \dots p_k(x)$  nguyên tố cùng nhau nên theo **định lý Bézout** thì tồn tại hai đa thức  $R(x), S(x)$  với hệ số nguyên sao cho

$$R(x) \cdot p_1(x) + S(x) \cdot p_1'(x) \cdot p_2(x) \dots p_k(x) = n \quad (n \in \mathbb{Z})$$

Chọn  $p > n$  nguyên tố sao cho tồn tại  $a$  để  $p_1(a)$  chia hết cho  $p$  thì  $p_1'(a)p_2(a) \dots p_k(a)$  không chia hết cho  $p$ , luôn tồn tại  $p$  theo **Schur**.

Nếu  $p_1(a)$  không chia hết cho  $p^2$  ta suy ra vô lý vì khi đó  $v_p(P(a))$  lẻ.

Nếu  $p_1(a)$  chia hết cho  $p^2$  ta xét  $p_1(a+p) \equiv p_1(a) + p \cdot p_1'(a) \pmod{p^2}$  thì  $p_1(a+p)$  không chia hết cho  $p^2$ .

Chứng minh tương tự như trên ta suy ra mâu thuẫn

Vậy  $P(x) = Q^2(x)$

**Nhận xét.**

- Bài toán có thể tổng quát cho trường hợp  $P(x)$  là lũy thừa bậc  $n$  của một số nguyên với cách chứng minh hoàn toàn tương tự.
- Bằng bài toán nhỏ trên ta có thể giải bài toán dưới đây với **lời giải** ngắn gọn hơn.

**Câu 38.** Tìm tất cả các đa thức hệ số nguyên thỏa mãn  $a+b$  là số chính phương thì  $P(a)+P(b)$  cũng là số chính phương, trong đó  $a, b$  là các số tự nhiên.

**Lời giải – Nguyễn Tiến Khải, Phạm Khoa Bằng – THPT chuyên KHTN**

**Bổ đề.** Nếu  $P(x) \in \mathbb{Z}[x]$  là số chính phương với mọi  $x$  thì nó là bình phương của một đa thức khác

Quay trở lại bài toán nhận xét rằng  $a+b$  chính phương thì  $(a+b)x^2$  chính phương.

Cố định  $a, b$ , ta xét đa thức  $Q(x) = P(ax^2) + P(bx^2)$  là số chính phương với vô số  $x$  nên là bình phương của đa thức  $G(x)$  nào đó.

Đặt  $G(x) = g_mx^m + \dots$  và  $P(x) = p_nx^n + \dots$ ,

Đồng nhất hệ số bậc cao nhất ta suy ra  $p_n((a^n + b^n)) = g^2$  nghĩa là với mọi  $a+b$  chính phương thì ta có điều trên



Cặp  $(1, 0)$  có  $1+0$  chính phương suy ra với mọi  $a+b$  số chính phương thì  $a^n+b^n$  là số chính phương với  $n \geq 1$

Với  $n=0$  cho ta  $P(x)=2k^2$ .

Với  $(2, 2)$  ta suy ra  $2 \cdot 2^n = 2^{n+1}$  suy ra  $n$  lẻ. Chọn  $(a, b) = (3, 1)$  ta có

$$3^n + 1 = u^2 \text{ hay } 3^n = (u-1)(u+1)$$

Ta có  $(3, 2) = 1$  và  $\gcd(u+1, u-1) | 2$ , mà 3 nguyên tố nên  $u-1=1$  hay  $u=2 \Rightarrow n=1$

Đặt  $P(x) = kx$  ta cần có  $k$  chính phương

Vậy các đa thức cần tìm:  $P(x) = k^2x; P(x) = 2k^2$ .

**Câu 39.** Giả sử  $m, p$  là các số nguyên tố khác nhau. Chứng minh rằng nếu có một số tự nhiên  $x$  nào đó mà  $p$  là ước của  $P(x) = (x^{m-1} + x^{m-2} + \dots + 1)$  thì ta có  $p \equiv 1 \pmod{m}$ .

### Lời giải

Giả sử  $p = mk + r$  ( $0 \leq r \leq m-1$ ), ta cần chỉ ra là  $r=1$  thì khi đó  $p-1 = mk$ .

Giả sử tồn tại số tự nhiên  $x$  sao cho  $(x^{m-1} + x^{m-2} + \dots + 1) : p \Rightarrow p | (x^m - 1) \Rightarrow x^m \equiv 1 \pmod{p}$  (1)

Do đó  $x$  không chia hết cho  $p$  nên  $(x, p) = 1$ .

Ta sẽ chứng minh  $x^{r-1} \equiv 1 \pmod{p}$ .

- Nếu  $p < m \Rightarrow r = p$  là số nguyên tố nên  $x^{r-1} \equiv 1 \pmod{p}$  (2) đúng do định lý Fermat.
- Nếu  $p \geq m$ . Ta có  $k = \frac{p-r}{m}$ . Trong (1) ta nâng lũy bậc  $k$  hai vế, ta được

$$x^{p-r} \equiv 1 \pmod{p} (*)$$

Nhưng theo **định lý Fermat** thì  $x^{p-1} \equiv 1 \pmod{p}$ .

Do đó trừ vế theo vế ta suy ra  $x^{p-r} (x^{r-1} - 1) \equiv 0 \pmod{p} \Rightarrow x^{r-1} \equiv 0 \pmod{p}$  do ta đã có (\*).

Cuối cùng ta chỉ ra  $r=1$ . Ngược lại nếu  $r > 1$ . Khi đó  $(m, r-1) = 1$  vì  $m$  là số nguyên tố.

Do đó  $(x^m - 1, x^{r-1} - 1) = x^{(m, r-1)} - 1 = x - 1$ . Nhưng từ (1), (2) ta có  $p | x^m - 1$  và  $p | x^{r-1} - 1$ , do đó  $p | x - 1 \Rightarrow x \equiv 1 \pmod{p}$ , điều này do ước chung lớn nhất thì chia hết cho mọi ước. Dẫn đến  $P(x) \equiv m \pmod{p}$ , điều này trái với giả thiết là  $p | P(x)$ . Vậy  $r=1$  nên  $p \equiv 1 \pmod{m}$ .





**Câu 40.** Cho đa thức  $P(x)$  có bậc  $n$  và có  $n$  nghiệm phân biệt  $x_1, x_2, \dots, x_n$ .

Chứng minh rằng:

$$a) \frac{P''(x_1)}{P'(x_1)} + \frac{P''(x_2)}{P'(x_2)} + \dots + \frac{P''(x_n)}{P'(x_n)} = 0$$

$$b) \frac{1}{P'(x_1)} + \frac{1}{P'(x_2)} + \dots + \frac{1}{P'(x_n)} = 0$$

**Lời giải**

a) Ta viết đa thức  $P$  dưới dạng  $P(x) = (x - x_1)(x - x_2) \dots (x - x_n)$ , giả sử rằng

$$x_1 < x_2 < \dots < x_n.$$

$$\text{Ta có } P'(x) = P(x) \left( \frac{1}{x - x_1} + \frac{1}{x - x_2} + \dots + \frac{1}{x - x_n} \right) = P(x) \sum_{i=1}^n \frac{1}{x - x_i} \quad (1)$$

Do  $P(x_i) = 0, i = \overline{1, n}$  nên theo **định lý Rolle** tồn tại

$$c_1, c_2, \dots, c_{n-1}; x_1 < c_1 < x_2 < c_2 < \dots < c_{n-1} < x_n$$

$$\text{Sao cho } P'(c_i) = 0, i = \overline{1, n-1} \quad (2)$$

$$\text{Lại có } P''(x) = P'(x) \left( \frac{1}{x - c_1} + \frac{1}{x - c_2} + \dots + \frac{1}{x - c_{n-1}} \right) = P'(x) \sum_{i=1}^{n-1} \frac{1}{x - c_i} \quad (3)$$

Từ (1), (2) suy ra:

$$\begin{cases} P'(c_1) = P(c_1) \left( \frac{1}{c_1 - x_1} + \frac{1}{c_1 - x_2} + \dots + \frac{1}{c_1 - x_n} \right) = P(c_1) \sum_{i=1}^n \frac{1}{c_1 - x_i} = 0 \\ P'(c_2) = P(c_2) \left( \frac{1}{c_2 - x_1} + \frac{1}{c_2 - x_2} + \dots + \frac{1}{c_2 - x_n} \right) = P(c_2) \sum_{i=1}^n \frac{1}{c_2 - x_i} = 0 \\ \dots\dots\dots \\ P'(c_{n-1}) = P(c_{n-1}) \left( \frac{1}{c_{n-1} - x_1} + \frac{1}{c_{n-1} - x_2} + \dots + \frac{1}{c_{n-1} - x_n} \right) = P(c_{n-1}) \sum_{i=1}^n \frac{1}{c_{n-1} - x_i} = 0 \end{cases}$$

Do  $P(c_i) \neq 0, i = \overline{1, n-1}$  nên ta có:

$$\begin{cases} \frac{1}{c_1 - x_1} + \frac{1}{c_1 - x_2} + \dots + \frac{1}{c_1 - x_n} = \sum_{i=1}^n \frac{1}{c_1 - x_i} = 0 \\ \frac{1}{c_2 - x_1} + \frac{1}{c_2 - x_2} + \dots + \frac{1}{c_2 - x_n} = \sum_{i=1}^n \frac{1}{c_2 - x_i} = 0 \\ \dots\dots\dots \\ \frac{1}{c_{n-1} - x_1} + \frac{1}{c_{n-1} - x_2} + \dots + \frac{1}{c_{n-1} - x_n} = \sum_{i=1}^n \frac{1}{c_{n-1} - x_i} = 0 \end{cases}$$

$$\text{Suy ra } \sum_{i=1}^n \frac{P''(x_i)}{P'(x_i)} = \sum_{i=1}^n \frac{1}{c_1 - x_i} + \sum_{i=1}^n \frac{1}{c_2 - x_i} + \dots + \sum_{i=1}^n \frac{1}{c_{n-1} - x_i} = 0$$





b) Xét phân tích  $P(x) = (x - x_1)(x - x_2) \dots (x - x_n) = \prod_{i=1}^n (x - x_i)$ .

Đặt  $P_i(x) = \prod_{j=1, j \neq i}^n (x - x_j) \Rightarrow P'(x) = \sum_{i=1}^n P_i(x)$ .

Ngoài ra  $P_i(x_j) = 0, \forall j \neq i; P_i(x_i) \neq 0, \forall i = \overline{1, n} \Rightarrow P'(x_i) = P_i(x_i), \forall i = \overline{1, n}$ .

Xét đa thức  $Q(x) = \sum_{i=1}^n \frac{P_i(x)}{P'(x_i)} - 1$  có bậc không vượt quá  $n - 1$ .

Ta có  $\forall i = \overline{1, n} \Rightarrow Q(x_i) = 0$ .

Suy ra đa thức này có  $n$  nghiệm thực, tức  $Q(x) = 0$  và hệ số cao nhất của  $Q$  cũng bằng 0.

Do đó  $\frac{1}{P'(x_1)} + \frac{1}{P'(x_2)} + \dots + \frac{1}{P'(x_n)} = 0$ .

**Câu 41.** Cho  $f$  là một đa thức có hệ số hữu tỉ và bậc không nhỏ hơn 2, và dãy  $(a_n)$  chỉ gồm các số hữu tỉ thỏa mãn  $f(a_{n+1}) = a_n$  với mọi số nguyên dương  $n$ . Chứng minh rằng dãy  $(a_n)$  tuần hoàn.

*Lời giải*

Để ý vì  $P(x)$  có bậc lớn hơn 2 nên  $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = \infty$ .

- Ta sẽ chỉ ra dãy  $(a_n)$  là bị chặn.

Vì  $f$  có bậc không nhỏ hơn 2 nên  $f$  có tính chất là khi  $|x|$  đủ lớn thì  $|f(x)| \rightarrow +\infty$ .

Điều đó có nghĩa là tồn tại số  $M > 0$  mà nếu  $|x| > M$  và đồng thời  $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = \infty$  thì ta có

$|f(x)| > |x| > M$ . Ta chọn được số  $M$  như vậy mà  $M > |a_1|$  vì do  $a_1 \in \mathbb{Q}$ .

Ta sẽ chỉ ra là  $|a_n| < M, \forall n \in \mathbb{N}^*$ .

Thật vậy. Giả sử phản chứng tồn tại số  $n$  để  $|a_n| > M$ .

Khi đó  $|f(a_n)| > |a_n| \Rightarrow |a_{n+1}| > |a_n| > M$ . Tiếp tục như vậy ta đi đến  $|a_1| > M$  là mâu thuẫn với cách chọn ban đầu. Như vậy dãy  $(a_n)$  bị chặn.

- Tiếp theo ta cần chỉ ra dãy  $(a_n)$  chỉ nhận hữu hạn giá trị.

Để làm việc đó ta cần chỉ ra là tồn tại một số nguyên dương  $N$  để  $N.a_n$  là số nguyên với mọi  $n$ . Như thế thì đi đến dãy  $(Na_n)$  chỉ có hữu hạn phần tử. Và đi đến dãy  $(a_n)$  cũng chỉ có hữu hạn phần tử.

Thật vậy. Gọi  $k$  là số thỏa mãn  $g(x) = k.f(x)$  là một đa thức có hệ số nguyên.

Đặt  $g(x) = k.f(x) = b_s x^s + b_{s-1} x^{s-1} + \dots + b_1 x + b_0$  thì  $b_s$  là các số nguyên.



Gọi  $N$  là số nguyên dương để cho  $N.a_1 \in \mathbb{Z}$ .

Khi đó ta thấy nếu  $Na_n \in \mathbb{Z}$  thì  $Na_{n+1} \in \mathbb{Z} (*)$ .

Chứng minh  $(*)$ .

Ta thấy  $Na_{n+1}$  là nghiệm của đa thức  $f\left(\frac{x}{N}\right) - a_n$ . Ta tạo ra **đa thức monic** bằng cách xét đa thức  $h(x) = \frac{k.N^s}{b^s} \left( f\left(\frac{x}{N}\right) - a_n \right)$  thì đa thức này nhận  $Na_{n+1}$  làm nghiệm nên nghiệm này phải là nghiệm nguyên. Vì vậy  $Na_{n+1} \in \mathbb{Z}$ . Từ đó theo nguyên lý quy nạp ta có  $(Na_n)$  nguyên với mọi số số nguyên dương  $n$ . Lại vì  $(a_n)$  là dãy bị chặn nên  $(Na_n)$  cũng bị chặn. Vì thế dãy  $(Na_n)$  chỉ có hữu hạn phần tử.

- Cuối cùng ta cần chỉ ra sự tồn tại của chu kỳ.

Giả sử dãy trên có tất cả  $m$  giá trị phân biệt.

Xét các bộ gồm  $m+1$  số của dãy là  $a_i, a_{i+1}, \dots, a_{i+m}$ .

Vì bộ này có tính thứ tự nên số các bộ khác nhau tối đa là  $m^{m+1}$ .

Điều này có nghĩa là sẽ có một loại bộ xuất hiện vô hạn lần trong dãy.

Trong mỗi bộ  $m+1$  số này luôn có hai số bằng nhau theo **nguyên lý Dirichlet**.

Ta giả sử hai số đó là  $a_j = a_{j+k}$ . Như thế luôn tồn tại  $k$  nguyên dương sao cho với  $j$  đủ lớn sao cho  $a_j = a_{j+k}$ . Từ  $a_j = a_{j+k}$  ta suy ra  $a_i = a_{i+k}$  với mọi  $i \leq j$  do cấu trúc của hàm số cho ban đầu. Mặt khác vì ta luôn chọn được  $j$  đủ lớn để có được điều trên nên ta suy ra  $a_i = a_{i+k}, \forall i \in \mathbb{N}$ .

**Câu 42.** Cho  $P(x)$  là đa thức bậc  $n$  với hệ số thực sao cho  $P(-1)$  khác 0 và  $-\frac{P'(-1)}{P(-1)} \leq \frac{n}{2}$

Chứng minh rằng  $P(x)$  luôn có ít nhất một nghiệm  $x_0$  sao cho  $|x_0| > 1$ .

### Lời giải

Giả sử  $x_i, i = \overline{1, n}$  là các nghiệm phức của đa thức  $P$ , khi đó ta xét với  $a \neq 0$ :

$$P(x) = a \prod_{i=1}^n (x - x_i) \Rightarrow \frac{P'(x)}{P(x)} = \sum_{i=1}^n \frac{1}{x - x_i} \Rightarrow -\frac{P'(-1)}{P(-1)} = \sum_{i=1}^n \frac{1}{1 + x_i}$$

$$\text{Suy ra } \frac{P'(-1)}{P(-1)} + \frac{n}{2} = \frac{n}{2} - \sum_{i=1}^n \frac{1}{1 + x_i} = \sum_{i=1}^n \left( \frac{1}{2} - \frac{1}{1 + x_i} \right) = \frac{1}{2} \sum_{i=1}^n \left( \frac{x_i - 1}{x_i + 1} \right)$$

$$\text{Theo tính chất của số phức } \frac{x_i - 1}{x_i + 1} = \frac{(x_i - 1)(\overline{x_i} + 1)}{|x_i + 1|^2} \Rightarrow \operatorname{Re} \left( \frac{x_i - 1}{x_i + 1} \right) = \frac{|x_i|^2 - 1}{|x_i + 1|^2}, i = \overline{1, n}$$



Mặt khác  $\frac{P'(-1)}{P(-1)} + \frac{n}{2} \in R \Rightarrow \frac{P'(-1)}{P(-1)} + \frac{n}{2} = \frac{1}{2} \sum_{i=1}^n \left( \frac{|x_i|^2 - 1}{|x_i + 1|^2} \right) \geq 0 \Rightarrow |x_i|^2 \geq 1 \Leftrightarrow |x_i| \geq 1$

Vậy ta có điều phải chứng minh.

**Câu 43.** Giả sử tồn tại đa thức hệ phức  $P, Q, R$  thỏa mãn  $P^a + Q^b = R^c$  ( $a, b, c \in \mathbb{N}$ ).

Chứng minh rằng  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$

*The IMO Compendium*

**Lời giải**

**Bổ đề.** Nếu  $A, B, C$  là các cặp đa thức “nguyên tố cùng nhau” (*coprime*) theo dạng  $A + B = C$ , khi đó bậc của mỗi đa thức nhỏ hơn số lượng các đa thức khác 0 của đa thức  $ABC$ .

**Chứng minh.** Ta đặt  $A(x) = \prod_{i=1}^k (x - p_i)^{a_i}, B(x) = \prod_{i=1}^l (x - q_i)^{b_i}, C(x) = \prod_{i=1}^m (x - r_i)^{c_i}$ .

Viết lại điều kiện  $A + B = C$  dưới dạng  $A(x)C(x)^{-1} + B(x)C(x)^{-1} = 1$ , đạo hàm hai vế biểu thức theo biến  $x$  ta được:

$$A(x)C(x)^{-1} \left( \sum_{i=1}^k \frac{a_i}{x - p_i} - \sum_{i=1}^m \frac{c_i}{x - r_i} \right) = -B(x)C(x)^{-1} \left( \sum_{i=1}^l \frac{b_i}{x - q_i} - \sum_{i=1}^m \frac{c_i}{x - r_i} \right)$$

Ta thấy rằng  $\frac{A(x)}{B(x)}$  có thể viết được dưới dạng thương của hai đa thức có bậc không vượt

quá  $k + l + m - 1$ , từ đây ta suy được rằng  $A$  và  $B$  “nguyên tố cùng nhau”

Áp dụng bổ đề trên với các đa thức  $P^a, Q^b, R^c$  có các bậc của chúng là

$a \deg P, b \deg Q, c \deg R$  lần lượt nhỏ hơn  $\deg P + \deg Q + \deg R$ , từ đó suy ra được rằng:

$$\frac{1}{a} > \frac{\deg P}{\deg P + \deg Q + \deg R} \dots$$

Cộng lần lượt về theo vế các bất đẳng thức, ta có điều phải chứng minh.

**Nhận xét.**

- Trong bài toán trên ta bắt gặp một khái niệm mới về “cặp đa thức nguyên tố cùng nhau” (*coprime polynomials*) được phát biểu tương tự như đối với cặp số nguyên tố cùng nhau, là khi các đa thức  $p(t), q(t)$  thỏa mãn  $\gcd(p(t), q(t)) = 1$
- Bài toán ta vừa thực hiện là mở rộng cho định lý lớn Fermat cho đa thức.

**Câu 44.** Cho đa thức  $P(x)$  và  $Q(x)$  với số thực  $k$  bất kì thỏa mãn  $P_k = \{z \in \mathbb{C} \mid P(z) = k\}$  và  $Q_k = \{z \in \mathbb{C} \mid Q(z) = k\}$ . Chứng minh rằng  $P_0 = Q_0$  và  $P_1 = Q_1$  suy ra được  $P(x) = Q(x)$

**Lời giải**



Không mất tính tổng quát, giả sử  $n = \deg P \geq \deg Q$ .

Đặt  $P_0 = \{z_1, z_2, \dots, z_k\}$  và  $P_1 = \{z_{k+1}, z_{k+2}, \dots, z_{k+m}\}$ .

Hai đa thức  $P$  và  $Q$  trùng nhau tại  $k+m$  điểm  $z_1, z_2, \dots, z_{k+m}$ .

Ta cần chứng minh  $k+m > n$

Ta có  $P(x) = (x-z_1)^{\alpha_1} \cdots (x-z_k)^{\alpha_k} = (x-z_{k+1})^{\alpha_{k+1}} \cdots (x-z_{k+m})^{\alpha_{k+m}} + 1$

Với  $\alpha_1, \dots, \alpha_{k+m}$  là các số tự nhiên.

Xét  $P'(x)$ , ta biết đa thức này chia hết cho  $(x-z_i)^{\alpha_i-1}$  với  $i = 1, 2, \dots, k+m$ .

Suy ra  $\prod_{i=1}^{k+m} (x-z_i)^{\alpha_i-1} \mid P'(x)$

Vì vậy  $2n - k - m = \deg \prod_{i=1}^{k+m} (x-z_i)^{\alpha_i-1} \leq \deg P' = n-1$ , hay  $k+m \geq n+1$ .

Vậy ta có điều phải chứng minh.

**Câu 45.** Cho đa thức  $P(x) \in \mathbb{Z}[x]$ ,  $\deg P \geq 2$ . Chứng minh rằng tồn tại  $m \in \mathbb{Z}^+$  để  $P(m!)$  là hợp số.

IMO Shortlist 2005

*Lời giải*

Xét số nguyên tố  $p$  và số tự nhiên chẵn  $k < p$ . Theo định lý Wilson ta có

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

Do đó  $(k-1)!P((p-k)!) = \sum_{i=0}^n a_i [(k-1)!]^{n-i} \cdot [(p-k)!(k-1)!]^i \equiv \sum_{i=0}^n a_i [(k-1)!]^{n-i} \pmod{p}$

Suy ra  $(k-1)!P((p-k)!) \equiv S((k-1)!) \pmod{p}$  với  $S(x) = a_n + a_{n-1}x + \dots + a_0x^n$

Từ đó suy ra  $p \mid P((p-k)!) \Leftrightarrow S((k-1)!) \not\equiv 0 \pmod{p}$

Chú ý rằng  $S((k-1)!)$  là đa thức phụ thuộc vào  $k$ .

Xét  $k > 2a_n + 1$  ta được  $s = \frac{(k-1)!}{a_n}$  là số nguyên dương chia hết cho mọi số nguyên tố nhỏ

hơn  $k$ .

Ta có  $S((k-1)!) = a_n b_k, b_k \equiv 1 \pmod{s}$ .

Suy ra  $b_k$  chỉ chia hết cho các số nguyên tố lớn hơn  $k$ .

Cho  $k$  càng lớn thì  $S((k-1)!)$  càng lớn. Với  $k$  đủ lớn thì  $|b_k| > 1$ .

Do đó tồn tại ước nguyên tố  $p$  của  $b_k$  mà  $p \mid P((p-k)!)$ .

Ta cần chọn  $k$  sao cho đủ lớn để  $|P((p-k)!)| > p$ .

Xét số nguyên tố  $q$  đủ lớn mà  $k = (q-1)!$



Nhận xét rằng  $k+i$  là hợp số với  $i=1, \dots, q-1$

Khi đó  $p$  là số nguyên tố lớn hơn  $k$  mà  $P((p-k)!):p$  nên  $p > k+q-1$ .

Suy ra  $p=k+q+r, r \geq 0$

Với số nguyên tố  $q$  đủ lớn, do  $\deg P \geq 2$  nên

$$|P((p-k)!)| = |P((q+r)!)| > (q+r)! > (q-1)! + q + r = p$$

Vậy ta có  $p|P((p-k)!)$  và  $p \neq P((p-k)!)$  nên ta có điều phải chứng minh.

**Câu 46.** Cho  $f(x)$  là đa thức với hệ số hữu tỉ bậc lớn hơn hoặc bằng 2. Xét dãy  $\{a_n\}$  các số hữu tỉ thỏa mãn điều kiện  $f(a_{n+1}) = a_n, n \geq 1$ . Chứng minh rằng tồn tại  $k \geq 1$  để  $a_{n+k} = a_n (n \geq 1)$

### Lời giải

Phần đầu ta chứng minh dãy  $\{a_n\}$  là giới nội (bị chặn), nghĩa là tồn tại số  $M$  sao cho  $|a_n| \leq M, \forall n \in \mathbb{N}$ .

Thật vậy, do  $\deg f \geq 2$  nên  $\lim_{x \rightarrow \infty} \frac{f(x)}{x} = \infty$ .

Do đó tồn tại số  $M$  sao cho khi  $|x| \geq M \Rightarrow |f(x)| \geq |x|$ , chẳng hạn có thể lấy  $M \geq |a_1|$ .

Với  $M$  chọn như thế ta chỉ ra  $|a_n| \leq M, \forall n \in \mathbb{N}$ .

Giả sử tồn tại số  $n$  để cho  $|a_n| > M$ . Khi đó  $|a_{n-1}| = |f(a_n)| \geq |a_n| > M$ .

Tương tự  $|a_{n-2}| = |f(a_{n-1})| \geq |a_{n-1}| > M, \dots, |a_1| > M$ .

Bằng cách tương tự ta có  $|a_1| \geq |a_2| \geq \dots \geq |a_n| > M$ , trái với cách chọn  $M \geq |a_1|$  như trên.

Vậy  $|a_n| \leq M, \forall n \in \mathbb{N}$  nên dãy  $\{a_n\}$  là dãy bị chặn.

Phần tiếp theo ta chứng minh rằng tồn tại  $k \geq 1$  để  $a_{n+k} = a_n (n \geq 1)$ .

Vì  $f(x)$  là đa thức với hệ số hữu tỉ nên ta luôn có thể viết  $f(x) = \frac{b_d x^d + \dots + b_0}{c}$ , trong đó  $b_0, \dots, b_d, c$  là các số nguyên.

Lại do dãy  $\{a_n\}$  gồm toàn các số hữu tỉ nên ta giả sử  $a_1 = \frac{r}{s}$  với  $r, s$  là các số nguyên.

Ta cần chọn ra số tự nhiên  $N$  để cho ta có  $N.a_n$  là số nguyên với mọi  $n$ .

Ta đặt  $N = s.b_d$ , ta chứng minh bằng quy nạp  $N.a_n$  là số nguyên. Thật vậy

Ta có  $N.a_1 = s.b_d \cdot \frac{r}{s} = r.b_d$  nguyên.

Giả sử là  $N.a_n$  cũng là số nguyên với  $n \geq 1$ . Ta xét số  $N.a_{n+1}$ .



Ta có  $f\left(\frac{x}{N}\right) = \frac{b_d \left(\frac{x}{N}\right)^d + \dots b_0}{c}$ . Nên ta xét đa thức  $P(x) = \frac{cN^d}{b_d} \left[ f\left(\frac{x}{N}\right) - a_n \right]$  thì đa thức

$P(x)$  là hệ số nguyên với hệ số bậc cao nhất là 1.

Mà ta có  $P(N.a_{n+1}) = \frac{cN^d}{b_d} [f(a_{n+1}) - a_n] = 0$  (do  $f(a_{n+1}) = a_n, n \geq 1$ ).

Nên  $N.a_{n+1}$  là nghiệm hữu tỉ của đa thức  $P(x)$  nên nó cũng là nghiệm nguyên.

Vậy  $N.a_{n+1}$  là số nguyên, do đó  $N.a_n$  là số nguyên với mọi  $n$ .

Dãy  $\{a_n\}$  là dãy bị chặn và do  $N.a_{n+1}$  là các số nguyên nên mỗi phần tử đều là một bội số nào đó của  $\frac{1}{N}$ .

Do đó dãy chỉ nhận hữu hạn giá trị khác nhau với vô hạn số hạng của nó.

Chẳng hạn ta giả sử dãy chỉ nhận  $m$  giá trị khác nhau.

Ta xét  $m+1$  số hạng của dãy là  $a_1, a_2, \dots, a_{m+1}$ . Khi đó tồn tại hai số nguyên dương  $i_1, k_1$  sao cho  $1 \leq i_1 < i_1 + k_1 \leq m+1$  và  $a_{i_1} = a_{i_1+k_1}$ . Tương tự tồn tại các số  $k_j$  cho mỗi đoạn  $(m+1)$  số hạng tiếp theo. Do các  $k_j$  chỉ nhận hữu hạn giá trị nên tồn tại số  $k = k_j$  với vô hạn giá trị khác nhau  $j$ .

Ta sẽ chứng minh  $k$  chính là chu kỳ của dãy  $\{a_n\}$ , tức là  $a_{n+k} = a_n, \forall n$ .

Ngược lại, giả sử có chỉ số  $n_0$  nào đó mà  $a_{n_0+k} \neq a_{n_0}$ .

Do dãy  $\{a_n\}$  chỉ nhận hữu hạn phần tử nên ta có thể chọn  $n_j$  đủ lớn ( $n_j > n_0$ ) để có thể xảy ra  $a_{n_j+k} = a_{n_j}$ . Khi đó theo giả thiết ta có  $a_{n_j+k-1} = f(a_{n_j+k}) = f(a_{n_j}) = a_{n_j-1}$ . Tiếp tục quá trình trên sau nhiều lần ta sẽ lùi chỉ số  $n_j$  về tới  $n_0$  và ta có  $a_{n_0+k} = a_{n_0}$  là vô lí.

Vậy  $a_{n+k} = a_n, \forall n$ .

Bài toán được chứng minh.

**Câu 47.** Tìm tất cả đa thức  $\mathcal{P} \in \mathbb{Z}[x]$  sao cho  $\mathcal{P}(p) \mid 2^p - p, \forall p$  là số nguyên tố

*IMOTC 2016 – Senior Batch*

**Lời giải**

Ta có  $\mathcal{P}(2) \mid 2, \mathcal{P}(5) \mid 27$  và  $3 \mid \mathcal{P}(5) - \mathcal{P}(2)$  nên  $\mathcal{P}(2) = \mathcal{P}(5) = 1$  hoặc  $\mathcal{P}(2) = \mathcal{P}(5) = -1$

Không mất tính tổng quát, giả sử  $\mathcal{P}(2) = 1$ , ta thấy  $\mathcal{P}(0) = 1$  bởi nếu tồn tại 1 ước nguyên tố lẻ của  $\mathcal{P}(0)$  là  $q$  thì  $q \mid \mathcal{P}(q)$ , hay  $q \mid 2^q$  (vô lý)

Xét  $p$  nguyên tố bất kỳ, gọi  $q$  là 1 ước nguyên tố bất kỳ của  $\mathcal{P}(p)$  thì  $q \mid 2^p - p$

Gọi  $m = \text{ord}_2(q)$ , giả sử  $m > 2$  có  $(m, q) = 1$  nên theo **định lý thặng dư Trung Hoa** thì:



$$\begin{cases} x \equiv p \pmod{q} \\ x \equiv p+v \pmod{m} \end{cases}$$

với  $v$  là 1 số thỏa mãn  $v$  không chia hết cho  $m$  và  $(p+v; m) = 1$ , hoàn toàn chọn được, do  $m > 2$  nên  $\phi(m) \geq 2$ , có 1 nghiệm  $x \pmod{qm}$

Để thấy do  $\mathcal{P}(0) = 1$  nên  $(p; q) = 1$  và  $(p+v; m) = 1$  nên  $(x; qm) = 1$

Theo **định lý Dirichlet**, tồn tại 1 số nguyên tố  $t$  để  $t \equiv x \pmod{qm}$ .

Ta có  $q \mid t-p$  nên  $q \mid \mathcal{P}(t) - \mathcal{P}(q) \Rightarrow q \mid \mathcal{P}(t) \Rightarrow q \mid 2^t - t \Rightarrow q \mid 2^p (2^{t-p} - 1) + p - t \Rightarrow q \mid 2^{t-p} - 1$ , vô lý do  $t-p$  không phải là bội của  $m$ .

Suy ra  $m = 2$  hay  $q = 3$ , vậy  $\mathcal{P}(p)$  có dạng  $3^t$  với mọi  $p$  nguyên tố (1)

Cố định  $p \neq 3$  và  $t$ , theo **định lý Dirichlet** thì tồn tại vô hạn số nguyên tố  $q$  thỏa mãn  $q \equiv p \pmod{3^{t+1}}$ .

Có  $3^{t+1} \mid q-p$  nên  $3^{t+1} \mid \mathcal{P}(q) - \mathcal{P}(p)$ .

Kết hợp với (1) ta có  $\mathcal{P}(q) = 3^t$  có vô số nghiệm nên đa thức là đa thức hằng.

Thử lại thấy  $\mathcal{P}(x) = 1$  hoặc  $\mathcal{P}(x) = -1$  thỏa mãn.

**Câu 48.** Xét đa thức  $T(x) = x^3 + 17x^2 - 1239x + 2001$ . Đặt

$$T_1(x) = T(x), T_2(x) = T(T_1(x)), \dots, T_{n+1}(x) = T(T_n(x)) \text{ với mọi } n = 1, 2, 3, \dots$$

Chứng minh rằng tồn tại số nguyên  $n > 1$  sao cho  $T_n(x) - x$  chia hết cho 2003 với mọi số nguyên  $x$ .

Lê Quang Năm – TPHCM

### Lời giải

Trước hết ta có các nhận xét sau:

**Nhận xét 1.**  $x \equiv y \pmod{2003} \Leftrightarrow x^3 \equiv y^3 \pmod{2003}$ .

Để thuận tiện trong quá trình viết, ta kí hiệu là  $x \equiv y$  thay cho  $x \equiv y \pmod{2003}$ .

Hiển nhiên ta có  $x \equiv y \Rightarrow x^3 \equiv y^3$  (do 2003 là số nguyên tố)

Ta cần chứng minh  $x^3 \equiv y^3 \Rightarrow x \equiv y$ .

Nếu  $x \equiv 0$  thì  $y \equiv 0$  do  $x^3 \equiv y^3$  mà 2003 là số nguyên tố.

Nếu  $x$  không chia hết cho 2003 thì suy ra  $x^3$  không chia hết cho 2003, suy ra  $y^3$  không chia hết cho 2003. Suy ra  $y$  không chia hết cho 2003.

Theo định lý Fermat nhỏ thì  $x^{2003} \equiv x, y^{2003} \equiv y \Rightarrow x^{2002} \equiv y^{2002} \equiv 1$ .

Do  $x^3 \equiv y^3 \Rightarrow x^{2001} \equiv y^{2001} \Rightarrow xy^{2001} \equiv x^{2002} \equiv y^{2002} \equiv y.y^{2001} \Rightarrow x \equiv y$ .

**Nhận xét 2.**  $T(x) \equiv T(y) \Leftrightarrow x \equiv y \pmod{2003}$



Ta phân tích  $T(x) = (x - 662)^3 + 2003(x^2 - 657x) + 2001 + 662^3$

Do đó  $T(x) \equiv T(y) \Leftrightarrow (x - 662)^3 \equiv (y - 662)^3 \Leftrightarrow x - 662 \equiv y - 662 \Leftrightarrow x \equiv y$ .

Trở lại với bài toán. Ta đặt  $A = \{0; 1; 2; \dots; 2002\}$ . Khi đó với mỗi  $x \in A$ , ta xét dãy các đa thức  $T_1(x), T_2(x), \dots, T_{2004}(x)$ . Theo **nguyên lý Dirichlet** sẽ tồn tại hai số  $1 \leq a < b \leq 2004$  mà  $T_a(x) \equiv T_b(x)$ , vì khi chia cho 2003 thì có tối đa 2003 số dư. Ở đây các  $T_k(x)$  này giờ là các số  $\Rightarrow T_a(x) \equiv T_a(T_{b-a}(x)) \Rightarrow T_{b-a}(x) \equiv x$ , theo nhận xét 2.

Như vậy với mỗi  $x \in A$  thì tồn tại một  $n_x \in \mathbb{N}^*$  sao cho  $T_{n_x} \equiv x$ , vì theo trên ta có thể xét một dãy 2004 đa thức khác, tức là một vòng mới mà có chỉ số tăng lên. Gọi  $n > 1$  là một bội chung của  $n_0, n_1, n_2, \dots, n_{2002}$ . Ta sẽ chứng minh  $n$  thỏa mãn bài toán.

- Nếu  $x \in A$  thì ta có  $T_{n_x}(x) \equiv x \Rightarrow T_{2n_x}(x) \equiv T_{n_x}(x) \equiv x$  (vì  $T_{2n_x}(x) = T_{n_x}(T_{n_x}(x))$ ).

Tương tự ta có  $T_{kn_x}(x) \equiv T_{n_x}(x) \equiv x, \forall k \in \mathbb{N}^*$ .

Do  $n : n_x$  tức là  $n$  là bội của  $n_x$  nên ta suy ra  $T_n(x) \equiv x \Rightarrow (T_n(x) - x) : 2003$ .

- Nếu  $x \notin A$  thì tồn tại  $y \in A$  sao cho  $x \equiv y$ . Do đó  $T_n(x) \equiv T_n(y) \equiv y \equiv x$ .

Vậy  $(T_n(x) - x) : 2003$ .

**Câu 49.** Tìm tất cả các cặp số nguyên  $a, b$  sao cho tồn tại đa thức  $P(x) \in \mathbb{Z}[x]$  sao cho tích  $(x^2 + ax + b) \cdot P(x)$  là đa thức được viết dưới dạng:

$$x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 \text{ với } c_0, c_1, \dots, c_{n-1} \text{ bằng } 1 \text{ hoặc } -1$$

**Polish MO 2006**

**Lời giải**

**Bổ đề.** Cho đa thức  $P(x) = c_nx^n + c_{n-1}x^{n-1} + \dots + c_0$ , nếu  $x_0$  là nghiệm của  $P(x)$  thì khi đó:

$$|x_0| \leq 1 + \max_{i=0, n-1} \left| \frac{c_i}{c_n} \right|$$

**Chứng minh.** Rõ ràng chúng ta chỉ cần phải xem xét trường hợp  $|x_0| > 1$ :

$$-c_nx_0^n = c_0 + c_1x_0 + \dots + c_{n-1}x_0^{n-1} \Rightarrow |x_0|^n = \left| \frac{c_0 + c_1x_0 + \dots + c_{n-1}x_0^{n-1}}{c_n} \right|$$

$$= \left| \sum_{i=0}^{n-1} \frac{c_i}{c_n} x_0^i \right| \leq \sum_{i=0}^{n-1} \left| \frac{c_i}{c_n} \right| |x_0|^i \leq \max_{i=0, n-1} \left| \frac{c_i}{c_n} \right| \sum_{i=0}^{n-1} |x_0|^i \leq \max_{i=0, n-1} \left| \frac{c_i}{c_n} \right| \cdot \frac{|x_0|^n}{|x_0| - 1} \Rightarrow |x_0| \leq 1 + \max_{i=0, n-1} \left| \frac{c_i}{c_n} \right|$$

Quay trở lại bài toán ta có  $b \cdot P(0) = c_0 \Rightarrow b \in \{-1, 1\}$ .

Hơn thế nữa, nếu  $x_0$  là nghiệm của  $x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$  thì khi ấy ta có

$$|x_0| \leq 1 + \max_{i=0, n-1} \left| \frac{c_i}{c_n} \right| = 2$$





Như vậy, với  $x_0$  là nghiệm của phương trình  $x^2 + ax + b$ , ta có:

$$x_0 \in \left\{ \frac{-a + \sqrt{a^2 - 4b}}{2}, \frac{-a - \sqrt{a^2 - 4b}}{2} \right\} \text{ và } |x_0| \leq 2$$

Kết hợp với dữ kiện  $b \in \{-1, 1\}$ , ta có thể tìm được giá trị của  $a$  với  $a \in \{-2, -1, 0, 1, 2\}$ .

**Câu 50.** Cho hai đa thức hệ số nguyên

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

Biết rằng  $a_n - b_n$  là một số nguyên tố và  $a_{n-1} = b_{n-1}$ . Gọi  $m$  là một nghiệm hữu tỷ chung của hai đa thức. Chứng minh rằng  $m$  là một số nguyên.

*Lời giải*

Đặt  $m = \frac{r}{s}$  ( $r, s \in \mathbb{Z}, \gcd(r, s) = 1$ ).

Ta có  $P\left(\frac{r}{s}\right) = 0 \Rightarrow r | a_0, s | a_n$ . Tương tự  $r | b_0, s | b_n$ .

Từ đó ta có  $s | a_n - b_n$ , mà  $a_n - b_n$  là một số nguyên tố nên  $s = 1$  hoặc  $s = a_n - b_n$

Nếu  $s = 1$  thì  $m = \frac{r}{s} = r \in \mathbb{Z}$ , ta có điều phải chứng minh!

Nếu  $s = a_n - b_n$  thì ta có  $P\left(\frac{r}{s}\right) - Q\left(\frac{r}{s}\right) = 0$

$$\Leftrightarrow (a_n - b_n) \left(\frac{r}{s}\right)^n + (a_{n-2} - b_{n-2}) \left(\frac{r}{s}\right)^{n-2} + \dots + (a_1 - b_1) \cdot \frac{r}{s} + (a_0 - b_0) = 0$$

$$\Leftrightarrow (a_n - b_n) \cdot r^n + (a_{n-2} - b_{n-2}) r^{n-2} + \dots + (a_1 - b_1) r \cdot s^{n-1} + (a_0 - b_0) s^n = 0$$

$$\Leftrightarrow s \cdot r^n + (a_{n-2} - b_{n-2}) r^{n-2} \cdot s^2 + \dots + (a_1 - b_1) r \cdot s^{n-1} + (a_0 - b_0) s^n = 0 \Rightarrow s | r^n$$

Lại có  $s$  nguyên tố nên  $s | r$ , mâu thuẫn với  $\gcd(r, s) = 1$ .

Vậy ta có điều phải chứng minh!

**Câu 51.** Hỏi có tất cả bao nhiêu đa thức  $P_n(x)$  bậc  $n$  chẵn thỏa mãn các điều kiện

- Các hệ số của  $P_n(x)$  thuộc tập  $M = \{0; -1; 1\}$  và  $P_n(0) \neq 0$ .
- Tồn tại đa thức  $Q(x)$  có các hệ số thuộc  $M$  sao cho  $P_n(x) \equiv (x^2 - 1) \cdot Q(x)$ .

*Nguyễn Viết Long – THPT Chuyên Lam Sơn – Thanh Hóa*

*Lời giải*

Đặt  $\deg P_n(x) = n = 2m$ . Xét đa thức  $Q(x) = b_0 x^{n-2} + b_1 x^{n-3} + \dots + b_{n-3} x + b_{n-2}$ .

Từ giả thiết ta có  $P_n(x) \equiv (x^2 - 1) \cdot Q(x)$  nên suy ra



$$P_n(x) = b_0x^n + b_1x^{n-1} + (b_2 - b_0)x^{n-2} + (b_3 - b_1)x^{n-3} + \dots + (b_{n-2} - b_{n-4})x^2 - b_{n-3}x - b_{n-2}.$$

Từ đó suy ra số các đa thức  $P_n(x)$  bằng số dãy số  $(b_0, b_1, \dots, b_{n-2})$  trong đó các số hạng của dãy  $\{b_n\}$  thỏa mãn điều kiện là  $b_k \in \{-1; 0; 1\}$  với mọi  $0 \leq k \leq n-2$  và  $b_{k+2} - b_k \in \{-1; 0; 1\}$  với mọi  $0 \leq k \leq n-4$  đồng thời  $b_{n-2} \neq 0$ .

- Để ý rằng nếu  $b_k = -1$  thì  $b_{k+2} \in \{0; -1\}$ .
- Để ý rằng nếu  $b_k = 0$  thì  $b_{k+2} \in \{-1; 0; 1\}$ .
- Để ý rằng nếu  $b_k = 1$  thì  $b_{k+2} \in \{0; 1\}$ .

Gọi  $x_k$  là số các dãy chỉ số chẵn  $(b_0; b_2; \dots; b_{2k})$  thỏa mãn  $b_{2i} \in M, 0 \leq i \leq k$  và

$$b_{i+2} - b_i \in M, 0 \leq i \leq 2k-2$$

Gọi  $y_k$  là số các dãy chỉ số lẻ  $(b_1; b_3; \dots; b_{2k-1})$  thỏa mãn  $b_{2i-1} \in M, 0 \leq i \leq k$  và

$$b_{i+2} - b_i \in M, 0 \leq i \leq 2k-3$$

Ta có  $x_0 = 2; x_1 = 4$  và  $x_{k+1} = x_k + 2x_{k-1}$  vì nếu  $b_{2k} \neq 0$  thì  $b_{2k+2} \in \{0; b_{2k}\}$  và nếu  $b_{2k} = 0$  thì có ba cách lấy  $b_{2k+2} \in M$ , số dãy  $(b_0; b_2; \dots; b_{2k})$  mà  $b_{2k} = 0$  bằng  $x_{k-1}$ .

Bằng cách sử dụng phương trình đặc trưng ta tìm được  $x_k = \frac{(1+\sqrt{2})^k + (1-\sqrt{2})^k}{\sqrt{2}}$ .

Tương tự ta có  $y_0 = 3, y_1 = 7, y_{k+1} = 2y_k + y_{k-1}, \forall k \geq 1$ .

Do đó số các dãy số  $(b_0, b_1, \dots, b_{n-2})$  bằng

$$\begin{aligned} (x_{m-1} - x_{m-2})y_{m-2} &= \left( (1+\sqrt{2})^{m-1} + (1-\sqrt{2})^{m-1} \right) \frac{1}{2} \left( (1+\sqrt{2})^m + (1-\sqrt{2})^m \right) \\ &= \frac{(1+\sqrt{2})^{2m-1} + (1-\sqrt{2})^{2m-1} + 2(-1)^{m-1}}{2} = \frac{(1+\sqrt{2})^{n-1} + (1-\sqrt{2})^{n-1}}{2} + (-1)^{\frac{n-1}{2}}. \end{aligned}$$

**Câu 52.** Cho dãy số nguyên  $(a_n)_{n=1}^\infty$  thỏa mãn  $m-n \mid a_m - a_n$  với mọi số tự nhiên  $m, n$  phân biệt. Giả sử tồn tại đa thức  $P(x)$  sao cho  $|a_n| < P(n), \forall n$ . Chứng minh rằng tồn tại đa thức  $Q(x)$  sao cho  $a_n = Q(n), \forall n$ .

### Lời giải

Đặt  $\deg P = d$ . Tồn tại đa thức  $Q$  duy nhất có bậc cao nhất là  $d$  sao cho  $Q(k) = a_k$  với  $k = 1, 2, \dots, d+1$ . Ta chứng minh  $Q(n) = a_n$  với mọi  $n$ .

Đặt  $n > d+1$ . Đa thức  $Q$  có thể không phải là đa thức hệ số nguyên nên ta không thể trực tiếp suy ra  $n-m \mid Q(n) - Q(m)$ , nhưng chắc chắn rằng  $Q$  là đa thức có hệ số hữu tỉ, khi đó tồn tại số tự nhiên  $M$  sao cho  $R(x) = MQ(x)$  là đa thức hệ số nguyên. Từ điều kiện đề bài ta có  $M(a_n - Q(n)) = M(a_n - a_k) - (R(n) - R(k))$  chia hết cho  $n-k$  với  $k = 1, 2, \dots, d+1$ . Vậy



với mỗi số  $n$  ta có  $a_n = Q(n)$  hoặc  $L_n = \text{lcm}(n-1, n-2, \dots, n-d-1) \leq M(a_n - Q(n)) < Cn^d$  với  $C$  là hằng số không phụ thuộc vào  $n$ .

Giả sử rằng  $a_n \neq Q(n)$  ở một vài giá trị  $n$ .

Lưu ý rằng  $L_n$  không nhỏ hơn tích  $(n-1) \cdots (n-d-1)$  được chia bởi tích  $P$  của số  $\text{gcd}(n-i, n-j)$  trên tất cả các cặp  $(i, j)$  phân biệt lấy từ tập  $\{1, 2, \dots, d+1\}$ .

Do  $\text{gcd}(n-i, n-j) \leq i-j$ , ta có  $P \leq 1^d 2^{d-1} \dots d$ . Từ đó ta được:

$$(n-1)(n-2) \cdots (n-d-1) \leq PL_n < CPn^d$$

Điều này sai với  $n$  đủ lớn vì vế trái có bậc là  $d+1$ .

Vậy  $a_n = Q(n)$  cho mỗi giá trị  $n$  đủ lớn, ta gọi tạm là  $n > N$ .

Nếu  $n \leq N$ , từ điều kiện đề bài  $M(a_n - Q(n)) = \overline{M}(a_n - a_k) - (R(n) - R(k))$  chia hết cho  $m-n$  với mọi giá trị  $m > N$ , vậy chúng phải bằng 0.

Vì vậy  $a_n = Q(n)$  với mọi  $n$ .

**Câu 53.** Cho  $n$  là số nguyên dương và  $a_1, a_2, \dots, a_n$  là các số thực dương.

Ta đặt  $g(x) = (x+a_1)(x+a_2) \cdots (x+a_n)$ .

Gọi  $a_0$  là một số thực bất kì và đặt  $f(x) = (x-a_0)g(x) = x^{n+1} + b_1x^n + \dots + b_nx + b_{n+1}$ .

Chứng minh rằng  $b_1, b_2, \dots, b_{n+1}$  đều là số âm khi và chỉ khi  $a_0 > a_1 + a_2 + \dots + a_n$ .

VMF – Diễn đàn Toán học

*Lời giải*

*Chiều suy ra.*

Thì theo **định lý Viète** ta có  $-b_1 = a_0 - \sum_{k=1}^n a_k$ , từ đó thì ta có điều phải chứng minh.

*Chiều ngược lại.*

Với  $x=0$  thì ta có  $-a_0 \prod_{k=1}^n a_k = b_{n+1}$  nên suy ra  $b_{n+1} < 0$ .

Ta giả sử rằng  $-a_1 \leq -a_2 \leq \dots \leq -a_n < a_0$

Mà ta có  $g(x) + (x-a_0)g'(x) = (n+1)x^n + \dots + b_{n-1}x + b_n$ .

Lại theo **định lý Lagrange** thì ta thấy tồn tại các số dương  $y_i, i = \overline{0, n-1}$  sao cho

$$-a_1 \leq -y_1 \leq -a_2 \leq -y_2 \leq \dots \leq -a_n \leq y_0 \leq a_0 \text{ và } f'(y_i) = 0, \forall i = \overline{0, n-1}$$

Do đó ta có  $\frac{1}{n+1} f'(x) = (x-y_0) \prod_{i=1}^n (x+y_i)$ .

Đồng nhất hệ số của  $x^{n-1}$  thì ta thu được  $y_0 - \sum_{i=1}^{n-1} y_i = \frac{n}{n+1} \left( a_0 - \sum_{i=1}^n a_i \right) > 0$ .

Từ ý tưởng trên ta sẽ dùng phương pháp quy nạp để chỉ ra các hệ số  $b_i$  đều là số âm.



**Câu 54.** Cho  $F$  là tập các đa thức  $\Gamma$  có hệ số nguyên và phương trình  $\Gamma(x)=1$  có nghiệm nguyên. Cho trước một số nguyên dương  $k$ , tìm giá trị nhỏ nhất của  $m > 1$  theo  $k$  thỏa mãn tồn tại  $\Gamma \in F$  sao cho  $\Gamma(x)=m$  có đúng  $k$  nghiệm nguyên phân biệt.

VMF – Diễn đàn Toán học

**Lời giải**

Do  $\Gamma(x)=m$  có  $k$  nghiệm nguyên phân biệt nên ta có:

$$\Gamma(x)=(x-x_1)(x-x_2)\dots(x-x_k)Q(x)+m$$

Với các số nguyên khác nhau  $x_1, x_2, \dots, x_k$  và  $Q(x) \in \mathbb{Z}[x]$

Gọi  $t$  là nghiệm của phương trình  $\Gamma(x)=1$  khi đó ta có:

$$\begin{aligned}(t-x_1)(t-x_2)\dots(t-x_k)Q(t) &= 1-m \\ \Rightarrow |1-m| &= |t-x_1||t-x_2|\dots|t-x_k||Q(t)| \\ \Rightarrow |1-m| &\geq 1.2.3\dots k.1 \Rightarrow m-1 \geq k! \Rightarrow m \geq k!+1\end{aligned}$$

Vậy từ đây ta suy ra giá trị nhỏ nhất của  $m$  là  $k!+1$ .

Và nó xảy ra khi và chỉ khi  $\Gamma(x)=(x-1)(x-2)\dots(x-k+1)(x+k)+k!+1$ .

**Câu 55.** Cho hai đa thức  $P(x), Q(x) \in \mathbb{R}[x]$  nguyên tố cùng nhau và khác đa thức hằng. Chứng minh rằng không có quá ba số thực  $\lambda$  thỏa mãn  $P(x)+\lambda Q(x)$  là bình phương của một đa thức.

USA December Team Selection Test 2016

**Lời giải**

Kí hiệu  $(A(x), B(x))$  là ước **đa thức monic** có bậc lớn nhất của  $A(x), B(x)$ .

Trước hết, ta phát biểu một bổ đề sau đây:

**Bổ đề.** Nếu  $ab \neq cd \Rightarrow \max(\deg(aP(x)+cQ(x)), \deg(bP(x)+dQ(x))) = \max(\deg(P(x)), \deg(Q(x)))$ .

**Chứng minh**

Đặt  $n = \max(\deg(P(x)), \deg(Q(x)))$  thì ta có vế trái rõ ràng không lớn hơn  $n$ .

Xét hệ số của  $x^n$  trong hai đa thức  $aP(x)+cQ(x), bP(x)+dQ(x)$  sẽ có một đa thức có hệ số khác không và dễ dàng suy ra vế trái bằng  $n$  nên ta có điều phải chứng minh.

**Quay lại với việc chứng minh bài toán**

Giả sử tồn tại ba số thực phân biệt  $\lambda_1, \lambda_2, \lambda_3, P(x)+\lambda_i Q(x)=R_i(x)^2$

Theo **bổ đề** trên thì tồn tại đa thức  $R_i(x)^2$  có bậc bằng  $\max(\deg(P(x)), \deg(Q(x)))$  giả sử là  $R_1(x)^2$

Ta đặt  $\lambda = \frac{\lambda_1 - \lambda_2}{\lambda_1 - \lambda_3}, A(x) = R_1(x) - R_2(x), B(x)$

$$= R_1(x) + R_2(x), C(x) = R_1(x) - R_3(x), D(x) = R_1(x) + R_3(x)$$



Khi đó thì ta có  $A(x) + B(x) = C(x) + D(x) = 2R_1(x)$ ,  $A(x)B(x) = \lambda C(x)D(x)$ ,  $\lambda \neq 1$ ,  $(A(x), B(x)) = (C(x), D(x)) = 1$

Và  $A(x)B(x)$  có bậc bằng  $\max(P(x), Q(x))$ .

Bây giờ ta sẽ đặt  $P_{A(x)C(x)}(x) = (A(x), C(x))$ ,  $P_{A(x)D(x)}(x) = (A(x), D(x))$ ,

$$P_{B(x)C(x)}(x) = (B(x), C(x)), P_{B(x)D(x)}(x) = (B(x), D(x))$$

Thì ta có các đa thức trên nguyên tố cùng nhau. Giả sử  $x_0$  là nghiệm bội  $n$  của  $A(x)$  thì nó cũng là nghiệm bội  $n$  của duy nhất một trong hai đa thức  $P_{A(x)C(x)}(x)$ ,  $P_{A(x)D(x)}(x)$  hay cũng là nghiệm bội  $n$  của đa thức  $P_{A(x)C(x)}(x) \cdot P_{A(x)D(x)}(x)$ .

Tương tự thì ta cũng có điều ngược lại.

Vậy  $A(x) = aP_{A(x)C(x)}(x) \cdot P_{A(x)D(x)}(x)$  với  $a$  là hằng số nào đó.

Tương tự thì ta cũng được:

$$B(x) = bP_{B(x)D(x)}(x) \cdot P_{B(x)C(x)}(x), C(x) = cP_{A(x)C(x)}(x) \cdot P_{B(x)C(x)}(x), D(x) = dP_{A(x)D(x)}(x) \cdot P_{B(x)D(x)}(x)$$

Mà ta có  $A(x) - C(x) = D(x) - B(x)$ .

Giả sử  $x_0$  là nghiệm bội  $n$  của  $P_{A(x)C(x)}(x) \cdot P_{B(x)D(x)}(x)$  thì nó cũng là nghiệm bội  $n$  của một trong hai đa thức  $P_{A(x)C(x)}(x)$ ,  $P_{B(x)D(x)}(x)$  nên là nghiệm bội ít nhất  $n$  của đa thức  $A(x) - C(x)$ .

Giả sử  $x_0$  là nghiệm bội  $n$  của  $A(x) - C(x)$  thì nó là nghiệm của nhiều nhất một trong hai đa thức  $P_{A(x)C(x)}(x)$ ,  $P_{B(x)D(x)}(x)$ , giả sử  $P_{B(x)D(x)}(x)$  không có nghiệm  $x_0$  và  $x_0$  nghiệm bội  $m$  có thể bằng không của  $P_{A(x)C(x)}(x)$ .

Giả sử  $m < n$  thì ta đạo hàm  $A(x) - C(x) = D(x) - B(x)$  từ 0 đến  $m+1$  lần.

Thay  $x = x_0$  thì ta có

$$A^{(i)}(x) = C^{(i)}(x) = 0, \forall 0 \leq i \leq m, A^{(m+1)}(x) = C^{(m+1)}(x) \neq 0, B(x) = D(x) \neq 0.$$

Đạo hàm  $A(x)B(x) = \lambda C(x)D(x)$   $(m+1)$  lần, thay  $x = x_0$  vào thì ta có

$$A^{(m+1)}(x)B(x) = \lambda C^{(m+1)}(x)D(x), \text{ dễ thấy điều vô lý.}$$

Vậy ta phải có  $m \geq n$  nên từ đây ta có

$$A(x) - C(x) = D(x) - B(x) = \alpha P_{A(x)C(x)}(x) \cdot P_{B(x)D(x)}(x)$$

$$\Rightarrow aP_{A(x)D(x)}(x) - bP_{B(x)C(x)} = \alpha P_{B(x)D(x)} \cdot dP_{A(x)D(x)}(x) - bP_{B(x)C(x)} = \alpha P_{A(x)C(x)}$$

Thay  $P_{A(x)C(x)}(x)$ ,  $P_{B(x)D(x)}(x)$  thì ta có

$$A(x)B(x) = \frac{ab}{\alpha^2} P_{A(x)D(x)}(x) \cdot P_{C(x)D(x)}(x) \left( aP_{A(x)D(x)}(x) - cP_{B(x)C(x)}(x) \right) \left( dP_{A(x)D(x)}(x) - bP_{B(x)C(x)}(x) \right)$$

$$2R_1(x) = \frac{1}{\alpha} \left( adP_{A(x)D(x)}(x) - bcP_{B(x)C(x)}(x) \right)$$

Áp dụng **bổ đề** trên thì ta được

$$\begin{aligned} & \max \left( \deg \left( P_{A(x)D(x)}(x) \right), \deg \left( P_{B(x)C(x)}(x) \right) \right) \geq 2 \deg \left( R_1(x) \right) \\ & \geq \deg \left( Q(x) \right) = \deg \left( A(x)B(x) \right) \\ & \geq \deg \left( P_{A(x)D(x)}(x) \right) + \deg \left( P_{B(x)C(x)}(x) \right) + \max \left( \deg \left( P_{A(x)D(x)}(x) \right), \deg \left( P_{B(x)C(x)}(x) \right) \right) \end{aligned}$$

Từ đây ta suy ra  $\deg \left( P_{A(x)D(x)}(x) \right) = \deg \left( P_{B(x)C(x)}(x) \right) = 0$ .

Từ đây thì ta có  $R_1(x), Q(x)$  là các đa thức hằng nên  $P(x)$  cũng là đa thức hằng, điều này là vô lý do giả thiết bài toán nói đa thức  $P(x)$  khác đa thức hằng.

Vậy từ đây suy ra tồn tại nhiều nhất hai số thỏa mãn điều kiện đề bài, nên từ đó ta suy ra điều phải chứng minh.

**Câu 56.** Chứng minh rằng nếu đa thức  $f(x) \in \mathbb{R}[x]$  có bậc  $n$  và nhận giá trị nguyên tại  $n+1$  giá trị nguyên liên tiếp từ  $a \rightarrow a+n, a \in \mathbb{Z}$  thì  $f(x) \in \mathbb{Z}, \forall x \in \mathbb{Z}$ .

**Lời giải**

Trước hết, ta cần có **công thức nội suy Abel – Newton** được phát biểu như sau:

Cho  $f(x) \in \mathbb{R}[x]$  có bậc  $n$  và  $n$  số thực  $a_1, a_2, \dots, a_n$  khi đó tồn tại duy nhất  $n+1$  số thực  $b_0, b_1, \dots, b_n$  sao cho:

$$f(x) = b_0(x-a_1)(x-a_2)\dots(x-a_n) + b_1(x-a_1)(x-a_2)\dots(x-a_{n-1}) + \dots + b_{n-1}(x-a_1) + b_n$$

Công thức này có thể chứng minh rất là đơn giản bằng phương pháp quy nạp Toán học.

**Quay trở lại bài toán**

Ta áp dụng **công thức nội suy Abel – Newton** cho  $n$  số thực  $a_i = a+i \in \mathbb{Z}, \forall i = \overline{1, n}$ .

$$f(x) = b_0(x-a-1)(x-a-2)\dots(x-a-n) + b_1(x-a-1)(x-a-2)\dots(x-a-n+1) + \dots + b_{n-1}(x-a-1) + b_n$$

$$\text{Từ đây suy ra } \begin{cases} f(a+1) = b_n \in \mathbb{Z} \\ f(a+2) = b_{n-1} \cdot 1! + b_n \in \mathbb{Z} \Rightarrow b_{n-1} \in \mathbb{Z} \\ f(a+3) = b_{n-2} \cdot 2! + b_{n-1} \cdot 1! + b_n \in \mathbb{Z} \Rightarrow b_{n-2} \cdot 2! \in \mathbb{Z} \\ \dots\dots\dots \\ f(a+n) \in \mathbb{Z} \Rightarrow b_1 \cdot (n-1)! \in \mathbb{Z} \\ f(a) \in \mathbb{Z} \Rightarrow b_0 \cdot n! \in \mathbb{Z} \end{cases}$$

Ta sẽ viết lại đa thức  $f(x)$  như sau  $f(x) = \sum_{k=0}^n k! b_{n-k} \binom{x-a}{k}$ .



Trong đó thì  $\binom{x-a}{k} = \frac{(x-a-1)(x-a-2)\dots(x-a-k)}{k!} \in \mathbb{Z}, \forall x \in \mathbb{Z}$  và  $b_{n-k}k! \in \mathbb{Z}$ , chứng minh trên.

Vậy từ đó ta được  $f(x) \in \mathbb{Z}, \forall x \in \mathbb{Z}$ .

**Câu 57.** Tìm tất cả các đa thức  $P(x) \in \mathbb{Z}[x]$  sao cho với mọi  $a, b$  mà  $a$  không là nghiệm của  $P(x)$  thì  $P(a) \mid P(a+b) - P(b)$ .

MYTS 2016

### Lời giải

Ta sẽ làm việc trên các số nguyên lớn hơn nghiệm thực lớn nhất của  $P(x)$ , nghĩa là ta không cần quan tâm đến việc  $P(\alpha) = 0$ .

Để ý rằng  $P(x) = c = \text{const}$  là một đa thức thỏa mãn yêu cầu đề bài, xét  $\deg(P(x)) \geq 1$ .

**Ta nhận xét thấy.**

Nếu  $P(x)$  là một đa thức thỏa mãn yêu cầu bài toán thì  $-P(x)$  cũng thỏa mãn yêu cầu đề bài

Không mất tính tổng quát, ta có thể giả sử hệ số cao nhất của  $P(x)$  là dương.

Ta có  $\lim_{x \rightarrow +\infty} P(x) = +\infty$  nghĩa là từ một lúc nào đó, đa thức của ta chỉ nhận giá trị dương, lớn hơn hẳn  $P(1)$ .

Theo đề bài thì ta có  $\frac{P(x+1) - P(1)}{P(x)} \in \mathbb{Z}^+ \Rightarrow \frac{P(x+1) - P(x) - P(1)}{P(x)} \in \mathbb{N}$ .

Đặt  $Q(x) = P(x+1) - P(x)$

**Trường hợp 1.**  $\deg(P(x)) \geq 2$  khi đó thì  $\deg(Q(x)) = \deg(P(x)) - 1 \geq 1$ .

Khi đó thì  $\frac{Q(x) - P(1)}{P(x)} \in \mathbb{N}$ . Mặt khác, ta lại có  $\lim_{x \rightarrow +\infty} \frac{Q(x) - P(1)}{P(x)} = 0$ .

Hay từ một chỉ số  $x_0$  nào đó trở đi thì

$$\frac{Q(x) - P(1)}{P(x)} < 1 \Rightarrow \frac{Q(x) - P(1)}{P(x)} = 0, \forall x \geq x_0 \Rightarrow Q(x) - P(1) = 0, \forall x \geq x_0$$

Nghĩa là một đa thức có  $\deg(Q(x) - P(1)) = \deg P(x) - 1 \geq 1$  và có vô số nghiệm, vô lý.

**Trường hợp 2.** Ta có  $\deg(P(x)) = 1$  thì ta đặt  $P(x) = ax + b, a > 0$ .

Khi đó  $\frac{ax}{ax+b} \in \mathbb{Z} \Rightarrow b = 0$  hay  $P(x) = ax, a > 0$  thử lại thấy thỏa mãn yêu cầu đề bài.

Vậy tất cả các hàm số thỏa mãn yêu cầu đề bài là  $P(x) = c = \text{const}$  và  $P(x) = ax, a > 0$ .



**Câu 58.** Xét đa thức  $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  với  $n \geq 2, n \in \mathbb{N}$ . Giả sử  $P(x)$  có  $n$  nghiệm là  $x_1, x_2, \dots, x_n$ . Kí hiệu  $\max(x_i)$  là số lớn nhất trong các số  $x_1, x_2, \dots, x_n$ . Chứng minh rằng  $P(x+\delta) \sum_{i=1}^n \frac{1}{x-x_i} \geq 2n^2\delta^{n-1}, \forall x > \max(x_i)$  với  $\delta > 0$ .

VMF – Diễn đàn Toán học

**Lời giải**

Do  $P(x)$  bậc  $n$  và có  $n$  nghiệm là  $x_1, x_2, \dots, x_n$  nên  $P(x) = \prod_{i=1}^n (x - x_i)$

Với  $x > \max(x_i), \forall i = \overline{1, n}$  thì  $x - x_i > 0, \forall i = \overline{1, n}$

Từ đó ta áp dụng **bất đẳng thức Cauchy – Schwarz** thì ta được:

$$P(x+\delta) \sum_{i=1}^n \frac{1}{x-x_i} \geq P(x+\delta) \cdot n \sqrt[n]{\prod_{i=1}^n \frac{1}{x-x_i}} = n \sqrt[n]{\prod_{i=1}^n \frac{(x-x_i+\delta)^n}{x-x_i}}$$

Do vậy ta cần chứng minh rằng

$$n \sqrt[n]{\prod_{i=1}^n \frac{(x-x_i+\delta)^n}{x-x_i}} \geq 2n^2\delta^{n-1} \Leftrightarrow \prod_{i=1}^n \frac{(x-x_i+\delta)^n}{x-x_i} \geq (2n)^n \delta^{n(n-1)}$$

Ta sẽ chứng minh  $(x-x_i+\delta)^n \geq 2n\delta^{n-1}(x-x_i), \forall i = \overline{1, n}$ .

Tổng quát, với mọi số thực không âm  $x, y$  và  $n \geq 2, n \in \mathbb{N}$ .

$$\begin{aligned} (x+y)^n &= \sum_{k=0}^n C_n^k x^{n-k} y^k \geq \sum_{k=0}^2 C_n^k x^{n-k} y^k = x^n + nx^{n-1}y + \frac{n(n-1)}{2} x^{n-2}y^2 \\ &\geq 2\sqrt{\frac{n(n-1)}{2} x^n \cdot x^{n-2}y^2} + nx^{n-1}y \geq 2nx^{n-1}y \end{aligned}$$

Do  $2\sqrt{\frac{n(n-1)}{2}} \geq n, \forall n \geq 2$  nên từ đây ta suy ra được  $(x-x_i+\delta)^n \geq 2n\delta^{n-1}(x-x_i), \forall i = \overline{1, n}$ .

Hay bất đẳng thức ban đầu được chứng minh.

**Câu 59.** Giả sử  $R$  là nghiệm của phương trình  $x^n - a_1x^{n-1} - \dots - a_{n-1}x - a_n = 0$  và đặt

$$A = \sum_{j=1}^n a_j, B = \sum_{j=1}^n ja_j. \text{ Khi đó thì ta có } A^A \leq R^B.$$

VMF – Diễn đàn Toán học

**Lời giải**

Đặt  $c_j = \frac{a_j}{A}$  suy ra  $c_j \geq 0$  và  $\sum_{j=1}^n c_j = 1$ .

Do hàm số  $y = -\ln(x)$  là hàm lồi trong khoảng từ  $(0, +\infty)$  nên theo **bất đẳng thức Jensen** thì





$$\left(-\ln\left(\frac{A}{R^j}\right)\right)\left(\sum_{j=1}^n c_j\right) \geq -\ln\left(\sum_{j=1}^n c_j \frac{A}{R^j}\right) = -\ln\left(\sum_{j=1}^n \frac{a_j}{R^j}\right) = -\ln f(R) = -\ln 1 = 0$$

Suy ra  $\sum_{j=1}^n (c_j \ln(R^j) - c_j \ln(A)) \geq 0$  và  $(\ln(A))\left(\sum_{j=1}^n c_j\right) \leq (\ln(R))\left(\sum_{j=1}^n j c_j\right)$

Hay  $\frac{1}{A} \sum_{j=1}^n a_j (\ln(A)) \leq \frac{1}{A} \sum_{j=1}^n j a_j (\ln(R))$ , do  $c_j = \frac{a_j}{A}$ ,  $A > 0$ .

Vậy nên ta được:  $\ln(A^A) \leq \ln(R^B) \Rightarrow A^A \leq R^B$

Hay từ đây ta được điều phải chứng minh.

**Câu 60.** Cho đa thức  $P(x)$  là đa thức monic bậc  $n > 1$  có  $n$  nghiệm thực là  $x_1, x_2, \dots, x_n$  phân biệt và khác 0. Chứng minh rằng:

$$\frac{1}{x_1 P'(x_1)} + \frac{1}{x_2 P'(x_2)} + \dots + \frac{1}{x_n P'(x_n)} = \frac{(-1)^{n+1}}{x_1 x_2 \dots x_n}$$

VMF – Diễn đàn Toán học

**Lời giải**

Từ giả thiết bài toán thì ta suy ra  $P(x) = (x - x_1)(x - x_2) \dots (x - x_n)$

Ta bổ sung  $x_0 = 0$  và với mọi  $j \neq 0$  thì ta có:

$$P'(x) = \sum_{j=1}^n \prod_{i=1; i \neq j}^n (x - x_i) \Rightarrow x_j P'(x_j) = x_j \prod_{i=1; i \neq j}^n (x_j - x_i) = \prod_{i=0; i \neq j}^n (x_j - x_i)$$

$$\text{Ta xét đa thức } Q(x) = 1 + \prod_{i=1}^n (x - x_i) \Rightarrow \begin{cases} Q(x_j) = 1, \forall j = \overline{1, n} \\ Q(0) = 1 + P(0) = 1 + (-1)^n \prod_{i=1}^n x_i \end{cases}$$

Ta dễ thấy  $\deg(Q(x)) = n$  nên ta áp dụng **công thức nội suy Lagrange** cho  $Q(x)$  tại  $n+1$

$$\begin{aligned} \text{điểm } x_i \text{ thì ta được } Q(x) &= \sum_{j=0}^n Q(x_j) \frac{\prod_{i=0; i \neq j}^n (x - x_i)}{\prod_{i=0; i \neq j}^n (x_j - x_i)} \\ &= \sum_{j=1}^n \frac{\prod_{i=0; i \neq j}^n (x - x_i)}{x_j P'(x_j)} + Q(0) \frac{\prod_{i=1}^n (x - x_i)}{(-1)^n \prod_{i=1}^n x_i} = \sum_{j=1}^n \frac{\prod_{i=0; i \neq j}^n (x - x_i)}{x_j P'(x_j)} + \frac{(-1)^n Q(0) P(x)}{\prod_{i=1}^n x_i} \end{aligned}$$

So sánh hệ số của  $x^n$  ở hai vế thì ta được:

$$1 = \sum_{j=1}^n \frac{1}{x_j P'(x_j)} + \frac{(-1)^n Q(0)}{\prod_{i=1}^n x_i} \Rightarrow \sum_{j=1}^n \frac{1}{x_j P'(x_j)} = 1 + \frac{(-1)^{n+1} \left[ 1 + (-1)^n \prod_{i=1}^n x_i \right]}{\prod_{i=1}^n x_i} = \frac{(-1)^{n+1}}{\prod_{i=1}^n x_i}$$

Và từ đây ta có điều phải chứng minh.

**Câu 61.** Cho  $n \geq 2$  và đa thức  $P(x)$  xác định bởi  $P(x) = \sum_{k=0}^n \frac{x^k}{k!}$ . Chứng minh rằng phương trình  $P(x) = 0$  không có nghiệm hữu tỉ.

VMF – Diễn đàn Toán học

*Lời giải*

Nếu  $\alpha \in \mathbb{Q}$  là nghiệm của  $P(x)$  thì  $\alpha$  cũng là nghiệm của phương trình:

$$\begin{aligned} x^n + nx^{n-1} + \dots + \frac{n!}{k!} x^k + \dots + n! &= 0 \\ \Rightarrow \alpha^n + n\alpha^{n-1} + \dots + \frac{n!}{k!} \alpha^k + \dots + n! &= 0 \quad (1) \end{aligned}$$

Vì  $P(x)$  là đa thức hệ số nguyên có hệ số cao nhất là 1 và có nghiệm  $\alpha \in \mathbb{Q}$  thì  $\alpha$  là số nguyên.

Gọi  $p$  là một ước nguyên tố bất kì của  $n$

Với  $k = \overline{1, n}$  ta đặt  $r_k = v_p(k!) \Rightarrow r_k = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \dots + \left\lfloor \frac{k}{p^s} \right\rfloor$ .

Trong đó,  $s$  là số tự nhiên thỏa mãn  $p^s \leq k < p^{s+1}$

$$\begin{aligned} \Rightarrow r_k &\leq \frac{k}{p} + \frac{k}{p^2} + \dots + \frac{k}{p^s} = k \cdot \frac{1-p}{1-p^s} < k \Rightarrow r_n - r_k > r_n - k \\ \Rightarrow r_n - r_k &\geq r_n - k + 1 \Rightarrow \frac{n!}{k!} \cdot p^{r_n - k + 1} \end{aligned}$$

Lại có, do  $p|n$  nên từ (1)  $\Rightarrow p|\alpha \Rightarrow p^k|\alpha^k \Rightarrow p^{r_n+1} \left| \frac{n!}{k!} \alpha^k, \forall k = \overline{1, n} \right.$

Do (1) nên  $p^{r_n+1} | n!$ , mâu thuẫn do  $r_n = v_p(n!)$  nên  $n!$  không chia hết cho  $p^{r_n+1}$ .

Vậy điều giả sử là sai hay đa thức  $P(x)$  không có nghiệm hữu tỉ.

**Câu 62.** Cho  $p$  là một số nguyên tố. Tìm tất cả các đa thức  $f(x)$  với hệ số nguyên sao cho với mọi số nguyên dương  $n$ ,  $f(x)$  là ước của  $p^n - 1$ .

THTT Tháng 12 – 2014

*Lời giải*



Ký hiệu  $A$  là tập các ước số nguyên của  $p-1$ . Khi đó tất cả các đa thức hằng  $f(x) \equiv b, b \in A$  đều thỏa mãn bài toán, vì  $\forall n \in \mathbb{N}^*, (p^n - 1) : (p-1) : b$ .

Ta sẽ chứng minh đó cũng là tất cả các đa thức thỏa mãn bài toán.

Thật vậy. Phản chứng giả sử tồn tại đa thức  $f(x)$  mà  $\deg f(x) \geq 1$  thỏa mãn bài toán.

Với  $n \in \mathbb{N}^*$  và giả sử  $q$  là ước số nguyên tố bất kỳ của  $f(n)$ .

Ta có  $f(n+q) - f(n) : (n+q-n) = q$ . Mà  $f(n) : q$  nên từ đó ta có  $f(n+q) : q$ .

Như vậy ta có  $p^n - 1 : f(n) : q, p^{n+q} - 1 : f(n+q) : q$ .

Nên suy ra  $p^{n+q} - 1 - (p^n - 1) = p^n(p^q - 1) : q$ .

Từ các sự kiện trên ta suy ra  $p \neq q$  (vì  $q | f(n), f(n) | p^n - 1 \Rightarrow q | p^n - 1$ ) và  $p^q - 1 : q$ .

Theo **định lý Fermat** ta lại có  $p^q \equiv p \pmod{q}$ , suy ra  $p^q - 1 - (p^q - p) = p - 1 : q$ .

Bây giờ ta xét các số tự nhiên  $n \in \mathbb{N}^*$  mà  $n-1 : p-1$ . Ta biết số các số  $n$  thỏa mãn là vô hạn, trong khi tập  $A$  ta xét là hữu hạn. Suy ra tồn tại số  $n$  mà  $f(n) \notin A$ .

Mặt khác  $p^n - 1 = (p-1)B$  với

$$B = p^{n-1} + p^{n-2} + \dots + p + 1 \equiv n \pmod{p-1} \equiv 1 \pmod{p-1} \Rightarrow (p-1, B) = 1.$$

Do  $f(n) \notin A$  suy ra có ước số nguyên tố  $q$  của  $f(n)$  mà  $B : q \Rightarrow p-1 \nmid q$ .

Mâu thuẫn với giả thiết quy nạp.

**Câu 63.** Cho số nguyên dương  $n$  và số nguyên tố  $p$  lớn hơn  $n+1$ . Chứng minh rằng đa thức  $P(x) = 1 + \frac{x}{n+1} + \frac{x^2}{2n+1} + \dots + \frac{x^p}{pn+1}$  không có nghiệm nguyên.

#### Lời giải

Ta viết lại  $P(x) = a_p x^p + a_{p-1} x^{p-1} + \dots + a_2 x^2 + a_1 x + a_0$  trong đó  $a_k = \frac{(n+1)(2n+1)\dots(pn+1)}{kn+1}$

là các số nguyên (chú ý là ta quy đồng hết nên trên tử chứa cả nhân tử dưới mẫu).

Do  $p$  là số nguyên tố lớn hơn  $n+1$  nên  $(p, n) = 1$ .

Vì thế tập  $A = \{1.n+1; 2n+1; \dots; pn+1\}$  là hệ thặng dư đầy đủ modulo  $p$ .

Do đó tồn tại duy nhất  $k \in \{1, 2, \dots, p\}$  sao cho  $kn+1 \equiv 0 \pmod{p}$ .

Ta lại có  $k \neq 1, 0 < kn+1 < p^2$  nên  $kn+1 \nmid p^2$ . Như vậy với số  $k$  đó thì  $a_k \nmid p$  (vì nhân tử  $kn+1$  đã bị rút gọn), đồng thời các hệ số còn lại đều chia hết cho  $p$  kể cả các hệ số  $a_0, a_1$  nhưng không chia hết cho  $p^2$ .

Bây giờ ta sử dụng lập luận đó để chứng minh phương trình trên không có nghiệm nguyên.

Ngược lại giả sử rằng phương trình có nghiệm nguyên là  $c$  thì khi đó ta có



$$P(c) = 0 \Leftrightarrow a_p c^p + a_{p-1} c^{p-1} + \dots + a_2 c^2 + a_1 c + a_0 = 0$$

Theo lập luận trên thì ta có  $a_i : p, \forall i \in \{0, 1, 2, \dots, p\}, i \neq k, k \neq 0; 1$ .

Do đó dẫn đến  $a_k c^k : p$  (do  $p$  là số nguyên tố).

Suy ra  $c^k : p \Rightarrow c : p \Rightarrow a_i c^i : p^2$  với mọi  $i \in \{2, 3, \dots, p\}$ .

Ta cũng có  $a_1 c : p^2$  vì cả  $a_1, c$  đều chia hết cho  $p$ .

Vì  $P(c) = 0 : p^2 \Rightarrow a_0 : p^2$  là điều vô lí.

**Câu 64.** Cho đa thức  $P(x) = x^3 - 11x^2 - 87x + m (m \in \mathbb{Z})$ . Chứng minh rằng với mọi  $m$  tồn tại số nguyên  $n$  sao cho  $P(n) : 191$ .

### Lời giải

Ta có  $P(n) = n^3 - 11n^2 - 87n + m$ .

Đối với bài này ta sẽ chứng tỏ với  $n \in A = \{1, 2, \dots, 191\}$  là hệ đầy đủ modulo 191 thì ta có hệ  $A^* = \{P(1), P(2), \dots, P(191)\}$  cũng là hệ đầy đủ modulo 191.

Như thế thì khi đó tồn tại  $n \in A$  để  $P(n) \equiv 0 \pmod{191}$ . Để chứng minh được  $A^*$  là hệ đầy đủ modulo 191 thì ta cần chỉ ra  $n_1, n_2 \in A$  và  $n_1 \not\equiv n_2 \pmod{191}$  thì

$$P(n_1) \not\equiv P(n_2) \pmod{191}.$$

Thật vậy.

Giả sử ta có  $P(n_1) \equiv P(n_2) \pmod{191} \Leftrightarrow 27P(n_1) \equiv 27P(n_2) \pmod{191}$ , vì  $(27, 191) = 1$ .

$$\Leftrightarrow (3n_1 - 11)^3 - 18 \cdot 191n_1 + 11^3 + 27m \equiv (3n_2 - 11)^3 - 18 \cdot 191n_2 + 11^3 + 27m \pmod{191}$$

$$\Leftrightarrow (3n_1 - 11)^3 \equiv (3n_2 - 11)^3 \Leftrightarrow n_1 \equiv n_2 \pmod{191}$$

Để hoàn thành được bước cuối, ta cần có bổ đề sau

**Bổ đề.** Giả sử  $p$  là SNT và  $p \equiv 2 \pmod{3}$  thì  $x^3 \equiv y^3 \pmod{p} \Rightarrow x \equiv y \pmod{p}$ .

**Chứng minh bổ đề**

- Nếu  $x \equiv 0 \pmod{p} \Rightarrow x^3 \equiv 0 \Rightarrow y^3 \equiv 0 \Rightarrow y \equiv 0 \pmod{p}$ . Vậy  $x \equiv y \pmod{p}$ .
- Nếu  $x \not\equiv 0 \pmod{p}$  thì dễ thấy  $x^3 \not\equiv 0 \pmod{p} \Rightarrow y^3 \not\equiv 0 \pmod{p} \Rightarrow y \not\equiv 0 \pmod{p}$ .

Do nên theo **định lý Fermat** ta có

$$x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^{3k+1} \equiv 1 \pmod{p}, y^{p-1} = y^{3k+1} \equiv 1 \pmod{p}.$$

Từ đó suy ra  $x^{3k+1} \equiv y^{3k+1} \pmod{p} \Leftrightarrow x \cdot (x^3)^k \equiv y \cdot (y^3)^k \pmod{p} \Leftrightarrow x \equiv y \pmod{p}$  do  $(x, p) = 1$

Bổ đề được chứng minh nên ta cũng kết thúc bài toán.



**Câu 65.** Cho  $m$  là số nguyên dương, tìm số nghiệm của phương trình  $x^2 \equiv x \pmod{m}$ .

**Lời giải**

Ta giả sử phân tích  $m$  ra số nguyên tố là  $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$  trong đó  $p_i$  là các số nguyên tố.

Khi đó phương trình  $x^2 \equiv x \pmod{m} \Leftrightarrow x^2 \equiv x \pmod{p_i^{\alpha_i}}, \forall i = \overline{1; k}$ .

Ta có  $x^2 \equiv x \pmod{p_i^{\alpha_i}} \Leftrightarrow x^2 - x \equiv 0 \pmod{p_i^{\alpha_i}} \Leftrightarrow x(x-1) \equiv 0 \pmod{p_i^{\alpha_i}}$ .

Vì  $(x, x-1) = 1$  nên phương trình tương đương  $x \equiv 0 \pmod{p_i^{\alpha_i}}$  hoặc  $x \equiv 1 \pmod{p_i^{\alpha_i}}$ .

Theo định lý thặng dư Trung hoa thì với mỗi bộ  $a_1, a_2, \dots, a_k$  thì hệ phương trình

$$\begin{cases} x \equiv a_i \pmod{p_i^{\alpha_i}} \\ i = \overline{1; k} \end{cases} \text{ luôn có nghiệm duy nhất theo modulo } m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Do mỗi phương trình  $x^2 - x \equiv 0 \pmod{p_i^{\alpha_i}}$  luôn có hai nghiệm theo modulo  $p_i^{\alpha_i}$  nên phương trình đã cho có tất cả  $2^k$  nghiệm.

**Câu 66.** Cho  $p$  là số nguyên tố ( $p \geq 3$ ). Xét đa thức

$$f(x) = (p-1)x^{p-2} + (p-2)x^{p-3} + 3x^2 + 2x + 1.$$

Biết rằng hệ  $A = \{a_1, a_2, \dots, a_p\}$  là một hệ thặng dư đầy đủ modulo  $p$ . Chứng minh rằng khi đó hệ  $B = \{f(a_1), f(a_2), \dots, f(a_p)\}$  cũng là một hệ thặng dư đầy đủ modulo  $p$ .

**Lời giải**

Xét  $x = 1 \Rightarrow f(1) = (p-1) + (p-2) + \dots + 2 + 1 = \frac{p(p-1)}{2} \equiv 0 \pmod{p}$ .

Nếu  $x \neq 1$  thì ta có  $f(x) = \frac{1}{x-1} \left[ (p-1)(x^{p-1} - x^{p-2}) + (p-2)(x^{p-2} - x^{p-3}) + \dots + x - 1 \right]$ .

Do đó  $(x-1)f(x) = (p-1)(x^{p-1} - x^{p-2}) + (p-2)(x^{p-2} - x^{p-3}) + \dots + 2(x^2 - x) + x - 1$

Suy ra  $(x-1)f(x) = (p-1)x^{p-1} - (x^{p-2} + x^{p-3} + \dots + 1)$ .

Áp dụng công thức tổng của cấp số nhân và quy đồng ta suy ra

$$(x-1)^2 f(x) = (p-1)(x-1)x^{p-1} - (x^{p-1} - 1) \equiv 1 - x \pmod{p} \quad (1).$$

Ta cần chỉ ra bằng phản chứng

Giả sử  $B$  không phải là hệ thặng dư đầy đủ.

Khi đó tồn tại  $a_i, a_j \in A$  ( $1 \leq i < j \leq p$ ) sao cho  $f(a_i) \equiv f(a_j) \pmod{p}$ .

Từ (1) ta suy ra  $\begin{cases} m(a_i - 1)^2 \equiv 1 - a_i \pmod{p} \\ m(a_j - 1)^2 \equiv 1 - a_j \pmod{p} \end{cases} \quad (m \in [0; p-1]).$

Nếu  $m = 0$  thì từ hệ ta suy ra  $a_i \equiv a_j \equiv 1 \pmod{p}$  là điều vô lý.



Nếu  $m \neq 0 \Rightarrow f(a_i) \equiv f(a_j) \not\equiv 0$ . Nhưng  $f(1): p \Rightarrow a_i \neq 1, a_j \neq 1$ .

Do  $a_i, a_j \in A$  nên  $(1 - a_i, 1 - a_j) = 1$ . Nên nhân phương trình trên và phương trình dưới của hệ lần lượt với  $1 - a_j$  và  $1 - a_i$  ta thu được

$$m(a_i - 1)^2(1 - a_j) \equiv m(a_j - 1)^2(1 - a_i) \pmod{p} \Leftrightarrow 1 - a_i \equiv 1 - a_j \pmod{p} \Leftrightarrow a_i \equiv a_j \text{ (vô lí)}.$$

**Câu 67.** Xét đa thức  $P(x) = x^3 + 14x^2 - 2x + 1$ . Chứng minh rằng tồn tại số nguyên dương  $n$  sao cho với mọi số nguyên  $x$  ta có  $101 \mid P(P \dots P(x) \dots) - x$ .

*Thặng dư bình phương – Nguyễn Duy Liên*

*Lời giải*

Ta sẽ chứng minh rằng  $x \equiv y \pmod{101} \Leftrightarrow P(x) \equiv P(y) \pmod{101}$ .

Ta có  $P(x) - P(y) = (x - y)(x^2 + xy + y^2 + 14x + 14y - 2)$

Do đó  $4[P(x) - P(y)] = (x - y)[(2x + y + 14)^2 + 3(y - 29)^2]$

Vì  $(4; 101) = 1$  nên  $P(x) \equiv P(y) \pmod{4} \Leftrightarrow \begin{cases} x \equiv y \pmod{101} \\ [(2x + y + 14)^2 + 3(y - 29)^2] \equiv 0 \pmod{101} \end{cases}$

Xét  $[(2x + y + 14)^2 + 3(y - 29)^2] \equiv 0 \pmod{101}$ .

Nếu  $(y - 29, 101) = 1$  thì khi đó  $\left(-\frac{3}{101}\right) = 1$  nên  $101 \equiv 1 \pmod{6}$ , vô lí.

Nếu  $101 \mid (y - 29) \Rightarrow 101 \mid (2x + y + 14) \Rightarrow x \equiv y \equiv 29 \pmod{101}$ .

Như vậy cả hai trường hợp ta có  $x \equiv y \pmod{101}$ . Nhận xét được chứng minh.

Xét 102 đa thức như sau  $P(x), P(P(x)), \dots, P(P(\dots P(x) \dots))$ .

Theo nguyên lý Dirichlet phải tồn tại hai số  $m, n \in \{1; 2; \dots; 102\}, m > n$  sao cho

$$\underbrace{P(P(\dots P(x) \dots))}_m \equiv \underbrace{P(P(\dots P(x) \dots))}_n \pmod{101}.$$

Từ nhận xét trên ta suy ra  $\underbrace{P(P(\dots P(x) \dots))}_{m-n} \equiv x \pmod{101}$  với mọi số nguyên  $x$ .

**Câu 68.** Cho tập  $S = \{p_1, p_2, \dots, p_k\}$  là tập hợp  $k$  số nguyên tố phân biệt và  $P(x)$  là đa thức với hệ số nguyên sao cho với mọi số nguyên dương  $n$  đều tồn tại  $p_i$  trong  $S$  sao cho  $p_i \mid P(n)$ . Chứng minh rằng tồn tại  $i$  sao cho  $p_i \mid P(n), \forall n \in \mathbb{N}^*$ .

*Lời giải*

Ta chứng minh phản chứng bằng cách sử dụng *định lý thặng dư Trung Hoa*.



Giả sử không tồn tại  $i$  sao cho  $p_i | P(n), \forall n \in \mathbb{N}^*$ .

Suy ra với mọi  $i = \overline{1, k}$ , luôn tồn tại  $a_i$  sao cho  $p_i \nmid P(a_i)$ .

Theo định lí thặng dư Trung Hoa luôn tồn tại  $x$  sao cho  $\begin{cases} x \equiv a_i \pmod{p_i} \\ i = \overline{1, k} \end{cases}$ .

Do đó ta có  $\begin{cases} P(x) \equiv P(a_i) \pmod{p_i} \\ i = \overline{1, k} \end{cases}$ .

Hay ta có  $p_i \nmid P(x), \forall i = \overline{1, k}$ . Điều này mâu thuẫn với giả thiết.

**Câu 69.** Cho đa thức  $P(x) = x^3 + 153x^2 - 111x + 38$ .

a) Chứng minh rằng trong đoạn  $[0; 3^{2000}]$  tồn tại ít nhất một số nguyên dương  $a$  sao cho  $P(a) \vdots 3^{2000}$ .

b) Hỏi trong đoạn  $[0; 3^{2000}]$  có tất cả bao nhiêu số nguyên dương  $a$  sao cho  $P(a)$  chia hết cho  $3^{2000}$ .

### Lời giải

Ta xét phương trình đồng dư  $P(x) \equiv 0 \pmod{3^{2000}}$ .

Ta để ý rằng  $P(x) \equiv 0 \pmod{3} \Leftrightarrow x^3 + 153x^2 - 111x + 38 \equiv 0 \pmod{3}$ .

$$\Leftrightarrow x^3 + 38 \equiv 0 \pmod{3} \Leftrightarrow x \equiv 1 \pmod{3}.$$

Đặt  $x = 3y + 1 (0 \leq y \leq 3^{1999} - 1)$ .

Vậy  $P(x) \equiv P(3y + 1) \equiv 27(y^3 + 52y^2 + 22y + 3) \pmod{3^{2000}}$ .

$$\Leftrightarrow Q(y) = y^3 + 52y^2 + 22y + 3 \equiv 0 \pmod{3^{1997}}, \text{ suy ra } \begin{cases} y = 3t \\ y = 3t + 1 \end{cases}, (1 \leq t \leq 3^{1998} - 1).$$

Nếu  $y = 3t + 1$  thì phương trình  $y^3 + 52y^2 + 22y + 3$  không chia hết cho 9, nên không chia hết cho  $3^{1997}$ .

Nếu  $y = 3t$  thì  $y^3 + 52y^2 + 22y + 3 = 3(9t^3 + 156t^2 + 22t + 1)$ .

Nên suy ra  $P(x) \equiv 0 \pmod{3^{2000}} \Leftrightarrow G(t) = 9t^3 + 156t^2 + 22t + 1 \equiv 0 \pmod{3^{1996}}$ .

Bây giờ ta xét đa thức  $G(t) = 9t^3 + 156t^2 + 22t + 1$ .

Ta nhận thấy  $G(t) \equiv 0 \pmod{3} \Leftrightarrow 22t + 1 \equiv 0 \pmod{3}$ .

Trong đoạn  $[0; 3]$  phương trình  $22t + 1 \equiv 0 \pmod{3}$  có nghiệm duy nhất  $t = 2$ , và có thêm điều kiện là  $G'(2) = 22 \equiv 1 \pmod{3}$  suy ra  $G'(2) \not\equiv 0 \pmod{3}$  nên áp dụng **định lí Hensel** thì phương trình  $G(t) \equiv 0 \pmod{3^{1996}}$  có nghiệm duy nhất  $t_0 \in [0; 3^{1996}]$ .



Với  $t \in \mathbb{Z}, t \in [1; 3^{2000}]$ ,  $G(t) \equiv 0 \pmod{3^{1998}}$  khi và chỉ khi tồn tại  $h \in \mathbb{Z}, 0 \leq h \leq 8$  sao cho  $t = t_0 + 3^{1996} \cdot h$ . Vậy phương trình đồng dư  $G(t) \equiv 0 \pmod{3^{1998}}$  có đúng 9 nghiệm nguyên thuộc đoạn  $[1; 3^{1998} - 1]$ . Từ đó suy ra trong đoạn  $[1; 3^{2000}]$  có đúng 9 số  $a$  sao cho  $P(a)$  chia hết cho  $3^{2000}$ .

**Câu 70.** Tìm tất cả các đa thức  $f$  với hệ số nguyên sao cho  $f(n) \mid f(m) \Rightarrow n \mid m$ .

*Iran TST*

### Lời giải

Ta dự đoán rằng đa thức thỏa mãn sẽ là  $ax^k$ . Nên ta đặt  $f(x) = x^k \cdot g(x)$  với  $g(0) \neq 0$ .

Ta sẽ chứng minh  $g(x)$  là đa thức hằng.

Từ giả thiết  $f(n) \mid f(m) \Rightarrow n \mid m$ , ta suy ra  $n^k g(n) \mid m^k g(m) \Rightarrow n \mid m$ . Nên để phản chứng  $g(x)$  không phải đa thức hằng thì ta có thể chọn  $n^k g(n) \mid m^k g(m)$  nhưng không suy ra được  $n \mid m$ . Từ đó có mâu thuẫn. Vấn đề ta chọn thế nào?

Nếu chọn cả  $n^k \mid m^k$  và  $g(n) \mid m^k$  thì dẫn đến  $n \mid m$ , việc chọn như vậy không có ý nghĩa gì. Vậy liệu ta có thể chọn  $n^k \mid m^k$  và  $g(n) \mid g(m)$ . Ta sẽ theo dõi lập luận sau.

Xét đa thức  $h(x) \in \mathbb{Z}[x], h(0) \neq 0$ . Ta sẽ chứng minh với mọi  $k$  tồn tại  $m, p > h(0)$  sao cho  $p^k \mid h(m)$ . Thật vậy, giả sử  $h(x) = h_1(x) \cdot h_2(x) \dots h_n(x)$ , trong đó  $h_i(x)$  bất khả quy và  $h_i(0) \neq 0$ . Do đó thay vì chọn  $h(x)$  bất kì ta có thể chọn luôn  $h(x)$  bất khả quy.

Khi  $h'(x)$  nguyên tố cùng nhau với  $h(x)$  thì tho **định lí Bézout** ta có tồn tại hai đa thức  $P, Q$  sao cho tồn tại số nguyên  $a$  ta có  $h \cdot P + h' \cdot Q = a$ . Khi đó theo **định lí Schur** luôn tồn tại số nguyên tố  $p$  đủ lớn sao cho  $p > a, p \mid h(n), p$  không là ước của  $h'(n)$ .

Áp dụng **định lí Hensel** ta thấy  $p^k \mid h(m)$ .

Đặt  $f(x) = x^k g(x), k \geq 0, g(0) \neq 0$ . Giả sử rằng  $g(x)$  khác đa thức hằng. Theo chứng minh trên thì tồn tại số nguyên tố  $p$  sao cho  $p > g(0)$  và  $p^k \mid g(m)$  với  $m$  nguyên dương.

Dễ thấy  $p$  không là ước của  $g(p)$  nên theo **định lí thặng dư Trung Hoa** thì tồn tại  $n$  sao cho

$$\begin{cases} n \equiv m \pmod{p^k} \\ n \equiv p \pmod{g(p)} \end{cases}$$

Khi đó  $p^k \mid g(n)$  và  $g(p) \mid g(n)$  nên dẫn đến  $f(p) \mid f(n)$ .

Do đó  $p \mid n$  mà  $p \mid g(n)$  nên  $p \mid g(0)$  là vô lí.

Do đó  $g(x)$  là đa thức hằng. Vậy  $f(x) = a \cdot x^k$ .





**Câu 71.** Cho  $a, b, c, d, e, f$  là các số nguyên dương. Giả sử rằng  $S = a + b + c + d + e + f$  là ước của các số  $abc + def$  và  $ab + bc + ca - de - ef - fd$ . Chứng minh rằng  $S$  là hợp số.

IMO Shortlist 2005

**Lời giải**

Xét đa thức  $P(x) = (x+a)(x+b)(x+c) - (x-d)(x-e)(x-f) = Sx^2 + Qx + R$ .

Trong đó  $S = a + b + c + d + e + f$ ;  $Q = ab + bc + ca - de - ef - fd$ ;  $R = abc + def$ .

Vì theo giả thiết  $S|Q$ ;  $S|R$  nên  $S|P(x), \forall x \in \mathbb{Z}$ .

Ta có  $S|P(d) = (d+a)(d+b)(d+c)$ .

Nếu  $S$  là số nguyên tố thì một trong 3 số  $d+a, d+b, d+c$  chia hết cho  $S$ . Nhưng điều đó là vô lý vì  $S > \max\{d+a, d+b, d+c\}$ .

Do đó  $S$  là hợp số.

**Câu 72.** Tìm tất cả các đa thức  $P$  với hệ số nguyên thỏa mãn

$$P(n) \mid 2557^n + 213.2014, \forall n \in \mathbb{N}^*$$

Thailand 2014

**Lời giải**

Dễ thấy  $P(n) = 1, \forall n \in \mathbb{N}^*$  và  $P(n) = -1, \forall n \in \mathbb{N}^*$  là những đa thức thỏa mãn điều kiện bài toán. Giả sử  $P$  là đa thức thỏa mãn bài toán và  $\exists n_0 \in \mathbb{N}^* : |P(n_0)| \geq 2$ .

Gọi  $p$  là ước nguyên tố của  $P(n_0)$ .

Ta có:  $P(n_0) \mid 2557^{n_0} + 213.2014$  và  $P(n_0 + p) \mid 2557^{n_0+p} + 213.2014$ .

Do đó  $p \mid P(n_0 + p) - P(n_0) \mid 2557^{n_0} (2557^p - 1)$ .

Mặt khác, vì  $p \mid P(n_0) \mid 2557^{n_0} + 213.2014$  nên  $p \notin \{2, 3, 19, 53, 71, 2557\}$ .

Do đó  $p \mid (2557^p - 1)$ . Hơn nữa, theo **định lý Fermat** nhỏ ta có  $p \mid (2557^p - 2557)$  nên  $p \mid 2556$ . Suy ra  $p \in \{2, 3, 71\}$ , vô lý.

Vậy chỉ có hai đa thức  $P(n) = 1, \forall n \in \mathbb{N}^*$  và  $P(n) = -1, \forall n \in \mathbb{N}^*$  thỏa mãn bài toán.

**Câu 73.** Cho  $P$  là đa thức hệ số nguyên, có bậc  $n > 1$  và  $k$  là số nguyên dương bất kỳ. Xét đa thức  $Q(x) = P^k(x)$  với  $P$  được tác động  $k$  lần. Chứng minh rằng có nhiều nhất  $n$  số nguyên  $t$  sao cho  $Q(t) = t$ .

IMO Shortlist 2006

**Lời giải**

**Bổ đề.** Nếu  $t$  là số nguyên thỏa mãn  $Q(t) = t$  thì  $P^2(t) = t$ .



Thật vậy. Ta có  $P(t) - t \mid P^2(t) - P(t) \dots \mid P^k(t) - P^{k-1}(t) \mid P^{k+1}(t) - P^k(t)$ .

Mà  $P^{k+1}(t) - P^k(t) = P(t) - t$  nên  $|P(t) - t| = |P^2(t) - P(t)| = \dots = |P^k(t) - P^{k-1}(t)|$

Đặt  $d = P(t) - t$ . Nếu  $d = 0 \Rightarrow P(t) = t \Rightarrow P^2(t) = P(t) = t$ .

Nếu  $d \neq 0$ . Giả sử  $i$  là chỉ số nhỏ nhất mà  $d = -[P^i(t) - P^{i-1}(t)]$ ,  $2 \leq i \leq k$  khi đó

$$P^{i-1}(t) - P^{i-2}(t) = P^{i-1}(t) - P^i(t)$$

Suy ra  $P^i(t) = P^{i-2}(t)$  nên  $P^2(t) = t$ .

Ngược lại nếu  $d = P(t) - t = P^2(t) - P(t) = \dots = P^k(t) - P^{k-1}(t)$  thì  $P^k(t) = t + kd \neq t$ , điều này mâu thuẫn.

Quay lại bài toán, giả sử rằng có  $(n+1)$  số nguyên  $t_1 < t_2 < \dots < t_n < t_{n+1}$  thỏa mãn

$$Q(t_i) = t_i, 1 \leq i \leq n+1$$

Khi đó theo bổ đề trên, ta có  $P^2(t_i) = t_i, 1 \leq i \leq n+1$ .

Với mọi  $i, j$  thỏa mãn  $1 \leq i < j \leq n+1$  ta có  $t_i - t_j \mid P(t_i) - P(t_j) \mid P^2(t_i) - P^2(t_j)$ .

Nên  $|P(t_i) - P(t_j)| = t_j - t_i$ . Theo bất đẳng thức về giá trị tuyệt đối, ta có:

$$t_{n+1} - t_1 = |P(t_{n+1}) - P(t_1)| \leq |P(t_{n+1}) - P(t_n)| + |P(t_n) - P(t_{n-1})| + \dots + |P(t_2) - P(t_1)| = t_{n+1} - t_1$$

Do đó, tất cả các hiệu  $P(t_{i+1}) - P(t_i)$  đều cùng dấu.

Giả sử tất cả các hiệu  $P(t_{i+1}) - P(t_i)$  đều cùng dấu dương, khi đó

$$P(t_{i+1}) - P(t_i) = t_{i+1} - t_i, \forall 1 \leq i \leq n$$

Suy ra  $P(t_{i+1}) - t_{i+1} = P(t_i) - t_i, \forall 1 \leq i \leq n$ .

Do đó, đa thức  $P(x) - x - (P(t_1) - t_1)$  có  $(n+1)$  nghiệm phân biệt  $t_1 < t_2 < \dots < t_n < t_{n+1}$ , điều này là vô lý vì  $P(x) - x - (P(t_1) - t_1)$  là một đa thức bậc  $n$ .

Tương tự cho trường hợp tất cả các hiệu  $P(t_{i+1}) - P(t_i)$  đều cùng dấu âm.

Vậy ta có điều phải chứng minh.

**Câu 74.** Cho  $A$  là tập vô hạn các số nguyên dương. Tìm tất cả các số nguyên dương  $n$  thỏa mãn với mọi  $a$  là phần tử của  $A$  thì

$$1 + a + a^2 + \dots + a^n \mid 1 + a^{1!} + a^{2!} + \dots + a^{n!}$$

Serbia MO 2010

*Lời giải*

Xét một số  $n$  thỏa mãn yêu cầu bài toán.

Ta đặt:  $P(x) = 1 + x + x^2 + \dots + x^n$ ,  $Q(x) = 1 + x^{1!} + x^{2!} + \dots + x^{n!}$

Theo kết quả trên, từ giả thiết  $P(a) \mid Q(a)$  với vô hạn  $a$  ta suy ra  $P(x) \mid Q(x)$ .



Ta thấy rằng  $x^{n+1} \equiv 1 \pmod{P(x)}$

Do vậy, gọi  $t_i$  là số dư trong phép chia  $i!$  cho  $n+1$  với  $i \leq n$  thì

$$Q(x) = x^0 + x^{t_1} + \dots + x^{t_n} = S(x) \pmod{P(x)}$$

Vì các  $t_i$  đều không vượt quá  $n+1$  và cả  $P(x), S(x)$  đều là tổng của  $n-1$  đơn thức nên để

$$P(x) \mid Q(x) \text{ thì } P(x) = S(x)$$

Như vậy, ta cần có  $\{0, 1!, \dots, n!\}$  lập thành một hệ thặng dư đầy đủ theo mod  $n+1$

Trước tiên, trong  $n+1$  số trên chỉ có một số chia hết cho  $n+1$  là 0 nên ta suy ra  $n!$  không là bội của  $n+1$ , điều này chỉ xảy ra khi  $n+1$  là số nguyên tố.

Với  $n > 2$  thì  $n! \equiv -1 \equiv n \pmod{n+1}$  theo **định lý Wilson**

Suy ra  $(n-1)! \equiv 1 \pmod{n+1}$  nên hệ  $\{0, 1!, \dots, n!\}$  không lập thành một hệ thặng dư đầy đủ mod  $n+1$ .

Và như vậy ta phải có  $n \leq 2$ , kiểm tra trực tiếp ta thấy  $n=1$  và  $n=2$  đều thỏa mãn.

Vậy tất cả các giá trị của  $n$  thỏa mãn yêu cầu bài toán là  $n=1$  và  $n=2$ .

**Câu 75.** Cho  $P, Q$  là hai đa thức hệ số nguyên không âm, khác đa thức hằng. Xét dãy số  $x_n = 2016^{P(n)} + Q(n), n \geq 1$ . Chứng minh rằng tồn tại vô hạn số nguyên tố  $p$  thỏa mãn: ứng với mỗi  $p$ , tồn tại số nguyên dương  $m$  sao cho  $p \mid x_m$ .

*Ukraine 2016*

### Lời giải

Ta có  $x_n = 2016^{P(n)} + Q(n) = 2016^{P(n)} - 2016^{P(1)} + Q(n) + 2016^{P(1)} = 2016^{P(n)} - 2016^{P(1)} + R(n)$

Trong đó  $R = Q + 2016^{P(1)}$  là một đa thức hệ số nguyên, khác đa thức hằng và  $R(0) > 0$ .

Theo **định lý Schur**, tồn tại vô hạn số nguyên tố  $p, p > \max\{R(0), 2016\}$  thỏa mãn ứng với mỗi  $p$ , tồn tại số nguyên dương  $n$  sao cho  $p \mid R(n)$ .

Nếu  $p \mid n$  thì  $p \mid R(n) - R(0)$  nên  $p \mid R(0)$ , vô lý nên  $(p, n) = 1$ .

Mặt khác  $(p, p-1) = 1$  nên theo **định lý thặng dư Trung Hoa**, tồn tại số nguyên  $m$  sao cho

$$m \equiv n \pmod{p}; m \equiv 1 \pmod{p-1}$$

Vì  $p \mid R(n)$  và  $m \equiv n \pmod{p}$  nên  $p \mid R(m)$ .

Hơn nữa  $m \equiv 1 \pmod{p-1}$  nên  $P(m) \equiv P(1) \pmod{p-1}$  do đó theo **định lý Fermat nhỏ** ta có  $p \mid 2016^{P(m)} - 2016^{P(1)}$ . Suy ra  $p \mid x_m$ .

Vậy ta có điều phải chứng minh!



**Câu 76.** Tìm tất cả các đa thức  $P$  hệ số nguyên thỏa mãn  $P(p) \mid 2^p - p$ , với mọi số nguyên tố  $p$ .

**Lời giải**

Dễ thấy nếu  $P$  là đa thức hằng thì  $P = \pm 1$  thỏa mãn điều kiện bài toán.

Xét  $P$  không phải là đa thức hằng. Theo **định lý Schur**, tồn tại vô hạn số nguyên tố  $p$  thỏa mãn: Ứng với mỗi  $p$  tồn tại số nguyên  $n$  sao cho  $p \mid P(n)$ .

Nếu  $p \mid n$  thì  $p \mid P(n) - P(p)$  nên  $p \mid P(p) \mid 2^p - p$ , vô lý nên  $(p, n) = 1$ .

Theo định lý Dirichlet về số nguyên tố, ta có thể chọn số nguyên  $k$  sao cho  $q = n + kp$  là số nguyên tố. Khi đó  $p \mid P(q) - P(n)$  nên  $p \mid P(q) \mid 2^q - q = 2^{n+kp} - (n + kp)$ . Kết hợp định lý Fermat nhỏ suy ra  $p \mid 2^{n+k} - n$ . Đặt  $h = \text{ord}_p(2)$ .

Nếu có các số nguyên  $k_1, k_2$  thỏa mãn  $p \mid 2^{n+k_1} - n$  và  $p \mid 2^{n+k_2} - n$  thì  $k_2 \equiv k_1 \pmod{h}$ .

Do đó, ta chỉ có thể chọn  $k$  theo một lớp thặng dư nào đó đối với modul  $h$ .

Nhưng, theo định lý Dirichlet, ta có thể chọn  $k$  sao cho số nguyên tố  $q = n + kp$  nguyên tố cùng nhau với  $h$ . Khi đó, vì  $h \mid p - 1$  nên  $(n + k, h) = 1$ , nghĩa là ta có  $\phi(h)$  cách chọn lớp thặng dư đối với modul  $h$  cho  $k$ . Vô lý.

Vậy chỉ có  $P = \pm 1$  là những đa thức thỏa mãn bài toán.

**Câu 77.** Cho  $P(x), Q(x)$  là các đa thức hệ số nguyên khác đa thức hằng. Giả sử rằng đa thức  $P(x).Q(x) - 2009$  có ít nhất 25 nghiệm nguyên phân biệt. Chứng minh rằng bậc của mỗi đa thức  $P(x), Q(x)$  đều không nhỏ hơn 3.

*Belarus 2009*

**Lời giải**

Giả sử  $T = \{a_i, 1 \leq i \leq 25, i \in \mathbb{Z}\}$  là tập hợp gồm 25 nghiệm nguyên của đa thức

$P(x).Q(x) - 2009$ .

Khi đó  $P(a_i)Q(a_i) = 2009, \forall 1 \leq i \leq 25$ .

Suy ra  $P(a_i) \mid 2009; Q(a_i) \mid 2009, \forall 1 \leq i \leq 25$ .

Vì  $2009 = 7^2 \cdot 41$  nên 2009 có tất cả 12 ước số nguyên.

Do đó, mỗi số  $P(a_1), P(a_2), \dots, P(a_{25})$  sẽ bằng với 1 trong 12 ước số nguyên của 2009, và theo **nguyên lý Dirichlet**, phải có ít nhất 3 trong số 25 số  $P(a_1), P(a_2), \dots, P(a_{25})$  có giá trị bằng nhau. Không mất tổng quát, giả sử  $P(a_1) = P(a_2) = P(a_3) = m$ .



Khi đó, đa thức  $P(x) - m$  có ít nhất 3 nghiệm phân biệt nên có bậc không nhỏ hơn 3, và do đó, đa thức  $P(x)$  có bậc không nhỏ hơn 3.

Tương tự, đa thức  $Q(x)$  cũng có bậc không nhỏ hơn 3. Ta có điều phải chứng minh.

**Câu 78.** Gọi  $d(n)$  là ước nguyên tố nhỏ nhất của số nguyên  $n$ , với  $n \neq \{-1, 0, 1\}$  và ta kí hiệu  $d(-1) = d(0), d(1) = 0$ . Tìm tất cả các đa thức  $P(x)$  với hệ số nguyên thỏa mãn

$$P(n + d(n)) = n + d(P(n))$$

*Turkey MO 2014*

### Lời giải

Trước tiên, ta có một đánh giá chung cho hai vế của đẳng thức ở đề bài.

Ta đã biết  $d(n)$  là ước nguyên tố nhỏ nhất của  $n$  thì  $d(n) < \sqrt{n}$  hoặc  $d(n) = n$ .

Do vậy ta dự đoán, nếu  $P(x)$  có bậc lớn hơn 1 thì chọn  $n$  đủ lớn sẽ có

$$P(n + d(n)) > n + d(P(n))$$

Thật vậy, giả sử  $P(x)$  có bậc không nhỏ hơn 2.

Chọn  $n = q$  nguyên tố thì  $d(n) = q$  thay vào phương trình ban đầu ta được

$$|P(2q)| = |q + d(P(q))| \leq q + |d(P(q))| \leq q + |P(q)|$$

$$\text{Suy ra } \left| \frac{P(2q)}{P(q)} \right| \leq \frac{q}{P(q)} + 1$$

Cho  $q$  tiến ra vô cùng, thì rõ ràng vế trái tiến về  $2^{\deg(P(x))}$ , còn vế phải tiến đến 1 nên điều này là vô lý.

Để thấy,  $P(x)$  là hằng số thì không thỏa mãn yêu cầu bài toán.

Cuối cùng, ta xét  $P(x)$  có bậc bằng 1 thì ta viết  $P(x) = bx + c; b, c \in \mathbb{Z}, b \neq 0$ .

Thay  $n = q$  là số nguyên tố một lần nữa, thì ta được:

$$2bq + c = q + d(bq + c)$$

Ta thấy rằng  $q + d(bq + c) \geq q$  nên chọn  $q$  đủ lớn thì ta suy ra phải có  $b$  là số dương, hay  $b \geq 1$ .

Mặt khác ta lại có  $(2b - 1)q + c = d(bq + c) \leq bq + c$  nên  $b \leq 1$ .

Từ đây ta phải có  $b = 1$ , thay lại vào phương trình đề bài thì ta được

$$n + d(n) + c = n + d(n + c)$$

Suy ra  $d(n + c) = d(n) + c, \forall n \in \mathbb{Z}^+$ .

Từ đây ta suy ra với mọi  $n$  đủ lớn nếu  $n + c$  là số nguyên tố thì  $n$  cũng là số nguyên tố và ngược lại. Ta chứng minh chỉ có  $c = 0$  thỏa mãn tính chất này.



Thật vậy, giả sử  $c \neq 0$  thì ta chọn được  $A > 2 + |c|$

Xét  $r$  là số nguyên tố nhỏ nhất lớn hơn  $A + 2$

Khi đó  $r > A + |c| + 2$  do tất cả các số từ  $A + 2$  đến  $A + |c| + 2$  đều là hợp số.

Ta cần có  $r + c$  và  $r - c$  đều là số nguyên tố, điều này không thể xảy ra vì một trong hai số này là  $r - |c|$  và là hợp số theo cách chọn  $r$ .

Vậy chỉ có  $c = 0$  thỏa mãn, khi đó thì  $P(x) = x$ , thử lại thấy thỏa mãn yêu cầu bài toán.

Vậy tất cả các đa thức thỏa mãn điều kiện bài toán là  $P(x) = x$ .

**Câu 79.** Tìm tất cả các số nguyên dương  $k$  thỏa mãn tồn tại đa thức  $f(x)$  với các hệ số đều nguyên, có bậc lớn hơn 1 sao cho với mọi số nguyên tố  $p$  và mọi số tự nhiên  $a, b$  mà  $p \mid ab - k$  thì  $p \mid f(a)f(b) - k$ .

### Lời giải

Với  $k = 1$  thì không khó để thấy rằng ta chọn được  $f(x) = x^n$  với  $n > 1$  là đa thức thỏa mãn.

Ta chứng minh các giá trị còn lại của  $k$  không thỏa mãn yêu cầu bài toán.

Giả sử có  $k > 1$  thỏa mãn yêu cầu bài toán.

Xét đa thức  $f(x)$  bậc  $n$  bất kì, giả sử  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

Ta lập đa thức  $g(x) = x^n f\left(\frac{k}{x}\right) = a_0 k^0 x^n + a_1 k^1 x^{n-1} + \dots + a_n k^n$

Với mỗi số nguyên dương  $a$  và số nguyên tố  $p$  mà  $(a, p) = 1$  thì ta chọn được  $b$  sao cho  $ab \equiv k \pmod{p}$ .

Khi đó thì ta thấy  $g(a) \equiv a^n f(b) \pmod{p}$

Như vậy, ta có với mọi số nguyên tố  $p$  mà  $(a, p) = 1$  thì

$$g(a)f(a) \equiv a^n f(b)f(a) \equiv ka^n \pmod{p}$$

Vì tập các số nguyên tố là vô hạn nên ta có thể cố định chọn  $p$  đủ lớn để

$$p > \max\{|g(a)f(a)| + |ka^n|\} + 3n, \forall a = \overline{1, 3n}$$

Khi đó thì ta suy ra  $g(a)f(a) - ka^n = 0, \forall a = \overline{1, 3n}$

Mặt khác, đa thức  $f(x)g(x) - kx^n$  chỉ có bậc  $2n$  mà lại nhận đến  $3n$  giá trị phân biệt là nghiệm nên đồng nhất với đa thức không.

Kết hợp với  $f(x)$  có bậc  $n$  ta suy ra  $g(x)$  phải là hằng số.

Từ công thức của  $g(x)$  ta suy ra  $g(x) = a_n k^n$ .

Ta cần có  $g(1)f(1) = k$  nên  $g(1) \mid k$  tuy nhiên điều này không thể xảy ra khi  $n \geq 2$  hay vô lý.



Vậy  $k = 1$  là số nguyên dương duy nhất thỏa mãn yêu cầu bài toán.

**Câu 80.** Cho  $P$  là đa thức hệ số nguyên thỏa mãn  $P(0) = 0$  và  $(P(0), P(1), \dots) = 1$ . Chứng minh rằng có vô hạn số  $n$  sao cho  $(P(n) - P(0), P(n+1) - P(1), \dots) = n$ .

USA TST 2010

**Lời giải**

Từ điều kiện  $P(0) = 0, (P(0), P(1), \dots) = 1$  suy ra  $P$  khác đa thức hằng.

Không mất tính tổng quát, giả sử  $P'(1) \neq 0$ .

Ta chứng minh rằng nếu  $p$  là một số nguyên tố bất kỳ sao cho  $p$  không là ước của  $P'(1)$  thì  $n = p^k$  thỏa điều kiện bài toán.

Vì  $p^k \mid P(p^k + i) - P(i)$  với mọi  $i$  nên  $p^k \mid (P(p^k) - P(0), P(p^k + 1) - P(1), \dots)$ .

Mặt khác theo nhận xét trong chứng minh **bổ đề Hensel**, ta có

$$P(p^k + 1) - P(1) \equiv P'(1)p^k \pmod{p^{k+1}}$$

Mà  $P'(1)$  không chia hết cho  $p$  nên  $P(p^k + 1) - P(1)$  không chia hết cho  $p^{k+1}$ .

Cuối cùng ta chỉ ra rằng, không có số nguyên tố  $p \neq q$  là ước số của

$$P(p^k) - P(0), P(p^k + 1) - P(1), \dots$$

Giả sử ngược lại với mọi  $i$ , ta có  $q \mid P(p^k + i) - P(i)$ .

Mặt khác ta cũng có  $q \mid P(q + i) - P(i)$  suy ra  $P(i + ap^k + bq) \equiv P(i) \pmod{q}$  với mọi số nguyên  $a, b$ . Vì  $(p^k, q) = 1$  nên tồn tại các số nguyên  $a, b$  sao cho  $ap^k + bq = 1$ .

Do đó  $q \mid P(i + 1) - P(i)$ .

Mà  $P(0) = 0$  nên  $q \mid P(i)$  với mọi  $i$ , mâu thuẫn với giả thiết.

Vậy  $p^k = (P(p^k) - P(0), P(p^k + 1) - P(1), \dots)$ . Ta có điều phải chứng minh!

**Câu 81.** Cho  $p$  là số nguyên tố và  $P(x)$  là các đa thức bậc  $d$  hệ số nguyên thỏa mãn

- $P(0) = 0, P(1) = 1$
- Với mọi số nguyên dương  $n$  thì số dư trong phép chia  $P(n)$  cho  $p$  là 0 hoặc 1.

Chứng minh rằng  $d \geq p - 1$ .

Italian Proposal to 1997 IMO

**Lời giải**

Giả sử  $d \leq p - 2$ . Áp dụng **công thức nội suy Lagrange** với  $(p - 1)$  mốc nội suy

$x_i = i, i = \overline{0, p - 2}$  ta được





$$P(x) = \sum_{i=0}^{p-2} P(i) \prod_{\substack{j=0 \\ j \neq i}}^{p-2} \frac{x-j}{i-j} \Rightarrow P(p-1) = \sum_{i=0}^{p-2} P(i) \cdot (-1)^{p-i} C_{p-1}^i$$

Do  $p$  nguyên tố nên  $C_{p-1}^i \equiv (-1)^i \pmod{p}, \forall i = \overline{0, p-2}$

$$\Rightarrow P(p-1) \equiv -\sum_{i=0}^{p-2} P(i) \pmod{p} \Rightarrow \sum_{i=0}^{p-1} P(i) \equiv 0 \pmod{p}$$

Nhưng từ 2 điều kiện ở giả thiết ta lại có  $\sum_{i=0}^{p-1} P(i) \equiv k \pmod{p}$  với  $k \in \{1, 2, \dots, p-1\}$ .

Điều này mâu thuẫn, suy ra  $d \geq p-1$ .

**Câu 82.** Chứng minh rằng không tồn tại đa thức  $P$  hệ số thực  $\deg P = n \geq 1$  sao cho  $P(m)$  là số nguyên tố với mọi số nguyên dương  $m$ .

**Lời giải**

Giả sử tồn tại đa thức  $P$  thỏa mãn điều kiện đề bài.

Trước hết, ta chứng minh  $n!P(x) \in \mathbb{Z}[x]$ .

Thật vậy, theo **công thức nội suy Lagrange**, ta có:  $P(x) = \sum_{i=0}^n P(i) \prod_{\substack{j=0 \\ j \neq i}}^n \frac{x-j}{i-j}$ .

Nên  $n!P(x) = x(x-1)\dots(x-n) \sum_{i=0}^n \frac{P(i)C_n^i(-1)^{n-i}}{x-i} \in \mathbb{Z}[x]$ .

Chọn 2 số nguyên tố  $p, q, p, q > n$  sao cho  $P(a) = p, P(b) = q, a, b \in \mathbb{N}^*$ .

Theo **định lý thặng dư Trung Hoa** thì tồn tại  $c \in \mathbb{N}^*$  sao cho

$$\begin{cases} c \equiv a \pmod{q} \\ c \equiv b \pmod{q} \end{cases} \Rightarrow \begin{cases} n!P(c) \equiv n!P(a) \equiv 0 \pmod{p} \\ n!P(c) \equiv n!P(b) \equiv 0 \pmod{q} \end{cases} \Rightarrow n!P(c) \equiv 0 \pmod{pq}$$

Điều này vô lý vì  $P(c)$  là số nguyên tố và  $(n!, pq) = 1$ .

Vậy ta có điều phải chứng minh.

**Câu 83.** Cho  $n \in \mathbb{N}, n > 3$  và đa thức  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x]$  thỏa mãn  $a_0$  chẵn,  $a_k + a_{n-k}$  chẵn với mọi  $k = \overline{1, n-1}$ .

Giả sử thêm rằng tồn tại hai đa thức  $g(x), h(x) \in \mathbb{Z}[x]$  thỏa mãn  $\deg g \leq \deg h$ , mọi hệ số của  $h(x)$  đều lẻ và  $f(x) = g(x) \cdot h(x), \forall x$ .

Chứng minh rằng  $f(x)$  có ít nhất một nghiệm nguyên.

**Romani TST 2007**

**Lời giải**

Giả sử  $\deg g = j, \deg h = k, 1 \leq j \leq k, j+k = n$  và





$$g(x) = b_0 + b_1x + \dots + b_jx^j, h(x) = c_0 + c_1x + \dots + c_kx^k$$

Ta có  $f(x) = (b_0 + b_1x + \dots + b_jx^j)(c_0 + c_1x + \dots + c_kx^k)$ . Đồng nhất hệ số, ta có

$$b_0 + b_1 + \dots + b_{j-1} = a_{j-1} \text{ và } b_1 + \dots + b_j = a_{k+1}$$

Giả sử  $j-1 > 0$  khi đó theo giả thiết  $a_{j-1} + a_{k+1}$  chẵn nên  $b_0 \equiv b_j \equiv 1 \pmod{2}$ .

Mà  $a_0$  chẵn nên  $c_0$  chẵn (mâu thuẫn giả thiết). Do đó  $j=1$  mà  $b_j = \pm 1$  nên  $g(x)$  có nghiệm nguyên. Suy ra  $f(x)$  cũng có nghiệm nguyên.

Vậy ta có điều phải chứng minh.

**Câu 84.** Cho đa thức  $f(x)$  monic, hệ số nguyên, bất khả quy và  $f(0)$  không phải là số chính phương. Chứng minh rằng  $g(x) = f(x^2)$  cũng là đa thức bất khả quy.

*Romani TST 2003*

#### Lời giải

Giả sử ta có phân tích  $g(x) = f(x^2) = p(x) \cdot q(x)$  với  $p(x), q(x)$  là 2 đa thức monic có hệ số nguyên và bậc không nhỏ hơn 1.

Gọi  $\alpha$  là một nghiệm (thực hoặc phức) của  $f(x)$  thì  $p(\sqrt{\alpha}) \cdot q(\sqrt{\alpha}) = f(\alpha) = 0$ . Không mất tổng quát, giả sử  $p(\sqrt{\alpha}) = 0$ .

$$\text{Đặt } p(x) = \sum_{i=0}^k a_i x^i, a_i \in \mathbb{Z} \text{ thì } \sum_{i=0}^k a_i \alpha^i = 0.$$

Do đó, tồn tại các đa thức hệ số nguyên  $t, u$  thỏa mãn  $t(\alpha) + \sqrt{\alpha} \cdot u(\alpha) = 0$ .

Do  $f$  là đa thức bất khả quy và  $\deg u < \deg f$  nên theo **định lý Bézout**, tồn tại số nguyên  $m$  và hai đa thức hệ số nguyên  $s, r$  sao cho  $s(x)u(x) + r(x)f(x) = m, \forall x \in \mathbb{Z}$ .

$$\text{Suy ra } s(\alpha)u(\alpha) = m \text{ nên } \sqrt{\alpha} = -\frac{s(\alpha)u(\alpha)}{m} \Rightarrow \alpha = \frac{[s(\alpha)u(\alpha)]^2}{m^2}.$$

Đặt  $\alpha_1, \alpha_2, \dots, \alpha_n$  là các nghiệm của đa thức  $f$  thì

$$\alpha_1 \alpha_2 \dots \alpha_n = \frac{s(\alpha_1)^2 t(\alpha_1)^2 s(\alpha_2)^2 t(\alpha_2)^2 \dots s(\alpha_n)^2 t(\alpha_n)^2}{m^{2n}}$$

là bình phương của một số hữu tỉ.

Mặt khác  $|f(0)| = |\alpha_1 \alpha_2 \dots \alpha_n|$  là số nguyên nên  $f(0)$  là số chính phương, trái giả thiết.

Vậy từ đó suy ra điều phải chứng minh!



**Câu 85.** Cho đa thức hệ số nguyên  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  thỏa mãn điều kiện  $|a_0| > |a_1| + |a_2| + \dots + |a_n|$  và  $|a_0|$  là số nguyên tố thì  $f(x)$  bất khả quy.

*Tiêu chuẩn Perron*

**Lời giải**

Giả sử  $f(x)$  có nghiệm  $z$  thỏa  $|z| \leq 1$  thì  $|a_0| = |a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z| \leq |a_1| + \dots + |a_n|$ , mâu thuẫn. Do đó tất cả các nghiệm của  $f$  đều có module lớn hơn 1.

Giả sử  $f(x) = P(x) \cdot Q(x)$  với  $P, Q$  là hai đa thức hệ số nguyên có bậc không nhỏ hơn 1.

Vì  $|a_0| = |f(0)| = |P(0)| |Q(0)|$  mà  $|a_0|$  là số nguyên tố nên  $|P(0)| = 1$  hoặc  $|Q(0)| = 1$ .

Không mất tính tổng quát ta giả sử  $|P(0)| = 1$ .

Gọi  $b$  là hệ số cao nhất của  $P$  và  $z_1, z_2, \dots, z_k$  là tất cả các nghiệm của  $P$ .

Khi đó  $|z_1 z_2 \dots z_k| = \frac{1}{|b|} \leq 1$ , mâu thuẫn vì tất cả các nghiệm của  $P$  cũng là nghiệm của  $f$ .

Vậy đa thức  $f(x)$  bất khả quy.

**Câu 86.** Tìm tất cả các đa thức  $P(x), Q(x)$  hệ số nguyên thỏa mãn với dãy số  $(x_n)$  xác định bởi  $x_0 = 2014, x_{2n+1} = P(x_{2n}), x_{2n+2} = Q(x_{2n+1}), \forall n \in \mathbb{N}$  thì mỗi số nguyên dương  $m$  là ước của một số hạng khác 0 nào đó của  $(x_n)$ .

*Việt Nam TST 2014*

**Lời giải**

Ta sẽ chứng minh rằng nếu các đa thức  $P(x), Q(x)$  thỏa mãn đề bài thì chúng đều có bậc bằng 1. Thật vậy:

Xét trường hợp một trong hai đa thức  $P(x), Q(x)$  là đa thức hằng.

(1) Nếu  $P(x) \equiv a, \forall x \in \mathbb{Z}$  thì  $(x_n)$  có dạng:

$$x_0 = 2014, x_1 = a, x_2 = Q(a), x_3 = a, \dots$$

Và dễ thấy mọi số hạng của dãy chỉ nhận một trong ba giá trị  $\{2014, a, Q(a)\}$ .

(2) Nếu  $Q(x) \equiv a, \forall x \in \mathbb{Z}$  thì  $(x_n)$  có dạng:

$$x_0 = 2014, x_1 = P(2014), x_2 = a, x_3 = P(a), \dots$$

Và dễ thấy mọi số hạng của dãy chỉ nhận một trong bốn giá trị  $\{2014, P(2014), a, P(a)\}$ .

Cả hai điều này đều không thỏa mãn điều kiện đề bài do mỗi số nguyên dương  $m$  phải là ước của một số hạng khác 0 nào đó của dãy số  $(x_n)$ .

Tiếp theo, nếu một trong hai đa thức  $P(x), Q(x)$  có bậc lớn hơn 1.



Không mất tính tổng quát, ta giả sử đó là  $Q(x)$  thì rõ ràng khi đó  $Q(P(x))$  cũng có bậc lớn hơn 1. Ta thấy nếu  $R(x)$  là đa thức có bậc lớn hơn 1 thì với mọi  $k > 0$  lớn tùy ý, tồn tại  $x$  có giá trị tuyệt đối đủ lớn sao cho  $|R(x)| > k|x|$ , điều này là dễ thấy do khi  $x \rightarrow +\infty$  thì

$$\text{ta có giới hạn } \lim_{x \rightarrow +\infty} \frac{|R(x)|}{|x|} = +\infty$$

Ta sẽ chứng minh rằng tồn tại  $N$  đủ lớn sao cho  $|Q(P(x))| > |P(x)| + |x|, \forall x > N$ .

Ta chỉ cần xét hai trường hợp. Nếu  $P(x)$  là bậc 1 thì dễ thấy tồn tại  $k$  đủ lớn sao cho  $k|P(x)| > |x|$ , với mọi  $x \in \mathbb{Z}$ .

Suy ra tồn tại  $N$  đủ lớn sao cho:

$$|Q(P(x))| > (k+1)|P(x)| = |P(x)| + k|P(x)| > |P(x)| + |x| \text{ với mọi } x > N$$

Nhận xét được chứng minh.

Theo giả thiết thì trong dãy số đã cho, phải tồn tại số hạng  $|x_i|$  lớn tùy ý và rõ ràng ta cũng phải có  $j > 0$  sao cho  $|x_{2j}| > N+1$  và  $x_{2j}$  có giá trị tuyệt đối lớn nhất trong  $2j$  số hạng đầu tiên của dãy  $(x_n)$ .

Thật vậy, ta thấy rằng, tồn tại vô số số hạng  $x_{2j}$  thỏa mãn điều kiện

$$|x_{2j}| = \max\{|x_k|\}, \forall k = \overline{0, 2j}$$

Gọi  $T$  là tập hợp các chỉ số thỏa mãn. Nếu như trong các số hạng như thế, không có số hạng nào thỏa mãn  $|x_{2j}| > N+1$  thì với mọi  $t \in T$

Ta có  $|x_i| \leq |x_t| \leq N+1$  với mọi  $i \leq t \in T$ .

Tuy nhiên, do  $|T|$  vô hạn nên điều giả sử ở trên là vô lý và nhận xét được chứng minh.

Với  $x_{2j}$  là số hạng thỏa mãn điều kiện trên, chọn  $m = |x_{2j+2} - x_{2j}|$  thì ta thấy

$$m = |Q(P(x_{2j})) - x_{2j}| \geq |Q(P(x_{2j}))| - |x_{2j}| > |P(x_{2j})| > |x_{2j}| \text{ và } |x_{2n+2}| = |Q(x_{2n+1})| > |x_{2n+1}|$$

Do đó, trong  $2j+1$  số hạng đầu tiên của dãy, không có số hạng nào chia hết cho  $m$ .

Mặt khác ta có:

$$x_{2k+2} - x_{2k} = (Q(P(x_{2k})) - Q(P(x_{2k-2}))) : (P(x_{2k}) - P(x_{2k-2})) : (x_{2k} - x_{2k-2}) = m$$

Và tương tự thì  $x_{2k+3} - x_{2k+1} = (P(x_{2k+2}) - P(x_{2k})) : (x_{2j} - x_{2j-2}) = m$

Từ đây suy ra với  $k \geq j$  thì  $x_{2k+2} - x_{2k}$  và  $x_{2k+3} - x_{2k+1}$  đều chia hết cho  $m$ , tuy nhiên  $x_{2j+1}$  và  $x_{2j+2}$  đều không chia hết cho  $m$  nên  $x_k$  không chia hết cho  $m$  với  $k > 2j+2$ .

Do đó, trong dãy đã cho không có số hạng nào chia hết cho  $m$ .

Điều mâu thuẫn này cho ta thấy nhận xét ban đầu là đúng và  $\deg(P(x)) = \deg(Q(x)) = 1$ .



Đặt  $P(x) = ax + b$  với  $|a| > 1$  và  $Q(x) = cx + d$  với  $a, b, c, d \in \mathbb{Z}$  và  $ab \neq 0$  thì ta có:

$$\begin{cases} x_{2n+1} = ax_{2n} + b \\ x_{2n+2} = cx_{2n+1} + d \end{cases}, \forall n \geq 0$$

Suy ra  $x_{2n+2} = cax_{2n} + bc + d$  và  $x_{2n+3} = cax_{2n+1} + ad + b$  với mọi  $n \geq 0$ .

Cả hai dãy này đều có công thức truy hồi dạng  $y_{n+1} = ky_n + h$  với  $k = ac, h \in \mathbb{Z}$ .

Giả sử  $k \neq 1$  thì công thức tổng quát của dãy này là  $y_n = k^n y_0 + h \left( \frac{k^n - 1}{k - 1} \right)$  với mọi  $n$ .

Rõ ràng nếu  $k = -1$  thì dãy số tương ứng không thỏa mãn, ta xét  $k \neq -1$ .

- Nếu  $h = 0$  thì ta có  $y_n = k^n y_0$ , rõ ràng không thỏa mãn điều kiện.
- Nếu  $h \neq 0$  thì do  $\left( k, \frac{k^n - 1}{k - 1} \right) = 1$  với mọi  $n$  nên giả sử  $t$  là số mũ lớn nhất mà  $k^t | h$  thì các số nguyên dương có dạng  $k^s$  với  $s > t$  đều không là ước của bất cứ số hạng nào của dãy, không thỏa mãn. Từ đây, suy ra  $k = 1$  hay  $ac = 1$ .

Cuối cùng, ta chỉ cần xét hai trường hợp:

**Trường hợp 1.** Nếu  $P(x) = x + a$  và  $Q(x) = x + b$  với  $a, b \in \mathbb{Z}$  thì bằng quy nạp, ta chứng minh được  $x_{2k} = 2014 + k(a + b)$  và  $x_{2k+1} = 2014 + a + k(a + b)$

Dễ thấy rằng nếu  $a + b = 0$  thì dãy này không thỏa mãn.

Nếu như  $a + b \neq 0$  thì gọi  $S, T, R$  lần lượt là tập hợp các ước nguyên của  $a + b, 2014$  và  $2014 + a$ .

**Ta xét các trường hợp sau:**

Với  $m \notin S$  thì giả sử  $a + b$  chia  $m$  dư  $t$  với  $t \neq 0$  do đó khi  $k$  chạy qua một hệ thặng dư đầy đủ mod  $m$  thì tồn tại một số hạng của dãy chia hết cho  $m$  và số lượng các số hạng như thế là vô hạn. Rõ ràng số các số hạng bằng 0 của dãy là hữu hạn, không quá hai nên tồn tại số hạng khác 0 của dãy chia hết cho  $m$ .

Với  $m \in S$  và  $m \notin T, R$  thì dãy số tương ứng không thỏa mãn.

Với  $m \in S$  và  $m \in T$  hoặc  $m \in R$  thì tương ứng, mọi số hạng có chỉ số chẵn hoặc mọi số hạng có chỉ số lẻ của dãy đều chia hết cho  $m$  và dễ thấy, tồn tại số hạng khác 0 của dãy chia hết cho  $m$ . Do đó, các số  $a, b$  phải thỏa mãn  $(S \setminus T) \cap (S \setminus R) = \emptyset$  hay mỗi ước của  $a + b$  phải là ước của 2014 hoặc là ước của  $2014 + a$ .

**Trường hợp 2.** Nếu  $P(x) = -x + a$  và  $Q(x) = -x + b$  thì cũng có lập luận tương tự vì các số hạng của dãy tương ứng khi đó là  $x_{2k} = 2014 - k(a - b)$  và  $x_{2k+1} = -2014 + a + k(a - b)$ .

Điều kiện của  $a, b$  là  $a - b \neq 0$  và mỗi ước của  $a - b$  phải là ước của 2014 hoặc là ước của  $a - 2014$ .

Vậy tất cả các đa thức  $P(x), Q(x)$  cần tìm là:



- $P(x) = x + a, Q(x) = x + b$  trong đó  $a, b \in \mathbb{Z}$  thỏa mãn  $a + b \neq 0$  và mỗi ước của  $a + b$  phải là ước của 2014 hoặc là ước của  $a + 2014$ .
- $P(x) = -x + a, Q(x) = -x + b$  trong đó  $a, b \in \mathbb{Z}$  thỏa mãn  $a - b \neq 0$  và mỗi ước của  $a - b$  phải là ước của 2014 hoặc là ước của  $a - 2014$ .

**Câu 87.** Chứng minh rằng không tồn tại đa thức

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x] \text{ bậc } n \geq 1$$

sao cho  $P(0), P(1), \dots$  đều là số nguyên tố.

*Lời giải*

Giả sử tồn tại đa thức thỏa mãn yêu cầu bài toán.

Khi đó,  $a_0 = P(0)$  là số nguyên tố.

Mặt khác, ta có  $a_0 \mid P(ka_0), \forall k = \overline{0, \infty}$ .

Nhưng vì  $P(ka_0)$  là số nguyên tố nên  $P(ka_0) = a_0, \forall k \geq 0$ .

Điều này suy ra đa thức  $Q(x) = P(a_0 x) - a_0$  có vô hạn nghiệm.

Dẫn đến  $Q(x) \equiv 0$  hay  $P(a_0 x) = a_0$ , mâu thuẫn với việc đa thức  $P(x)$  có bậc ít nhất là 1.

Vậy giả sử phản chứng là sai nên ta suy ra không tồn tại đa thức thỏa mãn yêu cầu bài toán.

**Câu 88.** Cho đa thức  $P(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, P(x) \in \mathbb{Z}[x]$  với  $a_0$  chẵn và  $a_{n-k} + a_k$  chẵn, với mọi  $k = \overline{1, n-1}$ . Giả sử  $P(x) = Q(x)R(x)$ , với  $Q(x), R(x)$  là các đa thức hệ số nguyên khác hằng,  $\deg(Q(x)) \leq \deg(R(x))$  và tất cả các hệ số của  $R(x)$  đều lẻ. Chứng minh rằng, đa thức  $P(x)$  có nghiệm nguyên.

*Lời giải*

Định nghĩa:  $\overline{P(x)} = x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_1} x + \overline{a_0}$  với  $\overline{a_i} \equiv a_i \pmod{2}, \forall i = \overline{1, n}$ .

Khi đó thì ta có  $\overline{P(x)} = \overline{Q(x)} \cdot \overline{R(x)}$

Đặt  $\deg(Q(x)) = r, \deg(R(x)) = s, r \leq s$  và  $Q(x) = x^r + \dots + b_1 x + b_0$ .

Khi đó nếu  $r > 1$  thì

$$x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_1} x + \overline{a_0} = (x^r + \overline{b_{r-1}} x^{r-1} + \dots + \overline{b_1} x + \overline{b_0}) (x^s + x^{s-1} + \dots + x + 1)$$

Đồng nhất hệ số của  $x^{r+1}$  và  $x^{s-1}$  thì ta được 
$$\begin{cases} \overline{a_{r+1}} = \overline{b_r} + \overline{b_{r-1}} + \dots + \overline{b_1} + \overline{b_0} \\ \overline{a_{s-1}} = \overline{b_r} + \overline{b_{r-1}} + \dots + \overline{b_1} + 1 \end{cases}$$

Vì  $\overline{a_{r+1}} = \overline{a_{s-1}}$  nên  $\overline{b_0} = 1$  hay  $Q(0)$  là số lẻ, vì  $R(0)$  là số lẻ nên dẫn đến  $P(0)$  là số lẻ, mà  $P(0) = a_0$  là số chẵn, điều này dẫn đến vô lý. Vậy  $r = 1$  chứng tỏ  $P(x)$  có nghiệm nguyên.



**Câu 89.** Chứng minh rằng với mọi số nguyên dương  $n$  thì đa thức  $P(x) = (x^2 + x)^{2^n} + 1$  là đa thức bất khả quy trên  $\mathbb{Z}$ .

*Romanian Team Selection Test 1998*

**Lời giải**

Với  $n = 0$  dễ dàng kiểm tra là đúng. Do đó ta giả sử  $n \geq 1$ . Ta liên kết mỗi đa thức

$$G(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

Với một đa thức  $\overline{G}(x) = \overline{a_n} x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_2[x]$

Với các hệ số lấy trong trường  $\mathbb{Z}_2$  modulo 2.

$$\text{Mà do } (x^2 + x + 1)^{2^n} = \left[ (x^2 + x)^2 + 1 \right]^{2^{n-1}} = \left[ (x^2 + x)^{2^2} + 1 \right]^{2^{n-2}} = \dots = (x^2 + x)^{2^n} + 1$$

$$\text{Nên suy ra } \overline{P}(x) = (x^2 + x + 1)^{2^n}$$

Bây giờ giả sử  $P(x)$  khả quy, tức là có thể phân tích được  $P(x) = G(x)H(x)$  với  $G(x), H(x) \in \mathbb{Z}[x]$ .

Từ đây ta suy ra  $\overline{P}(x) = \overline{G}(x) \cdot \overline{H}(x)$ , lại vì  $x^2 + x + 1$  là đa thức bất khả quy trên  $\mathbb{Z}_2$  nên suy

$$\text{ra } \overline{G}(x) = (x^2 + x + 1)^p, \overline{H}(x) = (x^2 + x + 1)^{2^n - p}, 1 \leq p \leq 2^n - 1$$

$$\text{Điều này dẫn đến } \begin{cases} G(x) = (x^2 + x + 1)^p + 2U(x) \\ H(x) = (x^2 + x + 1)^{2^n - p} + 2V(x) \end{cases}$$

Với  $U(x), V(x)$  là các đa thức hệ số nguyên. Gọi  $\alpha$  là một nghiệm của phương trình  $x^2 + x + 1 = 0$ .

Thay  $x$  bởi  $\alpha$  trong đẳng thức:

$$P(\alpha) = (\alpha^2 + \alpha)^{2^n} + 1 = \left[ (\alpha^2 + \alpha + 1)^p + 2U(\alpha) \right] \left[ (\alpha^2 + \alpha + 1)^{2^n - p} + 2V(\alpha) \right]$$

$$\text{Thì ta nhận được } 2 = 2U(\alpha) \cdot 2V(\alpha) \Rightarrow U(\alpha)V(\alpha) = \frac{1}{2}$$

Nhưng ta nhận thấy rằng  $U(x) \cdot V(x)$  là đa thức hệ số nguyên và  $\alpha^2 = -\alpha - 1$  nên  $U(\alpha)V(\alpha)$  là một số phức có dạng  $a + b\alpha, a, b \in \mathbb{Z}$ .

Do đó đẳng thức  $U(\alpha)V(\alpha) = \frac{1}{2}$  không thể xảy ra.

Vậy điều giả sử là sai và từ đó ta có điều phải chứng minh.



**Câu 90.** Giả sử  $n$  là số tự nhiên lớn hơn hoặc bằng 2 và  $P(x) = x^n - a_{n-1}x^{n-1} + \dots + a_1x + 1$  là đa thức hệ số nguyên dương. Giả sử  $a_k = a_{n-k}$  với mọi  $k = \overline{1, n-1}$ . Chứng minh rằng tồn tại vô hạn cặp số nguyên dương  $(x, y)$  sao cho:  $\begin{cases} y|P(x) \\ x|P(y) \end{cases} (*)$ .

### Lời giải

Trước tiên, ta nhận thấy rằng  $(1, P(1))$  là một cặp số thỏa mãn  $(*)$ .

Giả sử có một số hữu hạn các cặp số nguyên dương  $(x, y)$  thỏa mãn yêu cầu bài toán, ta chọn cặp  $(x, y)$  với  $x \leq y$  và  $y$  có giá trị lớn nhất.

Ta chứng minh cặp  $\left(y, \frac{P(y)}{x}\right)$  cũng thỏa mãn  $(*)$

Do  $(x, y)$  thỏa mãn  $(*)$  nên có  $\frac{P(y)}{x} \in \mathbb{Z}^+$  hiển nhiên  $\frac{P(y)}{x} | P(y)$

Ta cần chứng minh  $y | P\left(\frac{P(y)}{x}\right)$  (1)

Do  $y | P(x) \Rightarrow (x, y) = 1$  suy ra tồn tại  $z$  sao cho  $xz \equiv 1 \pmod{y}$ .

Theo tính chất  $a - b | P(a) - P(b)$  thì ta có  $\frac{P(y)}{z} - zP(y) | P\left(\frac{P(y)}{x}\right) - P(zP(y))$  (2)

Nhưng do  $\frac{P(y)}{x} - zP(y) = \frac{P(y) - xzP(y)}{x}$

Vì  $xz \equiv 1 \pmod{y}$  nên  $y | P(y) - xzP(y)$ . Ngoài ra  $x | P(y) - xzP(y)$  do  $x | P(y)$

Mà  $(x, y) = 1$  nên ta có  $y | \frac{P(y) - xzP(y)}{x}$

Từ đó theo (2) thì ta được  $P\left(\frac{P(y)}{x}\right) \equiv P(zP(y)) \equiv P(z) \pmod{y}$ , do  $P(y) \equiv 1 \pmod{y}$

Vì  $a_k = a_{n-k}$  nên ta suy ra  $x^n P\left(\frac{1}{x}\right) = P(x) \Rightarrow y | x^n P\left(\frac{1}{x}\right) \Rightarrow y | P(z)$

Hay  $y | P\left(\frac{P(y)}{x}\right)$ . Vậy cặp  $\left(y, \frac{P(y)}{x}\right)$  thỏa mãn yêu cầu bài toán.

Ngoài ra thì ta có  $P(y) > y^n + 1 > y^2 \geq yx \Rightarrow \frac{P(y)}{x} > y$

Mâu thuẫn với cách chọn  $y$  là lớn nhất.

Vậy điều giả sử là sai và từ đó ta có điều phải chứng minh.





**Câu 91.** Chứng minh rằng, với mỗi số nguyên dương  $n$  tồn tại đa thức  $P(x) \in \mathbb{Z}[x]$  bậc  $n$  sao cho  $P(0), P(1), \dots, P(n)$  phân biệt và tất cả các số đó đều có dạng

$$2 \cdot 2019^k + 3, k \in \mathbb{Z}^+.$$

### Lời giải

Bài toán chứng minh tồn tại đa thức, do đó phải chỉ ra đa thức thỏa mãn. Hãy để ý đến yêu cầu  $P(0), P(1), \dots, P(n)$  nhận giá trị đặc biệt, do đó bài toán này mang tư tưởng của **nội suy Lagrange**. Tuy nhiên không hoàn toàn là **nội suy Lagrange**, vì các giá trị của chúng chỉ có dạng chứ không có giá trị cụ thể. Do đó ta sẽ lấy đa thức đơn giản nhất của nội suy

$$\text{là } P(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + \dots + a_n \binom{x}{n}, a_i \in \mathbb{Z}, \forall i = \overline{1, n}$$

Lưu ý rằng đa thức  $P(x)$  trên nhận giá trị nguyên, nhưng hệ số của chúng là hữu tỉ. Rõ ràng muốn kết quả của chúng có dạng  $2 \cdot 2019^k + 3$ , đặt  $a = 2019$  thì dạng  $2a^k + 3$ . Do đó việc đầu tiên là cho các số  $P(i)$  có dạng  $a^k$  đã. Dẫn đến các hệ số  $a_0, a_1, \dots, a_n$  là hằng số được không? Nếu chúng là hằng số thì  $P(x) = k \cdot 2^x$  lại không được dạng mong muốn. Nhưng ý trên cho ta suy nghĩ, để các hệ số  $a_i$  cùng tham gia vào **khai triển Newton**. Do đó ta sẽ chọn  $a_i = (a^k - 1)^i$ .

Khi đó, với  $x = \overline{0, n}$  thì ta được:

$$P(x) = (a^k - 1)^0 + (a^k - 1)^1 \binom{x}{1} + \dots + (a^k - 1)^n \binom{x}{n} = [(a^k - 1) + 1]^n = a^{kn}$$

Đến đây thì ta gần thu được kết quả mong muốn. Vì khi đó ta chỉ cần chọn đa thức  $Q(x) = 2P(x) + 3$  thì sẽ có được đa thức thỏa mãn bài toán. Tuy nhiên đã đúng chưa? Hãy lưu ý rằng đa thức  $P(x)$  hệ số hữu tỉ nên đa thức  $Q(x)$  cũng có hệ số hữu tỉ. vậy ta phải cải tiến để đa thức  $Q(x)$  có hệ số nguyên. Lưu ý rằng đa thức  $P(x)$  hệ số hữu tỉ, với các hệ số có mẫu lớn nhất là  $n_1$ . Do đó ta sẽ phải nhân vào, nhưng không làm thay đổi một lượng. Lưu ý các hệ số của  $P(x)$  đều có nhân thêm  $(a^k - 1)$ . Vậy phải chọn  $k$  như thế nào? Chọn làm sao để  $(a^k - 1)$  chia hết cho  $n!$ . Việc này quá to tát, không thể được? Tuy nhiên ta sẽ chọn được  $k$  để  $(a^k - 1)$  chia hết cho một phần tử nào đó của  $n!$ . Liên quan đến lũy thừa ta nghĩ ngay đến **định lý Euler**. Phân tích  $n! = n_1 \cdot n_2$  trong đó  $n_1$  là ước nguyên tố lớn nhất của  $n!$  mà nguyên tố cùng nhau với  $a$ , khi đó tất nhiên  $n_2$  và  $a$  cũng có chung ước nguyên tố.

Khi đó thì ta có  $a^{\varphi(n_1)} \equiv 1 \pmod{n_1}$

Do đó ta chọn  $k = \varphi(n_1)$  thì  $n_1 \mid a^k - 1$ .





Tiếp đến ta phân tích  $n_2 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_i^{\alpha_i}$

Đặt  $s = \max\{\alpha_1, \alpha_2, \dots, \alpha_i\}$  thì  $n_2$  và  $a$  có chung ước nguyên tố  $p_1, p_2, \dots, p_i$  nên  $n_2 | s$ .

Từ đây dẫn đến  $n! | a^s (a^k - 1)$

Đến đây thì bài toán được sang tỏ, bằng cách lấy  $Q(x) = 2a^s P(x) + 3$

Với  $P(x) = \sum_{i=0}^n \binom{x}{i} (a^k - 1)^i$  là đa thức chúng ta cần tìm.

**Câu 92.** Chứng minh rằng tồn tại tập vô hạn các điểm  $\{..., P_{-3}, P_{-2}, P_{-1}, P_0, P_1, P_2, P_3, \dots\}$  trong mặt phẳng thỏa mãn tính chất: Với ba số nguyên  $a, b, c$  phân biệt thì các điểm  $P_a, P_b, P_c$  thẳng hàng khi và chỉ khi  $a + b + c = 2014$ .

USA MO 2014 Problem 3

### Lời giải

Trước hết, ta có thể đặt  $a_1 = a - 671, b_1 = b - 671, c_1 = c - 671$  ta có thể đưa điều kiện bài toán về thành  $a + b + c = 1$ .

Một điểm  $P_i(f(i), g(i))$  gồm hai thành phần hoành độ và tung độ. Để chứng minh tồn tại dãy vô hạn, ý tưởng tự nhiên là đi tìm biểu diễn tường minh cho hai hàm  $f(i)$  và  $g(i)$ .

Và tìm sự biểu diễn hợp lý nhất, đơn giản nhất chính là tìm trong lớp hàm đa thức.

Trước tiên, ta sẽ tìm điều kiện để  $P_a, P_b, P_c$  thẳng hàng.

Ta có  $P_a(f(a), g(a)), P_b(f(b), g(b)), P_c(f(c), g(c))$

Khi đó thì ta được 
$$\begin{cases} \overline{P_a P_b} = (f(b) - f(a), g(b) - g(a)) \\ \overline{P_a P_c} = (f(c) - f(a), g(c) - g(a)) \end{cases}$$

Khi đó ba điểm  $P_a, P_b, P_c$  thẳng hàng khi và chỉ khi  $\frac{f(c) - f(a)}{f(b) - f(a)} = \frac{g(c) - g(a)}{g(b) - g(a)}$

Dẫn đến 
$$\begin{aligned} f(b)g(c) - f(b)g(c) - f(a)g(c) + f(a)g(a) \\ = f(c)g(b) - f(c)g(a) - f(a)g(b) + f(a)g(a) \end{aligned}$$

Đến đây ta đặt:

$$F(a, b, c) = f(a)g(b) + f(b)g(c) + f(c)g(a) - (f(a)g(c) + f(c)g(b) + f(b)g(a))$$

Khi đó  $F(a, b, c)$  là đa thức ba biến và  $F(a, a, c) = F(a, b, b) = F(a, b, a)$  dẫn đến

$$F(a, b, c) = (a - b)(b - c)(c - a)G(a, b, c)$$

Mặt khác chúng ta muốn ba điểm  $P_a, P_b, P_c$  thẳng hàng khi và chỉ khi  $a + b + c = 1$  hay ta dịch qua ngôn ngữ của đa thức là  $F(a, b, c) = 0$  khi và chỉ khi  $a + b + c = 1$ .

Điều này cho ta thêm một nhân tử của  $F(a, b, c)$  khi đó thì

$$F(a, b, c) = (a + b + c - 1)(a - b)(b - c)(c - a)G(a, b, c)$$



Để đa thức này đơn giản nhất thì ta chọn  $G(a, b, c) = 1$ , khi đó thì

$$F(a, b, c) = (a + b + c - 1)(a - b)(b - c)(c - a)$$

Khai triển đa thức này, dẫn ta đến tìm đa thức  $f(x)$  và  $g(x)$  sao cho

$$f(a)g(b) - f(b)g(a) = ab^3 - a^3b + a^2b - ab^2 = a(b^3 - b^2) - b(a^3 - a^2)$$

Đồng nhất thì ta chọn  $f(x) = x, g(x) = x^3 - x^2$ , khi đó thì các điểm  $P_i$  của đề bài ban đầu có tọa độ là  $P_i = (i - 671, (i - 671)^3 - (i - 671)^2)$

Từ đây ta dễ dàng suy ra rằng, tồn tại tập vô hạn điểm thỏa mãn đề bài.

**Câu 93.** Cho  $x_1 < x_2 < \dots < x_n$  là  $n, n \geq 3$  số thực thỏa mãn:

$$x_2 - x_1 < x_3 - x_2 < x_4 - x_3 < \dots < x_n - x_{n-1}$$

Giả sử đa thức  $P(x)$  có  $n$  nghiệm thực là các giá trị  $x_1, x_2, \dots, x_n$ . Chứng minh rằng giá trị lớn nhất của  $|P(x)|$  đạt được tại một điểm  $x_0 \in [x_{n-1}, x_n]$ .

*Russia All – Russian Olympiad 2010*

#### Lời giải

Vì đa thức  $P(x)$  có  $n$  nghiệm là  $x_1, x_2, \dots, x_n$  nên  $P(x) = a(x - x_1)(x - x_2) \dots (x - x_n)$

Do đó bài toán quy về tìm giá trị lớn nhất của  $A = |x - x_1||x - x_2| \dots |x - x_n|, \forall x \in [x_1, x_n]$

Giả sử phản chứng  $A$  đạt max tại  $x_0 \in [x_{i-1}, x_i]$  với  $i = \overline{2, n-1}$ . Khi đó ta tính tiến giá trị này về  $\zeta = x_{n-1} + x_i - x_0$  thì

- $\zeta \geq x_{n-1}$  vì  $x_i - x_0 \geq 0$  do  $x_0 \in [x_{i-1}, x_i]$ .
- $\zeta \leq x_n$  vì  $x_{n-1} + x_i - x_0 \leq x_n \Leftrightarrow x_i - x_0 \leq x_n - x_{n-1}$  điều này đúng do giả thiết thì

$$x_i - x_0 \leq x_i - x_{i-1} < x_n - x_{n-1}$$

Ta có  $x_0 - x_k < \zeta - x_k, \forall k = \overline{1, i-2}$ .

Vì  $x_0 - x_k \leq x_i - x_k$  ( $x_0 \leq x_i$ )  $< \zeta - x_k$  ( $x_i < x_{n-1} < \zeta$ )

Ta có  $|x_0 - x_{n-1}| = x_{n-1} - x_0 \leq \zeta - x_i$  vì  $\zeta - x_{n-1} = x_i - x_0$ .

Tương tự thì ta có  $|x_0 - x_{n-2}| = x_{n-2} - x_0 < \zeta - x_{i+1}$

Vì  $\zeta - x_{n-2} = x_{n-1} - x_{n-2} + x_i - x_0 > x_{i+1} - x_0 \Leftrightarrow x_{n-1} - x_{n-2} > x_{i+1} - x_i$  đúng theo giả thiết.

Tiếp tục như vậy thì ta có  $|x_0 - x_{n-3}| = x_{n-3} - x_0 < \zeta - x_{i+3}, \dots$

Tổng quát luôn thì ta được  $\zeta - x_k \geq x_{n-1+i-k} - x_0 \geq 0, \forall k = \overline{i, n-1}$

Cuối cùng thì  $(x_n - \zeta)(\zeta - x_{i-1}) > (x_n - x_0)(x_0 - x_{i-1})$  (\*)

Thật vậy (\*) khai triển ra thì được:



$$\begin{aligned}
 (*) &\Leftrightarrow x_n \zeta - x_n x_{i-1} - \zeta^2 + \zeta x_{i-1} > x_n x_0 - x_n x_{i-1} - x_0^2 + x_0 x_{i-1} \\
 &\Leftrightarrow x_n (\zeta - x_0) > \zeta^2 - x_0^2 - x_{i-1} (\zeta - x_0) \\
 &\Leftrightarrow x_n > \zeta + x_0 - x_{i-1} \text{ do } \zeta - x_0 > 0 \\
 &\Leftrightarrow x_n > x_{n-1} + x_i - x_i + x_0 - x_{i-1} \\
 &\Leftrightarrow x_n - x_{n-1} > x_i - x_{i-1} \text{ (True)}
 \end{aligned}$$

Kết hợp tất cả các điều trên thì ta được:

$$\begin{aligned}
 &|(\zeta - x_1) \dots (\zeta - x_{i-2})| \cdot |(\zeta - x_{n-1}) \dots (\zeta - x_i)| \cdot |(\zeta - x_{i-1}) \dots (\zeta - x_n)| \\
 &= (\zeta - x_1) \dots (\zeta - x_{i-2}) (\zeta - x_{n-1}) \dots (\zeta - x_i) (\zeta - x_{i-1}) (x_n - \zeta) \\
 &> (x_0 - x_1) \dots (x_0 - x_{i-2}) (x_{n-1} - x_0) \dots (x_i - x_0) (x_0 - x_{i-1}) (x_n - x_0) \\
 &= |(x_0 - x_1) \dots (x_0 - x_{i-2})| \cdot |(x_0 - x_{n-1}) \dots (x_0 - x_i)| \cdot |(x_0 - x_{i-1}) \dots (x_0 - x_n)|
 \end{aligned}$$

Điều này mâu thuẫn với giả sử  $A$  đạt giá trị lớn nhất tại  $x_0$

Vậy điều giả sử là sai hay từ đó ta suy ra được điều phải chứng minh.

**Câu 94.** Cho  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  là đa thức hệ số nguyên thỏa mãn điều kiện  $P(r) = P(s) = 0$  trong đó  $r, s$  là các số nguyên thỏa mãn điều kiện  $0 < r < s$ . Chứng minh rằng tồn tại  $k \in \{0, 1, 2, \dots, n\}$  sao cho  $a_k \leq -s$ .

#### Lời giải

Do  $P(s) = 0$  nên  $P(x) = (x - s)Q(x)$ ,  $Q(x) \in \mathbb{Z}[x]$ ,  $\deg(Q(x)) = n - 1$

Đặt  $Q(x) = x^t R(x)$ , với  $R(0) \neq 0$ ,  $t \in \mathbb{N}$ ,  $R(x) \in \mathbb{Z}[x]$ ,  $\deg(R(x)) = n - t - 1$  với biểu thức tường minh của  $R(x)$  là  $R(x) = b_{n-t-1} x^{n-t-1} + \dots + b_1 x + b_0$

Khi đó thì  $0 = P(r) = (r - s)r^t R(r) \Rightarrow R(r) = 0$

Chứng tỏ  $R(x)$  có nghiệm nguyên dương  $r$  khi đó bắt buộc các hệ số của  $R(x)$  phải đổi dấu.

- **Trường hợp 1.** Nếu  $b_0 > 0$  thì khi đó  $P(x) = (x - s)x^t (b_{n-t-1} x^{n-t-1} + \dots + b_1 x + b_0)$

Đến đây thì  $a_t = -s b_0 \leq -s$ , tức  $a_t$  chính là hệ số cần tìm.

- **Trường hợp 2.** Nếu  $b_0 < 0$  do các hệ số của  $R(x)$  phải đổi dấu nên sẽ tồn tại  $i \in \{0, 1, \dots, n - t - 2\}$  sao cho:  $b_i < 0 < b_{i+1}$

Ta viết lại như sau:  $P(x) = (x - s)x^t (b_{n-t-1} x^{n-t-1} + \dots + b_{i+1} x^{i+1} + b_i x^i + \dots + b_1 x + b_0)$

Khi đó thì ta được  $a_{t+i+1} = b_i - s b_{i+1} \leq -s$  hay  $a_{t+i+1}$  chính là hệ số cần tìm

Vậy trong mọi trường hợp đều tồn tại  $k \in \{0, 1, 2, \dots, n\}$  sao cho  $a_k \leq -s$ .

**Câu 95.** Cho  $P(x), Q(x)$  là các đa thức hệ số nguyên. Đặt  $a_n = n! + n$ . Chứng minh rằng nếu  $\frac{P(a_n)}{Q(a_n)} \in \mathbb{Z}, \forall n$  thì  $\frac{P(n)}{Q(n)} \in \mathbb{Z}, \forall n$  và  $Q(n) \neq 0$ .

*Canadian Mathematical Olympiad 2010*

*Lời giải*

Chia đa thức  $P(x)$  cho  $Q(x)$  thì ta được  $\frac{P(x)}{Q(x)} = A(x) + \frac{R(x)}{Q(x)}$

Trong đó:  $A(x), R(x)$  là các đa thức hệ số hữu tỉ và  $R(x) \equiv 0$  hoặc

$$\deg(R(x)) < \deg(Q(x)).$$

Quy đồng tất cả các hệ số của đa thức  $A(x)$  thì ta có thể viết  $A(x) = \frac{B(x)}{b}$ ,

Với  $B(x)$  là đa thức hệ số nguyên, còn  $b$  là bội chung nhỏ nhất của tất cả các mẫu số của các hệ số trong  $A(x), b > 0$ .

Nếu  $R(x)$  không đồng nhất 0 thì, với chú ý nếu  $k$  nguyên thì hoặc  $A(k) = 0$  hoặc  $|A(k)| \geq \frac{1}{b}$ .

Nhưng với  $|k|$  đủ lớn thì  $0 < \left| \frac{R(k)}{Q(k)} \right| < \frac{1}{b}$

Dẫn đến với  $n$  đủ lớn thì  $\frac{P(a_n)}{Q(a_n)}$  không thể là số nguyên nên ta phải có  $R(x) \equiv 0$ .

Khi đó thì  $\frac{P(x)}{Q(x)} = \frac{B(x)}{b}$  biểu diễn này với những giá trị  $x$  mà  $Q(x) \neq 0$ .

Bây giờ với  $n_0$  là số nguyên cho trước, khi đó tồn tại vô hạn số nguyên dương  $k$  sao cho:

$$a_k \equiv n \pmod{b}$$

Có thể lấy các giá trị  $k = tn_0b + n_0, t \in \mathbb{Z}^+$ , với  $t$  nguyên dương đủ lớn thì  $k$  là số nguyên dương.

Khi đó thì  $\frac{B(a_k)}{b}$  là số nguyên hay  $b \mid B(a_k)$

Từ đó suy ra  $b \mid B(n)$  dẫn đến  $\frac{P(n)}{Q(n)}$  là một số nguyên.

Vậy từ đây ta có điều phải chứng minh.



**Câu 96.** Cho  $P(x)$  là đa thức bậc  $n \geq 5$  với hệ số nguyên và

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

Giả sử  $P(x)$  có  $n$  nghiệm nguyên phân biệt là  $0, \alpha_2, \dots, \alpha_n$ . Tìm tất cả các số nguyên  $k$  sao cho thỏa mãn  $P(P(k)) = 0$ .

*French Team Selection Test 2005*

### Lời giải

Nếu số nguyên  $k$  mà  $P(P(k)) = 0$  thì chứng tỏ  $P(k)$  là một nghiệm của  $P(x)$ . Nhưng các nghiệm nguyên của  $P(x)$  đã cho là  $0, \alpha_2, \dots, \alpha_n$ . Do đó phải có  $P(k) \in \{0, \alpha_2, \dots, \alpha_n\}$ . Ta phân tích  $P(k)$  dưới dạng:

$$P(x) = a_n x(x - \alpha_2) \dots (x - \alpha_n)$$

- Nếu  $P(k) = 0$  chứng tỏ  $k$  là một nghiệm của  $P(k)$  khi đó  $k \in \{0, \alpha_2, \dots, \alpha_n\}$ .
- Nếu  $P(k) = \alpha_2$  khi đó thì  $a_n k(k - \alpha_2) \dots (k - \alpha_n) = \alpha_2$  (\*).

Từ (\*) thì  $k \neq 0, k \neq \alpha_2, \dots, k \neq \alpha_n$  ta cũng có  $k - \alpha_i \neq k - \alpha_j$  với mọi  $i \neq j$

Mặt khác vì  $k \geq 5$  nên  $|\alpha_2| = |\alpha_n| \cdot |k| \cdot |k - \alpha_2| \cdot |k - \alpha_3| \dots |k - \alpha_n|$

$$\geq |k| \cdot |k - \alpha_2| \cdot |k - \alpha_3| \cdot |k - \alpha_4| \cdot |k - \alpha_5| \geq 4 = 1.1.2.|-1|.|-2|$$

Vì  $k - \alpha_2 \neq k - \alpha_3 \neq k - \alpha_4 \neq k - \alpha_5$  và  $|k|$  có thể bằng với một trong số  $|k - \alpha_i|$  với  $i = \overline{1, 5}$

Từ đó  $|\alpha_2| \geq 4$  mặt khác từ (\*) thì ta được  $|\alpha_2| \cdot |k| \cdot |k - \alpha_2| \Rightarrow \begin{cases} |\alpha_2| \cdot |k| \\ |\alpha_2| \cdot |k - \alpha_2| \end{cases}$

Mặt khác  $|k| \neq |\alpha_2|$  và  $|k - \alpha_2| \neq |\alpha_2|$  đẳng thức nếu có xảy ra thì  $k = 2\alpha_2$  tuy nhiên lại mâu thuẫn với (\*) do đó ta phải có  $2|k| \leq |\alpha_2|, 2|k - \alpha_2| \leq |\alpha_2|$

Nhưng từ đây ta suy ra  $|k| \cdot |k - \alpha_2| = \frac{|\alpha_2^2|}{4} = |\alpha_2| \cdot \frac{|\alpha_2|}{4} \geq |\alpha_2|$  do  $|\alpha_2| \geq 4$

Nhưng từ đây theo (\*) thì  $|a_n (k - \alpha_3)(k - \alpha_4) \dots (k - \alpha_n)| = \frac{|\alpha_2|}{|k(k - \alpha_2)|} \leq 1$

Nhưng cũng theo (\*) thì  $|a_n (k - \alpha_3)(k - \alpha_4) \dots (k - \alpha_n)| \geq |k - \alpha_3| \cdot |k - \alpha_4| \cdot |k - \alpha_5|$   
 $\geq 2 = 1.1.2 = 1.|-1|.|-2| = 1.|-1|.2 = 1.1.|-2|$

Hai kết quả trên là mâu thuẫn với nhau.

Chứng tỏ không tồn tại số nguyên  $k$  để  $P(k) = \alpha_2$ . Hoàn toàn tương tự, ta cũng chứng minh được không tồn tại số nguyên  $k$  để  $P(k) = \alpha_i, \forall i = \overline{2, n}$ .

Từ đó suy ra các số nguyên  $k$  cần tìm là  $k \in \{0, \alpha_2, \dots, \alpha_n\}$ .



**Câu 97.** Tìm số nguyên dương  $n$  nhỏ nhất sao cho tồn tại đa thức  $P(x)$  bậc  $n$  có hệ số nguyên thỏa mãn:  $P(0)=0, P(1)=1$  và với mọi  $\lambda \in \mathbb{N}^*$  thì

$$(P(\lambda)-2)(P(\lambda)-1)P(\lambda) \text{ là bội của } p \text{ với } p \text{ là số nguyên tố}$$

Doãn Quang Tiến

### Lời giải

Ta sẽ chứng minh  $n \geq p-1$  thỏa mãn yêu cầu bài toán.

Ta sẽ giả sử phản chứng rằng  $1 \leq n \leq p-2$  và tồn tại đa thức  $P(x)$  thỏa mãn bài toán.

Từ đây, ta sử dụng **công thức nội suy Lagrange** thì ta được:

$$P(x) = \sum_{k=0}^{p-2} P(k) \prod_{i=0, i \neq k}^{p-2} \frac{x-i}{k-i}$$

$$\text{Từ đây ta suy ra } P(p-1) = \sum_{k=0}^{p-2} P(k) \prod_{i=0, i \neq k}^{p-2} \frac{p-1-i}{k-i} = \sum_{k=0}^{p-2} (-1)^{k+1} P(k) C_{p-1}^k \quad (1)$$

Bây giờ, ta sẽ đi chứng minh một kết quả sau  $C_{p-1}^k \equiv (-1)^k \pmod{p}, \forall k = \overline{0, p-2}$

Ta sẽ chứng minh một cách nhanh chóng bằng phương pháp quy nạp như sau:

Với  $k=0$  thì  $C_{p-1}^0 = 1 \equiv (-1)^0 = 1 \pmod{p}$  điều này là hiển nhiên.

Giả sử mệnh đề đúng với  $k$  tức là ta có  $C_{p-1}^k \equiv (-1)^k \pmod{p}$ , ta sẽ chứng minh mệnh đề cũng đúng với  $k+1$ .

Mà ta có kết quả cơ bản của hệ số nhị thức như sau:  $C_{p-1}^{k+1} = C_p^{k+1} - C_{p-1}^k$  nên từ đó ta suy ra:

$$C_{p-1}^{k+1} = C_p^{k+1} - C_{p-1}^k \equiv 0 - (-1)^k = (-1) \cdot (-1)^k = (-1)^{k+1} \pmod{p}$$

Vậy từ đó theo nguyên lý quy nạp toán học thì kết quả trên được chứng minh.

Từ đây, kết hợp với kết quả của (1) thì ta được:

$$\begin{aligned} P(p-1) &= \sum_{k=0}^{p-2} (-1)^{k+1} P(k) C_{p-1}^k \equiv \sum_{k=0}^{p-2} (-1)^{k+1} P(k) (-1)^k \\ &= \sum_{k=0}^{p-2} (-1)^{2k+1} P(k) = - \sum_{k=0}^{p-2} P(k) \pmod{p} \Leftrightarrow \sum_{k=0}^{p-1} P(k) \equiv 0 \pmod{p} \quad (2) \end{aligned}$$

$$\text{Nhưng mà ta có } \sum_{k=0}^{p-1} P(k) = P(0) + P(1) + \sum_{k=2}^{p-1} P(k) = 1 + \sum_{k=2}^{p-1} P(k)$$

do giả thiết cho  $P(0)=0, P(1)=1$ .

Và từ giả thiết bài toán là  $(P(\lambda)-2)(P(\lambda)-1)P(\lambda)$  là bội của  $p$  nên ta suy ra được:

$$P(k) \equiv 0, 1, 2 \pmod{p}, \forall k = \overline{2, p-1}$$

$$\text{Do đó ta suy ra được } \sum_{k=0}^{p-1} P(k) = 1 + \sum_{k=2}^{p-1} P(k) \equiv 1, p-1, 2p-3 \not\equiv 0 \pmod{p}$$

Ta thấy điều này là hoàn toàn mâu thuẫn với (2)



Vậy giả sử phản chứng là sai nên ta phải có  $n \geq p-1$ .

Với  $n = p-1$  ta xét  $P(x) = x^{p-1}$  thỏa mãn yêu cầu bài toán.

Do đó giá trị nhỏ nhất của  $n$  là  $p-1$  và ta hoàn tất bài toán.

**Câu 98.** Chứng minh rằng với mọi  $m \in \mathbb{N}$  tồn tại đa thức  $P_m(x)$  có hệ số hữu tỉ thỏa mãn với mọi  $n \in \mathbb{N}^*$  thì  $1^{2m+1} + 2^{2m+1} + \dots + n^{2m+1} = P_m(n(n+1))$

Đề chọn đội tuyển VMO Đà Nẵng 2017

*Lời giải*

- Với  $m=0$  thì ta chọn được đa thức  $P_0(x) = \frac{x}{2}$
- Với  $m=1$  thì ta chọn được đa thức  $P_1(x) = \frac{x^2}{4}$
- Giả sử khẳng định đúng đến  $m-1$  thì ta xét đa thức:  

$$\varphi(x) = x(x^2 - 1^2)(x^2 - 2^2) \dots (x^2 - m^2) = x^{2m+1} - a_{m-1}x^{2m-1} - a_{m-2}x^{2m-3} - \dots - a_0x$$

$$\Leftrightarrow \varphi(x) + a_{m-1}x^{2m-1} + a_{m-2}x^{2m-3} + \dots + a_0x = x^{2m+1}$$

Thay  $x$  lần lượt bởi  $1, 2, \dots, n$  thì ta được:

$$\sum_{i=1}^n \varphi(i) + \sum_{i=0}^{m-1} a_i P_i(n(n+1)) = \sum_{i=1}^n i^{2m+1} \quad (*)$$

Mà ta có  $\varphi(x) = x(x-1)(x+1) \dots (x-m)(x+m) = (x-m)(x-m+1) \dots (x+m-1)(x+m)$

$$\text{Lại có } \varphi(x) = \frac{1}{2m+2} [\varphi(x)(x+m+1) - \varphi(x)(x-m-1)]$$

Bây giờ ta đặt:

$$\begin{aligned} d(x-m) &= (x+m+1)\varphi(x) = (x-m)(x-m+1) \dots (x+m+1) \\ \Rightarrow d(x-m-1) &= (x-m-1)(x-m) \dots (x+m) = (x-m-1)\varphi(x) \\ \Rightarrow \varphi(x) &= \frac{1}{2m+2} [d(x-m) - d(x-m-1)] \end{aligned}$$

$$\text{Do đó thì ta được } \sum_{i=1}^n \varphi(i) = \frac{1}{2m+2} [d(n-m) - d(-m)]$$

$$= \frac{1}{2m+2} d(n-m) = \frac{1}{2m+2} (n-m)(n-m+1) \dots (n+m+1)$$

Mà ta có  $(n-i)(n+i+1) = n^2 - i^2 + n - i = n(n+1) - i(i+1), \forall i = \overline{0, m}$

$$\text{Từ đây suy ra } \sum_{i=1}^n \varphi(i) = \frac{1}{2m+2} \prod_{i=0}^m [n(n+1) - i(i+1)] = Q_m(n(n+1)).$$

Khi đó  $Q_m$  là đa thức có hệ số hữu tỉ và từ (\*) ta chọn:

$$P_m(x) = Q_m(x) + a_{m-1}P_{m-1}(x) + a_{m-2}P_{m-2}(x) + \dots + a_0P_0(x)$$

Và từ đây ta có điều phải chứng minh.



**Câu 99.** Cho  $P(x), Q(x), R(x)$  là ba đa thức hệ số thực thỏa mãn:

$$P(Q(x)) + P(R(x)) = c, \forall x \in \mathbb{R} \text{ với } c = \text{const} \in \mathbb{R}$$

Chứng minh rằng:  $P(x)$  là hằng số hoặc  $(Q(x) + R(x))$  là hằng số.

*Đề chọn đội tuyển VMO Hà Nam 2017*

**Lời giải**

Bỏ qua trường hợp tầm thường  $P(x)$  là hằng số.

Bây giờ ta xét

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_n \neq 0, n \geq 1$$

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

$$R(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 x + c_0$$

Giả sử ta có  $m \geq k$  thì từ:

$$P(Q(x)) + P(R(x)) = c, \forall x \in \mathbb{R} \text{ với } c = \text{const} \in \mathbb{R} \quad (*)$$

Đồng nhất hệ số bậc cao nhất của  $(*)$  thì ta được:  $a_n b_m^n = 0$ .

Do đó hoặc  $b_m = 0$  suy ra  $\deg(R(x)) = \deg(Q(x)) = 0$  hoặc  $m = k$ .

Khi  $m = k$  thì  $a_n (b_m^n + c_m^n) = 0 \Rightarrow b_m = -c_m$  với  $n$  là số lẻ.

Khi đó thì ta được:

$$Q(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0, b_m \neq 0$$

$$R(x) = -b_m x^m + c_{m-1} x^{m-1} + \dots + c_1 x + c_0, b_m \neq 0$$

Bây giờ xét đa thức  $H(x) = a_n (Q^n(x) + R^n(x)) = a_n (Q(x) + R(x)) S(x)$ , trong đó

$$S(x) = Q^{n-1}(x) - Q^{n-2}(x)R(x) + Q^{n-3}(x)R^2(x) - \dots - Q(x)R^{n-2}(x) + R^{n-1}(x)$$

Xét hệ số của  $x^{m(n-1)}$  trong  $S(x)$  thì ta được:

$$b^{n-1} - b^{n-2}(-b) + \dots - b(-b)^{n-2} + (-b)^{n-1} = nb^{n-1} \neq 0$$

Do đó  $\deg(S(x)) = m(n-1)$ .

Ta sẽ giả sử phản chứng rằng  $\deg(Q(x) + R(x)) \geq 1$ .

Khi đó thì ta có  $\deg(H(x)) \geq m(n-1) + 1$

Ta xét đa thức  $T(x) = P(Q(x)) + P(R(x)) - H(x) = \sum_{i=0}^{n-1} a_i (Q^i(x) + R^i(x))$

Nhận thấy rằng:  $\deg(T(x)) \leq m(n-1)$  rõ ràng điều này là vô lý.

Từ đó ta phải có  $\deg(Q(x) + R(x)) = 0$  hay  $(Q(x) + R(x))$  là hằng số.

Vậy từ đây ta suy ra điều phải chứng minh.





**Câu 100.** Chứng minh rằng tồn tại các đa thức hệ số nguyên  $S_1, S_2, \dots$  tương ứng với các biến  $x_1, x_2, \dots, y_1, y_2, \dots$  thỏa mãn với mọi số nguyên  $n \geq 1$

$$\sum_{d|n} d \cdot S_d^{\frac{n}{d}} = \sum_{d|n} d \cdot \left( x_d^{\frac{n}{d}} + y_d^{\frac{n}{d}} \right) \quad (*)$$

Với hàm tổng chạy qua các ước nguyên dương  $d$  của  $n$ .

**Chú ý.** Lưu ý rằng ta chỉ xét đến các đa thức trong trường  $\mathbb{Z}[x]$ . Ví dụ, xét hàm

$S_1 = x_1 + y_1$  và  $S_2 = x_2 + y_2 - x_1 y_1$  trong trường hợp  $n = 2$  ta được

$S_1^2 + 2S_2 = (x_1^2 + y_1^2) + 2 \cdot (x_2 + y_2)$  là hàm  $(*)$  thỏa mãn yêu cầu bài toán.

2018 Brazil 4th TST Day 2

### Lời giải

Ta chứng minh rằng  $S_n$  có hệ số nguyên bằng phương pháp quy nạp

Với  $n = 1$  ta được hiển nhiên đúng

Giả sử điều ta cần chứng minh vẫn đúng đến  $n - 1$ , tức các đa thức  $S_1, S_2, \dots, S_{n-1}$  đều là đa thức có hệ số nguyên

Gọi  $p$  là số nguyên tố thỏa mãn  $v_p(n) = k > 0$ , từ đây ta có thể nhận thấy rằng:

$$p^k \mid \sum_{d|n} d \cdot \left( x_d^{\frac{n}{d}} + y_d^{\frac{n}{d}} \right) - \sum_{d|n, d \neq n} d \cdot S_d^{\frac{n}{d}}$$

Đặt  $n = pm$ , suy ra với mỗi giá trị  $d$  không phải là ước số của  $m$  sẽ bị triệt tiêu trong tổng trên khi lấy modulo  $p^k$ , do đó đủ để ta thấy được điều sau:

$$p^k \mid \sum_{d|m} d \cdot \left( x_d^{\frac{n}{d}} + y_d^{\frac{n}{d}} \right) - \sum_{d|m} d S_d^{\frac{n}{d}}$$

Đặt  $T_i(x_1, x_2, \dots, y_1, y_2, \dots) = S_i(x_1^p, x_2^p, \dots, y_1^p, y_2^p, \dots)$ ,  $\forall i$

Áp dụng giả thiết bài toán cho  $T_i, x_i^p, y_i^p$ , tổng trước đó trở thành:

$$\sum_{d|m} d \cdot \left( x_d^{\frac{pm}{d}} + y_d^{\frac{pm}{d}} \right) - \sum_{d|m} d S_d^{\frac{pm}{d}} = \sum_{d|m} d \left( T_d^{\frac{m}{d}} - S_d^{\frac{pm}{d}} \right)$$

Ta sẽ chứng minh  $p^k$  có thể chia cho mỗi phần trong tổng này.

Thật vậy, đặt  $\frac{m}{d} = p^l q$  với  $p \nmid q$ , dễ dàng thấy được  $p^{l+1} \mid T_d^{p^l q} - S_d^{p^{l+1} q}$

Theo giả thiết quy nạp:  $A = S_d^{p^l q}$  là đa thức hệ số nguyên, theo tính chất của tự đồng cấu Frobenius (Frobenius Endomorphism), ta có được  $T_d^q = A + Bp$  với hàm  $B$  có hệ số nguyên,

vậy ta có được điều sau  $p^{l+1} \mid (A + Bp)^{p^l} - A^{p^l} = \sum_{1 \leq i \leq p^l} (Bp)^i A^{p^l-i} \binom{p^l}{i}$

Lại có  $p^{l+1}$  chia hết cho mỗi phần trong tổng này vì



$$v_p \left( p^i \binom{p^l}{i} \right) = v_p \left( p^i \cdot \frac{p^l}{i} \binom{p^l-1}{i-1} \right) \geq i+l-v_p(i) \geq l+1 \Leftrightarrow i \geq v_p(i)+1,$$

Điều này đúng với  $\forall i \geq 1$ , ta có điều phải chứng minh.

**Nhận xét.** Đây là một bài toán khó với việc sử dụng lý thuyết về hàm tự đồng cấu rất ít gặp trong các bài toán dự thi Olympic, *tự đồng cấu Forbenius* sẽ được tìm hiểu rõ hơn trong chương trình đại học.

# TÀI LIỆU THAM KHẢO

Dưới đây là các tài liệu mà ebook này có tham khảo và đồng thời có cả những tài liệu mà bạn mình đề xuất cho bạn đọc

- [1]. A comprehensive course in number theory – Alan Baker – Cambridge University Press (2012).
- [2]. Problem – Solving and Selected Topics in Number Theory\_ In the Spirit of the Mathematical Olympiads – Michael Th. Rassias-Springer – Verlag New York (2011).
- [3]. Tính chất số học trong các bài toán về đa thức – Phạm Viết Huy – THPT Chuyên Lê Khiết – Quảng Ngãi.
- [4] Chuyên đề đa thức và số học – Nguyễn Thành Nhân – Chuyên Hùng Vương – Bình Dương
- [5]. Number Theory A Historical Approach – John J.Watkins.
- [6]. Number theory and polynomials (London Mathematical Society Lecture Note Series) – James McKee, Chris Smyth – CUP (2008).
- [7]. An Introduction to Theory of Functional Equations – Marek Kuczma, Attila Gilányi and Inequalities.
- [8]. The IMO Compendium. A Collection of Problems Suggested for The International Mathematical Olympiads: 1959 – 2009 – Djukic D., Vladimir Jankovic, Ivan Matic, Nikola Petrovic – Springer (2011).
- [9]. Problem – Solving and Selected Topics in Number Theory – Michael Th. Rassias.
- [10]. Number Theory Structures, Examples and Problems – Titu Andreescu, Dorin Andrica.
- [11]. Elementary Methods in Number Theory – Nathanson M.B.
- [12]. Elementary Number Theory Primes Congruences and Secrets A Computational Approach – William Stein.
- [13]. [http://maths.vn/tag/so-hoc/?fbclid=IwAR34ppP14Xm45I9dK8H\\_R6YKpjKPdSeCY-AT1eRjLwQATzvluVo4raqrVH4](http://maths.vn/tag/so-hoc/?fbclid=IwAR34ppP14Xm45I9dK8H_R6YKpjKPdSeCY-AT1eRjLwQATzvluVo4raqrVH4).
- [14]. diendantoanhoc.net.
- [15]. artofproblemsolving.com.
- [16]. Đột phá đỉnh cao bồi dưỡng học sinh giỏi chuyên đề số học – Văn Phú Quốc.
- [17]. A Computational Introduction To Number Theory And Algebra – Victor Shoups.
- [18]. Tuyển chọn các bài toán trong kì thi chọn đội tuyển của các tỉnh, thành phố năm học 2016 – 2017 – Toán học cho mọi người.
- [19]. Định hướng bồi dưỡng học sinh năng khiếu toán – Nhà xuất bản Giáo dục Việt Nam
- [20]. 104 Number Theory Problems: From the Training of the USA IMO Team – Titu Andreescu, Dorin Andrica, Zuming Feng.
- [21]. Tài liệu ôn đội tuyển VMO 2015 – Thầy Trần Minh Hiền – Chuyên Quang Trung – Bình Phước.



# **TẠP CHÍ VÀ TỦ LIỆU TOÁN HỌC**

Thôn 6 – Thạch Hòa – Thạch Thất – Hà Nội

Điện thoại: 0343763310; Email: tuangenk@gmail.com

Fanpage: <https://www.facebook.com/OlympiadMathematical/>

---

## **CHỊU TRÁCH NHIỆM NỘI DUNG**

DOÃN QUANG TIẾN

NGUYỄN MINH TUẤN

TÔN NGỌC MINH QUÂN

HUYỀN KIM LINH

## **BIÊN TẬP**

NGUYỄN MINH TUẤN

## **TRÌNH BÀY BẢN THẢO**

NGUYỄN MINH TUẤN

---

## **ĐA THỨC VÀ SỐ HỌC**

Đề nghị quý bạn đọc tôn trọng bản quyền của tác giả, không sao chép bản phụ.

Mọi ý kiến thắc mắc đóng góp vui lòng gửi về địa chỉ đã cung cấp ở trên.

Phiên bản sách điện tử được phát hành vào ngày 2/9/2019.



## CHINH PHỤC OLYMPIC TOÁN

MỌI Ý KIẾN THẮC MẮC XIN VUI LÒNG GỬI VỀ ĐỊA CHỈ  
**ĐOÀN QUANG TIẾN**



0817431404



doanquangtien1442001@gmail.com



<https://www.facebook.com/OlympiadMathematical/>



Đại học KHTN – Đại học Quốc Gia TP.HCM

LIMITED  
EDITION