ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—————————o0o—————————

TRẦN THỊ HƠN

VỀ SỐ ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG HỮU HẠN

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2020

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

——————————o0o——————————

TRẦN THỊ HƠN

VỀ SỐ ĐA THỨC BẤT KHẢ QUY TRÊN TRƯỜNG HỮU HẠN

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. NGÔ THỊ NGOAN

Thái Nguyên - 2020

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 TS. Ngô Thị Ngoan. 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 thời gian hướng dẫn và tận tình giải đáp những thắc mắc của tác giả trong suốt quá trình làm luận văn.

Tác giả cũng đã học tập được rất nhiều kiến thức chuyên ngành bổ ích cho công tác và nghiên cứu của bản thân. Tác giả xin bày tỏ lòng cảm ơn sâu sắc tới các thầy giáo, cô giáo đã tham gia giảng dạy lớp Cao học Toán K12A7; Nhà trường và các phòng chức năng của Trường; Khoa Toán – Tin, trường Đại học Khoa học – Đại học Thái Nguyên đã quan tâm và giúp đỡ tác giả trong suốt thời gian học tập tại trường.

Tác giả cũng xin gửi lời cảm ơn sâu sắc tới Trung tâm Nghiên cứu và Phát triển giáo dục Hải Phòng đã giúp đỡ, tạo mọi điều kiện thuận lợi giúp tôi có thể hoàn thành luận văn này.

Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp Cao học Toán K12A7 đã luôn động viên và giúp đỡ tác giả rất nhiều trong quá trình học tập và làm luận văn.

Cuối cùng, tôi xin gửi lời cảm ơn chân thành tới gia đình, bạn bè đã giúp đỡ và tạo điều kiện tốt nhất cho tôi khi học tập và nghiên cứu.

Thái Nguyên, tháng 6 năm 2020

Tác giả

Trần Thị Hơn

Mở đầu

Một trong những vấn đề được nghiên cứu trong lý thuyết số đó là sự phân bố các số nguyên tố. Người ta nhận thấy rằng các số nguyên tố nhỏ nằm tương đối gần nhau, trong khi các số nguyên tố càng lớn thì càng có xu hướng cách xa nhau hơn. Ta đặt câu hỏi về sự liên quan giữa mật độ của các số nguyên tố với độ lớn của chúng. Bằng cách lập bảng số nguyên tố và nghiên cứu mật độ, Gauss thấy rằng "xung quanh x mật độ của các số nguyên tố là xấp xỉ $\dfrac{1}{\log(x)}$ " theo [9]. Phát hiện này là chìa khóa để hình thành định lý số nguyên tố.

Để chứng minh phát hiện này, Gauss đã nghiên cứu hàm đếm số nguyên tố: Gọi x là số thực dương, $\pi(x)$ biểu thị số các số nguyên tố nhỏ hơn hoặc bằng x. Tức là ta có $\pi(x) = \sum_{p \leq x} 1$. Vì người ta đã dự đoán về mật độ các số nguyên tố quanh x là $\dfrac{1}{\log(x)}$, nên họ cũng dự đoán rằng $\pi(x)$ xấp xỉ với một tổng logarit hoặc một tích phân logarit. Chúng tương ứng được cho bởi:

$$\mathrm{ls}(x) := \sum_{2 \leq n \leq x} \frac{1}{\log(n)}, \quad \mathrm{li}(x) := \int_2^x \frac{dt}{\log(t)}.$$

Ta nói hai hàm f và g là hai hàm tương đương nếu thương số của chúng $\dfrac{f(x)}{g(x)}$ tiến tới 1 khi x tiến tới vô cùng. Ta sử dụng ký hiệu $f(x) \sim g(x)$ khi $x \to \infty$. Với mỗi $x \geq 2$, hiệu số giữa $\mathrm{ls}(x)$ và $\mathrm{li}(x)$ bị chặn bởi $\dfrac{1}{\log(2)}$ theo Hệ quả 1.5.1 trong [4]. Do đó, hai hàm tổng logarit và tích phân logarit là tương đương. Hai hàm này cũng tương đương với $\dfrac{x}{\log(x)}$ (Hệ quả 1.5.3 trong [4]).

Định lý số nguyên tố được cả Gauss (1792) và Legendre (1798) nêu ra

giả thuyết rằng hàm đếm số nguyên tố $\pi(x)$ tương đương với các hàm này. Nó được trình bày dưới dạng

$$\pi(x) \sim \frac{x}{\log(x)} \quad (x \to \infty). \tag{1}$$

Một trăm năm sau vào năm 1896 định lý này được chứng minh bởi cả Hadamard và La Vallée Muffsin một cách độc lập. Cả hai chứng minh của họ đều dựa trên hàm zeta Riemann, một mở rộng giải tích của tổng $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Riemann đã chỉ ra rằng sự phân bổ các số nguyên tố có liên quan trực tiếp đến tập các nghiệm của hàm này. Hadamard và La Vallée Muffsin đã chứng minh rằng hàm Riemann zeta không có nghiệm trên đường thẳng $\mathrm{Re}(s) = 1$, chúng đã được sử dụng để chứng minh định lý số nguyên tố.

Các giá trị xấp xỉ của $\mathrm{ls}(x)$ và $\mathrm{li}(x)$ tốt hơn $\frac{x}{\log(x)}$ do đó chúng thường được ưu tiên hơn khi nghiên cứu các phần sai số. Đối với các phần sai số, ta sử dụng ký hiệu $\mathcal{O}$: Với hai hàm f và g bất kỳ, ta có $f(x) = \mathcal{O}(g(x))$ nếu tồn tại hằng số C sao cho với x đủ lớn, giá trị tuyệt đối của $f(x)$ bị chặn bởi $Cg(x)$.

Vì $\mathrm{ls}(x)$ và $\mathrm{li}(x)$ chỉ khác nhau một số bị chặn, nên phần sai số cũng đúng với $\mathrm{ls}(x)$. Bằng cách sử dụng hàm ζ không có nghiệm trên đường thẳng $\mathrm{Re}(s) = 1$, theo Định lý 5.1.8 trong [4] đã chứng minh được tồn tại hằng số c sao cho:

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}\left(xe^{-c\sqrt{\log(x)}}\right) \tag{2}$$

Phần sai số ở đây có thể được khái quát hơn bởi các nghiệm của ζ. Đặt $\Theta = \sup_{\zeta(s)=0} \mathrm{Re}(s)$ là cận trên đúng của các phần thực các nghiệm của ζ. Khi đó theo [5] ta có:

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}\left(x^{\Theta}\log(x)\right) \tag{3}$$

Riemann đã cho rằng tất cả các nghiệm không tầm thường của ζ nằm trên đường thẳng $\mathrm{Re}(s) = \frac{1}{2}$. Giả thiết này được gọi là giả thuyết Riemann. Giả thuyết Riemann suy ra $\Theta = \frac{1}{2}$, điều này cho ta xấp xỉ

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}\left(\sqrt{x}\log(x)\right).$$

Trong luận văn này, ta sẽ tìm hiểu về một sự tương tự định lý số nguyên tố nhưng được phát biểu trong vành $\mathbb{F}_q[T]$ là vành các đa thức một biến T với các hệ số thuộc trường hữu hạn $\mathbb{F}_q$. Ta sẽ nghiên cứu các hàm tương đương với hàm đếm số các đa thức bất khả quy và có sự so sánh các kết quả này với hàm đếm số nguyên tố $\pi(x)$. Một trong những lợi thế khi làm việc với $\mathbb{F}_q[T]$ là công thức của Gauss, một công thức trực tiếp về số lượng đa thức monic bất khả quy bậc n. Đây là một công cụ rất mạnh để nghiên cứu các hàm tương đương hàm đếm.

Luận văn được chia thành ba chương. Chương 1 bao gồm một số kiến thức chuẩn bị về trường hữu hạn và Định lý nghịch đảo Mobius. Những kiến thức này phục vụ cho việc trình bày nội dung chính của luận văn trong những chương sau. Chương 2 nêu lên những tính chất cơ bản, chúng cho ta thấy sự tương tự giữa hai miền nguyên $\mathbb{Z}$ và $\mathbb{F}_q[T]$. Chương 3 trình bày về hàm đếm số đa thức bất khả quy trên trường hữu hạn q phần tử, đồng thời cũng cho ta thấy sự tương tự với Định lý về hàm đếm số nguyên tố trong vành các số nguyên.

Chương 1

Kiến thức chuẩn bị

Trong phần này, ta sẽ trình bày một số kết quả về các trường hữu hạn và khái niệm hàm Mobius. Những kết quả này sẽ được sử dụng để chứng minh công thức của Gauss về số đa thức bất khả quy định chuẩn bậc n và được sử dụng trong các chương sau của luận văn.

1.1 Một số khái niệm

Ta nhắc lại, một trường F là một vành giao hoán khác không và mọi phần tử khác không đều khả nghịch. Một trường có hữu hạn phần tử được gọi là một *trường hữu hạn.*

Định nghĩa 1.1.1. Trường F được gọi là một *trường nguyên tố* nếu nó không có trường con nào ngoài bản thân nó.

Nhận xét 1.1.2.
(i) Cho F là trường nguyên tố. Khi đó chỉ có thể xảy ra một trong hai trường hợp: nếu F có đặc số 0 thì $F \cong \mathbb{Q}$; nếu F có đặc số p thì $F \cong \mathbb{Z}_p$. Trường hợp $F \cong \mathbb{Z}_p$ ta thường kí hiệu $\mathbb{F}_p$ thay cho F.
(ii) Cho E là một trường tùy ý, khi đó nếu gọi F là giao của mọi trường con của E thì F cũng là một trường con của E, rõ ràng F là trường con nhỏ nhất của E, do đó F là trường nguyên tố. Trong trường hợp này, ta nói F là trường con nguyên tố của E. Như vậy, mọi trường đều chứa một trường con nguyên tố.

1.2 Trường hữu hạn

Giả sử p là số nguyên tố, vành $\mathbb{Z}/p\mathbb{Z}$ là một trường có đúng p phần tử. Đây là trường hữu hạn duy nhất (sai khác đẳng cấu) có đúng p phần tử. Nếu L là một trường với p phần tử, gọi p' là đặc số của L. Khi đó $\mathbb{Z}/p'\mathbb{Z}$ là đẳng cấu của một trường con của L, nên p' chia hết p. Điều này chỉ đúng nếu $p' = p$ do đó $L \cong \mathbb{Z}/p\mathbb{Z}$. Ta ký hiệu $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Tổng quát hơn, nếu q là lũy thừa của một nguyên tố, thì tồn tại một trường duy nhất với q phần tử, ký hiệu $\mathbb{F}_q$.

Bổ đề 1.2.1 (Cấu trúc trường hữu hạn)**.**
(i) Cho F là trường hữu hạn có q phần tử. Khi đó tồn tại số nguyên tố p sao cho $q = p^n$ với số tự nhiên n nào đó.
(ii) Với mỗi số nguyên tố p và số tự nhiên $n \neq 0$, tồn tại duy nhất một trường hữu hạn có p^n phần tử (sai khác một đẳng cấu trường).

Chứng minh.
(i) Gọi p là đặc số của trường F, khi đó p là số nguyên tố. Gọi $\mathbb{F}_p$ là trường con nguyên tố của F, khi đó $\mathbb{F}_p \cong \mathbb{Z}_p$. Ta biết rằng F là $\mathbb{F}_p-$không gian vectơ hữu hạn chiều. Giả sử $\dim_{\mathbb{F}_p}(F) = n < \infty$, khi đó F có một cơ sở là $\{e_1, \ldots, e_n\}$ và vì thế mỗi phần tử của F có dạng $x = \sum_{i=1}^{n} a_i e_i$ với $a_1, \ldots, a_n \in \mathbb{F}_p$. Từ đó suy ra số phần tử của F bằng số các bộ phần tử $(a_1, \ldots, a_n) \in \mathbb{F}_p \times \ldots \times \mathbb{F}_p$ (n lần). Do đó $q = p^n$.
(ii) Sự tồn tại của trường có $q = p^n$ phần tử. Xét đa thức $f(x) = x^q - x \in \mathbb{F}_p[x]$ với $\mathbb{F}_p \cong \mathbb{Z}_p$ là trường nguyên tố có đặc số nguyên tố p. Gọi E là trường phân rã của $f(x)$ trên $\mathbb{F}_p$. Đặt

$$K = \{\alpha \in E \mid f(\alpha) = 0\}$$

đó chính là tập hợp các nghiệm của $f(x)$. Khi đó K là một trường con của E. Thật vậy, với mọi $\alpha, \beta \in K$ ta có

$$(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta, (\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$$

Do đó $\alpha - \beta, \alpha\beta \in K$. Nếu $\alpha \in K^*$ thì $(\alpha^{-1})^q = (a^q)^{-1} = \alpha^{-1}$ suy ra $\alpha^{-1} \in K$. Ngoài ra, rõ ràng $1^q = 1$ nên $1 \in K$. Cuối cùng, ta thấy rằng mọi $a \in \mathbb{F}_p$ đều thỏa mãn $a^p = a$ do đó $a^q = a^{p^n} = a$ chứng tỏ $\mathbb{F}_p \subseteq K$.

Như vậy K chính là trường phân rã của $f(x)$ trên $\mathbb{F}_p$, trường này có $q = p^n$ phần tử (lưu ý rằng đa thức $f(x)$ không có nghiệm bội).

Tính duy nhất của trường có $q = p^n$ phần tử. Giả sử $\mathbb{F}_q$ là trường có $q = p^n$ phần tử. Khi đó $\mathbb{F}_q$ có đặc số là p (giả sử p_1 là đặc số của $\mathbb{F}_q$ thì theo (i) suy ra $q = p_1^{n'}$; do đó $p^n = p_1^{n'}$ vì thế $p = p_1$). Vì $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ là nhóm với phép nhân nên $\alpha^{q-1} = 1$ với mọi $\alpha \in \mathbb{F}_q^*$; do đó $\alpha^q = \alpha$ với mọi $\alpha \in \mathbb{F}_q$. Chứng tỏ mọi phần tử của $\mathbb{F}_q$ đều là nghiệm của đa thức $f(x) = x^q - x \in \mathbb{F}_p[x]$ với $\mathbb{F}_p$ là trường nguyên tố của $\mathbb{F}_q$. Suy ra trường $\mathbb{F}_q$ chính là trường phân rã của $f(x)$ trên $\mathbb{F}_p$. Điều đó khẳng định tính duy nhất của $\mathbb{F}_q$ sai khác một đẳng cấu trường. □

Ta nhắc lại, một mở rộng trường E/F ($F \subset E$) là một mở rộng Galois nếu nó là mở rộng chuẩn tắc và tách được (Chương 2 tài liệu [1]). Ta có kết quả sau:

Bổ đề 1.2.2. *Cho E/F là một mở rộng hữu hạn khi đó các khẳng định sau tương đương:*

(i) E/F là mở rộng Galois;

(ii) Nếu $p(x) \in F(x)$ là đa thức bất khả quy trên F có một nghiệm trong E thì nó tách được và có mọi nghiệm trong E (tức là $p(x)$ tách được và phân rã trên E);

(iii) E là trường phân rã của một đa thức tách được $f(x) \in F[x]$.

Định lý 1.2.3. *Cho q là lũy thừa của một số nguyên tố và a, b là số nguyên dương. Nếu a là ước của b, thì $\mathbb{F}_{q^a}$ là trường con của $\mathbb{F}_{q^b}$. Hơn nữa, mở rộng trường $\mathbb{F}_{q^b}/\mathbb{F}_{q^a}$ là mở rộng Galois. Mọi đa thức bất khả quy trên $\mathbb{F}_{q^a}$ đều tách được và nếu nó có nghiệm trong $\mathbb{F}_{q^b}$ thì mọi nghiệm của nó đều thuộc $\mathbb{F}_{q^b}$.*

Chứng minh. Giả sử a, b là các số nguyên dương sao cho a là ước của b. Áp dụng lập luận như trong chứng minh của Bổ đề 1.2.1, trường phân rã của $P(T) = T^{q^b} - T$ trên $\mathbb{F}_{q^a}$ có đúng q^b phần tử và đẳng cấu với $\mathbb{F}_{q^b}$. Trường phân rã này cũng chứa $\mathbb{F}_{q^a}$, và do đó $\mathbb{F}_{q^a}$ là một trường con của $\mathbb{F}_{q^b}$. Hơn nữa, vì $P(T)$ là đa thức tách được, $\mathbb{F}_{q^b}$ là trường phân rã của $P(T)$ trên