ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LƯƠNG THỊ HẰNG

PHƯƠNG TRÌNH NGHIỆM NGUYÊN VÀ GIẢ THIẾT CATALAN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2013

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LƯƠNG THỊ HẰNG

PHƯƠNG TRÌNH NGHIỆM NGUYÊN VÀ GIẢ THIẾT CATALAN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành : PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số : 60 46 36

NGƯỜI HƯỚNG DẪN KHOA HỌC:
GS. TSKH HÀ HUY KHOÁI

THÁI NGUYÊN - 2013

Mục lục

MỞ ĐẦU

0.1 Tóm tắt

Giả thuyết Catalan trong lý thuyết số một trong những bài toán rất dễ phát biểu, nhưng lại rất khó giải. Giả thuyết dự đoán rằng chỉ có 8 và 9 là cặp số liên tiếp duy nhất mà cả hai số đều là lũy thừa của số tự nhiên. Nói cách khác, phương trình Diophantine

$$x^u - y^v = 1 \qquad (x > 0, y > 0, u > 1, v > 1) \tag{1}$$

không có nghiệm nào khác ngoài $x^u = 3^2, y^v = 2^3$.

Giả thuyết này được công bố trên tạp trí *Journal fur die Reine und Angewandte Mathematik* bởi nhà toán học Bỉ Eugène Catalan (1814-1894). Bài báo được xuất bản năm 1944 ([1]). Trong thời gian Catalan giảng dạy tại trường đại học Bách khoa Paris ông đã nổi tiếng với việc giải một bài toán tổ hợp. Thuật ngữ số Catalan vẫn được sử dụng cho đến ngày này là nhắc đến công trình đó. Đối với phương trình (1) Catalan đã viết *Cho đến nay không thể chứng minh đầy đủ*. Ông cũng chưa bào giờ công bố bất kì kết quả riêng quan trọng nào về vấn đề này.

Giả thuyết trở thành thách thức của toán học và sớm thu được một số kết quả trong những trường hợp riêng quan trọng, tuy nhiên trong suốt 100 năm tất các các kết quả thu được đều ít nhiều mang đặc tính cô lập.

Tiếp đó vào cuối những năm 1950 đồng thời xuất hiện một số ý tưởng đáng kể. Sau đó đến những năm 1970, việc nghiên cứu được kích thích bởi một kết quả đưa bài toán tới việc tính toán hữu hạn. Tuy nhiên, khối lượng tính toán là quá lớn để có tính khả thi. Từ đó, hướng chính của việc nghiên cứu là các nỗ lực để giảm bới khối lượng tính toán.

Đó là tình hình cho đến năm 2002, khi nhà toán học Preda Mihăilescu, người chưa được biết đến trong lĩnh vực này đã chứng minh hoàn Chỉnh Giả thuyết. Điều ngạc nhiên là trong chứng minh, ông sử dụng rất ít tính toán, mà thay vào đó ông sử dụng các lý thuyết sâu sắc, đặc biệt lý thuyết các trường cyclotomic..

Preda Mihăilescu sinh năm 1955 tại Rumani, ông học toán tại ETH Zurich. Ông đã từng làm việc trong ngành công nghệ máy tính và tài chính, nhưng hiện tại ông đang nghiên cứu toán tại đại học Paderborn - Đức.

Luận văn nhằm trình bày một số điểm mốc quan trọng trong lịch sử của bài toán Catalan và mô tả sơ lược lời giải tuyệt vời của Mihăilescu.

Dù đã rất cố gắng, nhưng chắc chắn nội dung được trình bày trong luận văn không tránh khỏi thiếu sót nhất định, em rất mong nhận được sự góp ý của các thầy cô giáo và các bạn.

Em xin chân thành cảm ơn!

Thái Nguyên, ngày 20 tháng 3 năm 2013

Người thực hiện

Lương Thị Hằng

Chương 1

GIẢ THUYẾT CATALAN: THÊM MỘT PHƯƠNG TRÌNH DIOPHANTINE ĐƯỢC GIẢI

1.1 Lịch sử nghiên cứu

Khoảng 100 năm trước khi Catalan gửi thư cho Crelle, Euler đã chứng minh rằng trong số các lũy thừa bậc hai và bậc ba, chỉ có 8 và 9 là các số nguyên liên tiếp, tức là cặp số (8,9) là nghiệm duy nhất của phương trình

$$x^3 - y^2 = \pm 1 \qquad (x > 0, y > 0) \tag{1.1}$$

Chứng minh của Euler rất tài tình, nhưng có nhiều chỗ dài dòng. Ngoài nhiều kỹ thuật khác, chứng minh còn dùng phương pháp lùi vô hạn của Fermat.

Để tìm hiểu phương trình (1) ta xem trường hợp đặc biệt (1.1) có thể giải như thế nào nếu sử dụng lý thuyết số đại số. Giả sử (x, y) là một nghiệm, trước hết ta xét phương trình $x^3 - y^2 = -1$. Ta viết phương trình trong vành các số nguyên Gauss $\mathbb{Z}[i]$.

$$x^3 = (y + i)(y - i) \tag{1.2}$$

Do $\mathbb{Z}[i]$ là vành nhân tử duy nhất nên ta có thể xét ước chung lớn nhất của các phần tử của nó. Gọi d là ước chung lớn nhất của $y + i$ và $y - i$ (sai khác một nhân tử đơn vị). Từ các phương trình $y + i = d\lambda, y - i = d\mu$ ta có $d|2$. Từ (1.2) suy ra d chia hết x và x phải là số lẻ. Từ đó $y \equiv 0$ hoặc $1(\mod 4)$. Suy ra d là đơn vị. Do đó $d = \pm 1; \pm i$.

Ta có $y+i = d(a+bi)^3, a, b \in \mathbb{Z}$. Tuy nhiên d là lũy thừa bậc ba trong $\mathbb{Z}[i]$ nên có thể bỏ qua. Từ phần thực và phần ảo của phương trình $y+i = (a+bi)^3$

ta tìm được $y = 0$ và $(x = 1)$. Điều này mâu thuẫn. Do đó phương trình không có nghiệm.

Đối với phương trình $x^3 - y^2 = 1$, ta viết phương trình dưới dạng

$$x^3 = (y+1)(y-1)$$

Ước chung lớn nhất của $(y+1)$ và $(y-1)$ là 1 hoặc 2. Trong trường hợp thứ nhất, ta thấy rằng 2 sẽ là hiệu của hai lũy thừa bậc ba, điều này không thể xảy ra. Trong trường hợp thứ hai, sẽ dẫn đến phương trình

$$a^3 - 2b^3 = \pm 1$$

Do đó $a - b\alpha$ với $\alpha = \sqrt[3]{2}$ là đơn vị trong $\mathbb{Z}[\alpha]$, vành các số nguyên trong trường các số thực $\mathbb{Q}(\alpha)$. Các đơn vị của vành này là các lũy thừa của đơn vị $1 + \alpha + \alpha^2$. Từ đó, ta tìm được $|a - b\alpha|$ là lũy thừa bậc 0 nên $\alpha = \pm 1, b = 0$. Do đó phương trình ban đầu có nghiệm $x = 2, y = 3$.

Để chứng minh giả thuyết Catalan ta xét phương trình

$$x^p - y^q = 1 \qquad (x > 0, y > 0) \tag{1.3}$$

với p, q là các số nguyên tố khác nhau.

Năm 1850, V.A. Lebesgue (không phải là người cùng tên nổi tiếng với tích phân Lebesgue!) giải được trường hợp $q = 2$. Sử dụng đại số các số nguyên Gauss, ta viết phương trình dưới dạng tương tự phương trình (1.2). Ước chung lớn nhất của $y + i$ và $y - i$ là đơn vị. Do đó ta có hai phương trình

$$y + i = i^s(a + bi)^p, \qquad y - i = (-i)^s(a - bi)^p$$

trong đó $s \in \{0, 1, 2, 3\}$. Từ đó có thể khử y và các phương trình này dẫn đến mâu thuẫn, do đó phương trình $x^p - y^2 = 1$ không có nghiệm.

Đối với trường hợp $p = 2$ trong phương trình (2.4), năm 1961 có một kết quả chứng minh phương trình $x^2 - y^q = 1$ nếu có nghiệm thì $x > 10^{3.10^9}$. Cái tin nhà toán học Chaoko người Trung Quốc chứng minh được rằng phương trình này không giải được đã không được cộng đồng toán học biết đến. Chứng minh chỉ được biết đến năm 1964, khi nó công bố trên tạp chí Scientia Sinica [7].

Năm 1976, E.Z Chein công bố một chứng minh rất khéo léo dựa trên kết quả của T.Nagell nói rằng nghiệm (x, y) phải thỏa mãn $2|y$ và $q|x$. Xét phương trình có dạng

$$(x+1)(x-1) = y^q$$

Chein kết luận rằng ước chung lớn nhất của $(x+1)$ và $(x-1)$ là 2. Do đó có các số nguyên tố cùng nhau a và b, với a lẻ thỏa mãn phương trình

$$(x+1) = 2a^q, \qquad x-1 = 2^{q-1}b^q \tag{1.4}$$

hoặc các phương trình tương tự với $x+1$ và $x-1$ tráo đổi cho nhau. Nếu $q > 3$ thì (2.5) dẫn đến điều kiện

$$(ha)^2 + b^2 = (a^2 - b)^2$$

trong đó $h^2 = a - 2b$ và các phương trình thay thế thỏa mãn điều kiện tương tự. Đây là hai phương trình kiểu Pitago và do đó đã biết lời giải. Từ đó suy ra x và y không tồn tại với $q > 3$.

Chi tiết về cách giải trên có thể xem trong cuốn chuyên khảo của Paulo Ribenboim. Trong cuốn sách trình bày toàn diện lịch sử của giả thuyết Catalan cho đến năm 1994.

1.2 Cassels và trường hợp 1

Từ mục này để thuận tiện chúng ta xét phương trình Catalan đưới dạng

$$x^p - y^q = 1 (xy \neq 0, p, q \text{ là các số nguyên tố lẻ khác nhau.}) \tag{1.5}$$

Ta viết lại phương trình dưới dạng

$$(x-1)\frac{x^p - 1}{x-1} = y^q$$

Sử dụng đồng nhất thức $x^p = ((x-1)+1)^p$ ta dễ thấy ước chung lớn nhất của $(x-1)$ và $\frac{x^p-1}{x-1}$ là 1 hoặc p.

Một tình huống tương tự xảy ra khi nghiên cứu phương trình Fermat $x^p + y^p = z^p$, trong đó vế trái được phân tích thành tích của $x+y$ và $\frac{x^p+y^p}{x+y}$, ở đây ước chung lớn nhất của các thừa số là 1 hoặc p. Điều này dẫn đến *trường hợp 1* và *trường hợp 2* của bài toán Fermat. Trong lịch sử, trường hợp 1 "dễ dàng" hơn và nhiều người tin rằng cách tiếp cận này sẽ chứng minh hoàn thiện bài toán. Tuy nhiên, trong chứng minh của Andrew Wiles không sử dụng sự phân loại này.

Đối với phương trình (1.5) ta có thể nói tương tự về các trường hợp 1 và 2 tùy theo giá trị của các ước chung lớn nhất ở trên. Trong trường hợp 1, khi gcd bằng 1 chúng ta thu được các phương trình

$$x - 1 = a^q, \frac{x^p - 1}{x-1} = b^q, y = ab$$

trong đó a và b là các số nguyên tố cùng nhau và không chia hết cho p.

Năm 1960, J.W.S. Cassels đã chỉ ra rằng các phương trình này dẫn đến mâu thuẫn. Ông sử dụng các phương pháp sơ cấp và sự kết hợp đáng ngạc nhiên giữa tính chia hết và các bất đẳng thức. Sau đó, S. Hyyro có một chứng minh khác.

Điều này có nghĩa là chúng ta chỉ còn trường hợp 2. Đặc biệt, một trong hai số $x-1$ và $(x^p-1)\backslash(x-1)$ chứa lũy thừa bậc nhất của p. Nhưng số này không thể là $x-1$, vì trong trường hợp đó x^p-1 chỉ chia hết cho p^2. Vì vậy chúng ta có các phương trình

$$(x-1) = p^{q-1}a^q, \frac{x^p-1}{x-1} = pb^q, y = pab \tag{1.6}$$

trong đó a và b là các số nguyên tố cùng nhau và p không chia hết b (nhưng p có thể chia hết a). Các phương trình tương tự suy ra tự việc phân tích x^pthành tích của $y+1$ và $(y^p-1)\backslash(y+1)$. Đặc biệt y chia hết cho p và x chia hết cho q. Định lý Cassell là một trong những kết quả tổng quát đầu tiên về phương trình Catalan (1.5), nó là động lực quan trọng để nghiên cứu phương trình này.

1.3 Bài toán có thể giải bằng máy tính?

Khoảng giữa thế kỷ trước, giả thuyết Catalan bắt đầu nhận được quan tâm của những người làm việc trong giải tích Diophantine. Trước tiên người ta thấy rằng số nghiệm (x, y) của phương trình với số mũ p, q cố định là hữu hạn. Đây là một hệ quả của định lý tổng quát về số điểm nguyên trên đường cong được công bố năm 1929 của C.L. Siegel. Năm 1955, H. Davenport và K.F. Roth công bố một kết quả về chặn trên của số đó (mặc dù rất lớn) [2](các kết quả khác về số nghiệm có thể tham khảo trong phần giới thiệu).

Bước ngoặt trong hướng này là vào những năm 1970. Alan Baker thu được các ước lượng cơ bản đối với các dạng tuyến tính logarit. Đặt

$$\Lambda = b_1 \log r_1 + ... + b_n \log r_n$$

trong đó b_j là các số nguyên, r_j là các số hữu tỷ dương. Ta định nghĩa *độ cao* của một số hữu tỷ $r = \frac{s}{t}$ là $\log \max(|s|, |t|)$ và đặt $B = \max(|b_1|, ..., |b_n|\}$. Giả sử $\Lambda \neq 0$, Baker chứng minh bất đẳng thức sau:

$$|\Lambda| > \exp(-A \log B),$$

trong đó A là số dương tính toán được ,phụ thuộc vào n và độ cao của $r_1, ..., r_n$.

Kết quả này, thực ra là một sự làm mịn của nó, đã được Robert Tijdeman sử dụng để tìm chặn trên của nghiệm (x, y, p, q) (với x, y dương) của phương trình Catalan . Chiến lược ở đây là tìm dạng tuyến tính Λ và phụ thuộc vào nghiệm một cách đặc biệt: một chặn trên cho $|\Lambda|$ suy ra bởi (1.5) phải đủ gần với chặn dưới của Baker.

Robert Tijdeman chọn

$$\Lambda_1 = q \log q - p \log p + pq \log \frac{pa}{pa'} = \log \frac{(x-1)^p}{(y+1)^q}$$
$$\Lambda_2 = q \log q + \frac{p \log p^{q-1} a^q + 1}{q^q a'^q} = \log \frac{y^q + 1}{(y+1)^q}$$

trong đó a được xác định từ phương trình $x - 1 = p^{p-1} a'^p$ và a' xác định bởi phương trình tương tự $y + 1 = q^{p-1} a'^p$. Do

$$(x-1)^p < x^p = y^q + 1 < (y+1)^q$$

suy ra Λ_1, Λ_2 khác không. So sánh chặn dưới và chặn trên của $|\Lambda_1|$ dẫn đến bất đẳng thức giữa p và q, tương tự với $|\Lambda_2|$ Các bất đẳng thức này là đủ chặ để, khi khử q, ta có điều kiện sau

$$p < c_1 (\log p)^{c_2}$$

trong đó c_1, c_2 là các hằng số. Điều này yêu cầu $q < p$, nhưng trong trường hợp $q > p$ ta có các điều kiện tương tự cho q.

Từ đó suy ra các số mũ p, q bị chặn trên và chặn trên không phụ thuộc vào x và y. Do đó tính chất của bài toán hoàn toàn thay đổi: chỉ có hữu hạn nghiệm (x, y, p, q)., hơn nữa có thể tính toán được cận trên của các ẩn.

Thật vậy các hằng số c_1, c_2 ở trên là tính được Những kết quả tính toán chi tiết đầu tiên về chặn trên của p và q là vô cùng lớn, nhưng những cải tiến đã đem lại những ước lượng vừa phải hơn. Kết quả lớn nhất cho chặn trên của $\max(p, q)$ là 8.10^{16}.

Lưu ý rằng việc giả thiết x, y dương ở trên không làm mất tính tổng quát, vì (1.5) cũng có thể viết dưới dạng

$$(-y)^q - (-x)^p = 1. \tag{1.7}$$

Điều gì xảy ra khi ta thay bằng phương trình $x^p - y^q = c$, trong đó $c > 1$ là số nguyên? Cố định p và q, định lý Siefel suy ra số nghiệm (x, y) là hữu hạn.