ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

KHỔNG THỊ THÚY HỒNG

VỀ GIẢ THUYẾT ABC VÀ MỘT SỐ ỨNG DỤNG

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

KHỔNG THỊ THÚY HỒNG

VỀ GIẢ THUYẾT ABC VÀ MỘT SỐ ỨNG DỤNG

LUẬN VĂN THẠC SỸ TOÁN HỌC

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số 60 46 01 13

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

THÁI NGUYÊN - NĂM 2015

Mục lục

Mở đầu

Từ xa xưa, các nhà toán học đã biết chuyển các kết quả số học sang giải quyết trên các đa thức và từ những bài toán và giả thuyết cho đa thức, người ta phát biểu tương tự cho số học. Điều này hoàn toàn hợp lý, bởi tập số nguyên và tập các đa thức có sự tương tự rất lớn. Việc giải quyết bài toán trên đa thức thường đơn giản hơn do đa thức có phép tính đạo hàm. Vì vậy định lý Mason cho đa thức được phát biểu tương tự cho số nguyên là giả thuyết *abc*.

Giả thuyết này được phát biểu vào năm 1985 bởi J. Oesterle' trong một kết quả của đường cong Elliptic của bộ môn hình học đại số, ngay sau đó D.R. Mason phát biểu dựa vào sự tương tự của số nguyên và đa thức.

Giả thuyết *abc* kéo theo rất nhiều hệ quả và các giả thuyết liên quan.

Mục đích của luận văn là trình bày định lý Mason và một số ứng dụng của định lý này. Từ định lý Mason cho đa thức ta có sự tương tự số học đó là giả thuyết *abc*. Từ đó nghiên cứu một số hệ quả trong số rất nhiều các hệ quả của giả thuyết này. Bản luận văn **"Về giả thuyết *abc* và một số ứng dụng"** được tiến hành chủ yếu dựa vào một số tài liệu tham khảo.

Bài luận văn **"Về giả thuyết *abc* và một số ứng dụng"** gồm có: mở đầu, hai chương nội dung, kết luận và tài liệu tham khảo.

Chương 1 Các kiến thức chuẩn bị

Trong chương này trình bày định nghĩa ideal, radical, một số tính chất của ideal, radical. Phép lấy đạo hàm trong vành và các tính chất của phép lấy đạo hàm. Định lý Mason và một số ứng dụng của định lý này.

Chương 2 Giả thuyết *abc* và một số ứng dụng

Trong chương này trình bày giả thuyết *abc* và một số hệ quả của giả thuyết này. Định lý tiệm cận Fermat, Định lý tiệm cận Catalan và một số hệ quả khác.

Luận văn được hoàn thành dưới sự hướng dẫn và chỉ bảo tận tình của PGS. TS. Nông Quốc Chinh, trường Đại học Khoa học, Đại học Thái Nguyên. Em xin bày tỏ lòng biết ơn sâu sắc đối với sự quan tâm, động viên và sự chỉ bảo hướng dẫn tận tình của thầy.

Em xin trân trọng cảm ơn các thầy, cô trong Ban Giám hiệu, Khoa Toán - Tin, phòng đào tạo trường Đại học Khoa học. Đồng thời tôi xin gửi lời cảm ơn tới tập thể lớp Cao học Toán K7B Trường Đại học Khoa học, cùng gia đình tôi đã động viên giúp đỡ tôi trong quá trình học tập và làm luận văn này.

Tuy nhiên do sự hiểu biết của bản thân và khuôn khổ luận văn thạc sĩ, nên chắc chắn rằng trong quá trình nghiên cứu không tránh khỏi những thiếu sót, tôi rất mong nhận được sự chỉ dạy và đóng góp của các thầy, cô và các bạn đồng nghiệp.

Tác giả

Chương 1

Các kiến thức chuẩn bị

Mục đích của tôi trong chương này là trình bày một số kiến thức như ideal, radical, phép lấy đạo hàm trong vành, định lý Mason và một vài ứng dụng của định lý này.

Trong chương này ta quy ước một vành R là một vành giao hoán, có phần tử đơn vị.

1.1 Ideal và Radical

Định nghĩa 1.1. Một tập con I của vành R được gọi là ideal của R nếu:

i) I là nhóm con của nhóm $(R, +)$.

ii) $ax \in I, \forall a \in I, x \in R$.

Ví dụ 1.1.

i) R và $\{0\}$ là các ideal R.

ii) Tập các số nguyên chẵn là một ideal của vành $\mathbb{Z}$.

iii) Tập các đa thức có hạng tử tự do bằng 0 là một ideal của vành $R[t]$, trong đó $R[t]$ là vành các đa thức với hệ số trong vành R.

Mệnh đề 1.1. Giao của một họ các ideal của một vành R cho trước là một ideal của R.

Chứng minh

Giả sử $(A_i)_{i \in I}$ là một họ các ideal của R. Đặt

$$A = \bigcap_{i \in I} A_i$$

Khi đó A là nhóm con của nhóm cộng giao hoán R.
Ta có

$$\forall x \in R,\ \forall a \in A\ \Rightarrow a \in A_i\, \forall i\ \Rightarrow ax \in A_i\ \forall i$$

$$\Rightarrow ax \in A\ \Rightarrow\ \text{A là ideal của } R\ .$$

Mệnh đề được chứng minh.

Định nghĩa 1.2. Nếu A là một tập con khác rỗng của vành R thì tập tất cả các tổ hợp tuyến tính hữu hạn có dạng $a_1r_1 + a_2r_2 + ... + a_kr_k$ với $a_i \in A, r_i \in R, i = 1, ..., k$ là một ideal của R kí hiệu bởi $\langle A\rangle$ và gọi là ideal sinh bởi A.

Một ideal sinh bởi một phần tử $a \in R$ gọi là một ideal chính và kí hiệu bởi

$$\langle a\rangle = aR = \{ar : r \in R\}\,.$$

Định nghĩa 1.3. Vành chính là vành mà mọi ideal đều là ideal chính.
Ví dụ 1.2.

i) $\mathbb{Z}$ là vành chính.

ii) $\mathbb{Z}/m\mathbb{Z}$ là vành chính.

Định nghĩa 1.4. Một ideal I của vành R được gọi là ideal nguyên tố nếu:

i) $I \neq R$.

ii) $\forall a, b \in R$, $ab \in I$ kéo theo $a \in I$ hoặc $b \in I$.

Định nghĩa 1.5. Phổ của vành R kí hiệu là $\mathrm{Spec}(R)$, là tập tất cả các ideal nguyên tố của R.

Định lí 1.1. Phổ của vành các số nguyên là
$\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} : p$ là số nguyên tố hoặc $p = 0\}$.
Chứng minh

Vì $\mathbb{Z}$ là vành chính nên mọi ideal của nó có dạng $d\mathbb{Z}$ với d là số nguyên không âm.
Nếu $d = 0$ thì $d\mathbb{Z} = \{0\}$, ideal $\{0\}$ là ideal nguyên tố, vì $ab = 0$ khi và chỉ khi $a = 0$ hoặc $b = 0$.

Giả sử $d \geq 1$.

TH1 : $d = p$ là một số nguyên tố và $ab \in p\mathbb{Z}$ thì p là ước của ab. Theo bổ đề Euclid, p là ước của a hoặc p là ước của b, do đó $a \in p\mathbb{Z}$ hoặc $b \in p\mathbb{Z}$. Vậy $p\mathbb{Z}$ là iđêan nguyên tố với mọi số nguyên tố p.

TH2 : d là hợp số, ta có thể viết $d = ab$, trong đó $1 < a \leq b < d$.
Nếu $a \in d\mathbb{Z}$ thì $a = dk = abk$ với k nguyên dương, suy ra $1 = bk$, vô lý. Do đó $a \notin d\mathbb{Z}$.

Tương tự $b \notin d\mathbb{Z}$.

Vì $d = ab \in d\mathbb{Z}$, suy ra $d\mathbb{Z}$ không phải là một ideal nguyên tố. Do vậy, các ideal nguyên tố của vành $\mathbb{Z}$ là các ideal có dạng $p\mathbb{Z}$, với p là nguyên tố hoặc $p = 0$.
Định lý được chứng minh.

Định nghĩa 1.6. Một phần tử x của vành R được gọi là lũy linh nếu tồn tại một số nguyên dương k sao cho $x^k = 0$.

Ví dụ 1.3.

i) Phần tử không trong một vành bất kì là phần tử lũy linh.
Phần tử đơn vị 1 trong vành không là phần tử lũy linh.

ii) Lớp đồng dư $6 + 27\mathbb{Z}$ là phần tử lũy linh của vành $\mathbb{Z}/27\mathbb{Z}$.

Định nghĩa 1.7. Ta gọi tập tất cả các phần tử lũy linh của R là radical của vành R và kí hiệu bởi $N(R)$.

Nhận xét $N(R)$ là một ideal của vành R.
Thật vậy:

- $\forall a, b \in N(R)$, tồn tại các số nguyên k, h sao cho $a^k = 0$, $b^h = 0$.
  Dùng khai triển Newton có ngay mọi hạng tử trong khai triển $(a-b)^{k+h}$ đều bằng 0, suy ra $(a-b)^{k+h} = 0$ nên $(a-b) \in N(R)$.

- $\forall a \in N(R)$, $\forall x \in R$, do R là vành giao hoán ta có $(ax)^k = a^k.x^k = 0$, suy ra $ax \in N(R)$.

Định nghĩa 1.8. Ta gọi tích của các ước nguyên tố khác nhau của số nguyên khác không m là radical của số m và kí hiệu là $rad(m)$.
Ta có

$$rad(m) = \prod_{p|m} p.$$

Ví dụ 1.4.

$rad\,(72) = 2.3 = 6,\ \ rad\,(30) = 2.3.5 = 30,\ \ rad\,(-1) = 1.$
$rad\,(3^n) = 3,\ \ rad\,(n!) = \prod_{2\leq p\leq n} p$, p là số nguyên tố.
$rad\,(a^n) = rad\,a$ đối với mọi số nguyên a.

Định lí 1.2. Với $m \geq 2$ ta có:

i) $\mathbb{Z}/m\mathbb{Z}$ là vành chính và các ideal của $\mathbb{Z}/m\mathbb{Z}$ là các ideal sinh bởi các lớp đồng dư $d + m\mathbb{Z}$, với d là ước của m.

ii) Các ideal nguyên tố của $\mathbb{Z}/m\mathbb{Z}$ là các ideal sinh bởi các lớp đồng dư $p + m\mathbb{Z}$, trong đó p là một ước số nguyên tố của m.

iii) Radical của $\mathbb{Z}/m\mathbb{Z}$ là ideal sinh ra bởi lớp đồng dư $rad\,(m) + m\mathbb{Z}$.

Chứng minh

i) Giả sử J là một ideal bất kì của vành $\mathbb{Z}/m\mathbb{Z}$.
Xét phép chiếu chính tắc

$$p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}\ \ \left(p\,(x) = x + m\mathbb{Z}\right).$$

Ta có p là một đồng cấu vành và $p^{-1}\,(J) = I$ là một ideal của $\mathbb{Z}$.
Rõ ràng

$$I = \left\{a \in \mathbb{Z} | p\,(a) = a + m\mathbb{Z} \in J\right\}.$$

Do $\mathbb{Z}$ là vành chính nên I là ideal chính, ta có $I = d\mathbb{Z}$ (d là số nguyên dương nhỏ nhất trong I). Do $p\,(m) = m\mathbb{Z} \in J$ nên $m \in I = d\mathbb{Z}$ suy ra d là ước của m.
Mặt khác, do $d \in I$ nên $p\,(d) = d + m\mathbb{Z} \in J$ suy ra ideal chính trong $\mathbb{Z}/m\mathbb{Z}$ sinh bởi $\langle d + m\mathbb{Z}\rangle$ chứa trong J.
Ngược lại, lấy bất kì $a + m\mathbb{Z} \in J$ ta có $a \in I$ nên $a = dr$ với r nguyên. Suy ra

$$a + m\mathbb{Z} = dr + m\mathbb{Z} = (d + m\mathbb{Z})\,(r + m\mathbb{Z}) \in \langle d + m\mathbb{Z}\rangle.$$

Từ đó suy ra $J = \langle d + m\mathbb{Z}\rangle$ và $a + m\mathbb{Z} \in J$ khi và chỉ khi d là ước của a.

ii) Gọi J là ideal chính sinh bởi $d + m\mathbb{Z}$, trong đó d là ước của m, $d \geq 2$. Nếu $d = p$ là nguyên tố và

$$(a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z} \in J$$

thì p là ước của ab và do đó p là ước của a hoặc của b, tức là $a + m\mathbb{Z} \in J$ hoặc $b + m\mathbb{Z} \in J$ suy ra J là ideal nguyên tố.
Nếu $d = ab$ là hợp số, trong đó $1 < a \leq b < d$ thì $a + m\mathbb{Z} \notin J$ và $b + m\mathbb{Z} \notin J$ nhưng $(a + m\mathbb{Z})(b + m\mathbb{Z}) = d + m\mathbb{Z} \in J$, nên J không phải là ideal nguyên tố. Do đó, ideal nguyên tố của vành $\mathbb{Z}/m\mathbb{Z}$ là các ideal có dạng $p + m\mathbb{Z}$, trong đó p là ước nguyên tố của m.
Do vậy

$$Spec(\mathbb{Z}/m\mathbb{Z}) = \left\{ \langle p + m\mathbb{Z} \rangle \mid \text{với } p \text{ là ước nguyên tố của } m \right\}.$$

iii) Lớp đồng dư $a + m\mathbb{Z}$ là lũy linh trong R khi và chỉ khi với k nguyên dương

$$(a + m\mathbb{Z})^k = a^k + m\mathbb{Z} = m\mathbb{Z}.$$

Điều này tương đương với $a + m\mathbb{Z}$ là lũy linh khi và chỉ khi m là ước của a^k. Suy ra $rad(m)$ là ước của $rad\left(a^k\right) = rad(a)$.
Từ đó ta có $rad(m)$ là ước của a. Vì vậy $a + m\mathbb{Z} \in \langle rad(m) + m\mathbb{Z} \rangle$.
Ta có

$$N(\mathbb{Z}/m\mathbb{Z}) = \langle rad(m) + m\mathbb{Z} \rangle.$$

Định lý được chứng minh.

Cho $f(t) \in \mathbb{C}[t]$ là đa thức bậc n. Nếu $\alpha_1, ..., \alpha_r$ là các nghiệm phân biệt của $f(t)$ thì ta có thể phân tích $f(t)$ thành tích các số hạng tuyến tính dạng $f(t) = c_n \prod_{i=1}^{r} (t - \alpha_i)^{m_i}$, trong đó hệ số đầu tiên $c_n \neq 0$ và $m_1 + ... + m_r = n$.

Định nghĩa 1.9. Radical của đa thức $f(x)$ được định nghĩa bởi

$$rad(f) = \prod_{i=1}^{r} (t - \alpha_i).$$

Tập hợp các nghiệm của đa thức $f(t)$ là một tập hữu hạn

$$Z(f) = \{\alpha \in \mathbb{C} : f(\alpha) = 0\} = \{\alpha_1, ..., \alpha_r\}.$$