ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN NGỌC ÁNH

DÃY HỒI QUY BẬC HAI

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - 2016

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN NGỌC ÁNH

DÃY HỒI QUY BẬC HAI

LUẬN VĂN THẠC SĨ TOÁN HỌC

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

Mã số: **60 46 01 13**

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. NGUYỄN DUY TÂN

Thái Nguyên - 2016

Mục lục

Lời mở đầu

Dãy Lucas thực là dãy được định nghĩa theo công thức truy hồi như sau

$$u_0 = 0, u_1 = 1, \ldots, u_{n+2} = a_1 u_{n+1} + a_2 u_n,$$

ở đây $a_1 a_2 \neq 0$; a_1 và a_2 là các số nguyên nguyên tố cùng nhau thỏa mãn $a_1^2 - 4a_2 > 0$. Một cách tương đương, ta có thể định nghĩa $u_n = \dfrac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}$, $\forall n \geq 0$, với α_1, α_2 là nghiệm thực phân biệt của đa thức đặc trưng $f(X) = X^2 - a_1 X - a_2$. Một ví dụ quan trọng về dãy Lucas thực là dãy Fibonacci $(F_n)_{n\geq 0}$:

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n, \ \forall n \geq 0.$$

Cho (u_n) là một dãy Lucas thực như trên. Dễ thấy u_n là nguyên với mọi n. Một câu hỏi cơ bản là chúng ta có thể nói gì về các ước nguyên tố của các số hạng u_n.

Định nghĩa. Một số nguyên tố p được gọi là ước nguyên thủy của số hạng u_n nếu p chia hết u_n nhưng p không chia hết u_m với mọi $0 < m < n$.

Một định lý quan trọng của Carmichael [1] nói rằng, trừ một vài trường hợp riêng, mọi số hạng trong dãy Lucas đều có ước nguyên thủy.

Định lý Carmichael. Cho $(u_n)_{n\geq 0}$ là một dãy Lucas thực và $n \neq 1, 2, 6$. Khi đó u_n có một ước nguyên thủy trừ trường hợp $u_n = F_{12}$, số hạng thứ 12 trong dãy Fibonacci.

Mục đích chính của luận văn này là trình bày về Định lý Carmichael về sự tồn tại ước nguyên thủy trong dãy Lucas thực.

Cụ thể, luận văn được chia làm ba chương. Chương 1 trình bày các kiến thức chuẩn bị về đa thức chia đường tròn và số nguyên đại số. Chương 2

trình bày về dãy hồi quy bậc hai, ví dụ về dãy hồi quy bậc hai và dãy Lucas. Trong chương này cũng trình bày về ước số nguyên tố của số hạng trong dãy Lucas. Chương 3 trình bày phát biểu và chứng minh Định lý Carmichael về sự tồn tại ước nguyên thủy trong dãy Lucas thực, Định lý Zsigmondy liên quan. Ở cuối chương này chúng tôi cũng đưa ra một số bài tập ứng dụng trong toán sơ cấp.

Sau một thời gian nỗ lực nghiên cứu tôi đã hoàn thành luận văn tốt nghiệp của mình. Trong suốt quá trình học tập và nghiên cứu, tôi đã nhận được sự quan tâm, khích lệ của tất cả các thầy cô, bạn bè, đồng nghiệp và gia đình.

Trước tiên, tôi xin gửi lời cảm ơn chân thành và sâu sắc nhất đến thầy tôi- TS. Nguyễn Duy Tân. Thầy đã hết sức tận tình dìu dắt tôi từ những bước đi đầu tiên khi bắt đầu thực hiện luận văn.

Tôi cũng xin gửi lời cảm ơn chân thành tới các thầy cô ở trường Đại học Khoa học-Đại học Thái Nguyên đã luôn tận tình giúp đỡ, theo sát tôi trong suốt quá trình học tập và thực hiện luận văn này.

Tôi xin gửi lời cảm ơn tới các đồng nghiệp trong tổ Toán-Tin trường THPT Lý Thường Kiệt-tỉnh Yên Bái luôn tạo điều kiện tốt nhất giúp tôi hoàn thành khóa học.

Cuối cùng, tôi xin gửi lời cảm ơn tới các bạn bè, gia đình đã luôn ở bên hỗ trợ, cổ vũ và động viên tôi trong suốt quá trình học tập và nghiên cứu.

Tác giả

Nguyễn Ngọc Ánh

Chương 1

Kiến thức chuẩn bị

Trong chương này chúng tôi trình bày một số kiến thức chuẩn bị về đa thức chia đường tròn, công thức nghịch đảo Möbius và sơ lược về số nguyên đại số. Tài liệu thàm khảo chính được sử dụng là [2].

1.1 Đa thức chia đường tròn

1.1.1 Căn đơn vị

Định nghĩa 1.1.1. Cho n là một số nguyên dương. Một số phức ζ được gọi là căn bậc n của đơn vị nếu $\zeta^n = 1$. Ta biết rằng có n căn bậc n của đơn vị, là những số $e^{2\pi i/n}, e^{\frac{2\pi i}{n}2}, ..., e^{\frac{2\pi i}{n}n}$.

Định nghĩa 1.1.2. Cho n là số nguyên dương và ζ là một căn bậc n của đơn vị. Khi đó số nguyên dương nhỏ nhất k thỏa mãn $\zeta^k = 1$ được gọi là bậc của ζ và được kí hiệu là ord(ζ).

Bổ đề 1.1.3. *Cho n là số nguyên dương và ζ là một căn bậc n của đơn vị. Khi đó với mọi số nguyên k, $\zeta^k = 1$ nếu và chỉ nếu* ord$(\zeta)|k$. *Nói riêng,* ord$(\zeta)|n$.

Chứng minh. Gọi $d = \text{ord}(\zeta)$. Nếu $d \mid k$, thì rõ ràng ζ^k=1. Mặt khác giả sử rằng ζ^k=1. Khi đó tồn tại hai số nguyên q, r với $0 \leq r \leq d-1$ sao cho $k = dq + r$. Ta có

$$1 = \zeta^k = \zeta^{qd+r} = \zeta^r.$$

Nhưng $0 \leq r < d$ và d là số nguyên dương nhỏ nhất thỏa mãn $\zeta^d = 1$, do vậy $r = 0$. □

Hệ quả 1.1.4. *Cho ζ là một căn của đơn vị. Khi đó với hai số nguyên k và l bất kỳ, $\zeta^k = \zeta^l$ nếu và chỉ nếu $k \equiv l \bmod \mathrm{ord}(\zeta)$. Nói riêng, nếu $1 \leq k,l \leq \mathrm{ord}(\zeta)$, thì $\zeta^k = \zeta^l$ nếu và chỉ nếu $k = l$.*

Chứng minh. Chú ý rằng $\zeta^k = \zeta^l$ nếu và chỉ nếu $\zeta^{k-l} = 1$. Hệ quả được suy ra từ Bổ đề 1.1.3. □

Định nghĩa 1.1.5. Cho n là số nguyên dương và ζ là một căn bậc n của đơn vị. Khi đó ζ được gọi là căn nguyên thủy bậc n của đơn vị nếu $\mathrm{ord}(\zeta) = n$.

Bổ đề 1.1.6. *Giả sử rằng ζ là căn nguyên thủy bậc n của đơn vị. Khi đó tập $\{\zeta, \zeta^2, \ldots, \zeta^n\}$ là tập tất cả các căn bậc n của đơn vị.*

Chứng minh. Với mọi số nguyên k, ζ^k là một căn bậc n của đơn vị vì $\zeta^{kn} = 1$. Theo định nghĩa về căn nguyên thủy bậc n của đơn vị, các số $\zeta^1, \ldots, \zeta^n$ là phân biệt. Nhưng vì chỉ tồn tại n căn bậc n của đơn vị, nên ta có điều phải chứng minh. □

Bổ đề 1.1.7. *Cho n,k là các số nguyên dương và ζ là căn nguyên thủy bậc n của đơn vị. Khi đó ζ^k là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu* $\gcd(k,n) = 1$.

Chứng minh. Gọi $d = \mathrm{ord}(\zeta^k)$. Ta có $(\zeta^k)^n = (\zeta^n)^k = 1$. Do đó $d \mid n$. Mặt khác ta có $\zeta^{kd} = 1$. Từ Bổ đề 1.1.3, suy ra $n \mid kd$.

Nếu $\gcd(k,n) = 1$, thì $n \mid d$. Kết hợp với $d \mid n$, ta suy ra $d = n$. Do đó ζ^k là nguyên thủy.

Nếu $\gcd(k,n) = r > 1$ thì $(\zeta^k)^{\frac{n}{r}} = (\zeta^n)^{\frac{k}{r}} = 1$. Suy ra $d \mid n/r$. Do vậy $d \leq n/r < r$ và ζ^k không nguyên thủy bậc n. □

Định nghĩa 1.1.8. Hàm Euler $\varphi : \mathbb{N} \to \mathbb{N}$ được định nghĩa như sau. Với mỗi $n \geq 1$, $\varphi(n)$ là số các số k, $1 \leq k \leq n$, mà k nguyên tố cùng nhau với n. Chẳng hạn, $\varphi(1) = 1$, $\varphi(2)$=1, $\varphi(3)$=2, $\varphi(4)$=2.

Ta có ngay hệ quả sau.

Hệ quả 1.1.9. *Cho n là số nguyên dương. Khi đó có đúng $\varphi(n)$ căn nguyên thủy bậc n của đơn vị.*

1.1.2 Đa thức chia đường tròn

Định nghĩa 1.1.10. Cho n là số nguyên dương. Thì đa thức chia đường tròn thứ n, ký hiệu Φ_n, là đa thức (hệ số đầu bằng 1) mà các nghiệm của nó chính là các căn nguyên thủy bậc n, tức là

$$\Phi_n(X) \equiv \prod_{\substack{\zeta^n=1 \\ \text{ord}(\zeta)=n}} (X-\zeta).$$

Vì có đúng $\varphi(n)$ căn nguyên thủy bậc n của đơn vị, nên bậc của Φ_n là $\varphi(n)$.

Định lý 1.1.11. *Nếu n là một số nguyên dương, thì*

$$X^n - 1 \equiv \prod_{d|n} \Phi_d(X).$$

Chứng minh. Các nghiệm của $X^n - 1$ chính là các căn bậc n của đơn vị. Mặt khác, nếu ζ là một căn bậc n của đơn vị và $d = \text{ord}(\zeta)$, thì ζ là một căn nguyên thủy bậc d của đơn vị và do đó là một nghiệm của $\Phi_d(X)$. Vì $d \mid n$, nên ζ là một nghiệm của vế phải. Do vậy ta thấy rằng hai đa thức bên vế trái và vế phải có cùng tập các nghiệm. Vì chúng là cùng monic (đa thức hệ số đầu bằng 1), nên chúng bằng nhau. □

Chú ý rằng, việc so sánh bậc của đa thức cho ta $n = \sum_{d|n} \varphi(n)$.

Ta cũng có công thức truy hồi tính Φ_n như sau

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(X)}.$$

Do vậy $\Phi_n(X)$ có hệ số hữu tỷ. Hơn nữa vì các đa thức $\Phi_d(X)$ đều là monic, nên ta có thể chứng minh được $\Phi_n(X) \in \mathbb{Z}[X]$. (Nếu dùng khái niệm số nguyên đại số ở mục sau, ta có thể chứng minh khẳng định này như sau. Rõ ràng ζ^k đều là các số nguyên đại số, do vậy các hệ số của $\Phi_n(X)$ cũng là các số nguyên đại số. Mặt khác, chúng là các số hữu tỷ, do vậy chúng phải

là các số nguyên.) Dưới đây là một số giá trị của $\Phi_n(X)$

$$\begin{aligned}
\Phi_1(X) &= X-1,\\
\Phi_2(X) &= X+1,\\
\Phi_3(X) &= X^2+X+1,\\
\Phi_4(X) &= X^2+1,\\
\Phi_5(X) &= X^4+X^3+X^2+X+1,\\
\Phi_6(X) &= X^2-X+1.
\end{aligned}$$

Dùng công thức nghịch đảo Möbius ta có thể đưa ra công thức trực tiếp tính Φ_n. Ta nhắc lại hàm Möbius và công thức nghịch đảo Möbius ở dưới đây.

Định nghĩa 1.1.12. Hàm Möbius $\mu : \mathbb{Z}^+ \to \{-1,0,1\}$ được định nghĩa như sau

$$\mu(n) = \begin{cases} 1 \text{ nếu } n = 1 \\ (-1)^k \text{ nếu } n \text{ là tích của } k \text{ số nguyên tố phân biệt} \\ 0 \text{ trong các trường hợp còn lại.} \end{cases}$$

Dễ thấy μ là nhân tính, tức là, $\mu(mn) = \mu(m)\mu(n)$ nếu m và n nguyên tố cùng nhau.

Định lý 1.1.13. *Nếu n là một số nguyên dương, thì*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & khi \quad n = 1 \\ 0 & khi \quad n \geq 2. \end{cases}$$

Chứng minh. Điều này hiển nhiên đúng với $n = 1$.

Giả sử $n \geq 2$. Gọi T là tích của tất cả các số nguyên chia hết n, tức là

$$T = \prod_{p \text{ nguyên tố}, p|n} p.$$

Với ước d của n mà không chia hết T thì d sẽ không là tích của các số nguyên tố phân biệt (nó sẽ chứa một nhân tử bình phương), và do vậy $\mu(d) = 0$. Do

đó, ta có

$$\sum_{d|n}\mu(d)=\sum_{d|T}\mu(d).$$

Lấy p là số nguyên tố bất kỳ chia hết T. Thì

$$\sum_{d|T}=\sum_{d|\frac{T}{p}}\mu(d)+\mu(pd)=\sum_{d|\frac{T}{p}}\mu(d)-\mu(d)=0. \qquad \square$$

Định lý 1.1.14 (Công thức nghịch đảo Möbius)**.** *Giả sử rằng F và $f\colon \mathbb{Z}^+\to\mathbb{R}$ là các hàm sao cho*

$$F(n)=\sum_{d|n}f(d).$$

Khi đó

$$f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d}).$$

Chứng minh. Ta có

$$\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(d)\sum_{t|\frac{n}{d}}f(t).$$

Mỗi ước t của n/d cũng là ước của n. Do vậy ta có

$$\sum_{d|n}\mu(d)\sum_{t|\frac{n}{d}}f(t)=\sum_{t|n}f(t)\sum_{\substack{d|n\\ t|\frac{n}{d}}}\mu(d)=\sum_{t|n}f(t)\sum_{d|\frac{n}{t}}\mu(d).$$

Từ Định lý 1.1.13 , ta có

$$\sum_{d|\frac{n}{t}}\mu(d)=\begin{cases}1 & \text{nếu } t=n\\ 0 & \text{trong các trường hợp còn lại.}\end{cases}$$

Do vậy

$$\sum_{t|n}f(t)\sum_{d|\frac{n}{t}}\mu(d)=f(n). \qquad \square$$

Ta cũng có phiên bản nhân tính của Định lý 1.1.14 như ở dưới đây.