ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

MA THỊ YẾN

VỀ GIẢ THIẾT CỦA JEŚMANOWICZ LIÊN QUAN ĐẾN BỘ BA SỐ PYTHAGORAS NGUYÊN THỦY

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

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. Trần Đỗ Minh Châu

THÁI NGUYÊN - 2021

LỜI CẢM ƠN

Luận văn "*Về giả thuyết của Jeśmanowicz liên quan đến bộ ba số Pythagoras nguyên thủy*" được thực hiện tại Trường Đại học Khoa học - Đại học Thái Nguyên và hoàn thành dưới sự hướng dẫn của TS. Trần Đỗ Minh Châu. Tác giả xin bảy tỏ lòng biết ơn chân thành và sâu sắc tới cô, Người đã tận tình chỉ bảo, hướng dẫn, động viên khích lệ và tạo mọi điều kiện thuận lợi cho tác giả trong suốt quá trình nghiên cứu và hoàn thành luận văn.

Tác giả xin trân trọng cảm ơn Ban giám hiệu Trường Đại học Khoa họa - Đại học Thái nguyên, Ban chủ nhiệm Khoa Toán - Tin, cùng các giảng viên đã tham gia giảng dạy và tạo điều kiện tốt nhất để tác giả học tập và nghiên cứu.

Nhân dịp này, tác giả xin gửi lời cảm ơn tới gia đình và bạn bè đã động viên giúp đỡ tác giả rất nhiều trong quá trình học tập.

Tác giả xin chân thành cảm ơn!

Thái Nguyên, tháng 01 năm 2021

Tác giả

Ma Thi Yến

Mục lục

Lời cảm ơn **ii**

Mục lục **iii**

MỞ ĐẦU **1**

Chương 1. Một số kiến thức chuẩn bị **4**

1.1 Đồng dư thức 4

1.2 Ký hiệu Legendre 8

1.3 Ký hiệu Jacobi 17

Chương 2. Giả thuyết Jeśmanowicz liên quan đến bộ ba số Pythagoras nguyên thủy **23**

2.1 Bộ ba số Pythagoras nguyên thủy 24

2.2 Một trường hợp khi a không có ước nguyên tố đồng dư với 1 theo modulo 4 29

2.3 Một trường hợp khi b là bội của 8. 38

KẾT LUẬN **47**

TÀI LIỆU THAM KHẢO **48**

MỞ ĐẦU

Cho a, b, c là các số nguyên dương. Bộ ba số (a, b, c) được gọi là *bộ ba số Pythagoras nguyên thủy* nếu $a^2 + b^2 = c^2$ và a, b, c nguyên tố cùng nhau. Bộ ba số Pythagoras xuất hiện nhiều trong các vấn đề nghiên cứu của Toán học, đặc biệt là phương trình Diophantine.

Cho a, b, c là các số nguyên dương đôi một nguyên tố cùng nhau. Bài toán tìm nghiệm nguyên dương của phương trình Diophantine

$$a^x + b^y = c^z \tag{1}$$

đã được quan tâm từ những năm 1950. Đầu tiên, bài toán được giải quyết cho một vài bộ ba a, b, c cụ thể bằng các phép biến đổi đồng dư sơ cấp và luật tương hỗ bậc hai. Một số nhà toán học cũng tìm được nghiệm đầy đủ của phương trình (1) khi giá trị của các số a, b, c là nhỏ. Hiện nay, bằng lý thuyết xấp xỉ Diophantine, ta có thể kiểm tra được các nghiệm của (1). Sử dụng lý thuyết về dạng tuyến tính trong logarit của Baker, ta còn có thể đưa ra các chặn trên tốt về độ lớn của các nghiệm của (1). Đặc biệt đã có kết quả chỉ ra rằng số nghiệm của (1) không vượt quá 2^{36}. Trong trường hợp có thêm giả thiết về tính chia hết của x, y, z, ta có thể liên hệ phương trình (1) với các phương trình Diophantine khác, chẳng hạn phương trình Fermat suy rộng.

Hầu hết các kết quả gần đây về phương trình (1) đều liên quan đến các giả thiết khác nhau về bộ a, b, c, trong đó có trường hợp (a, b, c) là bộ ba số Pythagoras. Nếu (a, b, c) là bộ ba số Pythagoras thì phương trình (1)

luôn có một nghiệm là $(x, y, z) = (2, 2, 2)$. Một câu hỏi tự nhiên đặt ra là ngoài nghiệm này phương trình (1) có còn nghiệm nguyên dương nào khác không? Năm 1956, W. Sierpiński [11] đã chứng minh rằng phương trình (1) không có nghiệm nào khác nếu $(a, b, c) = (3, 4, 5)$. Sau đó, Jeśmanowicz [8] cũng đưa ra câu trả lời phủ định cho các trường hợp (a, b, c) lần lượt là các bộ $(5, 12, 13); (7, 24, 25), (9, 40, 41); (11, 60, 61)$. Từ đó, Jeśmanowicz đã đưa ra giả thuyết "*Nếu a, b, c là bộ ba số Pythagoras nguyên thủy thì phương trình (1) không có nghiệm nguyên dương nào khác ngoài nghiệm* $(2, 2, 2)$".

Nhiều nhà toán học đã chứng minh giả thuyết của Jeśmanowicz nhưng mới chỉ dừng lại ở một vài trường hợp riêng lẻ. Chú ý rằng theo Euclid, tồn tại các số nguyên m, n sao cho $a = m^2 - n^2, b = 2mn$ và $c = m^2 + n^2$, trong đó $m > n > 0, \gcd(m, n) = 1$ và $m \not\equiv n(\mod 2)$. Năm 1959, Lu[10] đã chứng minh giả thuyết cho trường hợp $n = 1$. Năm 1965, Dem'janenko [3] đưa ra chứng minh khi $m - n = 1$. Tuy nhiên, nhìn chung bài toán chưa được giải quyết cho trường hợp tổng quát.

Khó khăn thứ nhất khi chứng minh giả thuyết này là khẳng định các nghiệm (x, y, z) đều chẵn. Để giải quyết vấn đề này, trong [2, 4], các tác giả đã giả thiết a, b, c có các ước nguyên tố nhất định và sử dụng biến đổi đồng dư sơ cấp cùng với luật tương hỗ bậc hai để chứng minh các x, y, z đều chẵn. Đặc biệt, nếu x, y, z chẵn và 2 là ước thực sự của mn thì $y/2 = 1$ và giả thuyết luôn đúng (xem [9]). Chẳng hạn, nếu $m \equiv 1 \pmod 8$ và $n \equiv 6 \pmod 8$ thì luôn kéo theo $(x, y, z) = (2, 2, 2)$.

Khó khăn thứ hai là chứng minh lập luận "nếu (x, y, z) là chẵn

(do đó có thể viết $x = 2X, y = 2Y, z = 2Z$) và 4 là ước của mn thì $(X, Y, Z) = (1, 1, 1)$". Trong tình huống này, quan trọng là cần xác định được tính chẵn, lẻ của X, Y, Z. Ngay cả khi có giả thiết về tính chẵn, lẻ của X, Y, Z cũng rất khó chứng minh được giả thuyết. Hầu hết các kết quả về giả thuyết này đều xoay quanh giả thiết 2 là ước thực sự của mn. Rất ít các kết quả xét trường hợp mn chia hết cho 4 (xem [4]).

Mục đích của luận văn là trình bày lại kết quả của Takafumi Miyazaki trong bài báo *On the conjecture of Jeśmanowicz concerning Pythagorean triples* đăng trên tạp chí *Bull. Aust. Math. Soc* năm 2009. Trong bài báo này, ông xem xét giả thuyết khi b chia hết cho 8 và chứng minh giả thuyết đúng khi a không có ước nguyên tố nào đồng dư với 1 theo modulo 4. Ông cũng kiểm tra tính chẵn, lẻ của các biến x, y, z và đưa ra các bộ (a, b, c) mới thỏa mãn giả thuyết khi b chia hết cho 8. Về kỹ thuật chứng minh, ông chủ yếu sử dụng đồng dư sơ cấp và các kết quả về phương trình Fermat suy rộng của Darmon và Merel [5].

Nội dung luận văn được chia làm hai chương. Chương 1 trình bày các kiến thức chuẩn bị về đồng dư thức, ký hiệu Legendre, Ký hiệu Jacobi, Luật tương hỗ bậc hai. Trong chương này, các khái niệm đều được minh họa bằng những ví dụ cụ thể và các tính chất được chứng minh một cách rõ ràng, chi tiết. Nội dung chương 2 gồm tính chất của bộ ba số Pythagoras nguyên thủy, chứng minh giả thuyết Jeśmanowicz trong trường hợp a không có ước nguyên tố nào đồng dư với 1 theo modulo 4 và trường hợp b là bội của 8.

Thái Nguyên, tháng 01 năm 2021

Chương 1

Một số kiến thức chuẩn bị

Mục tiêu của chương này là trình bày một cách chi tiết các khái niệm và tính chất về đồng dư thức, ký hiệu Legendre, Ký hiệu Jacobi, luật tương hỗ bậc hai. Đây là các kỹ thuật được dùng để chứng minh các kết quả ở chương 2. Nội dung chương này được trình bày dựa theo [6].

1.1 Đồng dư thức

Lý thuyết đồng dư được nhà toán học Gauss bắt đầu xây dựng và phát triển từ đầu thế kỷ XIX. Đây là một nội dung quan trọng của số học. Theo lịch sử, nhiều nhà Toán học Trung Quốc đã có khái niệm về đồng dư và vận dụng nó trong việc giải nhiều bài toán từ nhiều thế kỷ trước đó. Việc hiểu biết các khái niệm và tính chất của đồng dư thức giúp ta giải nhiều bài toán khó trong số học một cách nhẹ nhàng, ngắn gọn.

Định nghĩa 1.1.1. Cho các số nguyên a, b, m. Ta nói *a đồng dư với b theo modulo m* nếu $m \mid (a - b)$.

Nếu a đồng dư với b theo modulo m thì ta viết $a \equiv b \pmod{m}$. Nếu $m \nmid (a - b)$ thì ta viết $a \not\equiv b \pmod{m}$ và ta nói a và b *không đồng dư theo modulo m*.

Sử dụng định nghĩa đồng dư thức, ta dễ dàng chứng minh được các tính chất sau của đồng dư thức.

Mệnh đề 1.1.2. *Nếu a, b là các số nguyên thì $a \equiv b \pmod{m}$ nếu và chỉ nếu tồn tại số nguyên k sao cho $a = b + km$.*

Mệnh đề 1.1.3. *Cho m là số nguyên dương. Quan hệ đồng dư theo modulo m thỏa mãn các tính chất sau*

(i) *Phản xạ: $a \equiv a \pmod{m}$ với mọi số nguyên a.*

(ii) *Đối xứng: Nếu a, b là các số nguyên sao cho $a \equiv b \pmod{m}$ thì $b \equiv a \pmod{m}$.*

(iii) *Bắc cầu: Nếu a, b, c là các số nguyên sao cho $a \equiv b \pmod{m}$ thì $b \equiv a \pmod{m}$.*

Cho số nguyên a và số nguyên dương m. Theo thuật toán chia với dư, ta viết được $a = bm + r$ với $0 \leq r \leq m - 1$. Đẳng thức này chứng tỏ $a \equiv r \pmod{m}$. Vì thế mỗi số nguyên đều đồng dư với một trong các số nguyên $0, 1, \ldots, m - 1$, là các phần dư có được khi chia cho m. Do hai số bất kì trong các số $0, 1, \ldots, m - 1$ không đồng dư với nhau theo modulo m nên có tất cả m số nguyên sao cho bất kỳ số nguyên nào đều đồng dư theo modulo m với đúng một trong m số đó.

Định nghĩa 1.1.4. *Một hệ thặng dư đầy đủ theo modulo m* là một tập hợp các số nguyên sao cho mỗi số nguyên đều đồng dư theo modulo m với đúng một số nguyên trong tập hợp đó.

Ví dụ 1.1.5. (i) Thuật toán chia với dư chứng tỏ rằng tập các số nguyên $\{0, 1, \ldots, m - 1\}$ là một hệ thặng dư đầy đủ theo modulo m. Hệ này được gọi là *hệ thặng dư không âm bé nhất theo modulo m.*

(ii) Cho m là số nguyên dương lẻ. Khi đó tập các số nguyên

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$$

là một hệ thặng dư đầy đủ.

Đồng dư thức có nhiều tính chất tương tự như đẳng thức. Trước hết, quan hệ đồng dư được bảo toàn khi cộng, trừ hoặc nhân hai vế của đồng dư thức với cùng một số nguyên.

Định lý 1.1.6. *Nếu a, b, c, m là các số nguyên với $m > 0$ sao cho $a \equiv b \pmod{m}$ thì*

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Chú ý rằng quan hệ đồng dư chưa chắc đã được bảo toàn khi chia hai vế của một đồng dư thức cho cùng một số nguyên khác 0. Chẳng hạn, $14 = 7.2 \equiv 4.2 = 8 \pmod{6}$ nhưng $7 \not\equiv 4 \pmod{6}$. Tuy nhiên, Định lý sau cho ta một kết quả đúng về phép chia hai vế của đồng dư thức cho cùng một số nguyên khác 0.

Định lý 1.1.7. *Nếu a, b, c và m là các số nguyên sao cho $m > 0$, và $d = \gcd(c, m)$ và $ac \equiv bc \pmod{m}$, thì $a \equiv b \pmod{m/d}$.*

Hệ quả 1.1.8. *Nếu a, b, c và m là các số nguyên sao cho $m > 0$ và $\gcd(c, m) = 1$, $ac \equiv bc \pmod{m}$ thì $a \equiv b \pmod{m}$.*

Ví dụ 1.1.9. Vì $42 \equiv 7 \pmod{5}$ và $\gcd(5, 7) = 1$ nên $42/7 \equiv 7/7 \pmod{5}$ hay $6 \equiv 1 \pmod{5}$.

Định lý 1.1.10. *Nếu a, b, c, d và m là các số nguyên sao cho $m > 0$, $a \equiv b \pmod{m}$ và $c \equiv d \pmod{m}$ thì*

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

Ví dụ 1.1.11. Vì $13 \equiv 8 \pmod{5}$ và $7 \equiv 2 \pmod{5}$ nên sử dụng Định lý 1.1.10 ta được $20 = 13 + 7 \equiv 8 + 2 \equiv 0 \pmod{5}$, $6 = 13 - 7 \equiv 8 - 7 = 1 \pmod{5}$, và $91 = 13.7 \equiv 8.2 = 16 \pmod{5}$.

Định lý 1.1.12. *Cho $b \in \mathbb{Z}$. Nếu $r_1, r_2, \ldots, r_m$ là một hệ thặng dư đầy đủ theo modulo m và a là số nguyên dương sao cho $\gcd(a, m) = 1$ thì*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

là một hệ thặng dư đầy đủ theo modulo m.

Chứng minh. Trước hết, ta chứng minh không có hai trong số các số nguyên

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

đồng dư với nhau theo modulo m. Thật vậy, nếu $ar_j + b \equiv ar_k + b \pmod{m}$ thì theo Định lý 1.1.6(ii) ta có

$$ar_j \equiv ar_k \pmod{m}.$$

Vì $\gcd(a, m) = 1$ nên theo Hệ quả 1.1.8 ta có

$$r_j \equiv r_k \pmod{m}.$$

Do $r_j \not\equiv r_k \pmod{m}$ nếu $j \neq k$ nên ta suy ra $j = k$. Vì tập $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ gồm m số nguyên đôi một không đồng dư với nhau theo modulo m nên tập này là một hệ thặng dư đầy đủ theo modulo m. □

Định lý sau khẳng định đồng dư thức được bảo toàn qua phép nâng lũy thừa.

Định lý 1.1.13. *Nếu a, b, k và m là các số nguyên sao cho $k > 0, m > 0$ và $a \equiv b \pmod{m}$, thì $a^k \equiv b^k \pmod{m}$.*