ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHAN THẾ CHIẾN

SỐ NGUYÊN GAUSS VÀ PHƯƠNG TRÌNH DIOPHANTUS

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

PHAN THẾ CHIẾN

SỐ NGUYÊN GAUSS VÀ PHƯƠNG TRÌNH DIOPHANTUS

Chuyên ngành: **Phương pháp Toán sơ cấp**
Mã số: **60 46 01 13**

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC

GS.TSKH. HÀ HUY KHOÁI

Thái Nguyên - 2015

Mục lục

Lời cảm ơn

Luận văn này được hoàn thành tại trường Đại học Khoa học - Đại học Thái Nguyên. Tác giả xin bày tỏ lòng biết ơn sâu sắc với GS.TS. Hà Huy Khoái, đã trực tiếp hướng dẫn tác giả trong suốt thời gian nghiên cứu.

Xin chân thành cảm ơn tới các thầy, cô giáo trong Khoa Toán - Tin, Phòng Đào tạo Khoa học, các bạn học viên lớp Cao học Toán K7D trường Đại học Khoa học - Đại học Thái Nguyên và các bạn đồng nghiệp đã tạo điều kiện thuận lợi, động viên tác giả trong quá trình học tập và nghiên cứu tại trường.

Tác giả cũng xin bày tỏ lòng biết ơn sâu sắc tới gia đình và người thân đã luôn khuyến khích, động viên tác giả trong suốt quá trình học tập và làm luận văn.

Mặc dù có nhiều cố gắng nhưng luận văn khó tránh khỏi những thiếu sót và hạn chế. Tác giả mong nhận được những ý kiến đóng góp quý báu của các thầy cô và bạn đọc để luận văn được hoàn thiện hơn.

Thái Nguyên, 2015 **Phan Thế Chiến**

Học viên Cao học Toán K7D,
Trường ĐH Khoa học - ĐH Thái Nguyên

Danh sách ký hiệu

ED	miền Euclide
PID	miền iđêan chính
UFD	miền nhân tử hóa duy nhất

Mở đầu

Số nguyên Gauss là một số phức có phần thực và ảo là các số nguyên. Các số nguyên Gauss với phép cộng và nhân các số phức lập thành một miền nguyên và kí hiệu là $\mathbb{Z}[i]$.

Phương trình Diophantus là phương trình có dạng

$$f(x_1, x_2, \ldots, x_n) = 0, \qquad (*)$$

trong đó f là một hàm n biến với $n \geq 2$, và các nghiệm được tìm trong tập hợp số nguyên hoặc số hữu tỷ. Nếu f là đa thức với các hệ số nguyên thì (*) là một *phương trình Diophantus đại số*. Bộ n phần tử $(x_1^0, x_2^0, \ldots, x_n^0) \in \mathbb{Z}^n$ thỏa mãn (*) được gọi là một nghiệm của phương trình (*).

Phương trình Diophantus là một chủ đề trong toán phổ thông và rất hay gặp trong các đề thi học sinh giỏi, thi quốc gia và quốc tế. Có rất nhiều nhà toán học nghiên cứu về vấn đề này và có một số phương pháp sơ cấp để giải phương trình Diophantus đó là: Phương pháp phân tích thành nhân tử, phương pháp bất đẳng thức, phương pháp tham số, phương pháp modul số học, phương pháp quy nạp ... Trong luận văn này chúng tôi trình bày vành số nguyên Gauss và một số phương pháp nâng cao để giải phương trình Diophantus.

Với những lý do trên, cùng với sự quan tâm và muốn đi sâu hơn về vấn đề này, em chọn đề tài "Số nguyên Gauss và phương trình Diophantus" cho bài luận văn cuối khóa của mình. Do nhiều yếu tố chủ quan và khách quan, nội

dung của bài viết có thể còn nhiều khiếm khuyết, em rất mong nhận được ý kiến đóng góp của quý thầy cô.

Cấu trúc luận văn

Nội dung chính của luận văn được trình bày thành 2 chương:

• Chương 1: Vành $\mathbb{Z}[i]$. Trong chương này, chúng tôi trình bày một cách sơ lược về vành $\mathbb{Z}[i]$ các số nguyên Gauss và vành các số $\mathbb{Z}[\sqrt{d}]$ mà sẽ được sử dụng trong các chương tiếp theo.

• Chương 2: Phương trình nghiệm nguyên. Trong chương này chúng tôi trình bày luật thuận nghịch và phương trình Diophantus; các ước số có dạng đặc biệt và ứng dụng để giải phương trình nghiệm nguyên.

Do khối lượng kiến thức lớn và thời gian nghiên cứu chưa đủ dài, chắc chắn luận văn không thể tránh khỏi những thiếu sót, tác giả rất mong muốn nhận được sự góp ý của các thầy cô và bạn bè đồng nghiệp

Thái Nguyên, ngày 20 tháng 11 năm 2015

Phan Thế Chiến

Email: phanchienmdc@gmail.com

Chương 1

Vành $\mathbb{Z}[i]$

1.1 Một số định nghĩa cơ sở

Trường là một tập k được trang bị hai phép toán hai ngôi, giao hoán cộng và nhân, sao cho

- $(k, +)$ là một nhóm cộng Aben;
- Mọi phần tử khác không của k đều có phần tử nghịch đảo và $(k^*, .)$ là một nhóm nhân Aben, trong đó $k^* = k\backslash\{0_k\}$;
- $0_k \neq 1_k$;
- tính chất phân phối xảy ra: $(a + b)c = ac + bc$ với mọi $a, b, c \in k$.

Vành giao hoán cũng giống như là một trường, nhưng không phải mọi phần tử khác không đều có nghịch đảo của phép nhân. Ví dụ vành giao hoán: $\mathbb{Z}, \mathbb{Z}_n$ (tập các phần tử môđun n), $k[x]$ (tập các đa thức với hệ số trong trường k).

Một phần tử của vành $\mathbb{R}$ khả nghịch với phép nhân được gọi là đơn vị. Tập các đơn vị của $\mathbb{R}$, kí hiệu $\mathbb{R}^*$ là một nhóm nhân với phép nhân của $\mathbb{R}$. Đối với các ví dụ đã nêu ở trên của vành giao hoán, ta có

$$\mathbb{Z}^* = \{-1, 1\}, \mathbb{Z}_n^* = \{\hat{a} \in \mathbb{Z}_n : \gcd(a, n) = 1\}, k[x]^* = k\backslash\{0_F\}$$

với k là một trường.

Một ước của không của vành $\mathbb{R}$ là một phần tử khác không $r \in \mathbb{R}$ nếu có $s \in \mathbb{R}$ nào đó khác không sao cho $rs = 0$. Một vành giao hoán không có ước của không được gọi là miền nguyên. Ví dụ về vành với ước của không: $\mathbb{Z}_n$ với n không nguyên tố (ví dụ trong $\mathbb{Z}_6, \hat{2}.\hat{3} = \hat{0}$). Một ví dụ không giáo hoán là trong $M_2(\mathbb{Q})$, trong đó

$$\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Phần tử bất kì là một đơn vị của vành sẽ không bao giờ là một ước của không. Ví dụ về miền nguyên: $\mathbb{Z}; k[x]$, trong đó k là một trường bất kì.

Vành $\mathbb{R}$ được gọi là miền Euclide (ED) nếu tồn tại một hàm $\lambda : \mathbb{R}\backslash\{0\} \to \mathbb{N}^0$ với tính chất sau: Với hai số bất kì $a, b \in \mathbb{R}, b \neq 0$ có thể tìm $c, d \in \mathbb{R}$ sao cho $a = cb + d$ và hoặc $d = 0$ hoặc $\lambda(d) < \lambda(b)$.

Ví dụ, vành $\mathbb{Z}$ và $k[x]$ (k là một trường) là 2 miền Euclide: lấy λ là giá trị tuyệt đối trong $\mathbb{Z}$ hoặc bậc của đa thức trong $k[x]$.

Một iđêan I của vành $\mathbb{R}$ là một tập con của $\mathbb{R}$ đóng với phép cộng, trừ và phép nhân bởi các phần tử của $\mathbb{R}$: nếu $x, y \in I$ và $r \in \mathbb{R}$ thì $x+y, x-y, rx \in \mathbb{R}$. Nói cách khác, I là một tập con của $\mathbb{R}$, là một $\mathbb{R}-$ môđun, cũng gọi là $\mathbb{R}-$ môđun con. Hơn nữa, một iđêan gọi là iđêan chính nếu nó sinh bởi một phần tử như một $\mathbb{R}-$ môđun: với $a \in I$ nào đó, $I = \{ra | r \in I\}$. Ta viết $I = (a)$.

Trong miền Euclide $\mathbb{R}$ mọi iđêan là iđêan chính.

Một vành $\mathbb{R}$ được gọi là miền iđêan chính (PID) nếu mọi iđêan là iđêan chính.

Do đó, mỗi ED cũng là một PID.

Cho vành $\mathbb{R}, a, b \in \mathbb{R}$ được gọi là liên kết nếu $a = ub$ với $u \in \mathbb{R}$ là đơn vị. Phần tử $p \in \mathbb{R}$ được gọi là bất khả quy nếu $a|p$ thì a là đơn vị hoặc a liên kết với p. Số không phải đơn vị $p \in \mathbb{R}$ là nguyên tố nếu $p \neq 0$ và $p|ab$ thì $p|a$ hoặc $p|b$.

Chú ý rằng các phần tử bất khả quy và nguyên tố không luôn luôn trùng trong các vành nhưng chúng trùng trong PID, trong đó các kí hiệu này có thể dễ dàng dịch sang ngôn ngữ của iđêan.

Tương tự, ta định nghĩa ước chung lớn nhất của hai hay nhiều phần tử của $\mathbb{R}$. Điều sau đây không đúng trong vành tuỳ ý, nhưng đúng trong các PID: nếu $a, b \in \mathbb{R}$ thì $\gcd(a, b)$ là một phần tử d sao cho $(a, b) = (d)$.

Cuối cùng, hai phần tử được gọi là nguyên tố cùng nhau nếu $\gcd(a, b) = 1$. Trong PID điều này có nghĩa là a và b sinh ra vành $\mathbb{R}$.

Trong PID, các khái niệm phần tử nguyên tố và bất khả quy là tương đương.

Trong một PID R, dãy tăng bất kì của iđêan cuối cùng được ổn định. Do đó, cho p là một số nguyên tố bất kì và $a \in \mathbb{R}, a \neq 0$ bất kì đều có một số nguyên không âm duy nhất sao cho $p^n \mid a$ nhưng $p^{n+1} \nmid a$.

Số n được gọi là bậc của p trong a, kí hiệu là $n = \operatorname{ord}_p a$. Chú ý rằng với $a, b \neq 0$ bất kì thì $\operatorname{ord}_P ab = \operatorname{ord}_p a + \operatorname{ord}_p b$. Sau đây là định lý chính của phần này. Lưu ý rằng một PID có thể được coi như là hợp rời của các tập con của các phần tử liên kết. Nếu một phần tử trong một tập con là nguyên tố thì tất cả các phần tử liên kết cũng nguyên tố. Từ mỗi tập con như vậy bao gồm các phần tử nguyên tố ta chọn một đại diện và kí hiệu tập các đại diện là S.

Ta có kết quả quan trọng sau:

Định lí 1.1.1. *Cho $\mathbb{R}$ là một PID và S tập các đại diện của các tập con của các phần tử nguyên tố liên kết trong $\mathbb{R}$. Khi đó, với mọi $a \in \mathbb{R}, a \neq 0$ ta có*

$$a = u \prod_p p^{e(p)}$$

trong đó u là một đơn vị trong $\mathbb{R}$ và tích lấy trên tất cả các phần tử $p \in S$. Phép phân tích này là duy nhất sai khác cách chọn S, và các số mũ là duy nhất được xác định bởi $e(p) = \operatorname{ord}_p a$.