ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ THỊ GÁI

LUẬT TƯƠNG HỖ BẬC HAI VÀ ĐIỂM NGUYÊN

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2016

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

VŨ THỊ GÁI

LUẬT TƯƠNG HỖ BẬC HAI VÀ ĐIỂM NGUYÊN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 60 46 01 13

NGƯỜI HƯỚNG DẪN KHOA HỌC:
TS. Hoàng Lê Trường

THÁI NGUYÊN - 2016

Mục lục

Lời nói đầu **1**

Chương 1. Một số kiến thức cơ bản **4**

1.1 Đồng dư 4

1.2 Số nguyên tố, sự phân tích duy nhất và trường hữu hạn . . 5

1.3 Lũy thừa của trường hữu hạn 6

1.4 Đa thức trên $\mathbb{Z}/p\mathbb{Z}$ 9

1.5 Định lý thặng dư Trung Hoa 10

Chương 2. Luật tương hỗ bậc hai **14**

2.1 Đa thức đồng dư và bổ đề Hensel 14

2.2 Thặng dư bậc hai và ký hiệu Legendre 18

2.3 Tiêu chuẩn Euler 20

2.4 Bổ đề Gauss 24

2.5 Luật tương hỗ bậc hai 27

2.6 Ứng dụng của luật tương hỗ bậc hai 31

2.6.1 Tính ký hiệu Legendre 31

2.6.2 Với p nào thì a là thặng dư bậc hai modulo p? . . . 35

2.6.3 Số nguyên tố là ước của các giá trị của đa thức bậc hai 38

2.6.4 Khi nào số Fermat là số nguyên tố? 40

2.6.5 Ứng dụng trong bài toán giải phương trình nghiệm nguyên 41

2.6.6 Ứng dụng trong bài toán chứng minh chia hết . . . 45

2.6.7 Một số ứng dụng khác 46

Kết luận **48**

Tài liệu tham khảo **49**

Lời nói đầu

Cho hai số nguyên tố lẻ p và q, khi đó ta có

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

trong đó

$$\left(\frac{a}{p}\right)=\begin{cases}0 & \text{nếu } \gcd(a,p)\neq 1\\ +1 & \text{nếu } a \text{ là thặng dư bậc hai}\\ -1 & \text{nếu } a \text{ là phi thặng dư bậc hai.}\end{cases}$$

Mệnh đề trên được gọi là luật tương hỗ bậc hai. Luật này được đưa ra lần đầu tiên nhưng không được chứng minh bởi Euler (Opusula analytica, Petersburg,1783). Vào năm 1785, Legendre cũng tìm ra luật tương hỗ một cách độc lập với Euler và đưa ra một phần chứng minh. Chứng minh đầy đủ đầu tiên được đưa ra bởi Gauss vào năm 1796 trong cuốn sách nổi tiếng Disquisitiones arithmeticae(1801). Cuốn sách đó đã đặt nền móng và cung cấp những ý tưởng sâu sắc cho Lí thuyết số hiện đại, được viết khi Gauss mới 20 tuổi. Kronecker đã nói về cuốn sách như sau: "It is really astonishing to think that a single man of such young years was able to produce such a wealth of results, and above all to present such a profound and well organized treatment of an entirely new discipline".

Bản thân Gauss đã đưa ra bẩy chứng minh khác nhau về luật tương hỗ bậc hai. Chúng ta có thể tìm thấy chúng trong cuốn sách "Klassiker des exakten Wissenshaften" của Ostwald. Luật tương hỗ bậc hai được cho là định lý quan trọng nhất được giảng dạy trong các giáo trình về Lí thuyết số sơ cấp. Tầm quan trọng của luật tương hỗ bậc hai đã làm cho nhiều nhà toán học khác như Jacobi, Cauchy, Liousville, Kronecker, Schering and

Frobenius nghiên cứu nó sau Gauss và chúng ta đã có hơn 100 chứng minh khác nhau đã được phát hiện. Có thể chứng minh đơn giản nhất trong tất cả các chứng minh là thông qua số học và hình học, bắt nguồn từ tổ hợp Bổ đề của Gauss (xem Gauss' Werke, vol. II, p.51) và ý tưởng hình học của Cayley (Arthur Cayley [1821–1895], Collected Mathematical Papers, vol.II). Luật tương hỗ bậc hai còn có rất nhiều ứng dụng trong Số học, vì thế nó là một phần kiến thức quan trọng trong các kì thi học sinh giỏi (nhất là các kì thi chọn đội tuyển Olympic Toán). Với những lý do đã nêu ở trên nên tác giả đã chọn đề tài " **Luật tương hỗ bậc hai và điểm nguyên**" để nghiên cứu. Mục đích của luận văn là trình bày lại chi tiết chứng minh Luật tương hỗ bậc hai dựa trên Bổ đề Gauss và đếm các điểm nguyên trên lưới hai chiều được đưa ra bởi Eisenstein. Hơn nữa luận văn còn giải thích được tại sao khi nghiên cứu phương trình đồng dư bậc hai tổng quát thực chất chỉ cần tìm hiểu phương trình bậc hai dạng đặc biệt. Cuối cùng, luận văn đưa ra một số ứng dụng của Luật tương hỗ bậc hai trong việc giải các bài toán phổ thông. Ngoài phần Lời nói đầu và Kết luận, luận văn được chia thành hai chương đề cập đến các vấn đề sau đây:

Chương 1: Một số kiến thức cơ bản

Chương này nhằm giới thiệu về các kiến thức cơ sở phục vụ chương 2 như đồng dư, đa thức trên $\mathbb{Z}/p\mathbb{Z}$, định lý thặng dư Trung Hoa,...

Chương 2: Luật tương hỗ bậc hai

Trình bày Luật tương hỗ bậc hai, chứng minh Luật tương hỗ bậc hai bằng phương pháp hình học là đếm số điểm nguyên trên lưới hai chiều; giải thích tại sao khi nghiên cứu phương trình đồng dư bậc hai tổng quát thực chất chỉ cần tìm hiểu phương trình đồng dư bậc hai dạng đặc biệt và đưa ra một số ứng dụng của luật tương hỗ bậc hai trong việc giải các bài toán phổ thông.

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. Hoàng Lê Trường-Viện Toán học, VAST, Việt Nam. Qua đây tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình - người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn. Đồng thời

tác giả xin trân trọng cảm ơn Ban Giám hiệu Trường Đại học Khoa học - Đại học Thái Nguyên, Ban Chủ nhiệm Khoa Toán-Tin, cùng các giảng viên đã tham gia giảng dạy, Ban giám hiệu và các đồng nghiệp trường THCS Dư Hàng Kênh (Quận Lê Chân, thành phố Hải Phòng) đã tạo mọi điều kiện tốt nhất để tác giả học tập và nghiên cứu, cuối cùng tác giả muốn dành những lời cảm ơn đặc biệt nhất đến gia đình và tập thể lớp Cao học Toán K8B (khóa 2014-2016) đã luôn động viên và chia sẻ những khó khăn để tác giả hoàn thành tốt luận văn.

Thái Nguyên, ngày 20 tháng 5 năm 2016

Tác giả

Vũ Thị Gái

Chương 1

Một số kiến thức cơ bản

Mục đích của chương này là nhắc lại một số kiến thức chuẩn bị cần thiết cho việc trình bày các kết quả trong chương sau. Nội dung của chương này là chúng tôi nhắc lại một số khái niệm về đồng dư, đa thức trên $\mathbb{Z}/p\mathbb{Z}$, định lý thặng dư Trung Hoa,.... Hầu hết các kết quả của chương này được trình bày dựa theo tài liệu [1], [2].

1.1 Đồng dư

Định nghĩa 1.1.1. Giả sử a, b và $m \geq 1$ là các số nguyên. Ta nói rằng số nguyên a và b là đồng dư modulo m nếu $m \mid a-b$.
Khi a đồng dư b modulo m, ta viết

$$a \equiv b (\bmod m).$$

Nếu a đồng dư b modulo m, ta viết

$$a \not\equiv b (\bmod m).$$

Mệnh đề 1.1.2. *Giả sử a, b, c, m là các số nguyên, $m \geq 1$. Khi đó ta có:*

(*i*) *Nếu $a \equiv b \pmod m$ và $c \equiv d \pmod m$. Khi đó: $a \pm c \equiv b \pm d \pmod m$ và $a.c \equiv b.d \pmod m$*

(*ii*) *Nếu $ac \equiv bc (\bmod m)$ và $d = (c, m)$. Khi đó $a \equiv b (\bmod \frac{m}{d})$.*

(*iii*) *Cho* $a,b \in \mathbb{Z}$. *Khi đó* $a.b \equiv 1 \pmod{m}$ *khi và chỉ khi* $\gcd(a,m) = 1$
Khi đó số nguyên b gọi là nghịch đảo của a modulo m.

Định lý 1.1.3. *Giả sử* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$,..., $a \equiv b \pmod{m_k}$, *trong đó* $a,b,m_1,m_2,...,m_k$ *là các số nguyên,* $m_1,m_2,...,m_k > 0$. *Khi đó*

$$a \equiv b(\bmod [m_1,m_2,...,m_k]).$$

trong đó $[m_1,m_2,...,m_k]$ *là bội chung nhỏ nhất của* $m_1,m_2,...,m_k$.

Định nghĩa 1.1.4. Vành các số nguyên modulo m được kí hiệu là $\mathbb{Z}/m\mathbb{Z}$ và được xác định như sau:

$$\mathbb{Z}/m\mathbb{Z} = \{0,1,2,\cdots,m-1\}.$$

Tập tất cả các phần tử khả nghịch trong $\mathbb{Z}/m\mathbb{Z}$ kí hiệu là $(\mathbb{Z}/m\mathbb{Z})^*$ và

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a,m) = 1\}$$

$$= \{a \in \mathbb{Z}/m\mathbb{Z} : a \text{ có một nghịch đảo modulo } m\}.$$

Nếu a_1 và a_2 là khả nghịch modulo m thì a_1a_2 cũng là khả nghịch modulo m. Nhưng nếu cộng hai phần tử khả nghịch, ta có thể không được một phần tử khả nghịch.

1.2 Số nguyên tố, sự phân tích duy nhất và trường hữu hạn

Định nghĩa 1.2.1. Số nguyên p được gọi là số nguyên tố nếu $p \geq 2$ và p chỉ chia hết cho 1 và p. Số nguyên dương khác 1 và không là số nguyên tố được gọi là hợp số.

Bổ đề 1.2.2. *Giả sử* a,b,c *là các số nguyên dương,* $(a,b) = 1$ *đồng thời* $a \vdots bc$. *Khi đó* $a \vdots c$.

Hệ quả 1.2.3. *Nếu* $p \mid a_1a_2...a_n$, *trong đó p là số nguyên tố và* $a_1,a_2,...,a_n$ *là các số nguyên dương thì tồn tại i,* $1 \leq i \leq n$ *sao cho* $p \mid a_i$.
Định lý sau đây là một định lý quan trọng nhất của Số học, nó cho thấy các số nguyên tố là nền tảng để xây dựng số nguyên.

Định lý 1.2.4. (Định lý cơ bản của số học) *Cho $a \geq 2$ là một số nguyên, thì a có thể được phân tích thành tích của các số nguyên tố $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Hơn nữa, không kể thứ tự của các số nguyên tố thì sự phân tích này là duy nhất.*

Mệnh đề 1.2.5. *Nếu p là số nguyên tố thì mỗi phần tử a khác không trong $\mathbb{Z}/p\mathbb{Z}$ có một nghịch đảo nhân, nghĩa là có một số b thỏa mãn*

$$ab \equiv 1 (\bmod p).$$

Ta kí hiệu giá trị b này bởi $a^{-1} (\bmod p)$. Khi đó tập các phần tử khả nghịch là

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, 4, \cdots, p-1\}.$$

Mệnh đề 1.2.6. *Giả sử p là một số nguyên tố. Số nguyên a là nghịch đảo modulo p của chính nó khi và chỉ khi*

$$a \equiv 1 (\bmod p) \quad \text{và} \quad a \equiv p-1 (\bmod p).$$

Định nghĩa 1.2.7. Nếu p là số nguyên tố, thì tập $\mathbb{Z}/p\mathbb{Z}$ của các số nguyên modulo p cùng với phép cộng, trừ, nhân và quy tắc chia là trường. Trường $\mathbb{Z}/p\mathbb{Z}$ các số nguyên modulo p chỉ có hữu hạn phần tử và thường được kí hiệu bởi $\mathbb{F}_p$.

1.3 Lũy thừa của trường hữu hạn

Trong phần này, chúng ta đề cập đến lũy thừa trong $\mathbb{F}_p$, nhờ có một chứng minh kết quả cơ bản của Fermat và đó là một tính chất quan trọng của nhóm các phần tử khả nghịch $(\mathbb{F}_p)^*$.

Ví dụ 1.3.1. Từ bảng lũy thừa của các số modulo 7 (Bảng 1.1), ta thấy các cột bên phải bao gồm toàn bộ 1.
Tức là:

$$a^6 \equiv 1 \pmod 7 \qquad \text{với mỗi } a = 1, 2, 3, \cdots 6.$$