ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

TRẦN HOÀNG ĐẠO

MỘT SỐ TÍNH CHẤT SỐ HỌC CỦA ĐỊNH THỨC WENDT

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

TRẦN HOÀNG ĐẠO

MỘT SỐ TÍNH CHẤT SỐ HỌC CỦA ĐỊNH THỨC WENDT

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 mở đầu

Tính chất số học, mà cụ thể là tính chất chia hết và đồng dư số học luôn là chủ đề cổ điển nhưng luôn ẩn chứa nhiều kết quả đẹp đẽ rất sâu sắc và nhiều thú vị, thu hút các nhà toán học trong quá trình nghiên cứu. Tính chất số học của định thức chu trình của hệ số nhị thức mang tên nhà toán học E. Wendt là một trong số đó. Trong bài báo "On a resultant connected with Fermat's last theorem" của nhà toán học Emma Lehmer, bà đánh giá dường như E. Wendt là người đầu tiên giới thiệu định thức trong mối quan hệ với định lý Fermat lớn.

Năm 1894 Wendt đã chỉ ra rằng có một tiêu chuẩn dạng định thức cho sự tồn tại của một nghiệm không tầm thường của đồng dư thức Fermat $x^p + y^p = z^p \pmod q$, trong đó p, q là các số nguyên tố lẻ khác nhau mà $p \mid q - 1$. Kết quả nghiên cứu của E. Wendt đã tạo tiền đề và cảm hứng cho các nhà toán học khác trong việc mở rộng hơn các tính chất số học của định thức Wendt W_n. Nhiều kết quả được Wendt nêu lên nhưng chưa được giải quyết thì đã được các nhà toán học khác giải quyết triệt để, cùng với đó thì rất nhiều tính chất số học rất thú vị liên quan đến định thức Wendt cũng đã được các nhà toán học khác phát hiện thêm. Tiêu biểu như công trình của các nhà toán học Matthews (1895), E. Lehmer (1935), Bang (1935), Frame (1980).... Chẳng hạn

E. Lehmer đã chứng minh rằng $W_n = 0$ khi và chỉ khi $n \equiv 0 (\mathrm{mod} 6)$, nếu p là số nguyên tố lẻ thì W_{p-1} là số chia hết cho $p^{p-2}q_p(2)$, trong đó $q_p(2) = \dfrac{2^{p-1}-1}{p}$ là thương Fermat.

Mục đích của luận văn là tìm hiểu định thức Wendt, một số tính chất số học cơ bản của nó và mối liên hệ của định thức Wendt với định lý Fermat lớn.

Luận văn có cấu trúc như sau: Mở đầu, ba chương, Kết luận và Tài liệu tham khảo.

Chương 1: *Một số kiến thức chuẩn bị*
Chương này phát biểu các khái niệm về định thức của ma trận chu trình, kết thức, cùng với đó là một số kết quả liên quan tới kiến thức trong chương.

Chương 2: *Một số tính chất cơ bản của định thức Wendt*
Chương này được trình bày định thức Wendt và định lý Fermat lớn, mối quan hệ giữa chúng và một số tính chất cơ bản của định thức Wendt.

Chương 3: *Một số tính chất số học của định thức Wendt*
Chương này trình bày một số tính chất chia hết và tính chất đồng dư của định thức Wendt.

Luận văn này được thực hiện và hoàn thành vào tháng 5 năm 2018 tại trường Đại học Khoa học - Đại học Thái Nguyên. Để hoàn thành khóa luận tốt nghiệp này, tôi xin bày tỏ lòng biết ơn sâu sắc tới Tiến sĩ Nguyễn Duy Tân, người thầy đã tận tình hướng dẫn tôi trong suốt quá trình làm việc để hoàn thành luận văn này. Tác giả xin gửi lời cảm ơn chân thành đến Khoa Toán, Trường Đại học Khoa học - Đại học Thái Nguyên nói chung, cùng các thầy cô giảng dạy lớp Cao học 10C nói riêng, 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 10C đã đồng hành cùng tác giả trong suốt 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 Gia Bình số 1 đã tạo điều kiện cho tác giả trong suốt quá trình học tập và hoàn thành luận văn.

Thái Nguyên, tháng 05 năm 2018

Tác giả

Trần Hoàng Đạo

Chương 1

Một số kiến thức chuẩn bị

Trong chương này chúng ta sẽ giới thiệu khái niệm và một số kiến thức về định thức của ma trận chu trình, kết thức của hai đa thức để hỗ trợ cho các chương tiếp theo.

1.1 Định thức của ma trận chu trình

Định nghĩa 1.1.1. Cho $a_0, a_1, \ldots, a_{n-1}$ là n số phức. Định thức chu trình $Circ(a_0, a_1, \ldots, a_{n-1})$ là định thức $n \times n$ có hàng được lấy từ hàng thứ nhất $(a_0, a_1, \ldots, a_{n-1})$ bởi sự hoán vị vòng tròn liên tiếp, tức là

$$Circ(a_0, \ldots, a_{n-1}) = \begin{vmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{vmatrix}.$$

Bổ đề 1.1.2. *Ta có*

$$Circ(a_0, a_1, ..., a_{n-1}) = \prod_{j=0}^{n-1} P(\xi_n^j),$$

ở đây $P(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, *và* $\xi_n = e^{2\pi i/n}$.

Chứng minh. Đặt

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_0. \end{pmatrix}$$

Để đơn giản ta ký hiệu $\epsilon_j = \xi_n^j,\ j = 1, \dots, n$. Khi đó $\epsilon_j,\ j = 1, \dots, n$ là n căn bậc n của đơn vị, $\epsilon_j^n = 1$. Xét ma trận

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \epsilon_1 & \epsilon_2 & \cdots & \epsilon_n \\ \epsilon_1^2 & \epsilon_2^2 & \cdots & \epsilon_n^2 \\ . & . & \cdots & . \\ \epsilon_1^{n-1} & \epsilon_2^{n-1} & \cdots & \epsilon_n^{n-1} \end{pmatrix}.$$

Nhân A với V ta được ma trận $AV = B = [b_{ij}]$ cỡ $n \times n$. Ta có hệ số b_{ij} bằng

$$\begin{aligned} b_{ij} &= a_{n-i+1} + a_{n-i+2}\epsilon_j + \cdots + a_{n-1}\epsilon_j^{i-2} + a_0\epsilon_j^{i-1} + \cdots + a_{n-i}\epsilon_j^{n-1} \\ &= \epsilon_j^{i-1}(a_0 + a_1\epsilon_j + \cdots + a_{n-1}\epsilon_j^{n-1}) \\ &= \epsilon_j^{i-1}P(\epsilon_j). \end{aligned}$$

Do vậy ta có

$$AV = V \begin{pmatrix} P(\epsilon_1) & 0 & \cdots & 0 \\ 0 & P(\epsilon_2) & \cdots & 0 \\ . & . & \cdots & . \\ 0 & 0 & \cdots & P(\epsilon_n) \end{pmatrix}.$$

Lấy định thức hai vế của đẳng thức trên ta suy ra

$$|A||V| = |B| = P(\epsilon_1)\cdots P(\epsilon_n)|V|.$$

Vì $|V| = \prod_{1\le i<j\le n}(\epsilon_j - \epsilon_i) \neq 0$ (đây là định thức Vandermonde), nên $|A| = P(\epsilon_1)\cdots P(\epsilon_n) = \prod_{j=0}^{n-1} P(\epsilon_n^j)$. □

1.2 Kết thức của hai đa thức

Định nghĩa 1.2.1. Cho $f = \sum_{i=0}^{m} a_i x^i = a_m x^m + \cdots + a_0$ và $g = \sum_{i=0}^{n} b_j x^j = b_n x^n + \cdots + b_0$ là hai đa thức bậc m, n tương ứng, tức là $a_m b_n \neq 0$, với hệ số trong tập số phức $\mathbb{C}$. Kết thức của f và g là $(m+n)\times(m+n)$ định thức $R(f,g)$ cho bởi

$$\begin{pmatrix} a_m & a_{m-1} & a_{m-2} & \cdots & 0 & 0 & 0 \\ 0 & a_m & a_{m-1} & \cdots & 0 & 0 & 0 \\ . & . & . & \cdots & . & . & . \\ 0 & 0 & 0 & \cdots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \cdots & a_2 & a_1 & a_0 \\ b_n & b_{n-1} & b_{n-2} & \cdots & 0 & 0 & 0 \\ 0 & b_n & b_{n-1} & \cdots & 0 & 0 & 0 \\ . & . & . & \cdots & . & . & . \\ 0 & 0 & 0 & \cdots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \cdots & b_2 & b_1 & b_0 \end{pmatrix}.$$

Nói cách khác $R(f,g) = \det(c_{i,j})$ trong đó:

$$c_{i,j} = \begin{cases} a_{i+m-j}\ , & khi\ \ 1 \le i \le n \\ b_{i-j}\ \ , & khi\ \ n+1 \le i \le n+m \end{cases}$$

ở đây $1 \le j \le m+n$, với $a_k = 0$ nếu $k \notin [0,m]$ và $b_k = 0$ nếu $k \notin [0,n]$.

Ví dụ 1.1. (a) Giả sử $m = n = 1$. Khi đó

$$R(f, g) = \begin{vmatrix} a_1 & a_0 \\ b_1 & b_0 \end{vmatrix} = a_1 b_0 - a_0 b_1.$$

(b) Giả sử $m = 2$, $n = 1$. Khi đó

$$R(f, g) = \begin{vmatrix} a_2 & a_1 & a_0 \\ b_1 & b_0 & 0 \\ 0 & b_1 & b_0 \end{vmatrix} = a_2 b_0^2 - a_1 b_1 b_0 + a_0 b_1^2.$$

(c) Giả sử $m = 2, n = 2$. Khi đó

$$R(f, g) = \begin{vmatrix} a_2 & a_1 & a_0 & 0 \\ 0 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 \\ 0 & b_2 & b_1 & b_0 \end{vmatrix} = (a_2 b_0 - a_0 b_2)^2 - (a_2 b_1 - a_1 b_2)(a_1 b_0 - a_0 b_1).$$

Ta liệt kê một số tính chất cơ bản của kết thức ở dưới đây.

Định lý 1.2.2. *Cho $f = \sum_{i=0}^{m} a_i X^i$ và $g = \sum_{j=0}^{n} b_j X^j$ là hai đa thức với hệ số phức, với bậc m và n tương ứng. Khi đó ta có các khẳng định sau.*

(1) Kết thức $R(f, g)$ là một đa thức thuần nhất với hệ số nguyên theo các hệ số $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n$. Nó là đa thức thuần nhất bậc n theo các a_i và là đa thức thuần nhất bậc m theo các b_j.

(2) Gọi $\alpha_1, \alpha_2, \ldots, \alpha_m$ là các nghiệm phức của f, và $\beta_1, \beta_2, \ldots, \beta_n$ là các nghiệm phức của g. Khi đó

$$R(f, g) = a_m^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\beta_j) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$