ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

———————o0o———————

NGUYỄN THỊ NGUYỆT THƯ

ĐỊNH LÝ BỐN BÌNH PHƯƠNG CỦA LAGRANGE VÀ MỘT SỐ CẢI TIẾN

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN, 5/2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

———————o0o———————

NGUYỄN THỊ NGUYỆT THƯ

ĐỊNH LÝ BỐN BÌNH PHƯƠNG CỦA LAGRANGE VÀ MỘT SỐ CẢI TIẾN

Chuyên ngành: Phương pháp toán sơ cấp
Mã số: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

GIÁO VIÊN HƯỚNG DẪN
TS. ĐOÀN TRUNG CƯỜNG

THÁI NGUYÊN, 5/2019

Mục lục

Mở đầu

Định lý bốn bình phương của Lagrange (hay Định lý Lagrange) nói rằng mọi số nguyên dương luôn có thể biểu diễn được dưới dạng tổng của bình phương của bốn số nguyên (tổng bốn số chính phương). Ví dụ $23 = 1^2 + 2^2 + 3^2 + 3^2$. Định lý bốn bình phương lần đầu tiên được nhà toán học Hy Lạp Diophantus đề cập trong bộ sách Arithmetica của ông. Bộ sách này được Bachet (Claude Gaspard Bachet de Méziriac) dịch ra tiếng La tinh vào năm 1621 và Bachet đã phát biểu định lý trong sổ ghi của mình. Tuy nhiên đã không có chứng minh nào được đưa ra cho đến năm 1770 khi nhà toán học người Ý Joseph-Louis Lagrange (1736-1813) đưa ra chứng minh đầu tiên của định lý.

Năm 1797 nhà toán học người Pháp Adrien-Marie Legendre (1752-1833) đã tiến thêm một bước nữa bằng cách đưa ra định lý ba bình phương. Định lý này phát biểu rằng một số nguyên dương có thể được biểu diễn dưới dạng tổng của ba bình phương khi và chỉ khi nó không có dạng $4^k(8l+7)$ với $k,\ l$ là các số nguyên. Sau đó, vào năm 1834, Carl Gustav Jakob Jacobi (1804-1851, nhà toán học người Đức) đã tìm ra một công thức đơn giản cho số biểu diễn của một số nguyên thành tổng của bốn bình phương.

Định lý bốn bình phương của Lagrange có thể được cải tiến theo nhiều cách khác nhau. Gần đây, Zi-Wei Sun [SUN17] đã chứng minh rằng mỗi số tự nhiên có thể được viết dưới dạng tổng của sáu lũy thừa (hoặc bốn lũy thừa) và ba bình phương. Hoặc giả thuyết 1-3-5 của Z.W. Sun nói rằng số tự nhiên bất kỳ luôn có thể được viết dưới dạng $a^2 + b^2 + c^2 + d^2$ với a, b, c, d là các số nguyên không âm sao cho $a + 3b + 5c$ là một bình phương. Ngoài ra có các cải tiến của Zhi Wei Sun - Yu Chen Sun [SS18], Leo Goldmakher - Paul Pollack [GP18] bằng cách thêm thông tin về các số a, b, c, d. Một cách tiếp cận khác của Paul Pollack - Enrique Treviño [PT17] là đưa ra các thuật toán hữu hiệu để tìm các số nguyên a, b, c, d khi biết số n.

Mục đích của luận văn là dựa theo một số tài liệu tìm hiểu về Định lý bốn bình phương Lagrange và một số cải tiến định lý này do Z.W. Sun, Y.C.

Sun-Z.W. Sun, L. Goldmakher-P. Pollack đưa ra.

Luận văn được chia thành 3 chương.

Chương 1 được dành để trình bày về biểu diễn của một số tự nhiên như tổng của bốn bình phương, trong đó kết quả chính là Định lý Bốn bình phương của Lagrange. Một số mở rộng cổ điển của Định lý của Lagrange như Định lý Ba bình phương của Legendre - Gauss, Bài toán Waring và một vài bài tập ứng dụng trong toán phổ thông được đề cập trong phần sau của Chương 1.

Chương 2 tập trung trình bày một số cải tiến Định lý bốn bình phương của Zhi-Wei Sun và Zhi Wei Sun - Yu Chen Sun.

Trong Chương 3 chúng tôi sẽ trình bày một số cải tiến Định lý Bốn bình phương của Goldmakher và Pollack và một số hệ quả. Phần cuối của chương chúng tôi đề cập đến thuật toán để phân tích một số thành tổng của bốn bình phương.

Luận văn này được thực hiện tại Trường Đại học Khoa học – Đại học Thái Nguyên và hoàn thành dưới sự hướng dẫn của TS. Đoàn Trung Cường. Tác giả xin bày tỏ lòng biết ơn sâu sắc nhất tới thầy, người đã tận tình hướng dẫn tác giả trong quá trình nghiên cứu và viết bản luận văn này.

Tác giả xin chân thành cảm ơn toàn thể các thầy cô trong Khoa Toán-Tin, trường Đại học Khoa học - Đại học Thái Nguyên, cùng toàn thể các thầy cô trong trường đã tận tình hướng dẫn, truyền đạt kiến thức trong suốt thời gian theo học, thực hiện và hoàn thành luận văn.

Tác giả xin bày tỏ lòng cảm ơn tới tập thể lớp Cao học Toán K11D (khóa 2017-2019), bạn bè, đồng nghiệp và gia đình đã tạo điều kiện, động viên, giúp đỡ tác giả trong quá trình học tập, nghiên cứu.

Thái Nguyên, ngày 12 tháng 5 năm 2019

Tác giả luận văn

Nguyễn Thị Nguyệt Thư

Chương 1. Định lý bốn bình phương của Lagrange

Mục đích của chương này là trình bày về biểu diễn một số tự nhiên thành tổng các bình phương, trong đó trung tâm là Định lý bốn bình phương của Lagrange. Chúng tôi cũng đề cập (phát biểu, không chứng minh) Định lý ba bình phương của Legendre-Gauss và một vài bài tập toán phổ thông có liên quan. Các kết quả chính của chương được tham khảo từ tài liệu [Lal02].

1.1 Biểu diễn tổng bình phương và Định lý bốn bình phương của Lagrange

Trong số học vấn đề biểu diễn một số tự nhiên thành tổng bình phương của các số nguyên là một vấn đề cổ điển và dành được sự quan tâm của nhiều người. Ta bắt đầu với một số biểu diễn cụ thể

$$3 = 1^2 + 1^2 + 1^2,$$

$$7 = 2^2 + 1^2 + 1^2 + 1^2,$$

$$25 = 5^2 = 3^2 + 4^2,$$

$$2017 = 18^2 + 21^2 + 24^2 + 26^2.$$

Tổng quát, ta có định lý rất đẹp sau đây của Lagrange.

Định lý 1.1.1 (Định lý Lagrange). *Mọi số nguyên không âm có thể được viết dưới dạng tổng của bốn bình phương các số nguyên, nghĩa là với mọi $n \in \mathbb{N}$, ta có*

$$n = a^2 + b^2 + c^2 + d^2. \tag{1.1}$$

với $a, b, c, d \in \mathbb{Z}$.

Chứng minh. Trước hết nhận xét là chỉ cần chứng minh định lý cho trường hợp n là số nguyên tố. Thật vậy, ta có đồng nhất thức Euler

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)&(y_1^2 + y_2^2 + y_3^2 + y_4^2)\\ =&(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2\\ &+ (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned}$$

Do đó, nếu ta chứng minh được khẳng định đúng trong trường hợp các số nguyên tố thì ta có biểu diễn

$$m_i = a_i^2 + b_i^2 + c_i^2 + d_i^2,$$

với các số nguyên a_i, b_i, c_i, d_i, $i = 1, \ldots, r$. Sử dụng đồng nhất thức Euler, ta suy ra

$$m_1m_2 = (a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = x_2^2 + y_2^2 + z_2^2 + w_2^2.$$

$$m_1m_2m_3 = (x_2^2 + y_2^2 + z_2^2 + w_2^2)(a_3^2 + b_3^2 + c_3^2 + d_3^2) = x_3^2 + y_3^2 + z_3^2 + w_3^2.$$

Tương tự

$$n = (m_1 \ldots m_{r-1})m_r = x_r^2 + y_r^2 + z_r^2 + w_r^2.$$

Vì vậy ta chỉ cần chứng minh khẳng định cho trường hợp n là số nguyên tố.

Trường hợp $n = 2$ ta luôn có $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Giả sử n là một số nguyên tố lẻ. Trước hết ta chứng minh có các số x, y và k thỏa mãn $1 + x^2 + y^2 = nk \quad (0 < k < n)$. Cho $x_0 = 0, x_1 = 1, x_2 = 2, \ldots, x_{\frac{n-1}{2}} = \frac{n-1}{2}$. Khi đó các số x_i^2 đôi một không đồng dư với nhau theo modulo n. Thật vậy, nếu $x_i^2 \equiv x_j^2 \pmod{n}$ $(i, j = 0, \ldots, \dfrac{n-1}{2}, i \neq j)$ thì

$$n \mid (x_i - x_j)(x_i + x_j)$$

Nếu $n \mid (x_i - x_j)$ thì vì $-\frac{n-1}{2} \leq x_i - x_j \leq \frac{n-1}{2}$ nên $x_i - x_j = 0$, hay $x_i = x_j$ (mâu thuẫn). Mặt khác, nếu $n \mid (x_i + x_j)$ thì $x_i + x_j = 0$ vì $0 \leq x_i + x_j \leq n - 1$, dẫn đến $x_i = -x_j = 0$ cũng là vô lý.

Đặt $y_0 = 0, y_1 = 1, y_2 = 2, \ldots, y_{\frac{n-1}{2}} = \dfrac{n-1}{2}$. Khi đó các số $-1 - y_i^2$ đôi một không đồng dư với nhau theo modulo n. Ta thu được một tập hợp $X = \{x_0^2, x_1^2, \ldots, x_{\frac{n-1}{2}}^2\}$ gồm $\dfrac{n+1}{2}$ lớp đồng dư khác nhau theo modulo n và một tập hợp $Y = \{-1 - y_0^2, -1 - y_1^2, \dots, -1 - y_{\frac{n-1}{2}}^2\}$ gồm $\dfrac{n+1}{2}$ lớp đồng dư khác nhau theo modulo n. Vì có nhiều nhất n lớp đồng dư theo modulo n nên X và Y phải giao nhau, nghĩa là có các chỉ số i, j sao cho

$$x_i^2 \equiv -1 - y_j^2 \pmod{n}.$$

Từ đó suy ra $x_i^2 + y_j^2 + 1 = nk$ với $k \in \mathbb{N}$ nào đó. Do cách chọn $x_i^2 < \left(\dfrac{n}{2}\right)^2$ và $y_j^2 < \left(\dfrac{n}{2}\right)^2$ nên

$$nk = 1 + x_i^2 + y_j^2 < 1 + \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = 1 + \frac{n^2}{2} < n^2,$$

dẫn đến $nk < n^2$ hay $k < n$. Từ $1 + x^2 + y^2 = nk$ ta suy ra

$$nk = x^2 + y^2 + z^2 + w^2. \tag{1.2}$$

Quay lại chứng minh n có biểu diễn $n = a^2 + b^2 + c^2 + d^2$ với $a, b, c, d \in \mathbb{N}$. Gọi $m_0 > 0$ là số nhỏ nhất để $m_0 n$ có biểu diễn

$$m_0 n = \text{tổng bốn bình phương}.$$

Ta có nhận xét là m_0 luôn tồn tại và $m_0 \leq k$ vì luôn có $nk = 1 + x^2 + y^2 = 0^2 + 1^2 + x^2 + y^2$ theo (1.2). Bài toán quy về chứng minh $m_0 = 1$.

Giả sử $m_0 > 1$, đặt

$$m_0 n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Nếu m_0 chẵn, thì $m_0 n$ chẵn nên ta có hoặc x_i là các số chẵn hoặc x_i là các số lẻ hoặc hai số chẵn hai số lẻ.

Giả sử x_1, x_2 chẵn. Khi đó ta xét $x_1 \neq x_2$ và $x_3 \neq x_4$ đều chẵn, ta viết

$$\begin{aligned}\left(\frac{m_0}{2}\right) n = &\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 \\ &+ \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.\end{aligned}$$

Vì m_0 là nhỏ nhất nên điều này mâu thuẫn.

Như vậy m_0 là số lẻ. Ta chọn y_i sao cho

$$y_i \equiv x_i \pmod{n}, \quad |y_i| < \frac{m_0}{2}.$$

Do đó $-\dfrac{m_0-1}{2} \le y \le \dfrac{m_0-1}{2}$ là một hệ thặng dư đầy đủ (tập các lớp thặng dự modulo n của các số này trùng với hệ thặng dư $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Ta có $m_0 \nmid x_i$ vì nếu $y_1^2+y_2^2+y_3^2+y_4^2=0$ suy ra $y_1^2=y_2^2=y_3^2=y_4^2=0$ thì $n \mid x_i, \forall i$ suy ra $m_0 \mid x_i, \forall i$ và $m_0^2 \mid \sum x_i^2 = m_0 n$. Vậy $m_0 \mid n$. Suy ra m_0 là số lẻ. Vậy

$$y_1^2+y_2^2+y_3^2+y_4^2>0.$$

Khi đó $-\dfrac{m_0-1}{2} \le y_i^2, \dfrac{m_0-1}{2} \le \dfrac{m_0}{2}$ suy ra $y_i^2 < \dfrac{m_0^2}{4}$. Do đó

$$y_1^2+y_2^2+y_3^2+y_4^2<m_0^2$$

và

$$y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 (\text{mod } m_0).$$

Do đó

$$\begin{aligned} x_1^2+x_2^2+x_3^2+x_4^2 &= m_0 n \quad (m_0<n) \\ y_1^2+y_2^2+y_3^2+y_4^2 &= m_0 m_1 \quad (0<m_1<m_0) \end{aligned}$$

và

$$\begin{aligned} m_1 m_0^2 n &= (x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) \\ &= z_1^2+z_2^2+z_3^2+z_4^2. \end{aligned}$$

Với $z_1 = x_1y_1+x_2y_2+x_3y_3+x_4y_4$ thì

$$z_1 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \ (\text{mod } m_0).$$

Suy ra $m_0 \mid z_1$. Tương tự ta chứng minh được

$$z_2 \equiv x_1x_2-x_2x_1+x_3x_4-x_4x_3 \equiv 0 \ (\text{mod } m_0).$$

$$z_3 \equiv x_1x_3-x_3x_1+x_2x_4-x_4x_2 \equiv 0 \ (\text{mod } m_0).$$

$$z_4 \equiv x_1x_4-x_4x_1+x_2x_3-x_3x_2 \equiv 0 \ (\text{mod } m_0).$$

Ta viết $z_i = m_0 w_i$. với số nguyên w_i nào đó. Chia $m_1 m_0^2 n$ cho m_0^2, ta có $m_1 n = w_1^2+w_2^2+w_3^2+w_4^2$. Điều này mâu thuẫn với giả thiết m_0 là nhỏ nhất. Từ đó suy ra $m_0 = 1$. $\square$

Định lý bốn bình phương được Joseph-Louis Lagrange (1736 – 1813) chứng minh vào năm 1770. Ông là một nhà toán học và nhà thiên văn học và nhà chính trị Pháp gốc Ý. Lagrange có nhiều thời gian làm việc tại Ý, Đức và Pháp. Ông đã có những đóng góp quan trọng trong nhiều lĩnh vực của giải tích toán học, lý thuyết số, cơ học cổ điển và cơ học thiên thể.

Liên quan đến biểu diễn bốn bình phương, một cách tự nhiên quan tâm tiếp theo sẽ là số lượng biểu diễn. Nghiên cứu theo hướng này được nhà toán học người Đức Carl Gustav Jakob Jacobi tiến hành và được ông công bố năm 1834, ngày nay được gọi là Định lý bốn bình phương của Jacobi. Kết quả này đưa ra một công thức cho số cách biểu diễn một số nguyên dương n dưới dạng tổng của bốn bình phương.

Để phát biểu kết quả của Jacobi, với mỗi số tự nhiên n, ký hiệu $Q(n)$ là số các bộ các số nguyên (x_1, x_2, x_3, x_4) (không tính sai khác thứ tự) thoả mãn

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Định lý 1.1.2 (Định lý bốn bình phương của Jacobi)**.** *Cho số tự nhiên n và viết n dưới dạng $n = 2^r(2t+1)$. Khi đó*

$$Q(n) = \begin{cases} 8S(2t+1) & \text{với } r = 0, \\ 24S(2t+1) & \text{với } r \neq 0 \end{cases}$$

trong đó

$$S(n) = \sum_{d|n} d.$$

Có một số cách chứng minh cho định lý của Jacobi, ví dụ có thể xem một chứng minh của Hirschhorn [HIR85] sử dụng một đồng nhất thức tích ba thừa số.

1.2 Định lý Legendre-Gauss và Bài toán Waring

Có rất nhiều tác giả đã cố gắng mở rộng định lý Lagrange theo nhiều khía cạnh khác nhau, ta sẽ xét một số mở rộng gần đây của định lý này trong các chương sau. Trong tiết này ta xét một số mở rộng cổ điển là định lý Legendre-Gauss và Bài toán Waring.

Định lý Lagrange khẳng định bốn bình phương đủ để biểu diễn một số tự nhiên bất kỳ. Nói cách khác, tổng ba bình phương là không đủ để biểu diễn tất cả số tự nhiên. Thật vậy, vì $x_i^2 \equiv 0, 1$ hoặc $4 \pmod 8$ nên

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8,$$