ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

LÊ THỊ HẢI YẾN

SỐ NGUYÊN TỐ VÀ ĐA THỨC BẤT KHẢ QUY

LUẬN VĂN THẠC SỸ TOÁN HỌC

THÁI NGUYÊN - NĂM 2014

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

– – – – – – – – – –

LÊ THỊ HẢI YẾN

SỐ NGUYÊN TỐ VÀ ĐA THỨC BẤT KHẢ QUY

LUẬN VĂN THẠC SỸ TOÁN HỌC

Chuyên nghành: PHƯƠNG PHÁP TOÁN SƠ CẤP
Mã số 60.46.01.13

Người hướng dẫn khoa học
TS. NGUYỄN VĂN HOÀNG

THÁI NGUYÊN - NĂM 2014

Mục lục

Mở đầu

Sự tương tự giữa các số nguyên tố và các đa thức bất khả quy đã là một chủ đề thống trị trong sự phát triển của lý thuyết số và hình học đại số. Có các giả thuyết chỉ ra rằng mối liên hệ đó đã vượt hơn cả sự tương tự. Ví dụ, có một giả thuyết nổi tiếng của Buniakowski được phát biểu vào năm 1854: *Cho đa thức $f(x)$ hệ số nguyên thỏa mãn ba điều kiện sau*

i) Hệ số đầu của $f(x)$ là dương;

ii) Đa thức $f(x)$ bất khả quy trên $\mathbb{Q}$;

iii) Tập các giá trị $f(\mathbb{Z}^+)$ không có ước chung lớn hơn 1

khi đó đa thức $f(x)$ nhận vô hạn các giá trị nguyên tố? (xem tài liệu S. Lang [2, Trang 323]).

Một cách độc lập nó được phát biểu lại bởi Schinzel, nói về tác động của đa thức bất khả quy $f(x) \in \mathbb{Z}[x]$ (mà tập các giá trị $f(\mathbb{Z}^+)$ không có ước số chung lớn hơn 1) biểu diễn vô hạn các nguyên tố. Trong trường hợp này, vấn đề dẫn đến việc quan tâm đến các số nguyên tố sinh ra từ các đa thức bất khả quy. Giả thuyết này vẫn là một trong những vấn đề lớn chưa được giải quyết trong lý thuyết số khi bậc của f lớn hơn một (Lưu ý khi f là đa thức bậc nhất, giả thuyết đó là đúng). Không khó để thấy rằng mệnh đảo của giả thuyết của Buniakowski là đúng. Một cách cụ thể hơn, nếu một đa thức biểu diễn vô hạn các số nguyên tố, thì nó là một đa thức bất khả quy. Để thấy điều này, chúng ta hãy cố gắng để phân tích ra thừa số $f(x) = g(x)h(x)$ với $g(x)$ và $h(x)$ trong $\mathbb{Z}[x]$ có bậc dương. Thực tế, do $f(x)$ lấy vô hạn giá trị nguyên tố, nên một trong hai $g(x)$ hoặc $h(x)$ nhận vô hạn giá trị ± 1. Đây là một mâu thuẫn, bởi vì một đa thức có bậc dương chỉ có thể có nhận một giá trị tại hữu hạn lần.

Mục đích của luận văn này là tiếp tục tìm hiểu thêm những liên hệ quan trọng giữa đa thức bất khả quy và các số nguyên tố liên quan đến giả thuyết của Buniakowski và bài toán ngược của nó như đã nêu trên. Trên cơ sở nghiên

cứu một số tài liệu về số nguyên tố và về đa thức bất khả quy, trong luận văn này chúng tôi lựa chọn và trình bày chi tiết lại một số tiêu chuẩn quan trọng về đa thức bất khả quy liên quan đến ứng dụng của số nguyên tố. Tài liệu tham khảo chính mà chúng tôi sử dụng là hai bài báo:

- M. R. Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly 109 (2002) No. 5, 452-458 (tài liệu số [8]).
- A. I. Bonciocat, N. C. Bonciocat and A. Zaharescu, *On the irreducibility of polynomials that take a prime power value*, Bull. Math. Soc. Sci. Math. Roumanie Tome 54 (102), No. 1 (2011), 41-54 (tài liệu số [2]).

Luận văn được trình bày trong hai chương.

Chương I: Một số kiến thức chuẩn bị. Nội dung của chương là trình bày tóm lược một số kiến thức cơ bản cần dùng cho chứng minh của các kết quả trong chương sau, chẳng hạn: sơ lược về số nguyên tố, về đa thức, bậc đa thức, đa thức bất khả quy, sự phân tích một đa thức thành tích các đa thức bất khả quy, một số ví dụ về đa thức bất khả quy,... .

Chương II: Số nguyên tố và đa thức bất khả quy. Đây là chương chính của luận văn. Chương này trình bày về một số tiêu chuẩn để kiểm tra tính chất bất khả quy của một số lớp đa thức.

+) Mục 2.1. Trình bày về sự liên hệ giữa số nguyên tố và đa thức bất khả quy (dựa trên bài báo [8]). Kết quả chính là định lý sau

Định lý 2.1.3. *Cho* $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *là một đa thức bậc* m. *Đặt* $H = \max\limits_{0\leq i\leq m-1} |\frac{a_i}{a_m}|$. *Khi đó, nếu có số nguyên* $n \geq H + 2$ *sao cho* $f(n)$ *là số nguyên tố thì* $f(x)$ *bất khả quy trên* $\mathbb{Z}$.

Định lý 2.1.7 *Cho* $b > 2$ *và cho* p *là số nguyên tố có khai triển* $b-adic$

$$p = a_n b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0.$$

Khi đó $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *là bất khả quy trên* $\mathbb{Q}$.

+) Mục 2.2. Nghiên cứu mối liên hệ giữa đa thức bất khả quy và lũy thừa số nguyên tố (dựa theo bài báo [2]). Trước hết chương này chứng minh chi tiết cho kết quả sau đây đó là một mở rộng cho Định lý 2.1.7:

Định lý 2.2.3. *Cho p là số nguyên tố. Giả sử p^s (với $s \geq 2$) có biểu diễn qua hệ thống cơ số $b \geq 2$ dưới dạng*

$$p^s = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0,$$

trong đó $0 \leq a_i \leq b-1$ và $p \nmid \sum_{i=1}^{n} i a_i b^{i-1}$. Khi đó đa thức $\sum_{i=0}^{n} a_i x^i$ là bất khả quy trên $\mathbb{Q}$.

Phần tiếp theo của mục này là trình bày các dấu hiệu bất khả quy cho các đa thức có một hệ số nào đó đủ lớn và nó có giá trị chia hết một lũy thừa nguyên tố nào đó.

Định lý 2.2.4. *Cho $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ với $a_0 a_n \neq 0$. Cho $m, s, q \in \mathbb{Z}$ ($s \geq 2$) và p là số nguyên tố sao cho $f(m) = p^s q$, $p \nmid q f'(m)$, và $|a_0| > \sum_{i=1}^{n} |a_i|(|m| + |q|)^i$. Khi đó $f(x)$ bất khả quy trên $\mathbb{Q}$.*

Định lý 2.2.5. *Cho $f(x) = \sum_{i=0}^{n} a_i x^{d_i} \in \mathbb{Z}[x]$, với $0 = d_0 < d_1 < \ldots < d_n$ và $a_0 a_1 \ldots a_n \neq 0$. Cho $m, s, q \in \mathbb{Z}$ (với $s \geq 2$), và p là số nguyên tố mà $f(m) = p^s q$, $|m| > |q|$ và $p \nmid q f'(m)$. Khi đó nếu có $1 \leq j \leq n-1$ sao cho $|a_j| > (|m| + |q|)^{d_n - d_j} \sum_{i \neq j} |a_i|$, thì $f(x)$ bất khả quy trên $\mathbb{Q}$.*

Định lý 2.2.6. *Cho $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x], a_0 a_n \neq 0$. Cho $f(m) = p^s q$ với $m, s, p \in \mathbb{Z}$, p là số nguyên tố, $s \geq 2$, $|m| > |q|$, $p \nmid q f'(m)$ và $|a_n| > \sum_{i=0}^{n-1} |a_i|(|m| - |q|)^{i-n}$ thì $f(x)$ bất khả quy trên $\mathbb{Q}$.*

Nói một cách vắn tắt thì cả ba định lý trên đều cho ta trường hợp đặc biệt khi $q = 1$ đó là: "Nếu $f(m)$ là một lũy thừa của số nguyên tố (trong đó $m \geq 2$ là số nguyên thỏa mãn $f(m)$ và $f'(m)$ là nguyên tố cùng nhau) và $f(x)$ có một hệ số nào đó đủ lớn thì $f(x)$ là đa thức bất khả quy trên $\mathbb{Q}$."

+) Mục 2.3 dành để trình bày một số ví dụ minh họa.

Trong thời gian thực hiện luận văn này, tôi đã nhận được sự chỉ dẫn tận tình, chu đáo của Tiến sĩ Nguyễn Văn Hoàng. Tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy Nguyễn Văn Hoàng đã giúp đỡ tôi hoàn thành luận văn này.

Tôi xin chân thành cảm ơn Ban giám hiệu cùng các bạn đồng nghiệp trường THPT Đông Thành - Quảng Ninh đã nhiệt tình giúp đỡ tôi trong suốt quá trình học tập và hoàn thành luận văn.

Tác giả

Chương 1

Một số kiến thức chuẩn bị

Chương này nhằm mục đích trình bày lại một số kiến thức căn bản về số nguyên tố, vành đa thức, đa thức bất khả quy. Bên cạnh đó cũng trình bày một vài tiêu chuẩn bất khả quy quen biết và một số ví dụ minh họa. Những kiến thức ở chương này một phần là cần thiết cho chương sau một phần là giúp cho việc trình bày chủ đề có tính hệ thống.

1.1 Số nguyên tố

Mục này ta chỉ xét trên tập các số tự nhiên $\mathbb{N}$.

Định nghĩa 1.1.1. Số nguyên tố là số tự nhiên lớn hơn 1 chỉ gồm có hai ước là 1 và chính nó.

Kí hiệu 1.1.2. Ký hiệu "$b|a$" nghĩa là b là ước của a, ký hiệu $a\vdots b$ nghĩa là a chia hết cho b.

Tính chất 1.1.3. *i) Ước khác 1 nhỏ nhất của một số tự nhiên lớn hơn 1 là số nguyên tố.*

ii) Cho p là số nguyên tố, $a \in N$ với $a \neq 0$. Khi đó

$$(a,p) = p \Leftrightarrow p|a; \qquad (a,p) = 1 \Leftrightarrow p \nmid a.$$

iii) Cho $a, b \in \mathbb{Z}$. Khi đó $(a,b) = 1$ nếu và chỉ nếu tồn tại $x, y \in \mathbb{Z}$ sao cho $ax + by = 1$.

iv) Nếu tích của nhiều số chia hết cho một số nguyên tố p thì có ít nhất một thừa số chia hết cho p.

Chứng minh. i) Cho a là số tự nhiên > 1. Giả sử d là ước nhỏ nhất khác 1 của a. Nếu d không nguyên tố thì $d = d_1 d_2$ (với $d_1, d_2 > 1$). Suy ra $d_1 | a$ với $d_1 < d$, điều này mâu thuẫn với d nhỏ nhất. Vậy d là nguyên tố.

ii) Nếu $p = (a, p)$ thì hiển nhiên $p|a$. Ngược lại nếu $p|a$ thì $(a, p) = p$.

+ Nếu $1 = (a, p)$ thì $p \nmid a$ (vì nếu $p|a$ thì $(a, p) = p$). Ngược lại, nếu $p \nmid a$ thì $(a, p) = 1$ (vì nếu $(a, p) = d > 1$ thì $d|p$, từ đó vì p nguyên tố nên $d = p$, suy ra $p|a$, đây là điều mâu thuẫn).

iii) Xét tập $I = \{ax + by \mid x, y \in \mathbb{Z}\}$. Ta thấy I là iđêan của $\mathbb{Z}$, nên tồn tại $d \in \mathbb{Z}, d > 0$ sao cho $I = d\mathbb{Z}$. Lúc đó ta dễ thấy $(a, b) = d$. Ngược lại, nếu $(a, b) = d$ thì $a \in d\mathbb{Z}$ và $b \in d\mathbb{Z}$. Từ đó $I \subseteq d\mathbb{Z}$. Mặt khác, bằng thuật toán Euclid, ta tìm được $x_0, y_0 \in \mathbb{Z}$ sao cho $d = ax_0 + by_0$, suy ra $d \in \{ax + by \mid x, y \in \mathbb{Z}\} = I$, do đó $d\mathbb{Z} \subseteq I$.

Áp dụng kết quả trên khi $d = 1$ ta có điều cần chứng minh.

iv) Bằng quy nạp ta chỉ cần chứng minh rằng $p|ab$ thì $p|a$ hoặc $p|b$ (với p là số nguyên tố, và $a, b \in \mathbb{Z}$). Ta giả sử trái lại rằng $p \nmid a$ và $p \nmid b$, khi đó theo ii), ta có $1 = ax + py$ và $1 = bx' + py'$ với $x, y, x', y' \in \mathbb{Z}$. Từ đó $1 = (ax + py)(bx' + py') = abxx' + p(axy' + bx'y + pyy')$. Do đó ta lại áp dụng ý ii) nên ta được $(ab, p) = 1$, đây là điều mâu thuẫn. □

Tính chất 1.1.4. *Tập hợp các số nguyên tố là vô hạn.*

Chứng minh. Giả sử chỉ có hữu hạn n số nguyên tố $p_1, p_2, \ldots, p_n$. Ta xét số tự nhiên $q = p_1 p_2 \ldots p_n + 1$. Rõ ràng $q > 2$. Gọi p là ước nhỏ nhất khác 1 của q. Khi đó p là số nguyên tố (theo Tính chất 1.1.3 i)). Mặt khác ta thấy $p \notin \{p_1, \ldots, p_n\}$ (vì nếu trái lại thì $p|1$ đó là điều mâu thuẫn). Như vậy ta lại tìm thêm được số nguyên tố nữa là p khác với mọi $p_1, p_2, \ldots, p_n$. Đó là điều mâu thuẫn với điều giả sử chỉ có n số nguyên tố $p_1, \ldots, p_n$. □

Ta có định lý quan trọng sau đây nói về vai trò của các số nguyên tố trong thành phần cấu tạo nên các số tự nhiên.

Định lý 1.1.5. *(Định lý cơ bản của số học) Mọi số tự nhiên n lớn hơn 1 đều phân tích được thành tích những thừa số nguyên tố, và sự phân tích này là duy nhất nếu không kể đến thứ tự của các thừa số. Từ đó có dạng phân tích tiêu chuẩn của một số tự nhiên $n > 1$ bất kỳ có dạng như sau*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$$

trong đó $p_1, p_2, \ldots, p_m$ là các số nguyên tố đôi một khác nhau, và $k_1, k_2, \ldots, k_m$ là các số tự nhiên khác 0.

1.2 Vành đa thức

Mục này nhắc lại một số kiến thức căn bản về đa thức với hệ tử trên vành giao hoán A có đơn vị.

Định nghĩa 1.2.1. Cho A là một vành giao hoán có đơn vị, $n \in \mathbb{N}$, và $a_0, a_1, \ldots, a_n \in A$. Một biểu thức có dạng

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n$$

được gọi là một đa thức một biến x lấy hệ tử trong A. Tập tất cả các đa thức một ẩn x lấy hệ tử trên A được ký hiệu là $A[x]$. Nếu $a_n \neq 0$ thì ta nói bậc của $f(x)$ là n và ký hiệu là $\deg(f(x)) = n$; trong trường hợp này ta nói a_n là hệ tử cao nhất của $f(x)$. Hai đa thức là *bằng nhau* nếu nó có cùng bậc và các hệ tử tương ứng là bằng nhau.

Với hai đa thức $f(x), g(x) \in A[x]$, khi đó tồn tại $m \in \mathbb{N}$ sao cho $f(x) = \sum_{i=0}^{m} a_i x^i$ và $g(x) = \sum_{i=0}^{m} b_i x^i$ (lưu ý rằng không nhất thiết $a_m \neq 0$ và $b_m \neq 0$), ta định nghĩa *tổng* của $f(x)$ và $g(x)$ như sau:

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

Trong trường hợp $f(x) = \sum_{i=0}^{n} a_i x^i$ và $g(x) = \sum_{i=0}^{m} b_i x^i$ (với n, m bất kì), ta định nghĩa *tích* của $f(x)$ và $g(x)$ bởi:

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k,$$

trong đó $c_k = \sum_{i+j=k} a_i b_j$ với mọi $k = 0, \ldots, n+m$.

Chú ý 1.2.2. Tập $A[x]$ cùng với phép cộng và nhân các đa thức như định nghĩa trên tạo thành một vành giao hoán, ta gọi là vành đa thức một ẩn x lấy hệ tử trên A. Trong đó đa thức không trong $A[x]$ chính là phần tử 0 của A. Phần tử 1 của A đóng vai trò phần tử đơn vị của vành $A[x]$. Khi A là các tập số $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ thì các hệ tử của các đa thức còn gọi là các hệ số.

Từ định nghĩa đa thức ta dễ dàng thu được một số tính chất sau đây về bậc của đa thức.

Định lý 1.2.3. *Giả sử $f(x)$ và $g(x)$ là hai đa thức khác 0 của vành $A[x]$.*

i) Nếu $\deg f(x) \neq \deg g(x)$, *thì ta có* $f(x) + g(x) \neq 0$ *và*

$$\deg(f(x) + g(x)) = \max\{\deg f(x), \deg g(x)\}.$$

Nếu $deg f(x) = \deg g(x)$ *và* $f(x) + g(x) \neq 0$ *thì ta có*

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}.$$

ii) Nếu $f(x)g(x) \neq 0$ *thì* $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$.

Chú ý 1.2.4. Giả sử A là miền nguyên. Khi đó nếu $f(x), g(x)$ là các đa thức khác 0 của $A[x]$ thì ta dễ thấy $f(x)g(x) \neq 0$. Từ đó ta thấy rằng $A[x]$ cũng là miền nguyên.

Định nghĩa 1.2.5. Cho A là một miền nguyên, và $f(x), g(x) \in A[x]$ với $g(x) \neq 0$. Nếu tồn tại $q(x) \in A[x]$ sao cho $f(x) = q(x)g(x)$ thì ta nói rằng $g(x)$ là *ước* của $f(x)$, hay $f(x)$ là *bội* của $g(x)$, ta viết là $g(x)|f(x)$ hoặc $f(x)\vdots g(x)$ (trong trường hợp này ta cũng nói $g(x)$ *chia hết* $f(x)$, hoặc $f(x)$ *chia hết cho* $g(x)$).

Tiếp theo ta nhắc lại vài tính chất đơn giản sau đây:

Bổ đề 1.2.6. *Cho A là miền nguyên. Khi đó các phát biểu sau là đúng.*

i) Với $a \in A$ và m là số tự nhiên ta có $(x - a)|(x^m - a^m)$.

ii) Nếu $f(x) \in A[x]$ và $a \in A$ thì tồn tại $q(x) \in A[x]$ sao cho

$$f(x) = (x - a)q(x) + f(a).$$

Chứng minh. i) Kết quả được suy ra từ hằng đẳng thức

$$x^m - a^m = (x - a)(x^{m-1} + ax^{m-2} + \ldots + a^{m-2}x + a^{m-1}).$$

ii) Giả sử $f(x) = a_n x^n + a_{n-1}x^{n-1} \ldots + a_1 x + a_0$. Khi đó $f(a) = a_n a^n + a_{n-1}a^{n-1} \ldots + a_1 a + a_0$. Từ đó

$$f(x) - f(a) = a_n(x^n - a^n) + a_{n-1}(x^{n-1} - a^{n-1}) + \ldots + a_1(x - a).$$

Theo ý i), ta có $x^n - a^n, x^{n-1} - a^{n-1}, \ldots, x - a$ chia hết cho $x - a$. Từ đó tồn tại $q(x) \in A[x]$ sao cho $f(x) - f(a) = (x - a)q(x)$, hay $f(x) = (x - a)q(x) + f(a)$. □