ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—————————o0o—————————

ĐỖ THỊ THOA

ỨNG DỤNG CỦA LUẬT THUẬN NGHỊCH VÀ THẶNG DƯ BẬC HAI

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC
——————o0o——————

ĐỖ THỊ THOA

ỨNG DỤNG CỦA LUẬT THUẬN NGHỊCH VÀ THẶNG DƯ BẬC HAI

CHUYÊN NGÀNH: PHƯƠNG PHÁP TOÁN SƠ CẤP
MÃ SỐ: 8 46 01 13

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS. TS. NGUYỄN VĂN HOÀNG

THÁI NGUYÊN - 2019

Mục lục

Mở đầu

Có thể nói Số học là lĩnh vực xuất hiện sớm nhất trong lịch sử Toán học, nó ra đời từ khi con người bắt đầu làm việc với những con số. Số học là một phân môn quan trọng trong toán học đã gắn bó với tất cả chúng ta xuyên suốt quá trình học toán từ bậc Tiểu học đến Trung học phổ thông. Sự kì diệu của Số học thường tiềm ẩn những thử thách sâu sắc để thách thức trí tuệ của con người. Trong các thành tựu của số học thì luật thuận nghịch và thặng dư bậc hai là một nội dung quan trọng. Đây là những mảng kiến thức liên quan đến lý thuyết đồng dư và có nhiều ứng dụng trong việc giải các bài toán số học hay và khó liên quan đến tính giải được của phương trình đồng dư bậc hai. Nội dung này cho phép ta xác định tính giải được của phương trình đồng dư bậc hai bất kỳ, tuy nhiên nó không cung cấp một phương pháp hiệu quả để tìm nghiệm. Luật thuận nghịch bậc hai (hay còn gọi là luật thuận nghịch của các thặng dư bậc hai) được tiên đoán bởi Euler và Legendre và lần đầu tiên được chứng minh thuyết phục bởi Gauss. Gauss gọi đó là "định lý vàng" và rất tự hào về nó đến mức ông tiếp tục tìm ra tám chứng minh khác cho nó cho đến cuối đời.

Đề tài luận văn "Ứng dụng của luật thuận nghịch và thặng dư bậc hai" có mục đích là hệ thống lại mảng kiến thức liên quan đến luật thuận nghịch và thặng dư bậc hai, từ đó trình bày một số ví dụ ứng dụng hay của chúng nhằm cung cấp một tài liệu tốt để dạy và học cho giáo viên và học sinh phổ thông trung học.

Luận văn ngoài phần mở đầu, kết luận thì nội dung chính gồm 2 chương trình bày lại một cách hệ thống về luật thuận nghịch và thặng dư bậc hai cùng một số ứng dụng của chúng, với bố cục cụ thể như sau:

Chương 1. Kiến thức chuẩn bị. trình bày phát biểu và chứng minh định

lý Fermat nhỏ, định lý Euler. Trình bày khái niệm và cách giải phương trình đồng dư tuyến tính, hệ phương trình đồng dư tuyến tính (định lý thặng dư Trung Hoa).

Chương 2. Ứng dụng của luật thuận nghịch và thặng dư bậc hai. Chương 2 trình bày định nghĩa và các tính chất của phương trình đồng dư bậc hai, thặng dư bậc hai, cách tính bằng định nghĩa, cách tính thông qua ký hiệu Legendre, cách tính thông qua luật thuận nghịch bậc hai. Sau đó ứng dụng thặng dư bậc hai và luật thuận nghịch bậc hai để tính toán và giải một số bài toán chứng minh, tìm căn nguyên thủy, kiểm tra tính nguyên tố.

Luận văn được hoàn thành tại trường Đại học Khoa học, Đại học Thái Nguyên. Lời đầu tiên tác giả xin được bày tỏ lòng biết ơn sâu sắc tới thầy giáo PGS.TS. Nguyễn Văn Hoàng. Thầy đã dành nhiều thời gian hướng dẫn cũng như giải đáp các thắc mắc của tôi trong suốt quá trình làm luận văn. Tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy.

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 đã tận tình hướng dẫn, truyền đạt kiến thức trong suốt thời gian theo học, thực hiện và hoàn thành luận văn.

Cảm ơn sự giúp đỡ của bạn bè, người thân và các đồng nghiệp trong thời gian làm luận văn.

Thái Nguyên, tháng 05 năm 2019

Người viết luận văn

Đỗ Thị Thoa

Chương 1

Kiến thức chuẩn bị

Chương 1 trình bày phát biểu và chứng minh định lý Fermat nhỏ, định lý Euler. Trình bày khái niệm và cách giải phương trình đồng dư tuyến tính, hệ phương trình đồng dư tuyến tính (định lý thặng dư Trung Hoa). Các kiến thức ở chương này giúp việc trình bày ở chương sau được hệ thống và dễ theo dõi hơn.

1.1 Định lý Fermat nhỏ và định lý Euler

Mục này trình bày hai định lý quan trọng trong lý thuyết đồng dư là định lý Fermat nhỏ và định lý Euler.

Định lý 1.1.1 (Định lý Fermat nhỏ)**.** *Cho p là số nguyên tố và a là số nguyên. Nếu $p \nmid a$ thì*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Chứng minh. Xét $p-1$ số nguyên $a, 2a, 3a, \ldots, (p-1)a$. Chú ý rằng $p \nmid ia$ với mọi $i = 1, 2, \ldots, p-1$ (vì nếu ngược lại, tồn tại $1 \leq i \leq p-1$ để $p \mid ia$, kéo theo $p \mid a$ hoặc $p \mid i$; nhưng vì $p \nmid a$, nên ta có $p \mid i$ điều này mâu thuẫn). Cũng chú ý rằng không có hai số nào trong $p-1$ số nguyên $a, 2a, 3a, \ldots, (p-1)a$ đồng dư modulo p (vì nếu ngược lại, thì tồn tại nghịch đảo a' của a modulo p; nên từ $ia \equiv ja \pmod{p}$ với $i \neq j$ thì $iaa' \equiv jaa' \pmod{p}$, từ đó $i \equiv j \pmod{p}$, điều này là không thể). Do đó tập các số dư trong phép chia cho p của các số nguyên $a, 2a, 3a, \ldots, (p-1)a$ phải là $\{1, 2, 3, \ldots, p-1\}$. Khi đó,

$$(a)(2a)(3a)\cdots(p-1)a \equiv (1)(2)(3)\cdots(p-1) \pmod{p}$$

hay tương đương với

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Mặt khác ta thấy $(p-1)!$ và p là hai số nguyên tố cùng nhau, nên từ đồng dư bên trên cho ta thấy $a^{p-1} \equiv 1 \pmod{p}$, điều phải chứng minh. □

Ví dụ 1.1.2. Với $a = 3, p = 5$ suy ra $3^4 = 81 \equiv 1 \pmod{5}$. Tương tự, ta tính được $9^{10} \equiv 1 \pmod{11}$.

Tiếp theo ta trình bày định lý Euler đó là một dạng tổng quát hoá của định lý Fermat nhỏ.

Định lý 1.1.3 (Định lý Euler)**.** *Nếu m là số nguyên dương và a là số nguyên sao cho a nguyên tố cùng nhau với m, thì*

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

trong đó $\phi(m)$ là ký hiệu của phi hàm Euler (hàm này đếm số các số nguyên trong phạm vi từ 1 đến m mà nguyên tố cùng nhau với m).

Chứng minh. Gọi $r_1, r_2, \ldots, r_{\phi(m)}$ là $\phi(m)$ số nguyên dương không lớn hơn m sao cho $(r_i, m) = 1$ với $i = 1, 2, \ldots, \phi(m)$. Xét $\phi(m)$ số nguyên xác định bởi $r_1a, r_2a, \ldots, r_{\phi(m)}a$. Chú ý rằng $(r_ia, m) = 1$ với mọi $i = 1, 2, \ldots, \phi(m)$ (vì nếu ngược lại, tồn tại i để $(r_ia, m) > 1$ thì tồn tại ước nguyên tố p của (r_ia, m), từ đó $p \mid r_ia$ và $p \mid m$. Ta có $p \mid r_ia$ kéo theo $p \mid r_i$ hoặc $p \mid a$; nên hoặc ta có $p \mid r_i$ và $p \mid m$ hoặc ta có $p \mid a$ và $p \mid m$. Nhưng $p \mid r_i$ và $p \mid m$ là không thể vì $(r_i, m) = 1$; còn lại nếu $p \mid a$ và $p \mid m$ thì đó cũng là không thể vì $(a, m) = 1$). Ngoài ra cũng chú ý rằng không có hai số nào trong các số $r_1a, r_2a, \ldots, r_{\phi(m)}a$ đồng dư modulo m (vì nếu ngược lại thì do $(a, m) = 1$, nên tồn tại nghịch đảo modulo a' của a. Do đó, nếu $r_ia \equiv r_ja \pmod{m}$ với $i \neq j$, kéo theo $r_iaa' \equiv r_jaa' \pmod{m}$, từ đó $r_i \equiv r_j \pmod{m}$, điều này là không thể). Do đó tập các số dư khi chia cho m của các số nguyên $r_1a, r_2a, \ldots, r_{\phi(m)}a$ là $\{r_1, r_2, \ldots, r_{\phi(m)}\}$. Do đó, ta có

$$(r_1a)(r_2a)\cdots(r_{\phi(m)}a) \equiv r_1r_2\cdots r_{\phi(m)} \pmod{m},$$

hay tương đương với

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Bây giờ, $m \mid (a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} - r_1 r_2 \cdots r_{\phi(m)})$ kéo theo $m \mid (r_1 r_2 \cdots r_{\phi(m)}) \times (a^{\phi(m)} - 1)$. Chú ý vì $(r_i, m) = 1$ với $i = 1, 2, \ldots, \phi(m)$ nên $(r_1 r_2 \ldots r_{\phi(m)}, m) = 1$. Do đó ta suy ra $m \mid (a^{\phi(m)} - 1)$ và do đó $a^{\phi(m)} \equiv 1 \pmod{m}$, điều phải chứng minh. □

Định lý Euler là tổng quát hóa của định lý nhỏ Fermat vì nếu $n = p$ là số nguyên tố thì $\phi(p) = p - 1$. Định lý này có thể được sử dụng để dễ dàng giản ước với những modulo m rất lớn.

Ví dụ 1.1.4. Ví dụ tìm chữ số tận cùng của số 7^{222}.

Giải. Chú ý rằng 7 và 10 là nguyên tố cùng nhau và $\phi(10) = 4$. Bởi vậy $7^4 \equiv 1 \pmod{10}$. Và ta có

$$7^{222} \equiv 7^{4.55+2} 7^2 \equiv 1^{55} 7^2 \equiv 49 \equiv 9 \pmod{10}.$$

Vậy 7^{222} có chữ số tận cùng là 9. □

1.2 Sơ lược về phương trình đồng dư

Định nghĩa 1.2.1. *Phương trình đồng dư đại số bậc n* là một đồng dư thức có dạng

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod{m} \tag{1.1}$$

trong đó x là ẩn, $a_i \in \mathbb{Z}$ (với $i = 1, 2, \ldots, n$) và $a_0 \not\equiv 0 \pmod{m}$.

Chú ý 1.2.2. (i) Giải phương trình (1.1) là tìm tất cả các giá trị nguyên của x thoả mãn đồng dư thức (1.1). Nếu $x = x_0$ thoả mãn phương trình (1.1) thì mọi số $x \equiv x_0 \pmod{m}$ đều thoả mãn (1.1); trong trường hợp này tập hợp $\{x \in \mathbb{Z} \mid x \equiv x_0 \pmod{m}\}$ được gọi là một *nghiệm* của phương trình đồng dư (1.1), kí hiệu là $\overline{x_0}$ hoặc $x \equiv x_0 \pmod{m}$.

(ii) Số nghiệm của phương trình (1.1) là số các phần tử trong một hệ thặng dư đầy đủ theo modulo m mà thỏa mãn (1.1).

(iii) Hai phương trình đồng dư được gọi là tương đương nếu tập hợp các số nguyên thỏa mãn các phương trình đó là trùng nhau.

Ví dụ 1.2.3. Xét phương trình $x^2 \equiv 1 \pmod 5$.

Giải. Ta thấy trong các số 0, 1, 2, 3, 4 của hệ thặng dư không âm bé nhất theo modulo 5, có hai số 1 và 4 thỏa mãn phương trình đã cho. Vậy phương trình có hai nghiệm là $x \equiv 1 \pmod 5$ và $x \equiv 4 \pmod 5$. □

Ví dụ 1.2.4. Giải phương trình đồng dư $x^4 + 7x + 4 \equiv 0 \pmod 9$.

Giải. Dễ thấy phương trình $x^4 + 7x + 4 \equiv 0 \pmod 3$ có nghiệm là $x \equiv 1 \pmod 3$ (hay $x = 3t + 1$ với $t \in \mathbb{Z}$). Thay x vào phương trình cần giải và bỏ đi những số hạng chia hết cho 9 ta được

$$\begin{aligned} & 6t + 3 \equiv 0 \pmod 9 \\ \Leftrightarrow\ & 2t + 1 \equiv 0 \pmod 3 \\ \Leftrightarrow\ & t \equiv 1 \pmod 3 \\ \Leftrightarrow\ & t = 3k + 1. \end{aligned}$$

Vậy phương trình có nghiệm là $x = 3(3k + 1) + 1$ hay $x \equiv 4 \pmod 9$. □

Định nghĩa 1.2.5. Phương trình đồng dư $ax \equiv b \pmod m$ được gọi là *phương trình đồng dư tuyến tính* với a, b, m là các số nguyên đã biết. Khi đó $x \equiv x_0 \pmod m$ là một nghiệm của phương trình khi và chỉ khi $ax_0 \equiv b \pmod m$.

Định lý 1.2.6 ([6])**.** *Phương trình đồng dư tuyến tính* $ax \equiv b \pmod m$ *có nghiệm khi và chỉ khi* $d \mid b$*, trong đó* $d = (a, m)$*. Nếu* $d \mid b$ *thì phương trình có* d *nghiệm.*

Hệ quả 1.2.7 ([6])**.** *Phương trình đồng dư tuyến tính* $ax \equiv b \pmod m$ *có nghiệm duy nhất khi và chỉ khi* $(a, m) = 1$.

Hệ quả 1.2.8 ([6])**.** *Cho phương trình đồng dư tuyến tính* $ax \equiv b \pmod m$ *và gọi* $d = (a, m)$*. Nếu* $d \mid b$ *thì* d *nghiệm modulo* m *của phương trình là*

$$(x_0 + \frac{mt}{d}) \pmod m \text{ với } t = 0, 1, 2, \ldots, d - 1$$

trong đó x_0 là một số nguyên thỏa mãn của phương trình $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Ví dụ 1.2.9. Giải phương trình đồng dư $12x \equiv 7 \pmod{23}$.

Giải. Ta có (12, 23) =1 nên phương trình có nghiệm duy nhất. Phương trình đã cho tương đương với $12x = 23t + 7$ ($t \in \mathbb{Z}$). Lấy $t = 7$ suy ra $x = 14$. Vậy nghiệm của phương trình đã cho là $x \equiv 14 \pmod{23}$. □

Ví dụ 1.2.10. Giải phương trình đồng dư $17x \equiv 13 \pmod{11}$.

Giải. Ta có $17 \equiv 6 \pmod{11}$ suy ra

$$17x \equiv 6x \pmod{11}. \tag{1.2}$$

Mặt khác

$$13 \equiv 2 \pmod{11}. \tag{1.3}$$

Từ (1.2) và (1.3) và theo tính chất bắc cầu ta có $6x \equiv 2 \pmod{11}$. Do (2, 11) =1 nên giản ước hai vế cho 2 ta được $3x \equiv 1 \pmod{11}$ hay $3x = 11t + 1$. Lấy $t = 1$ suy ra $x = 4$. Do (3, 11) = 1 nên phương trình có nghiệm duy nhất là $x \equiv 4 \pmod{11}$. □

Định lý 1.2.11 (Định lý thặng dư Trung Hoa, [5])**.** *Cho $m_1, m_2, \ldots, m_n$ là các số nguyên dương đôi một nguyên tố cùng nhau và cho $b_1, b_2, \ldots, b_n$ là các số nguyên bất kỳ. Khi đó hệ phương trình đồng dư tuyến tính*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots\cdots\cdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

có nghiệm duy nhất modulo $m_1 m_2 \cdots m_n$.

Chứng minh. Đầu tiên ta xây dựng một số nguyên thỏa mãn hệ đã cho. Đặt $M = m_1 m_2 \cdots m_n$. Với mỗi $i = 1, 2, \ldots, n$ đặt $M_i = M/m_i$. Bây giờ với mỗi $i = 1, 2, \ldots, n$ ta có $(M_i, m_i) = 1$. Do đó theo Hệ quả 1.2.7, phương trình $M_i x \equiv 1 \pmod{m_i}$ có một nghiệm $x_i \pmod{m_i}$. Đặt

$$x = b_1 M_1 x_1 + b_2 M_2 x_2 + \cdots + b_n M_n x_n.$$