ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ HOÀN

VỀ ĐỒNG DƯ ĐA THỨC

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2019

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ HOÀN

VỀ ĐỒNG DƯ ĐA THỨC

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. Nguyễn Thị Kiều Nga

THÁI NGUYÊN - 2019

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 đối với TS Nguyễn Thị Kiều Nga, cô đã trực tiếp hướng dẫn tận tình và động viên tác giả trong suốt thời gian nghiên cứu vừa qua.

Tác giả cũng xin chân thành cảm ơn tới các quý thầy, cô giáo đã giảng dạy lớp cao học Toán K11A, các bạn học viên và đồng nghiệp đã tạo điều kiện thuận lợi, giúp đỡ 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 luôn khuyến khích động viên tác giả trong suốt quá trình học cao học và viết luận văn này.

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 của các thầy cô và các bạn đọc để luận văn được hoàn thiện hơn.

Xin chân thành cảm ơn!

Thái Nguyên, tháng 4 năm 2019
Tác giả

Nguyễn Thị Hoàn

Mục lục

Mở đầu **1**

1 Kiến thức chuẩn bị **3**

1.1 Một số kiến thức cơ bản về đa thức một ẩn 3

1.1.1 Định nghĩa 3

1.1.2 Bậc của đa thức 4

1.1.3 Phép chia với dư 5

1.1.4 Nghiệm của đa thức 6

1.1.5 Ước chung lớn nhất, bội chung nhỏ nhất của đa thức 7

1.2 Một số định lý cơ bản của số học 8

2 Đồng dư đa thức **10**

2.1 Đồng dư đa thức với môđun một đa thức 10

2.2 Tập hợp gồm các lớp tương đương theo quan hệ đồng dư môđun một đa thức 15

2.3 Trường $A[x]\Big/(p(x))$ 17

2.4 Đồng dư đa thức với môđun nguyên tố 18

2.5 Đồng dư đa thức với môđun lũy thừa nguyên tố 23

2.6 Đồng dư $x^2 \equiv a \pmod m$ 29

2.7 Phương trình đồng dư bậc hai tổng quát 35

3 Một số ứng dụng của đồng dư đa thức trong giải toán sơ cấp **38**

3.1 Tìm đa thức dư khi chia đa thức $f(x)$ cho $g(x)$ trong $A[x]$. 38

3.2 Chứng minh đa thức $f(x)$ chia hết cho đa thức $g(x)$ trong $A[x]$ 40

3.3 Tìm điều kiện để $f(x)$ chia hết cho $g(x) \neq 0$ trong $A[x]$ . . 43

3.4 Bài toán về nghiệm của đa thức 51
3.5 Một số bài toán khác 51

Kết luận **56**

Tài liệu tham khảo **57**

Mở đầu

Đa thức là một khái niệm cơ bản và quan trọng của toán học. Đa thức không chỉ là đối tượng nghiên cứu của Đại số mà còn là công cụ quan trọng được sử dụng trong các nghiên cứu của Giải tích như Lý thuyết điều khiển, Lý thuyết tối ưu... Trong các kỳ thi học sinh giỏi trong và ngoài nước các bài toán về đa thức cũng thường được đề cập đến. Vì thế trong chương trình toán phổ thông đa thức là một chuyên đề quan trọng và cần thiết trong việc bồi dưỡng học sinh giỏi.

Đồng dư đa thức là một vấn đề được nhiều nhà toán học quan tâm khi nghiên cứu về đa thức mà trường hợp đặc biệt là các phương trình đồng dư hoặc các đồng dư thức. Theo [4], cho A là một trường, $f(x), g(x)$, $p(x) \in A[x], p(x) \neq 0$. Ta nói $f(x)$ đồng dư với $g(x)$ theo môđun $p(x)$ nếu và chỉ nếu $f(x) - g(x)$ chia hết cho $p(x)$ trong $A[x]$. Vì thế "đồng dư đa thức theo môđun một đa thức" có thể coi là tổng quát của khái niệm "đồng dư thức" đã biết.

Luận văn "Về đồng dư đa thức" nghiên cứu về đồng dư đa thức theo môđun một đa thức, đồng dư đa thức theo môđun số nguyên tố và lũy thừa một số nguyên tố. Các kết quả trong luận văn được tham khảo ở các tài liệu [2], [4], [6], [7]. Hơn nữa, chúng tôi cũng đưa ra được đặc trưng của đồng dư đa thức theo môđun một đa thức (Mệnh đề 2.1.2) và một số tính chất của đồng dư đa thức theo môđun một đa thức (Định lý 2.1.3). Sử dụng đồng dư đa thức, chúng tôi nghiên cứu một số ứng dụng của đồng dư đa thức trong giải toán sơ cấp.

Luận văn gồm 3 chương.

Chương 1: Trình bày một số kiến thức chuẩn bị về đa thức và một số tính chất số học cần thiết cho các chương sau.

Chương 2: Nghiên cứu về đồng dư đa thức: Đồng dư đa thức theo môđun một đa thức và một số trường hợp đặc biệt là môđun số nguyên tố và lũy thừa số nguyên tố.

Chương 3: Trình bày một số ứng dụng của đồng dư đa thức trong toán sơ cấp.

Mặc dù đã rất cố gắng nhưng do thời gian và năng lực nghiên cứu còn hạn chế nên rất mong được sự góp ý của các thầy cô và các bạn đọc để luận văn được hoàn thiện hơn.

Chương 1

Kiến thức chuẩn bị

Trong chương này, chúng tôi nhắc lại một số kiến thức về đa thức một ẩn và kiến thức về số học như khái niệm đa thức, bậc, nghiệm của đa thức, một số định lý thường gặp như Định lý phép chia với dư, Định lý Bezout, Viete, hàm Euler, một số định lý quan trọng của số học,... nhằm thuận tiện cho việc theo dõi các chương sau.

1.1 Một số kiến thức cơ bản về đa thức một ẩn

1.1.1 Định nghĩa

Định nghĩa 1.1.1. Cho A là một vành giao hoán có đơn vị. Một đa thức một ẩn với hệ số trên A là một biểu thức có dạng:

$$f(x) = a_0 + a_1x + ... + a_mx^m,$$

trong đó $a_i \in A$ với mọi $i = \overline{0, m}$ và x là một kí hiệu gọi là biến. Khi đó, a_i gọi là các hệ số thứ i của đa thức, a_ix^i gọi là hạng tử thứ i của đa thức, a_0 gọi là hạng tử tự do. Kí hiệu $A[x]$ là tập các đa thức một biến x với hệ số trong A.

Cho hai đa thức

$$f(x) = a_0 + a_1x + ... + a_nx^n$$

và

$$g(x) = b_0 + b_1x + ... + b_mx^m$$

thuộc $A[x]$. Không giảm tính tổng quát, ta có thể giả sử $m \geqslant n$ và $m = n + t$. Khi đó

$$g(x) = b_0 + b_1x + ... + b_nx^n + b_{n+1}x^{n+1} + ... + b_{n+t}x^{n+t}.$$

Ta nói hai đa thức $f(x)$ và $g(x)$ là bằng nhau nếu $a_i = b_i$ với mọi $i = \overline{0, n}$ và $b_{n+1} = ... = b_{n+t} = 0$.

Định nghĩa 1.1.2. Cho hai đa thức

$$f(x) = a_0 + a_1x + ... + a_nx^n$$

và

$$g(x) = b_0 + b_1x + ... + b_mx^m$$

thuộc $A[x]$. Khi đó

$$f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i.$$

$$f(x)g(x) = \sum_{i=0}^{m+n} \Big(\sum_{j=0}^{i} a_jb_{i-j} \Big) x^i.$$

Quy ước $a_i = 0$ nếu $i > n$ và $b_i = 0$ nếu $i > m$.

Khi đó $A[x]$ là một vành giao hoán có đơn vị với phép cộng và phép nhân các đa thức, $A[x]$ gọi là vành đa thức một ẩn với hệ số trong A.

1.1.2 Bậc của đa thức

Định nghĩa 1.1.3. Bậc của đa thức khác 0 trong $A[x]$

$$f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n$$

là n nếu $a_n \neq 0$, kí hiệu $\deg f(x) = n$.

Quy ước, đa thức 0 không có bậc hoặc có bậc là $-\infty$.

Sau đây là tính chất về bậc của đa thức

Định lý 1.1.4. *Giả sử $f(x), g(x)$ là hai đa thức khác 0 thuộc $A[x]$.*

(i) *Nếu* $f(x) + g(x) \neq 0$ *thì*

$$deg\,\Big(f(x) + g(x)\Big) \leqslant max\,\Big\{deg\,f(x),\, deg\,g(x)\Big\}$$

(ii) *Nếu* $f(x)g(x) \neq 0$ *thì*

$$deg\,\Big(f(x)g(x)\Big) \leqslant\ deg\,f(x) + deg\,g(x),$$

đẳng thức sẽ xảy ra nếu A *là miền nguyên.*

1.1.3 Phép chia với dư

Định lý 1.1.5. (Định lý phép chia với dư). *Cho* A *là một vành giao hoán có đơn vị và* $f(x), g(x)$ *là hai đa thức thuộc* $A[x], g(x)$ *là đa thức có hệ số cao nhất khả nghịch trong* A. *Khi đó tồn tại duy nhất* $q(x), r(x) \in A[x]$ *sao cho* $f(x) = g(x)q(x) + r(x)$ *và* $deg\,r(x) <\ deg\,g(x)$ *nếu* $r(x) \neq 0$.

Các đa thức $q(x)$ và $r(x)$ trong định lý trên lần lượt gọi là đa thức thương và dư trong phép chia $f(x)$ cho $g(x)$. Nếu $r(x) = 0$ thì ta nói $f(x)$ chia hết cho $g(x)$.

Kết quả sau đây là hệ quả trực tiếp của Định lý phép chia với dư trong trường hợp đa thức $g(x)$ là đa thức bậc nhất có hệ số cao nhất là 1.

Hệ quả 1.1.6. (Định lý Bezout). *Cho* A *là một vành giao hoán có đơn vị và* $g(x) \in A[x], \alpha \in A$. *Khi đó dư của phép chia* $f(x)$ *cho* $x - \alpha$ *là* $f(\alpha)$.

Chú ý 1.1.7. Cho $f(x) \in A[x], \alpha \in A$. Ta có lược đồ sau gọi là lược đồ Horner để tìm thương và dư của phép chia $f(x)$ cho $x - \alpha$. Giả sử $f(x) = \sum_{i=0}^{n} a_i x^i, a_n \neq 0$. Theo Định lý phép chia với dư, chia $f(x)$ cho $x - \alpha$, ta được $f(x) = (x - \alpha)q(x) + r$ với $r = f(\alpha)$ và deg $q(x) = n - 1$.

Giả sử $q(x) = b_{n-1}x^{n-1} + ... + b_1x + b_0$. Đồng nhất các hệ số, ta có $b_{n-1} = a_n, b_{n-2} = a_{n-1} + \alpha b_{n-1}, ..., b_{k-1} = a_k + \alpha b_k, ..., b_0 = a_1 + \alpha b_1$, $r =\ a_0 + \alpha b_0$.

	a_n	a_{n-1}	...	a_1	a_0
α	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + \alpha b_{n-1}$	...	$b_0 = a_1 + \alpha b_1$	$r = a_0 + \alpha b_0$