ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—o0o—

NGUYỄN QUANG TUẤN

ĐA THỨC CANTOR VÀ ĐỊNH LÝ FUETER-PÓLYA

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

—————o0o—————

NGUYỄN QUANG TUẤN

ĐA THỨC CANTOR VÀ ĐỊNH LÝ FUETER-PÓLYA

Chuyên ngành: Phương pháp toán sơ cấp
Mã số: 8460113

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. NGUYỄN DUY TÂN

THÁI NGUYÊN - 2018

Mục lục

Lời nói đầu

Một hàm đa thức $F\colon \mathbb{R}^2 \to \mathbb{R}$ được gọi là một đa thức xếp trên $\mathbb{N}_0^2$ nếu F hạn chế xuống $\mathbb{N}_0^2$ cho ta một song ánh từ $\mathbb{N}_0^2$ tới $\mathbb{N}_0$. Cantor đã xây dựng tường minh hai đa thức xếp bậc hai như vậy. Đó là

$$C_1(x,y) = \frac{(x+y)^2}{2} + \frac{(x+3y)}{2}, \text{ và}$$
$$C_2(x,y) = \frac{(x+y)^2}{2} + \frac{(3x+y)}{2}$$

Sau đó Fueter cùng với Pólya dùng phương pháp lý thuyết số giải tích đã chứng minh rằng nếu F là một đa thức xếp bậc hai trên $\mathbb{N}_0^2$ thì $F = C_1$ hoặc $F = C_2$. Mục đích của luận văn này là tìm hiểu chứng minh của Vsemirnov chỉ dùng luật thuật nghịch bậc hai và định lý Dirichlet về số nguyên tố trong cấp số cộng (và một số lập tương đối sơ cấp) cho định lý này của Fueter và Pólya. Người ta cũng giả thuyết rằng nếu F là một đa thức xếp (bậc tùy ý) thì $F = C_1$ hoặc $F = C_2$. Giả thuyết này đến nay vẫn còn mở.

Luận văn có cấu trúc như sau: gồm phần Mở đầu, tiếp theo là ba Chương nội dung, phần Kết luận và Tài liệu tham khảo.

Chương 1: *Một số kiến thức liên quan*

Chương này phát biểu luật thuận nghịch bậc hai, định lý thặng dư Trung hoa, kèm theo một số hệ quả của chúng.

Chương 2: *Chứng minh sơ cấp của định lý Fueter-Pólya*

Chương này giới thiệu đa thức xếp Cantor và chứng minh đa thức xếp đó không thể là tuyến tính, trình bày một số kết quả, bổ đề trong lý thuyết số và trình bày chứng minh của định lý Fueter-Pólya.

Chương 3: *Đa thức Cantor trên hình quạt*

Chương này trình bày khái niệm hình quạt và vị nhóm, kết quả của Nathanson về đa thức bậc hai xếp Cantor trên một số vị nhóm.

Luận văn này được thực hiện và hoàn thành vào tháng 5 năm 2018 tại trường Đại học Khoa học- Đại học Thái Nguyên. Qua đây, tác giả xin bày tỏ lòng biết ơn sâu sắc tới TS. Nguyễn Duy Tân, người đã tận tình hướng dẫn trong suốt quá trình làm việc để hoàn thành luận văn này. Tác giả xin gửi lời cảm ơn chân thành đến Khoa Toán-Tin học, Trường Đại học Khoa học - Đại học Thái Nguyên, đã tạo mọi điều kiện để giúp tác giả học tập và hoàn thành luận văn cũng như chương trình thạc sĩ. Tác giả cũng xin gửi lời cảm ơn tới tập thể lớp cao học K10C, khóa 05/2016 - 05/2018 đã động viên giúp đỡ tác giả trong quá trình học tập và hoàn thành luận văn này. Đồng thời tác giả xin gửi lời cảm ơn tới Ban giám hiệu và các đồng nghiệp tại trường THPT Hàn thuyên, Bắc ninh đã tạo điều kiện cho tác giả trong suốt quá trình học tập và hoàn thành luận văn.

Thái Nguyên, tháng 5 năm 2018

Người viết luận văn

Nguyễn Quang Tuấn

Chương 1

Một số kiến thức liên quan

Chương này phát biểu luật thuận nghịch bậc hai, định lý thặng dư Trung hoa và một số ví dụ. Tài liệu tham khảo sử dụng cho chương này là tài liệu [1] và [4].

1.1 Luật thuận nghịch bậc hai

1.1.1 Thặng dư bậc hai

Định nghĩa 1.1.1. Cho p là một số nguyên tố và a là một số nguyên sao cho $p \nmid a$. Số a được gọi là một thặng dư bậc hai modulo p nếu tồn tại một số nguyên y sao cho $y^2 \equiv a(\mathrm{mod}\, p)$. Nếu không tồn tại một số nguyên y nào sao cho $y^2 \equiv a(\mathrm{mod} p)$ thì ta nói a là không thặng dư bậc hai modulo p.

Ví dụ. Các số $1, 3, 4$ là các thặng dư bậc hai modulo 13, trong khi đó 2 là không thặng dư bậc hai modulo 5 vì phương trình $y^2 \equiv 2(\mathrm{mod} 5)$ vô nghiệm.

1.1.2 Tiêu chuẩn Euler

Định lý 1.1.2 (Tiêu chuẩn Euler)**.** *Cho p là một số nguyên tố lẻ không là ước của số nguyên a. Khi đó a là một thặng dư bậc hai (tương ứng, không thặng dư bậc hai) modulo p nếu và chỉ nếu $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod} p)$ (tương ứng, $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod} p)$).*

Ví dụ. Ta có $3^5 = 243 \equiv 1 \pmod{11}$ và 5 là thặng dư bậc hai modulo 11. Trong khi đó $2^5 = 32 \equiv -1 \pmod{11}$ và 2 là không thặng dư bậc hai modulo 11.

1.1.3 Ký hiệu Legendre

Định nghĩa 1.1.3. Cho p là một số nguyên tố lẻ không chia hết số nguyên a.

Ta định nghĩa: $\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ } \textit{nếu } a \textit{ là thặng dư bậc hai modulo } p \\ -1 \text{ } \textit{nếu } a \textit{ không là bình phương modulo } p \end{cases}$

Ký hiệu này được gọi là ký hiệu Legendre (Adrien Legendre (1752 - 1833) là nhà toán học người Pháp).

Một số tính chất

Cho p là số nguyên tố lẻ không chia hết các số nguyên a và b. Khi đó ta có các tính chất sau.

1. $\left(\frac{a^2}{p}\right) = 1$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$ (Tiêu chuẩn Euler).
4. Nếu $a \equiv b (\mathrm{mod} p)$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
5. $\left(\frac{-1}{p}\right)$ bằng 1 hoặc -1 tùy theo $p \equiv 1 (\mathrm{mod} 4)$ hay $p \equiv 3 (\mathrm{mod} 4)$.
6. Khi đó $\left(\frac{2}{p}\right) = 1$ và nếu $p \equiv 1 (\mathrm{mod} 8)$ hoặc $p \equiv 7 (\mathrm{mod} 8)$; và $\left(\frac{2}{p}\right) = -1$ nếu $p \equiv 3 (\mathrm{mod} 8)$ hoặc $p \equiv 5 (\mathrm{mod} 8)$.

Ví dụ. Tính ký hiệu Legendre $\left(\frac{65}{47}\right)$.

Ta có $\left(\frac{65}{47}\right) = \left(\frac{18}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{9}{47}\right) = \left(\frac{2}{47}\right) = 1$.

Định lý 1.1.4 (Luật thuận nghịch bậc hai Gauss)**.** *Giả sử p và q là các số nguyên tố lẻ phân biệt. Khi đó* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ *trừ khi* $p \equiv q \equiv 3 (\mathrm{mod} 4)$ *thì* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Ví dụ. Tính ký hiệu Legendre $\left(\frac{12345}{331}\right)$.

Lời giải

$$\begin{aligned}
\left(\frac{12345}{331}\right) &= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{823}{331}\right) \\
&= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{161}{331}\right) \\
&= \left(\frac{3}{331}\right)\left(\frac{5}{331}\right)\left(\frac{7}{331}\right)\left(\frac{23}{331}\right) \\
&= (-1)\left(\frac{331}{3}\right)\left(\frac{331}{5}\right)(-1)\left(\frac{331}{7}\right)(-1)\left(\frac{331}{23}\right) \\
&= -\left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{2}{7}\right)\left(\frac{9}{23}\right) \\
&= -\left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{2}{7}\right)\left(\frac{3}{23}\right)^2 \\
&= -\left(\frac{1}{3}\right)\left(\frac{1}{5}\right)\left(\frac{2}{7}\right)\left(\frac{9}{23}\right) \\
&= -(1)(1)(1)(1) \\
&= -1
\end{aligned}$$

1.2 Định lý thặng dư Trung hoa

Định lý Thặng dư Trung Hoa là tên người phương Tây đặt cho định lý này. Người Trung Quốc gọi nó là Bài toán Hàn Tín điểm binh. Tục truyền rằng khi Hàn Tín điểm quân số, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo cáo số dư. Từ đó ông tính được chính xác quân số đến từng người. Trong mục này, chúng tôi sẽ trình bày nội dung của định lý Thặng dư Trung Hoa và một số ví dụ.

Định lý 1.2.1. *Giả sử rằng $m_1, m_2, \ldots, m_t$ là các số nguyên dương và đôi một nguyên tố cùng nhau. Đặt $m = m_1 \cdots m_t$. Cho $a_1, \ldots, a_t \in \mathbb{Z}$ là các số nguyên tùy ý. Khi đó ta có các khẳng định sau.*

1) Tồn tại $c \in \mathbb{Z}$ thỏa mãn

$$\begin{cases} c \equiv a_1 (\mathrm{mod} m_1), \\ c \equiv a_2 (\mathrm{mod} m_2), \\ ... \\ c \equiv a_t (\mathrm{mod} m_t). \end{cases}$$

2) Nếu c là một nghiệm của hệ đồng dư ở trên thì nghiệm tổng quát của hệ này là $x = c + ms, s \in \mathbb{Z}$.

Chứng minh.
1) Với $i = 1, 2, \ldots, t$ đặt $n_i = \dfrac{m}{m_i}$. Vì vậy $m = m_i n_i$. Chú ý rằng $(m_i, n_i) = 1, \forall i = 1, 2, \ldots, t$ do các số $m_1, m_2, \ldots, m_t$ đôi một nguyên tố cùng nhau. Bởi vậy, với mỗi i, phương trình đồng dư

$$n_i x \equiv 1 (\mathrm{mod} m_i)$$

là giải được; tức là, với mỗi i đều tồn tại một số nguyên b_i thỏa mãn

$$n_i b_i \equiv 1 (\mathrm{mod} m_i). \tag{1.1}$$

Mặt khác nếu j khác i thì

$$n_j b_j \equiv 0 (\mathrm{mod} m_j) \text{ do } m_i | n_j. \tag{1.2}$$

Bây giờ, đặt

$$c := a_1 n_1 b_1 + \cdots + a_t n_t b_t.$$

Khi đó với mọi i, ta có

$$c \equiv a_i n_i b_i \equiv a_i \pmod{m_i}.$$

Ta đã chứng minh xong khẳng định thứ nhất.
2) Giả sử d là một nghiệm khác của hệ đồng dư trên. Khi đó

$$c \equiv d (\mathrm{mod} m_i) \text{ với mọi } i$$

Suy ra $c \equiv d(\mathrm{mod} m)$. Vì vậy $d = c + ms$ với s nào đó.
Ngược lại, nếu $d = c + ms$ với s nào đó thì $d \equiv c(\mathrm{mod} m)$, và vì vậy với mỗi i, $d \equiv c \equiv a_i(\mathrm{mod} m)$. Điều này có nghĩa là d cũng là một nghiệm. □

Ví dụ 1. Giải hệ đồng dư

$$\begin{cases} x \equiv 2(\mathrm{mod}3) \\ x \equiv 3(\mathrm{mod}5) \\ x \equiv 5(\mathrm{mod}7) \end{cases}$$

Lời giải. Ở ví dụ này và ví dụ tiếp theo ta dùng ký hiệu N_i^{-1} để chỉ một nghiệm b_i như trong chứng minh định lý thặng dư Trung Hoa. Ta có

$$N_1 = 5.7 = 35 \equiv 2(\mathrm{mod}3) \Rightarrow N_1^{-1} = 2,$$
$$N_2 = 3.7 = 21 \equiv 1(\mathrm{mod}5) \Rightarrow N_2^{-1} = 1,$$
$$N_3 = 3.5 = 15 \equiv 1(\mathrm{mod}7) \Rightarrow N_3^{-1} = 1.$$

Từ đó ta có nghiệm của hệ trên là

$$x = 2.35.2 + 1.21.3 + 1.15.5 = 278 \equiv 68(\mathrm{mod}105).$$

Ví dụ 2. Giải hệ đồng dư

$$\begin{cases} x \equiv 3(\mathrm{mod}5) \\ x \equiv 7(\mathrm{mod}8) \\ x \equiv 5(\mathrm{mod}7) \end{cases}$$

Lời giải. Ta có

$$N_1 = 8.7 = 56 \equiv 1(\mathrm{mod}5) \Rightarrow N_1^{-1} = 1,$$
$$N_2 = 5.7 = 35 \equiv 3(\mathrm{mod}8) \Rightarrow N_2^{-1} = 3,$$
$$N_3 = 5.8 = 40 \equiv 5(\mathrm{mod}7) \Rightarrow N_3^{-1} = 3.$$