

**BỘ GIÁO DỤC VÀ ĐÀO TẠO
ĐẠI HỌC ĐÀ NẴNG**

TRIỆU THỊ VY VY

**THẠNG DƯ CHÍNH PHƯƠNG, KÍ HIỆU
LEGENDRE,
KÍ HIỆU JACOBI VÀ ỨNG DỤNG**

**Chuyên ngành: Phương pháp Toán sơ cấp
Mã số: 60.46.40**

TÓM TẮT LUẬN VĂN THẠC SĨ KHOA HỌC

Đà Nẵng - Năm 2011

**Công trình được hoàn thành tại
ĐẠI HỌC ĐÀ NẴNG**

Người hướng dẫn khoa học: TS. NGUYỄN DUY THÁI SON

Phản biện 1: TS. Nguyễn Ngọc Châu

Phản biện 2: GS. TSKH. Nguyễn Văn Mậu

Luận văn được bảo vệ trước hội đồng chấm
Luận văn tốt nghiệp thạc sĩ Khoa học hợp tại Đại
học Đà Nẵng vào ngày 23 tháng 10 năm 2011

Có thể tìm hiểu luận văn tại:

- Trung tâm Thông tin - Học liệu, Đại học Đà Nẵng
- Thư viện trường Đại học Sư phạm, Đại học Đà
Nẵng

MỞ ĐẦU

1. Lý do chọn đề tài

Có thể nói: thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi là những mảng kiến thức hay và khó liên quan đến lý thuyết đồng dư, đồng thời có nhiều ứng dụng trong Số học. Vì thế, trong các kì thi chọn học sinh giỏi ở các nước (nhất là các kì thi chọn đội tuyển Olympic Toán), những mảng kiến thức này thường được quan tâm đáng kể. Ở nước ta, theo chỗ chúng tôi biết, mãi đến năm 2008 mới có một tài liệu tiếng Việt [2] chính thức đề cập đến cả ba mảng thặng dư chính phương, kí hiệu Legendre và kí hiệu Jacobi; do đó việc giảng dạy các kiến thức này một cách đầy đủ ở bậc trung học phổ thông gặp không ít khó khăn, nhất là khi mà giáo viên thường chưa được đào tạo chuyên sâu về chúng.

Vì những lý do trên, tôi chọn đề tài “*Thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi và ứng dụng*” để nghiên cứu.

2. Mục đích và nhiệm vụ nghiên cứu

Chương 1, chương 2 của luận văn sẽ trình bày một cách đầy đủ nhất – theo cách hiểu của chúng tôi – về lý thuyết thặng dư chính phương, thặng dư không chính phương, kí hiệu Legendre, kí hiệu Jacobi với nhiều ví dụ minh họa.

Trong chương 3, chúng tôi tìm cách đưa ra các ứng dụng và xây dựng một hệ thống các bài toán theo mức độ từ dễ đến khó liên quan đến các vấn đề về thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi.

3. Đối tượng và phạm vi nghiên cứu

3.1. Đối tượng nghiên cứu

Đối tượng nghiên cứu là thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi và ứng dụng.

3.2. Phạm vi nghiên cứu

Nghiên cứu lý thuyết và ứng dụng của thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi dựa trên lý thuyết về đồng dư.

4. Phương pháp nghiên cứu

Trong luận văn này, chúng tôi thu thập và đọc các tài liệu tìm được từ nhiều nguồn khác nhau (đặc biệt là các thư mục trên internet có liên quan đến đề tài) để phân tích, nghiên cứu lý thuyết về thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi và viết lại một cách hệ thống theo cách chúng tôi hiểu.

5. Ý nghĩa khoa học và thực tiễn của đề tài

Xây dựng được một tài liệu tham khảo bổ ích cho giáo viên và học sinh trung học phổ thông về thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi, trong đó phần lý thuyết được chứng minh chặt chẽ và các bài toán được hệ thống tương đối đầy đủ và cập nhật theo mức độ từ dễ đến khó.

6. Cấu trúc của luận văn

Ngoài phần mở đầu và kết luận, luận văn gồm có 3 chương:

Chương 1. Thặng dư chính phương, thặng dư không chính phương và kí hiệu Legendre.

Chương 2. Kí hiệu Jacobi và số giả nguyên tố Euler.

Chương 3. Một số ứng dụng và các bài toán.

Chương 1
THẶNG DƯ CHÍNH PHƯƠNG
THẶNG DƯ KHÔNG CHÍNH PHƯƠNG
KÍ HIỆU LEGENDRE

1.1. Thặng dư chính phương - thặng dư không chính phương

Định nghĩa 1.1. Cho m là số nguyên dương và a là số nguyên nguyên tố cùng nhau với m . Nếu đồng dư thức $x^2 \equiv a(\text{mod } m)$ có nghiệm thì ta nói rằng a là một thặng dư chính phương của m . Ngược lại, nếu đồng dư thức $x^2 \equiv a(\text{mod } m)$ không có nghiệm, ta nói rằng a là một thặng dư không chính phương của m .

Ví dụ 1.1. Để xác định các số nguyên là thặng dư chính phương của 13, chúng ta tính bình phương của các số nguyên 1, 2, ..., 12.

Ta thấy rằng:

$$1^2 \equiv 12^2 \equiv 1(\text{mod } 13); \quad 2^2 \equiv 11^2 \equiv 4(\text{mod } 13)$$

$$3^2 \equiv 10^2 \equiv 9(\text{mod } 13); \quad 4^2 \equiv 9^2 \equiv 3(\text{mod } 13)$$

$$5^2 \equiv 8^2 \equiv 12(\text{mod } 13); \quad 6^2 \equiv 7^2 \equiv 10(\text{mod } 13).$$

Như vậy, các thặng dư chính phương của 13 là 1, 3, 4, 9, 10, 12; các số nguyên 2, 5, 6, 7, 8, 11 là các thặng dư không chính phương của 13.

Trong chương 1 này, chúng ta sẽ nghiên cứu thặng dư chính phương, thặng dư không chính phương của số nguyên tố lẻ p .

Chúng ta sẽ chỉ ra rằng, nếu p là một số nguyên tố lẻ thì số các thặng dư chính phương của p bằng số các thặng dư không chính phương của p trong tập $S = \{1, 2, \dots, p-1\}$.

Bổ đề 1.1. Cho p là một số nguyên tố lẻ và a là một số nguyên nguyên tố cùng nhau với p . Khi đó, đồng dư thức $x^2 \equiv a \pmod{p}$ hoặc là không có nghiệm, hoặc là có đúng hai nghiệm không đồng dư mod p .

Bổ đề trên dẫn dắt chúng ta đến định lí sau:

Định lí 1.1. Nếu p là một số nguyên tố lẻ thì có đúng $\frac{p-1}{2}$ thặng dư chính phương của p và $\frac{p-1}{2}$ thặng dư không chính phương của p trong tập $S = \{1, 2, \dots, p-1\}$.

Một kí hiệu liên kết đặc biệt với thặng dư chính phương được mô tả trong định nghĩa sau:

1.2. Kí hiệu Legendre

1.2.1. Định nghĩa 1.2. Cho p là một số nguyên tố lẻ và a là một số nguyên nguyên tố cùng nhau với p . Kí hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{nếu } a \text{ là thặng dư chính phương của } p \\ -1 & \text{nếu } a \text{ là thặng dư không chính phương của } p. \end{cases}$$

Kí hiệu này được đặt tên sau khi nhà Toán học người Pháp là Adrien-Marie Legendre giới thiệu việc sử dụng kí hiệu này.

Ví dụ 1.2. Theo ví dụ 1.1, kí hiệu Legendre $\left(\frac{a}{13}\right)$, với $a = 1, 2, \dots, 12$, có giá trị như sau:

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1;$$

$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

1.2.2. Tiêu chuẩn Euler. Cho p là một số nguyên tố lẻ và a là một số nguyên nguyên tố cùng nhau với p . Khi đó:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Ví dụ 1.3. Trường hợp $p = 13$, ta có:

$$3^{\frac{13-1}{2}} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13}.$$

Vì vậy, $\left(\frac{3}{13}\right) = 1$, tức là 3 là một thặng dư chính phương của

13.

1.2.3. Các tính chất của kí hiệu Legendre

Định lí 1.2. Cho p là một số nguyên tố lẻ và a, b là các số nguyên nguyên tố cùng nhau với p . Khi đó:

$$(i) \text{ Nếu } a \equiv b \pmod{p} \text{ thì } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \quad (1.1)$$

$$(ii) \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \quad (1.2)$$

$$(iii) \left(\frac{a^2}{p}\right) = 1. \quad (1.3)$$

Ví dụ 1.4. Tính $\left(\frac{317}{13}\right)$.

Vì $317 \equiv 5 \pmod{13}$ nên theo công thức (1.1), ta được:

$$\left(\frac{317}{13}\right) = \left(\frac{5}{13}\right) = -1.$$

Sử dụng tiêu chuẩn Euler, chúng ta có thể phân lớp những số nguyên tố có -1 là một thặng dư chính phương hoặc -1 là một thặng dư không chính phương.

Định lí 1.3. Nếu p là một số nguyên tố lẻ thì

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod{4} \\ -1 & \text{nếu } p \equiv -1 \pmod{4}. \end{cases}$$

Một kết quả đẹp sau đây của nhà toán học Gauss cung cấp một tiêu chuẩn khác để xác định khi nào số nguyên a nguyên tố cùng nhau với số nguyên tố p là một thặng dư chính phương của p .

Bổ đề 1.2. (Bổ đề Gauss). Cho p là một số nguyên tố lẻ và a là một số nguyên nguyên tố cùng nhau với p . Nếu s là số các thặng dư dương bé nhất modulo p của các số nguyên $a, 2a, 3a, \dots, \frac{p-1}{2}a$ mà lớn hơn $\frac{p}{2}$ thì $\left(\frac{a}{p}\right) = (-1)^s$.

Ví dụ 1.5. Cho $a = 5$ và $p = 13$. Sử dụng bổ đề Gauss, tính $\left(\frac{5}{13}\right)$.

Ta tính các thặng dư dương bé nhất modulo 13 của 1.5, 2.5, 3.5, 4.5, 5.5 và 6.5. Đó tương ứng là 5, 10, 2, 7, 12 và 4.

Có 3 số trong các số này lớn hơn $\frac{13}{2}$.

$$\text{Vậy, } \left(\frac{5}{13}\right) = (-1)^3 = -1.$$

Sử dụng bổ đề Gauss, ta có thể định rõ đặc điểm của tất cả các số nguyên tố có 2 là một thặng dư chính phương.

Định lý 1.4. Nếu p là một số nguyên tố lẻ thì

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (1.4)$$

Như vậy, 2 là một thặng dư chính phương của các số nguyên tố p thỏa $p \equiv \pm 1 \pmod{8}$ và là một thặng dư không chính phương của các số nguyên tố p thỏa $p \equiv \pm 3 \pmod{8}$.

$$\left(\frac{2}{p}\right) = 1 \text{ nếu } p \equiv \pm 1 \pmod{8};$$

$$\left(\frac{2}{p}\right) = -1 \text{ nếu } p \equiv \pm 3 \pmod{8}.$$

Ví dụ 1.6. Theo định lí 1.4, ta thấy rằng:

$$\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right) = \left(\frac{2}{23}\right) = \left(\frac{2}{31}\right) = 1;$$

$$\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{19}\right) = \left(\frac{2}{29}\right) = -1.$$

Ví dụ 1.7. Tính $\left(\frac{89}{13}\right)$.

$$\text{Ta có } 89 \equiv -2 \pmod{13} \text{ nên } \left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{2}{13}\right).$$

$$\text{Vì } 13 \equiv 1 \pmod{4} \text{ nên theo định lí 1.3, ta có } \left(\frac{-1}{13}\right) = 1.$$

$$\text{Từ } 13 \equiv -3 \pmod{8}, \text{ theo định lí 1.4, ta có } \left(\frac{2}{13}\right) = -1.$$

$$\text{Vậy } \left(\frac{89}{13}\right) = -1.$$

Tiếp theo, chúng ta trình bày định luật về tính thuận nghịch chính phương, một nền tảng quan trọng cho sự đánh giá kí hiệu Legendre.

1.3. Định luật về tính thuận nghịch chính phương

Cho p và q là hai số nguyên tố khác nhau, q là một thặng dư chính phương của p . Khi đó, ta có biết được rằng p là một thặng dư chính phương của q ? Định lí sau đây giúp ta trả lời câu hỏi này.

Định lí 1.5. (Định luật về tính thuận nghịch chính phương) Cho p và q là hai số nguyên tố lẻ khác nhau. Khi đó

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Ta chú ý rằng số $\frac{p-1}{2}$ là số chẵn khi $p \equiv 1 \pmod{4}$ và là số lẻ khi $p \equiv 3 \pmod{4}$.

Do vậy:

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ là chẵn nếu $p \equiv 1 \pmod{4}$ hoặc $q \equiv 1 \pmod{4}$;

$\frac{p-1}{2} \cdot \frac{q-1}{2}$ là lẻ nếu $p \equiv 3 \pmod{4}$ và $q \equiv 3 \pmod{4}$.

Từ đó, ta có:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod{4} \text{ hoặc } q \equiv 1 \pmod{4} \\ -1 & \text{nếu } p \equiv 3 \pmod{4} \text{ và } q \equiv 3 \pmod{4}. \end{cases}$$

Vì giá trị của $\left(\frac{p}{q}\right)$ và $\left(\frac{q}{p}\right)$ chỉ có thể là 1 hoặc -1 nên:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{nếu } p \equiv 1 \pmod{4} \text{ hoặc } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{nếu } p \equiv 3 \pmod{4} \text{ và } q \equiv 3 \pmod{4}. \end{cases}$$

Ví dụ 1.8. Cho $p = 13$ và $q = 17$. Tính $\left(\frac{13}{17}\right)$ và $\left(\frac{17}{13}\right)$.

Ta có $p \equiv q \equiv 1 \pmod{4}$.

Do vậy $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$.

Vì $17 \equiv 4 \pmod{13}$ nên theo (1.1), ta có $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right)$.

Theo (1.3), ta có $\left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$.

$$\text{Vậy } \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1.$$

Ví dụ 1.9. Cho $p = 7$ và $q = 19$. Tính $\left(\frac{7}{19}\right)$.

Ta có $p \equiv q \equiv 3 \pmod{4}$.

Áp dụng định luật về tính thuận nghịch chính phương, ta được:

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right).$$

Vì $19 \equiv 5 \pmod{7}$ nên theo (1.1), ta có $\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right)$.

Lại có $5 \equiv 1 \pmod{4}$, sử dụng định luật về tính thuận nghịch chính phương một lần nữa, ta được $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$.

Vì $7 \equiv 2 \pmod{5}$ và $5 \equiv -3 \pmod{8}$ nên theo (1.1) và (1.6), ta được:

$$\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

$$\text{Vậy } \left(\frac{7}{19}\right) = 1.$$

Ví dụ 1.10. Biết rằng 1009 là số nguyên tố. Tính $\left(\frac{713}{1009}\right)$.

Ta phân tích $713 = 23 \cdot 31$.

Theo (1.2):

$$\left(\frac{713}{1009}\right) = \left(\frac{23 \cdot 31}{1009}\right) = \left(\frac{23}{1009}\right) \cdot \left(\frac{31}{1009}\right).$$

Từ $1009 \equiv 1 \pmod{4}$, ta được:

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right); \quad \left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right).$$

Vì $1009 \equiv 20 \pmod{23}$, $1009 \equiv 17 \pmod{31}$ nên theo (1.1):

$$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right); \quad \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right).$$

Theo (1.2) và (1.3), ta có:

$$\left(\frac{20}{23}\right) = \left(\frac{2^2 \cdot 5}{23}\right) = \left(\frac{2^2}{23}\right) \left(\frac{5}{23}\right) = \left(\frac{5}{23}\right).$$

Do $5 \equiv 1 \pmod{4}$ nên theo định luật về tính thuận nghịch chính phương:

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right).$$

Vì $23 \equiv 3 \pmod{5}$ nên theo (1.2):

$$\left(\frac{23}{5}\right) = \left(\frac{3}{5}\right).$$

Áp dụng định luật về tính thuận nghịch chính phương một lần nữa, ta được $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)$.

Vì $5 \equiv 2 \pmod{3}$ nên theo (1.1) và (1.6), ta được $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Như vậy $\left(\frac{23}{1009}\right) = -1$.

$$\begin{aligned} \text{Tương tự, } \left(\frac{17}{31}\right) &= \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right) \left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) \\ &= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2^2}{3}\right) = -1. \end{aligned}$$

Như vậy $\left(\frac{31}{1009}\right) = -1$.

$$\text{Vậy } \left(\frac{713}{1009} \right) = 1.$$

Bổ đề 1.3. Nếu p là một số nguyên tố lẻ và a là một số nguyên lẻ không chia hết cho p thì

$$\left(\frac{a}{p} \right) = (-1)^{T(a, p)}$$

$$\text{trong đó, } T(a, p) = \sum_{j=1}^{p-1} \left[\frac{ja}{p} \right].$$

Ví dụ 1.11. Tính $\left(\frac{7}{11} \right)$ và $\left(\frac{11}{7} \right)$.

Sử dụng bổ đề 1.3, ta tính tổng:

$$\sum_{j=1}^5 \left[\frac{7j}{11} \right] = \left[\frac{7}{11} \right] + \left[\frac{14}{11} \right] + \left[\frac{21}{11} \right] + \left[\frac{28}{11} \right] + \left[\frac{35}{11} \right] = 0 + 1 + 1 + 2 + 3 = 7.$$

$$\text{Vậy } \left(\frac{7}{11} \right) = (-1)^7 = -1.$$

Tương tự, ta có:

$$\sum_{j=1}^3 \left[\frac{11j}{7} \right] = \left[\frac{11}{7} \right] + \left[\frac{22}{7} \right] + \left[\frac{33}{7} \right] = 1 + 3 + 4 = 8.$$

$$\text{Vậy } \left(\frac{11}{7} \right) = (-1)^8 = 1.$$

Hệ quả. Nếu p là số nguyên tố lẻ thì

$$\text{a) } \left(\frac{3}{p} \right) = \begin{cases} 1 & \text{nếu } p \equiv \pm 1 \pmod{12} \\ -1 & \text{nếu } p \equiv \pm 5 \pmod{12} \end{cases}$$

$$\text{b) } \left(\frac{-3}{p} \right) = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod{6} \\ -1 & \text{nếu } p \equiv -1 \pmod{6}. \end{cases}$$

Chương 2

KÍ HIỆU JACOBI VÀ SỐ GIẢ NGUYÊN TỐ EULER

Trong phần này, chúng ta định nghĩa kí hiệu Jacobi. Kí hiệu này được giới thiệu bởi nhà Toán học người Đức tên là Carl Jacobi.

Kí hiệu Jacobi là một sự mở rộng của kí hiệu Legendre. Nó được sử dụng để đánh giá kí hiệu Legendre và định nghĩa số giả nguyên tố Euler.

2.1. Kí hiệu Jacobi

Định nghĩa 2.1. Cho n là một số nguyên dương lẻ có phân tích tiêu chuẩn $n = p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}$ (p_i ($i = \overline{1, m}$) là các số nguyên tố, t_i ($i = \overline{1, m}$) là các số nguyên dương) và a là một số nguyên nguyên tố cùng nhau với n . Khi đó, kí hiệu Jacobi $\left(\frac{a}{n}\right)$ được định nghĩa như sau:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}}\right) = \left(\frac{a}{p_1}\right)^{t_1} \left(\frac{a}{p_2}\right)^{t_2} \dots \left(\frac{a}{p_m}\right)^{t_m}$$

trong đó $\left(\frac{a}{p_1}\right), \left(\frac{a}{p_2}\right), \dots, \left(\frac{a}{p_m}\right)$ là các kí hiệu Legendre.

Ví dụ 2.1. Từ định nghĩa kí hiệu Jacobi, ta thấy rằng:

$$\begin{aligned} \left(\frac{2}{75}\right) &= \left(\frac{2}{3 \cdot 5^2}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right)^2 = (-1)(-1)^2 = (-1); \\ \left(\frac{37}{385}\right) &= \left(\frac{37}{5 \cdot 7 \cdot 11}\right) = \left(\frac{37}{5}\right) \left(\frac{37}{7}\right) \left(\frac{37}{11}\right) = \left(\frac{2}{5}\right) \left(\frac{2}{7}\right) \left(\frac{4}{11}\right) \\ &= (-1) \cdot 1 \cdot \left(\frac{2}{11}\right)^2 = (-1) \cdot 1 \cdot (-1)^2 = -1. \end{aligned}$$

Khi n là số nguyên tố, kí hiệu Jacobi chính là kí hiệu Legendre.

Ta thấy rằng, nếu $x^2 \equiv a \pmod{n}$ có nghiệm và $p_i \left(i = \overline{1, m} \right)$ là ước nguyên tố của n thì $x^2 \equiv a \pmod{p_i}$ cũng có nghiệm. Vì vậy,

$$\left(\frac{a}{p_i} \right) = 1. \text{ Do đó:}$$

$$\left(\frac{a}{n} \right) = \left(\frac{a}{p_1^{t_1} p_2^{t_2} \dots p_m^{t_m}} \right) = \left(\frac{a}{p_1} \right)^{t_1} \left(\frac{a}{p_2} \right)^{t_2} \dots \left(\frac{a}{p_m} \right)^{t_m} = 1.$$

Ngược lại, cho $n = 15$ và $a = 2$. Ta có $\left(\frac{2}{15} \right) = \left(\frac{2}{3} \right) \left(\frac{2}{5} \right) = (-1)(-1) = 1$. Tuy nhiên, đồng dư thức $x^2 \equiv 2 \pmod{15}$ không có nghiệm do $x^2 \equiv 2 \pmod{3}$ và $x^2 \equiv 2 \pmod{5}$ không có nghiệm. Như vậy, nếu $\left(\frac{a}{n} \right) = 1$, ta chưa thể kết luận được $x^2 \equiv a \pmod{n}$ có nghiệm hay không.

2.2. Các tính chất của kí hiệu Jacobi

Định lí 2.1. Cho n là số nguyên dương lẻ và a, b là hai số nguyên nguyên tố cùng nhau với n . Khi đó

$$(i) \quad \text{Nếu } a \equiv b \pmod{n} \text{ thì } \left(\frac{a}{n} \right) = \left(\frac{b}{n} \right). \quad (2.1)$$

$$(ii) \quad \left(\frac{ab}{n} \right) = \left(\frac{a}{n} \right) \left(\frac{b}{n} \right). \quad (2.2)$$

$$(iii) \quad \left(\frac{-1}{n} \right) = (-1)^{\frac{n-1}{2}}. \quad (2.3)$$

$$(iv) \quad \left(\frac{2}{n} \right) = (-1)^{\frac{n^2-1}{8}}. \quad (2.4)$$

2.3. Định luật về tính thuận nghịch đối với kí hiệu Jacobi

Định lí 2.2. Cho n, m là hai số nguyên dương lẻ nguyên tố cùng nhau. Khi đó

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

Bây giờ, chúng ta sẽ giới thiệu một thuật toán để đánh giá kí hiệu Jacobi.

Cho a và b là hai số nguyên dương với $(a, b) = 1, a > b$.

Gọi $R_0 = a, R_1 = b$. Sử dụng thuật toán chia, chia R_0 cho R_1 và phân tích số dư thành tích của lũy thừa cao nhất của 2 và một số nguyên dương lẻ, ta được:

$$R_0 = R_1 q_1 + 2^{s_1} R_2,$$

trong đó, s_1 là một số nguyên không âm và R_2 là một số nguyên dương lẻ với $R_2 < R_1$.

Ta lại lấy R_1 chia cho R_2 và phân tích số dư thành tích của lũy thừa cao nhất của 2 và một số nguyên dương lẻ, ta được:

$$R_1 = R_2 q_2 + 2^{s_2} R_3,$$

trong đó, s_2 là một số nguyên không âm và R_3 là một số nguyên dương lẻ với $R_3 < R_2$.

Tiếp tục như vậy cho đến khi $R_n = 1$, tức là:

$$R_2 = R_3 q_3 + 2^{s_3} R_4$$

...

$$R_{n-3} = R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1}$$

$$R_{n-2} = R_{n-1} q_{n-1} + 2^{s_{n-1}} \cdot 1,$$

trong đó, s_j là một số nguyên không âm và R_{j+1} là một số nguyên dương lẻ với $R_{j+1} < R_j, j = \overline{2, n-1}$.

Ta minh họa dãy các đẳng thức này bởi ví dụ sau:

Ví dụ 2.2. Cho $a = 401$, $b = 111$. Khi đó:

$$401 = 111.3 + 2^2.17$$

$$111 = 17.6 + 2^0.9$$

$$17 = 9.1 + 2^3.1.$$

Định lí 2.3. Cho a và b là hai số nguyên dương với $a > b$. Khi đó:

$$\left(\frac{a}{b}\right) = (-1)^{s_1 \frac{R_1^2-1}{8} + s_2 \frac{R_2^2-1}{8} + \dots + s_{n-1} \frac{R_{n-1}^2-1}{8} + \frac{R_1-1}{2} \cdot \frac{R_2-1}{2} + \frac{R_2-1}{2} \cdot \frac{R_3-1}{2} + \dots + \frac{R_{n-2}-1}{2} \cdot \frac{R_{n-1}-1}{2}}$$

trong đó, các số nguyên R_j và s_j , $j = \overline{1, n-1}$ được mô tả như trên.

Ví dụ 2.3. Tính $\left(\frac{401}{111}\right)$.

Từ ví dụ 2.2, ta được:

$$\left(\frac{401}{111}\right) = (-1)^{2 \cdot \frac{111^2-1}{8} + 0 \cdot \frac{17^2-1}{8} + 3 \cdot \frac{9^2-1}{8} + \frac{111-1}{2} \cdot \frac{17-1}{2} + \frac{17-1}{2} \cdot \frac{9-1}{2}} = 1.$$

2.4. Số giả nguyên tố Euler

Cho p là một số nguyên tố lẻ và b là một số nguyên nguyên tố cùng nhau với p . Khi đó, theo tiêu chuẩn Euler:

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}.$$

Vì vậy, nếu ta kiểm tra được n là số nguyên tố, b là một số nguyên với $(b, n) = 1$ thì ta được:

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

trong đó, $\left(\frac{b}{n}\right)$ là kí hiệu Jacobi.

Nếu chúng ta chỉ ra được rằng đồng dư thức $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$

là sai, tức là $b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n}$ thì n là hợp số.

Ví dụ 2.4. Cho $n = 341$ và $b = 2$.

Ta tính được $2^{\frac{341-1}{2}} = 2^{170} \equiv 1 \pmod{341}$.

Lại có, từ $341 \equiv -3 \pmod{8}$, theo định lí 2.1, ta được $\left(\frac{2}{341}\right) = -1$.

Do đó $2^{\frac{341-1}{2}} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$.

Vậy $n = 341$ là hợp số.

Định nghĩa 2.2. Cho b là một số nguyên dương. Nếu n là một hợp số nguyên dương lẻ thỏa mãn đồng dư thức

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

thì n được gọi là số giả nguyên tố Euler cơ sở b .

Một số giả nguyên tố Euler cơ sở b là một hợp số, nó được trá hình như là một số nguyên tố bằng cách thỏa mãn đồng dư thức được cho trong định nghĩa.

Ví dụ 2.5. Cho $n = 1105$ và $b = 2$.

Ta có: $1105 = 5 \cdot 13 \cdot 17$.

$$2^{\frac{1105-1}{2}} = 2^{552} = (2^4)^{138} = (16)^{138} \equiv 1 \pmod{5}.$$

$$2^{\frac{1105-1}{2}} = 2^{552} = \left((2^6)^2\right)^{46} = \left((64)^2\right)^{46} \equiv 1 \pmod{13}.$$

$$2^{\frac{1105-1}{2}} = 2^{552} = \left((2^4)^2\right)^{69} = \left((16)^2\right)^{69} \equiv 1 \pmod{17}.$$

Suy ra $2^{\frac{1105-1}{2}} = 2^{552} \equiv 1 \pmod{1105}$.

Từ $1105 \equiv 1 \pmod{8}$ nên $\left(\frac{2}{1105}\right) = 1$.

Do đó $2^{\frac{1105-1}{2}} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$.

Vì 1105 là hợp số nên 1105 là số giả nguyên tố Euler cơ sở 2.

Định lí 2.4. Nếu n là số giả nguyên tố Euler cơ sở b thì n là số giả nguyên tố cơ sở b .

Định lí 2.5. Nếu n là số giả nguyên tố mạnh cơ sở b thì n là số giả nguyên tố Euler cơ sở b .

Như ta đã biết một số giả nguyên tố Euler cơ sở b chưa hẳn là số giả nguyên tố mạnh cơ sở b . Tuy nhiên, khi gặp điều kiện ràng buộc, một số giả nguyên tố Euler cơ sở b là số giả nguyên tố mạnh cơ sở b . Hai định lí sau đây cho chúng ta biết điều đó.

Định lí 2.6. Nếu $n \equiv 3 \pmod{4}$ và n là số giả nguyên tố Euler cơ sở b thì n là số giả nguyên tố mạnh cơ sở b .

Định lí 2.7. Nếu n là số giả nguyên tố Euler cơ sở b và $\left(\frac{b}{n}\right) = -1$ thì n là số giả nguyên tố mạnh cơ sở b .

Chương 3

MỘT SỐ ỨNG DỤNG VÀ CÁC BÀI TOÁN

3.1. Chứng minh đồng dư thức bậc hai có dạng
 $ax^2 + bx + c \equiv 0 \pmod{p}$ **có nghiệm với** p **là số nguyên tố lẻ,**
 $(a, p) = 1$.

$$\text{Xét đồng dư thức } ax^2 + bx + c \equiv 0 \pmod{p} \quad (3.1)$$

với p là số nguyên tố lẻ và $(a, p) = 1$.

Vì $(a, p) = 1$ nên ta cũng có $(4a, p) = 1$.

Đồng dư thức (3.1) tương đương với

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

Sử dụng phân tích $4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$, ta được:

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}.$$

Đặt $y = (2ax + b)$ và $d = (b^2 - 4ac)$, ta được:

$$y^2 \equiv d \pmod{p}. \quad (3.2)$$

Nếu $x \equiv x_0 \pmod{p}$ là nghiệm của (3.1) thì
 $y \equiv (2ax_0 + b) \pmod{p}$ thỏa mãn (3.2). Ngược lại, nếu $y \equiv y_0 \pmod{p}$
 là nghiệm của (3.2) thì từ $2ax \equiv (y_0 - b) \pmod{p}$ ta có thể tìm được
 nghiệm của (3.1).

Bài toán 1. Tìm tất cả các thặng dư chính phương của 29.

Bài toán 2. Tìm giá trị của các kí hiệu Legendre sau:

$$\text{a) } \left(\frac{2}{29} \right) \qquad \text{b) } \left(\frac{-1}{29} \right) \qquad \text{c) } \left(\frac{5}{29} \right)$$

$$\text{d) } \left(\frac{2}{127} \right) \qquad \text{e) } \left(\frac{-1}{127} \right) \qquad \text{f) } \left(\frac{5}{127} \right).$$

Bài toán 3. Những đồng dư thức nào sau đây có nghiệm:

$$\text{a) } x^2 \equiv 2 \pmod{29} \qquad \text{b) } x^2 \equiv 28 \pmod{29}$$

$$\text{c) } x^2 \equiv 5 \pmod{29} \qquad \text{d) } x^2 \equiv 2 \pmod{127}$$

$$\text{e) } x^2 \equiv 126 \pmod{127} \qquad \text{f) } x^2 \equiv 5 \pmod{127}.$$

Bài toán 4. Chứng minh rằng $x^2 \equiv 196 \pmod{1357}$ có nghiệm.

Bài toán 5. Đồng dư thức nào sau đây có nghiệm. Tìm nghiệm của chúng nếu có.

$$\text{a) } 5x^2 + 4x + 7 \equiv 0 \pmod{19};$$

$$\text{b) } 2x^2 + 7x - 13 \equiv 0 \pmod{61}.$$

Bài toán 6. Chứng minh rằng nếu p là số nguyên tố có dạng $4k+1$ thì $x = p'!$ là nghiệm của đồng dư thức $x^2 + 1 \equiv 0 \pmod{p}$ với $p' = \frac{p-1}{2}$.

3.2. Tìm nghiệm của đồng dư thức bậc hai có dạng $x^2 \equiv a \pmod{p^n}$, $n \in \mathbb{N}^*$ với p là số nguyên tố lẻ và $(a, p) = 1$.

Bài toán 7. Chứng minh rằng nếu p là một số nguyên tố lẻ thì đồng dư thức $x^2 \equiv a \pmod{p^n}$, $n \in \mathbb{N}^*$ có nghiệm khi và chỉ khi $\left(\frac{a}{p} \right) = 1$.

3.3. Một số bài toán khác

Bài toán 8. Chứng minh rằng 19 không phải là ước của $4n^2 + 4$ với bất kì số nguyên n nào.

Bài toán 9. Khi các số nguyên dương a và b thay đổi sao cho cả hai số $15a+16b$ và $16a-15b$ đều là các số chính phương dương, hãy tìm giá trị bé nhất có thể có của $\min\{15a+16b, 16a-15b\}$.

Bài toán 10. Cho $k = 2^{2^n} + 1$ với $n \in \mathbb{N}$. Chứng minh rằng k là số nguyên tố khi và chỉ khi k là một ước của $3^{\frac{k-1}{2}} + 1$.

Bài toán 11. Cho m, n là các số nguyên dương thỏa mãn

$$A = \frac{(m+3)^n + 1}{3m}$$

là một số nguyên. Chứng minh rằng A là số lẻ.

Bài toán 12. Tính

$$\left[\frac{1}{2003} \right] + \left[\frac{2}{2003} \right] + \left[\frac{2^2}{2003} \right] + \dots + \left[\frac{2^{2001}}{2003} \right].$$

Bài toán 13. Chứng minh rằng $2^n + 1$ không có ước nguyên tố có dạng $8k + 7$.

Bài toán 14. Chứng minh rằng nếu a là một thặng dư chính phương của số nguyên tố p thì nghiệm của $x^2 \equiv a \pmod{p}$ là

a) $x \equiv \pm a^{n+1} \pmod{p}$ nếu $p = 4n + 3$.

b) $x \equiv \pm a^{n+1} \pmod{p}$ hoặc $x \equiv \pm 2^{2n+1} a^{n+1} \pmod{p}$ nếu $p = 8n + 5$.

Bài toán 15. Chứng minh rằng phương trình $x^2 = y^3 - 5$ không có nghiệm nguyên (x, y) .

Bài toán 16. a) Chứng minh rằng không tồn tại các số tự nhiên x, y sao cho $4xy - x - y$ là một số chính phương.

b) Chứng minh rằng không tồn tại các số tự nhiên x, y, z sao cho $4xyz - x - y$ là một số chính phương.

Bài toán 17. Chứng minh rằng nếu n là số giả nguyên tố Euler cơ sở a và b thì n cũng là số giả nguyên tố Euler cơ sở ab .

Bài toán 18. Chứng minh rằng nếu n là số giả nguyên tố Euler cơ sở b thì n cũng là số giả nguyên tố Euler cơ sở $n - b$.

3.4. Bài tập tham khảo

- 1) Tính $\left(\frac{7}{43}\right)$. Tìm một số nguyên x thỏa mãn $x^2 \equiv 7 \pmod{43}$.
- 2) Cho p là một số nguyên tố. Chứng minh rằng tồn tại $x \in \mathbb{Z}$ thỏa mãn $p \mid x^2 - x + 3$ nếu và chỉ nếu tồn tại $y \in \mathbb{Z}$ thỏa mãn $p \mid y^2 - y + 25$.
- 3) Cho p là một số nguyên tố lẻ. Chứng minh rằng $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.
- 4) Chứng minh rằng với $n \in \mathbb{Z}$, mọi ước nguyên tố p của $n^4 - n^2 + 1$ đều có dạng $12k + 1$, $k \in \mathbb{Z}$.
- 5) Chứng minh rằng một số nguyên a là thặng dư chính phương của mọi số nguyên tố p nếu và chỉ nếu a là số chính phương.
- 6) Chứng minh rằng $\frac{x^2 + 1}{y^2 - 5}$ không phải là số nguyên với bất kì các số nguyên $x, y > 2$.
- 7) Tìm tất cả các số nguyên dương N là thặng dư chính phương của tất cả các số nguyên tố lớn hơn N .

KẾT LUẬN

Luận văn đã trình bày một cách đầy đủ nhất về lý thuyết thặng dư chính phương, thặng dư không chính phương, kí hiệu Legendre, kí hiệu Jacobi với nhiều ví dụ minh họa.

Luận văn đã xây dựng được một hệ thống các bài toán liên quan đến các vấn đề về thặng dư chính phương, kí hiệu Legendre, kí hiệu Jacobi và trình bày một số bài toán trong các kì thi quốc gia, quốc tế, một số bài toán trên các tạp chí Crux,

Luận văn là một tài liệu tham khảo cho giáo viên và học sinh chuyên Toán.