ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THU GIANG

VÀNH CÁC HÀM SỐ HỌC VÀ MỘT VÀI ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN, NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THU GIANG

VÀNH CÁC HÀM SỐ HỌC VÀ MỘT VÀI ỨNG DỤNG

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số: 60.46.01.13

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học:
PGS.TS NÔNG QUỐC CHINH

THÁI NGUYÊN, NĂM 2015

Mục lục

Mở đầu

Trong lý thuyết số, các hàm số học có vai trò hết sức quan trọng. Nhiều nhà toán học nổi tiếng thế giới khi nghiên cứu về các hàm số học đã có nhiều kết quả hết sức lý thú và có giá trị, được ứng dụng rộng rãi trong lý thuyết số nói riêng và trong toán học nói chung.

Mục đích của luận văn là hệ thống các tính chất của vành các hàm số học, đạo hàm của hàm số học. Tiếp theo, trình bày một số kết quả, tính chất của một vài hàm số học đặc biệt và các dạng bài toán ứng dụng liên quan.

Ngoài phần Mở đầu và Kết luận, luận văn được chia thành ba chương đề cập đến các vấn đề sau đây:

Chương 1 trình bày về các kiến thức chuẩn bị liên quan đến khái niệm nhóm, vành, các vấn đề về ước số và ước chung lớn nhất.

Chương 2 trình bày các tính chất và các dạng toán về vành số học.

Chương 3 trình bày một số lớp hàm số học như hàm Möbius (thuận và đảo), hàm nhân tính, phi - hàm Euler và các ứng dụng liên quan trong số học.

Tôi xin bày tỏ lòng biết ơn sâu sắc đối với Phó Giáo sư, Tiến sĩ Nông Quốc Chinh, người thầy đã trực tiếp hướng dẫn, cung cấp tài liệu và truyền đạt những kinh nghiệm nghiên cứu cho tôi.

Tôi xin chân thành cảm ơn các thầy, cô giáo trong khoa Toán - Tin, phòng Đào tạo trường Đại học Khoa học - Đại học Thái Nguyên, Trường THPT Hòn Gai và bạn bè đồng nghiệp đã giúp đỡ tạo điều kiện cho tôi hoàn thành bản luận văn này.

Chương 1

Các kiến thức chuẩn bị

1.1 Định nghĩa nhóm, nhóm xyclic, nhóm con

Định nghĩa 1.1 (Định nghĩa nhóm)**.** Một tập hợp G được gọi là một nhóm nếu tồn tại một ánh xạ từ tích Descartes $G \times G$ vào G (ảnh của phần tử $(a, b) \in G \times G$, với a, b là những phần tử tùy ý của G, qua ánh xạ này ta kí hiệu là ab) thỏa mãn các tính chất sau đây

(G1) *Kết hợp*: $a(bc) = (ab)c,\ \forall a, b, c \in G$.

(G2) *Có đơn vị*: Tồn tại một phần tử $a \in G$ sao cho $ae = ea = a,\ \forall a \in G$.

(G3) *Có nghịch đảo*: Với mỗi phần tử $a \in G$ luôn tồn tại một phần tử $b \in G$ sao cho $ab = ba = e$. Phần tử ab được gọi là tích của a và b và ánh xạ xác định tích ở trên được gọi là phép toán trên nhóm nhân G. Phần tử e trong(G2) được gọi là phần tử đơn vị của G, phần tử b trong (G3) được gọi là phần tử nghịch đảo của a trong G và kí hiệu là a^{-1}.

Nếu $ab = ba, \forall a, b \in G$, thì nhóm G được gọi là nhóm Abel, hay là nhóm giao hoán.

Một nhóm G được gọi là *hữu hạn* hay *vô hạn* nếu tập hợp G là hữu hạn hay vô hạn phần tử. Trường hợp nhóm G là hữu hạn thì số phần tử của G được gọi là *cấp* của nhóm đó và kí hiệu là $|G|$.

Định nghĩa 1.2. Một nhóm G được gọi là *nhóm xyclic* nếu mọi phần tử của nó đều là lũy thừa của một phần tử $a \in G$. Khi đó ta gọi a là phần tử sinh của nhóm xyclic G và kí hiệu là $G = \langle a \rangle$.

Theo định nghĩa, một nhóm xyclic G với phần tử sinh là a có thể viết dưới dạng $G = \{a^n | \ n \in \mathbb{Z}\}$.

Định nghĩa 1.3. Một tập hợp con H của của một nhóm G được gọi là một *nhóm con* của G nếu các điều kiện sau đây được thõa mãn:

(i) Phép toán nhân là đóng đối với H, tức $xy \in H \ \forall \, x, y \in H$;

(ii) H chứa phần tử đơn vị e của G;

(iii) $x^{-1} \in H, \forall x \in H$.

Nói cách khác, $H \neq \emptyset$ và là một nhóm con với phép toán nhân chính là phép toán của G.. Để chỉ H là nhóm con của G kí hiệu $H \leq G$.

Định lý 1.1. *Một tập hợp con H là một nhóm con của một nhóm G khi và chỉ khi $H \neq \emptyset$ và $xy^{-1} \in H, \forall x, y \in H$.*

1.2 Định nghĩa vành, idean, miền nguyên

Định nghĩa 1.4. (Định nghĩa vành): Một tập hợp R được gọi là một *vành* nếu trên R có hai phép toán hai ngôi, một gọi là phép cộng và một gọi là phép nhân, sao cho các điều kiện sau được thỏa mãn:

(R1) Tập hợp R là một nhóm Abel đối với phép cộng.(R_1) Tập hợp R là một nhóm Abel đối với phép cộng.

(R2) Phép nhân trên R là kết hợp và có đơn vị.

(R3) *Luật phân phối:* Phép nhân là phân phối đối với phép cộng, nghĩa là với các phần tử $x, y, z \in \mathbb{R}$ tùy ý, ta luôn có

$$(x + y)z = xz + yz \ \text{ và } \ z(x + y) = zx + zy.$$

Như thông thường ta kí hiệu phần tử đơn vị đối với phép nhân của R và e_R và phần tử không của nhóm Abel cộng của R và 0_R. Trường

hợp vành R đã xác định cụ thể trước thì ta kí hiệu đơn giản 1 cho phần tử đơn vị và 0 cho phần tử không của R.

Một vành R được gọi là *vành giao hoán*, nếu phép nhân của R thỏa mãn thêm điều kiện

$$xy = yx,\ \forall x, y \in \mathbb{R}.$$

Định nghĩa 1.5. Một vành giao hoán không có ước của không được gọi là một miền nguyên

Định nghĩa 1.6. Một vành R được gọi là một trường, nếu R là một vành giao hoán và mọi phần tử khác không của R đều có nghịch đảo, nghĩa là tập hợp $R^* = R\backslash\{0\}$ lập thành một nhóm đối với phép nhân của R.

Định nghĩa 1.7. (i) Một tập hợp con A của một vành R được gọi là một vành con của R, nếu A lập thành một nhóm con Abel với phép cộng của R và đóng đối với phép nhân, tức $ab \in A$. Trường hợp R là một trường thì một vành con của R được gọi là một trường con nếu nó là một trường với phép toán trên R.

(ii) Một tập hợp con a của một vành R được gọi là một idean trái (hoặc idean phải) của R, nếu a là một vành con của R và thỏa mãn tính chất

$$Ra \subseteq a \text{ (hoặc } aR \subseteq a).$$

Nếu a vừa là idean phải vừa là idean trái của R thì được gọi là một idean của R.

Định nghĩa 1.8. Cho R là một vành giao hoán, phần tử $x \in R$.

- x được gọi là một ước của y nếu tồn tại $z \in R$ sao cho $xz = y$. Khi đó, ta kí hiệu $x|y$.
- x được gọi là một ước của 0 nếu x khác 0 và tồn tại phần tử y khác 0 thuộc R sao cho $xy = 0$.
- x được gọi là phần tử khả nghịch nếu tồn tại y thuộc R sao cho $xy = 1$.

Ví dụ 1.1. Trong $6\mathbb{Z}$, các ước của 0 là $\bar{2}, \bar{3}, \bar{4}$. Các phần tử khả nghịch là $\bar{1}, \bar{5}$.

Trong $m\mathbb{Z}$, các ước của 0 là $\bar{a}$ sao cho a không chia hết m và $(a, m) > 1$. Các phần tử khả nghịch là $\bar{a}$ sao cho $(a, m) = 1$.

1.3 Ước chung lớn nhất

Định nghĩa 1.9. Cho $A \subset \mathbb{Z}; A \neq \{0\}$; nếu với mọi $a \in A$ ta đều có a chia hết cho d thì ta nói d là ước chung của tập A. Số nguyên d được gọi là ước chung lớn nhất của A nếu $c|d$ với mọi ước chung c của A, kí hiệu là $d = \gcd(A)$.

Định lý 1.2. Cho H là một nhóm con của nhóm các số nguyên với phép cộng. Tồn tại duy nhất một số nguyên không âm d sao cho H là tập gồm tất cả các bội của d, đó là $H = \{0, \pm d, \pm 2d, \ldots\} = d\mathbb{Z}$.

Chứng minh. Ta có $0 \in H$ với mọi nhóm con H. Nếu $H = \{0\}$ thì ta chọn $d = 0$ và $H = 0$. Hơn nữa, $d = 0$ là phần tử sinh duy nhất của nhóm con này.

Nếu $H \neq \{0\}$ thì tồn tại $a \in H, a \neq 0$.. Vì $-a$ cũng thuộc H nên kéo theo H chứa số nguyên dương. Do tập hợp số nguyên dương là tập sắp thứ tự tốt nên H chứa số nguyên dương nhỏ nhất d.

Với mọi $q \in \mathbb{Z}$, ta có $dq = \underbrace{d + d + \ldots + d}_{q}$ thuộc H do H là nhóm con của $\mathbb{Z}$, từ đó suy ra $d\mathbb{Z} \subseteq H$. Giả sử a là phần tử bất kì của H, theo thuật toán chia, ta có thể viết $a = dq + r$ với q, r là số nguyên dương $0 \leq r < d - 1$. Vì dq thuộc H và H là nhóm nên suy ra $r = a - dq$ thuộc H. Vì $0 \leq r < d$ và d là số nguyên dương nhỏ nhất trong H, ta phải có $r = 0$ tức là $a = dq \in d\mathbb{Z}$ và $H \subseteq d\mathbb{Z}$. Dẫn đến $H = d\mathbb{Z}$.

Nếu $H = d\mathbb{Z} = d'\mathbb{Z}$, với d, d' là các số nguyên dương thì $d' \in d\mathbb{Z}$ suy ra $d' = dq$. Q là số nguyên và $d \in d'\mathbb{Z}$ suy ra $d = s'q', q'$ là số nguyên. Do đó, $d = d'q' = dqq'$ tức là $qq' = 1$ nên $q = q' = \pm 1$ và $d = \pm d'$. Vì d và d' là các số nguyên dương nên $d = d'$. Và d là số nguyên duy nhất sinh nhóm con H. ■

Ví dụ 1.2. Nếu H là nhóm con chứa tất cả các số nguyên có dạng $35x + 91y$ thì $7 = 35(-5) + 91.2 \in H$ và $H = 7\mathbb{Z}$.

Định lý 1.3. Giả sử $A \subset \mathbb{Z}; A \neq \{0\}$, khi đó A có ước chung lớn nhất duy nhất và tồn tại các số nguyên $a_1, \ldots, a_k \in A$ và $x_1, \ldots, x_k \in \mathbb{Z}$ sao cho

$$\gcd(A) = a_1, x_1 + \ldots a_k x_k.$$

Chứng minh. Kí hiệu H là tập con của $\mathbb{Z}$ chứa tất cả các số nguyên tố có dạng

$$a_1, x_1 + \ldots a_k x_k \text{ với } a_1, \ldots a_t \in A \text{ và } x_1, \ldots, x_t \in \mathbb{Z}, \text{ với } t \in \mathbb{N}.$$

Khi đó H là nhóm con của $\mathbb{Z}$ và $A \subseteq H$. Theo định lí 1.2, tồn tại duy nhất số nguyên dương d sao cho $H = d\mathbb{Z}$, tức là H chứa tất cả các bội của d và do đó mọi số nguyên $a \in A$ đều là bội của d, suy ra d là ước chung của A. Vì $d \in H$ nên tồn tại các số nguyên $a_1, \ldots, a_k \in A$ và $x_1, \ldots, x_t \in \mathbb{Z}$ sao cho

$$d = a_1 x_1 + \ldots + a_k x_k.$$

Giả sử c là một ước chung bất kì của A, ta có c là ước của $a_1, \ldots, a_k$ nên c là ước của d. Vậy mọi ước chung của A đều là ước của d nên d là ước chung lớn nhất của A.

Nếu các số nguyên dương d và d' cùng là ước chung lớn nhất thì $d|d'$ và $d'|d$ nên $d = d'$. Tức là ước chung $\gcd(A)$ là duy nhất. ■

Kí hiệu: Nếu $A = \{a_1, \ldots, a_k\}$ là tập hữa hạn số nguyên không đồng thời bằng không, ta viết $\gcd(A) = (a_1, \ldots, a_k)$. Ví dụ $(35, 91) = 7 = 35.(-5) + 91.2$.

Định lý 1.4. *Cho $a_1, \ldots, a_k$ là các số nguyên không đồng thời bằng 0. Thì $(a_1, \ldots, a_k) = 1$ khi và chỉ khi tồn tại các số nguyên $x_1, \ldots, x_k$ sao cho*

$$a_1 x_1 + \ldots + a_k x_k = 1.$$

Chứng minh. Điều này dễ dàng thu được từ định lý 1.3 ■

Định nghĩa 1.10. Ta nói các số $a_1, \ldots, a_k$ là nguyên tố cùng nhau nếu ước chung lớn nhất của chúng là 1. Các số nguyên $a_1, \ldots, a_k$ là đôi một nguyên tố cùng nhau nếu $(a_i, a_j) = 1, i \neq j$.

Ví dụ 1.3. Ba số nguyên 6,10,15 là nguyên tố cùng nhau nhưng không là đôi một nguyên tố cùng nhau vì $(6, 10, 15) = 1$ nhưng $(6, 10) = 2$; $(6, 15) = 3$; $(10, 15) = 5$.