ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**VŨ ĐỨC CẢNH**

# ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG $Z_p$ THUẬT TOÁN BERLEKAMP VÀ PHÂN TÍCH ĐA THỨC TRÊN TRƯỜNG $Q$

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**THÁI NGUYÊN - 2016**

ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**VŨ ĐỨC CẢNH**

# ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG $Z_p$ THUẬT TOÁN BERLEKAMP VÀ PHÂN TÍCH ĐA THỨC TRÊN TRƯỜNG $Q$

## LUẬN VĂN THẠC SĨ TOÁN HỌC

**Chuyên ngành: Phương pháp Toán sơ cấp**

**Mã số: 60 46 01 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC:
**GS.TS. Lê Thị Thanh Nhàn**

**THÁI NGUYÊN - 2016**

# Mục lục

# Lời cảm ơn

Luận văn này được thực hiện tại Trường Đại học Khoa học - Đại học Thái Nguyên và hoàn thành dưới sự hướng dẫn của GS.TS. Lê Thị Thanh Nhàn. Tác giả xin được bày tỏ lòng biết ơn chân thành và sâu sắc tới người hướng dẫn khoa học của mình, người đã đặt vấn đề nghiên cứu, dành nhiều thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn.

Tác giả xin trân trọng cảm ơn Ban Giám hiệu Trường Đại học Khoa học - Đại học Thái Nguyên, Ban Chủ nhiệm Khoa Toán-Tin, cùng các giảng viên đã tham gia giảng dạy, đã tạo mọi điều kiện tốt nhất để tác giả học tập và nghiên cứu.

Tác giả cũng xin chân thành cảm ơn Phòng Giáo dục và Đào tạo huyện Tiên Lãng, Ban giám hiệu và các đồng nghiệp trường THCS Vinh Quang, huyện Tiên Lãng, thành phố Hải Phòng đã tạo điều kiện cho tác giả hoàn thành tốt nhiệm vụ học tập và công tác của mình.

Nhân dịp này, tác giả cũng xin gửi lời cảm ơn tới tập thể lớp cao học Toán K8B (khóa 2014-2016), cảm ơn gia đình bạn bè đã động viên và giúp đỡ tác giả rất nhiều trong quá trình học tập.

# Mở đầu

Luận văn quan tâm đến bài toán phân tích đa thức với hệ số nguyên thành nhân tử bất khả quy trên $\mathbb{Q}$. Đây là một trong những bài toán quan trọng nhất của Lí thuyết đa thức.

Ta biết rằng bài toán xét tính bất khả quy của đa thức trên $\mathbb{Q}$ có liên quan mật thiết với bài toán xét tính bất khả quy của đa thức trên trường hữu hạn. Cho $f(x)$ là đa thức với hệ số nguyên. Nếu tồn tại một số nguyên tố $p$ sao cho khi chuyển vào $\mathbb{Z}_p[x]$ bậc của đa thức $f(x)$ không đổi và $f(x)$ bất khả quy trên $\mathbb{Z}_p$, thì $f(x)$ là bất khả quy trên $\mathbb{Q}$. Chú ý rằng điều ngược lại là không đúng. D. Hilbert đã chỉ ra một đa thức bậc 4 bất khả quy trên $\mathbb{Q}$ nhưng khả quy trên mọi trường $\mathbb{Z}_p$. Quan hệ trên về tính bất khả quy trên $\mathbb{Q}$ và trên $\mathbb{Z}_p$ gợi ý cho chúng ta nghĩ đến việc tìm một thuật toán phân tích bất khả quy của đa thức trên trường hữu hạn và sử dụng nó để tìm phân tích bất khả quy của đa thức trên $\mathbb{Q}$.

Mục đích của luận văn là trình bày chi tiết những kết quả chọn lọc trong một số tài liệu gần đây về đa thức bất khả quy và sự phân tích đa thức thành nhân tử bất khả quy. Trong luận văn này, trước hết chúng tôi xét tính bất khả quy của đa thức trên trường $\mathbb{Z}_p$ và thuật toán Berlekamp phân tích đa thức thành nhân tử bất khả quy trên trường $\mathbb{Z}_p$. Sau đó, sử dụng các kết quả thu được, chúng tôi trình bày một phương pháp phân tích đa thức thành nhân tử trên trường $\mathbb{Q}$ các số hữu tỷ.

Nội dung nghiên cứu của luận văn là hoàn toàn chưa được tiếp cận ở bậc phổ thông và đại học, nhưng gắn liền với toán sơ cấp, đặc biệt là bài toán phân tích đa thức thành nhân tử rất được quan tâm ở bậc học phổ thông.

Luận văn gồm phần mở đầu, hai chương và tài liệu tham khảo. Trong Chương 1, chúng tôi nhắc lại khái niệm đa thức bất khả quy và một số tiêu

chuẩn bất khả quy trên $\mathbb{Q}$. Chương 2 là nội dung chính của luận văn. Mục 2.1 dành để nghiên cứu khái niệm trường phân rã của đa thức, từ đó xét cấu trúc của trường hữu hạn. Mục tiếp theo mô tả huật toán Berlekamp phân tích đa thức thành nhân tử trên trường hữu hạn. Mục cuối là ứng dụng kết quả vào bài toán phân tích đa thức trên trường $\mathbb{Q}$.

*Thái Nguyên, ngày 25 tháng 5 năm 2016*

***Tác giả***

***Vũ Đức Cảnh***

# Chương 1

# Đa thức bất khả quy

## 1.1 Khái niệm đa thức bất khả quy

Trước khi trình bày khái niệm đa thức bất khả quy, chúng ta nhắc lại khái niệm phần tử bất khả quy trong một miền nguyên. Cho $V$ là một miền nguyên và $a \in V$. Ta nói $a$ là *ước* của $b$ nếu tồn tại $c \in V$ sao cho $b = ac$. Một *ước* $a$ của $b$ được gọi là *ước thực sự* nếu $b$ không là ước của $a$. Phần tử $p \in V$ được gọi là phần từ *bất khả quy* nếu nó khác 0, không khả nghịch và không có ước thực sự. Từ đây ta có khái niệm đa thức bất khả quy trong vành đa thức $V[x]$. Trong suốt tiết này ta luôn giả thiết $V$ là miền nguyên.

**Định nghĩa 1.1.1.** Cho $f(x) \in V[x]$ là đa thức khác 0 và không khả nghịch. Ta nói $f(x)$ *là bất khả quy* trên $V$ nếu nó không có ước thực sự. Ta nói $f(x)$ *khả quy* nếu $f(x)$ có ước thực sự.

**Bổ đề 1.1.2.** *Đa thức $f(x)$ là bất khả quy nếu và chỉ nếu $f(x+a)$ là bất khả quy với mọi $a \in V$.*

*Chứng minh.* Cho $a \in V$. Với mỗi $h(x) \in V[x]$ ta đặt $h_1(x) = h(x-a)$. Chú ý rằng $\deg h_1(x) = \deg h(x)$. Vì thế $f(x+a) = k(x)g(x)$ là phân tích của $f(x+a)$ thành tích của hai đa thức có bậc thấp hơn khi và chỉ khi $f(x) = k_1(x)g_1(x)$ là phân tích của $f(x)$ thành tích của hai đa thức có bậc thấp hơn. Vì vậy $f(x)$ bất khả quy khi và chỉ khi $f(x+a)$ bất khả quy. □

Từ nay đến hết mục này chúng ta làm việc với đa thức có các hệ số trên một trường $K$. Trong trường hợp này, các đa thức hằng khác 0 đều khả nghịch. Do đó ta có ngay kết quả sau:

**Bổ đề 1.1.3.** *Đa thức f(x) với hệ số trên trường K là bất khả quy nếu và chỉ nếu* $\deg f(x) > 0$ *và* $f(x)$ *không phân tích được thành tích của hai đa thức có bậc bé hơn.*

Sau đây là tính bất khả quy của các đa thức bậc thấp.

**Bổ đề 1.1.4.** *Trên một trường K, các phát biểu sau là đúng.*
*(i) Đa thức bậc nhất luôn bất khả quy.*
*(ii) Đa thức bậc 2 và bậc 3 là bất khả quy nếu và chỉ nếu nó không có nghiệm trong K.*

*Chứng minh.* (i) Rõ ràng đa thức bậc nhất không thể là tích của hai đa thức bậc thấp hơn, do đó nó bất khả quy.
(ii) Giả sử $f(x)$ có nghiệm $x = a \in K$. Vì $\deg f(x) > 1$ nên ta có $f(x) = (x-a)g(x)$, trong đó $g(x) \in K[x]$ và $\deg g(x) = \deg f(x) - 1 \geq 1$. Do đó $f(x)$ khả quy. Ngược lại, giả sử $f(x)$ khả quy. Vì $f(x)$ có bậc 2 hoặc 3 nên $f(x)$ phân tích được thành tích của hai đa thức có bậc thấp hơn, một trong hai đa thức đó phải có bậc 1. Rõ ràng đa thức bậc 1 trên một trường có nghiệm trong trường đó, vì thế $f(x)$ có nghiệm trong $K$ □

Chú ý rằng phát biểu (ii) trong bổ đề trên là không đúng cho trường hợp bậc của đa thức lớn hơn 3. Cụ thể, nếu $f(x)$ bậc lớn hơn 3 và có nghiệm trong $K$ thì $f(x)$ khả quy. Tuy nhiên, tồn tại những đa thức không có nghiệm trong $K$ nhưng vẫn khả quy. Chẳng hạn đa thức $(x^2+1)(x^2+2)$ không có nghiệm trong $\mathbb{R}$ nhưng nó khả quy trên $\mathbb{R}$.

Từ nay về sau, nếu $a$ là ước của $b$ thì ta kí hiệu là $a \mid b$.

**Mệnh đề 1.1.5.** *Cho* $p(x) \in K[x]$ *là đa thức có bậc dương. Khi đó p(x) bất khả quy nếu và chỉ nếu* $p(x) \mid a(x)b(x)$ *kéo theo* $p(x) \mid a(x)$ *hoặc* $p(x) \mid b(x)$ *với mọi* $a(x), b(x) \in K[x]$. *Đặc biệt, nếu đa thức bất khả quy* $p(x)$ *là ước của một tích hữu hạn thì đa thức* $p(x)$ *phải là ước của ít nhất một trong các đa thức đó.*

*Chứng minh.* Cho $p(x)$ bất khả quy. Giả sử $p(x) \mid a(x)b(x)$ và $a(x), b(x)$ đều không là bội của $p(x)$. Do $p(x)$ bất khả quy nên $\gcd(p(x), a(x)) = 1$ và $\gcd(p(x), b(x)) = 1$. Vì thế, tồn tại $s(x), r(x), e(x), f(x)$ sao cho $1 = s(x)p(x) + r(x)a(x)$ và $1 = e(x)p(x) + f(x)b(x)$. Nhân vế với vế của hai

đẳng thức này ta có

$$1 = p(x)g(x) + r(x)f(x)a(x)b(x)$$

với $g(x)$ là một đa thức nào đó. Vì $p(x)$ là ước của $a(x)b(x)$ nên đa thức bên vế phải của đẳng thức trên là bội của $p(x)$, trong khi đó đa thức bên vế trái là 1 không chia hết cho $p(x)$. Điều này là vô lí.

Ngược lại, do $p(x)$ có bậc dương nên $p(x) \neq 0$ và không khả nghịch. Giả sử $p(x) = a(x)b(x)$ với $a(x), b(x) \in K[x]$. Khi đó $p(x) \mid a(x)b(x)$. Theo giả thiết, $p(x) \mid a(x)$ hoặc $p(x) \mid b(x)$. Vì thế $p(x)$ không có ước thực sự, do đó $p(x)$ bất khả quy. □

Định lý cơ bản của Số học nói rằng mỗi số tự nhiên lớn hơn 1 đều phân tích được thành tích các thừa số nguyên tố và sự phân tích đó là duy nhất nếu không kể đến thứ tự các thừa số. Kết quả sau đây là một sự tương tự đối với đa thức.

**Định lý 1.1.6.** *Mỗi đa thức dạng chuẩn bậc dương trong $K[x]$ có thể phân tích được thành tích các đa thức bất khả quy dạng chuẩn và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.*

*Chứng minh.* Trước hết, ta chứng minh sự tồn tại phân tích bằng quy nạp theo bậc của đa thức. Giả sử $f(x) \in K$[x] là đa thức dạng chuẩn bậc $d > 0$. Nếu $d = 1$ thì $f(x)$ là bất khả quy, và sự phân tích bất khả quy của $f(x)$ là $f(x) = f(x)$. Cho $d > 1$ và giả sử kết quả đã đúng cho các bậc nhỏ hơn $d$. Nếu $f(x)$ bất khả quy thì $f(x)$ có sự phân tích bất khả quy là $f(x) = f(x)$. Vì thế ta giả thiết $f(x)$ không bất khả quy. Khi đó $f(x) = g(x)h(x)$ với deg$g(x)$, deg $h(x)$<deg$f(x)$. Đặt $g^*(x) = a^{-1}g(x)$ với $a$ là hệ số cao nhất của $g(x)$. Khi đó ta có $f(x) = g^*(x)(ah(x))$. Đồng nhất hệ số cao nhất ở hai vế ta suy ra $ah(x)$ có dạng chuẩn. Do đó $f(x) = g^*(x)h^*(x)$ với $g^*(x), h^*(x) = ah(x)$ là các đa thức dạng chuẩn có bậc nhỏ hơn $d$. Theo giả thiết quy nạp, $g^*(x)$ và $h^*(x)$ phân tích được thành tích của hữu hạn các đa thức bất khả quy dạng chuẩn. Vì thế, $f(x)$ phân tích được thành tích của hữu hạn đa thức bất khả quy dạng chuẩn.

Bây giờ ta chứng minh tính duy nhất của phân tích. Giả sử $f(x)$ có hai

sự phân tích thành nhân tử bất khả quy dạng chuẩn

$$f(x) = p_1(x)p_2(x)...p_n(x) = q_1(x)q_2(x)...q_m(x).$$

Ta chứng minh bằng sự quy nạp theo $n$ rằng $n = m$ và sau khi đánh lại thứ tự các nhân tử về bên phải ta có $p_i(x) = q_i(x)$ với mọi $i = 1,...,n$. Do $p_1(x) \mid q_1(x)q_2(x)...q_m(x)$ và $p_1(x)$ bất khả quy nên theo mệnh đề trên ta có $p_1(x) \mid q_i(x)$ với $i$ nào đó. Không mất tính tổng quát ta giả thiết $p_1(x) \mid q_1(x)$. Biểu diễn $q_1(x) = p_1(x)t_1(x)$. Vì $q_1(x)$ bất khả quy nên $t_1(x) = a \in K$. Do đó $q_1(x) = ap_1(x)$. Do $p_1(x)$ và $q_1(x)$ có dạng chuẩn nên $a = 1$. Vì thế $p_1(x) = q_1(x)$. Cho $n = 1$. Nếu $m > 1$ thì giản ước cả hai vế cho $p_1(x)$ ta được $1 = q_2(x)...q_m(x)$, điều này là vô lí. Vậy, kết quả đúng cho $n = 1$. Cho $n > 1$. Vì $p_1(x) = q_1(x)$ nên

$$f(x) = p_2(x)p_3(x)...p_n(x) = q_2(x)q_2(x)...q_m(x).$$

Theo giả thiết quy nạp ta có $n-1 = m-1$ và bằng việc đánh số lại thứ tự các nhân tử bất khả quy ở vế phải ta có $p_i(x) = q_i(x)$ với $i = 2,...,n.$, suy ra $p_i(x) = q_i(x)$ với mọi $i = 2,...,n$. □

Từ định lý trên, ta có kết quả sau.

**Hệ quả 1.1.7.** *Cho $f(x) \in K[x]$ là đa thức với hệ số cao nhất là $a_n$. Khi đó tồn tại phân tích $f(x) = a_n f_1(x)...f_k(x)$ với $f_1(x),...,f_k(x)$ là các nhân tử bất khả quy dạng chuẩn, và sự phân tích này là duy nhất nếu không kể đến thứ tự các nhân tử.*

Euclid đã chứng minh rằng có vô hạn số nguyên tố. Kết quả sau đây là một sự tương tự cho đa thức bất khả quy.

**Hệ quả 1.1.8.** *Trên một trường K bất kỳ, có vô hạn đa thức bất khả quy dạng chuẩn.*

*Chứng minh.* Chú ý rằng $x+1 \in K[x]$ là đa thức bất khả quy dạng chuẩn. Giả sử $f_1(x),...,f_n(x) \in K[x]$ là tất cả các đa thức bất khả quy dạng chuẩn. Đặt $f(x) = f_1(x)...f_n(x)+1$. Theo định lý trên, tồn tại $p(x)$ là ước bất khả quy dạng chuẩn của $f(x)$. Do đó $p(x) = f_i(x)$ với $i$ nào đó. Suy ra $p(x) \mid f_1(x)...f_n(x)$. Vì $p(x) \mid f_(x)$ nên $p(x) \mid 1$, điều này vô lí, tức là phải có vô hạn các đa thức bất khả quy dạng chuẩn. □