ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THUỲ NINH

ĐA THỨC CHIA ĐƯỜNG TRÒN VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2013

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ THUỲ NINH

ĐA THỨC CHIA ĐƯỜNG TRÒN VÀ ỨNG DỤNG

Chuyên ngành: **PHƯƠNG PHÁP TOÁN SƠ CẤP**
Mã số: **60460113**

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS. LÊ THỊ THANH NHÀN

Thái Nguyên - Năm 2013

Mục lục

LỜI CẢM ƠN

Trước hết, tôi xin gửi lời biết ơn chân thành và sâu sắc tới PGS.TS Lê Thị Thanh Nhàn. Cô đã dành nhiều thời gian và tâm huyết trong việc hướng dẫn. Sau quá trình nhận đề tài và nghiên cứu dưới sự hướng dẫn khoa học của Cô, luận văn \Đa thức chia đường tròn" của tôi đã được hoàn thành. Có được kết quả này, đó là nhờ sự nhắc nhở, đôn đốc, dạy bảo hết sức tận tình và nghiêm khắc của Cô.

Tôi cũng xin gửi lời cảm ơn chân thành đến Ban Giám hiệu, Phòng Đào tạo-Khoa học-Quan hệ quốc tế và Khoa Toán-Tin của Trường Đại học Khoa học - Đại học Thái Nguyên đã tạo điều kiện thuận lợi nhất trong suốt quá trình học tập tại trường cũng như thời gian tôi hoàn thành đề tài này. Sự giúp đỡ nhiệt tình và thái độ thân thiện của các cán bộ thuộc Phòng Đào tạo và Khoa Toán-Tin đã để lại trong lòng mỗi chúng tôi những ấn tượng hết sức tốt đẹp.

Tôi xin cảm ơn Phòng Giáo dục và Đào tạo Quận Lê Chân - thành phố Hải Phòng và Trường trung học cơ sở Nguyễn Bá Ngọc - nơi tôi đang công tác đã tạo điều kiện cho tôi hoàn thành khóa học này.

Tôi xin cảm ơn gia đình, bạn bè đồng nghiệp và các thành viên trong lớp cao học Toán K5B (Khóa 2011-2013) đã quan tâm, tạo điều kiện, động viên cổ vũ để tôi có thể hoàn thành nhiệm vụ của mình.

LỜI NÓI ĐẦU

Ta biết rằng với mỗi số nguyên dương n, có đúng n căn bậc n của đơn vị: $\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$. Chú ý rằng ϵ_k là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu $\gcd(k, n) = 1$. Vì thế có đúng $\varphi(n)$ căn nguyên thủy bậc n của đơn vị, trong đó φ là hàm Euler. Gọi $\epsilon_{k_1}, \ldots, \epsilon_{k_{\varphi(n)}}$ là các căn nguyên thủy bậc n của đơn vị. Khi đó *đa thức chia đường tròn* thứ n, kí hiệu là $\Phi_n(x)$, là đa thức bậc $\varphi(n)$ được cho bởi công thức $\Phi_n(x) = (x - \epsilon_{k_1}) \ldots (x - \epsilon_{k_{\varphi(n)}})$. Mục đích của luận văn này là trình bày một số kết quả về đa thức chia đường tròn, những ứng dụng của đa thức chia đường tròn trong một số bài toán sơ cấp, và chứng minh tính bất khả quy của đa thức chia đường tròn.

Luận văn gồm 3 chương. Các kiến thức chuẩn bị về số phức và đa thức được nhắc lại trong Chương 1. Phần đầu của Chương 2 dành để trình bày một số tính chất quan trọng của đa thức chia đường tròn. Chúng tôi chứng tỏ rằng $x^n - 1 = \prod_{d|n} \Phi_d(x)$ (Định lí 2.3.3), và từ đó ta suy ra $\Phi_n(x)$ có các hệ số đều nguyên (Hệ quả 2.3.5). Hơn nữa, nếu $x \in \mathbb{Z}$ và p là một ước nguyên tố của $\Phi_n(x)$ thì $p \equiv 1 \pmod{n}$ hoặc $p|n$ (Định lí 2.3.11). Phần cuối Chương 2 trình bày một số ứng dụng của đa thức chia đường tròn để chứng minh lại một Định lý của Dirichlet và giải quyết một số bài toán thi học sinh giỏi toán quốc tế liên quan đến phương trình nghiệm nguyên và đánh giá số ước của một số tự nhiên. Chương 3 trình bày một số phương pháp chứng minh tính bất khả quy trên $\mathbb{Q}$ của đa thức chia đường tròn.

Chú ý rằng đa thức bất khả quy đóng vai trò quan trọng giống như vai trò của số nguyên tố trong tập các số nguyên. Với n là số nguyên dương, đa thức chia đường tròn $\Phi_n(x)$ là một đa thức bất khả quy đặc biệt, nó là

một ước của $x^n - 1$ nhưng không là ước của $x^k - 1$ với mọi $k < n$. Khi p là số nguyên tố, tính bất khả quy của $\Phi_p(x)$ đã được giải quyết vào đầu Thế kỷ thứ 19, được chứng minh lần đầu tiên bởi C. F. Gauss 1801 [Gau] với cách chứng minh khá phức tạp và dài dòng. Sau đó chứng minh được đơn giản hoá đi nhiều bởi các nhà toán học L. Kronecker 1845 [K] và F. G. Eisenstein 1850 [E]. Còn việc chứng minh tính bất khả quy của $\Phi_n(x)$ với n tuỳ ý được giải quyết vào khoảng giữa Thế kỷ 19, được chứng minh lần đầu tiên bởi Kronecker 1854 [K2]. Sau đó, R. Dedekind 1857 [D] và một số nhà toán học khác đã đưa ra chứng minh đơn giản hơn.

Nội dung của luận văn được viết dựa theo cuốn sách \Lý thuyết Galois" của S. H. Weintraub [W1], bài báo \Elementary Properties of Cyclotomic Polynomials" của Y. Ge [Ge] và bài báo \Several proofs of the irreducibility of the cyclotomic polynomial" của S. H. Weintraub [W2]. Bên cạnh đó có tham khảo một số bài báo cổ điển của C.F. Gauss [Gau], F. G. Eisenstein [E], L. Kronecker [K] và R. Dedekind [D] về tính bất khả quy của $\Phi_n(x)$.

Chương 1

Kiến thức chuẩn bị

Trước khi trình bày các kết quả về đa thức chia đường tròn ở Chương 2, chúng ta nhắc lại kiến thức cơ sở về số phức và đa thức.

1.1 Số phức và các phép toán trên số phức

1.1.1 Định nghĩa. Số phức là một biểu thức có dạng $z = a + bi$ trong đó $a, b \in \mathbb{R}$ và $i^2 = -1$. Ta gọi a là *phần thực* và b là *phần ảo* của z. Số phức i được gọi là *đơn vị ảo*. Nếu $a = 0$ thì $z = bi$ được gọi là số *thuần ảo*. Nếu $b = 0$ thì $z = a$ là số thực. Tập các số phức được kí hiệu là $\mathbb{C}$. Số phức $\overline{z} = a - bi$ được gọi là số phức *liên hợp* của $z = a + bi$.

1.1.2 Chú ý. (i) Hai số phức bằng nhau nếu và chỉ nếu phần thực và phần ảo tương ứng bằng nhau: $a + bi = c + di \Leftrightarrow a = c, b = d$.

(ii) Nếu $z = a + bi$ thì $z\,\overline{z} = a^2 + b^2$ là một số thực.

(iii) Liên hợp của tổng (hiệu, tích, thương) bằng tổng (hiệu, tích, thương) của các liên hợp: $\overline{z \pm z'} = \overline{z} \pm \overline{z'}$, $\overline{z\ z'} = \overline{z}\ \overline{z'}$ và $\overline{\dfrac{z}{z'}} = \dfrac{\overline{z}}{\overline{z'}}$ với mọi $z' \neq 0$.

Biểu diễn số phức $z = a + bi$ được gọi là biểu diễn đại số của z. Các

phép toán trên số phức được thực hiện như sau:

$$(a+bi) \pm (c+di) = (a+c) \pm (b+d)i;$$
$$(a+bi)(c+di) = (ac-bd) + (bc+ad)i;$$
$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Tập $\mathbb{C}$ các số phức với phép cộng và phép nhân là một trường chứa trường số thực $\mathbb{R}$, trong đó mỗi số thực a được đồng nhất với số phức $a+0i$.

1.1.3 Định nghĩa. Trong mặt phẳng P với hệ trục tọa độ vuông góc xOy, mỗi số phức $z = a+bi$ được đồng nhất với điểm $Z(a,b)$. Khi đó tập số phức lấp đầy P và ta gọi P là *mặt phẳng phức*. Xét góc α tạo bởi chiều dương trục hoành với véc tơ $\overrightarrow{OZ}$ và gọi r là độ dài của véc tơ $\overrightarrow{OZ}$, khi đó

$$z = a+bi = r(\cos\alpha + i\sin\alpha).$$

Biểu diễn $z = r(\cos\alpha + i\sin\alpha)$ được gọi là *biểu diễn lượng giác* của z. Ta gọi r là *môđun* của z và ký hiệu là $|z|$. Góc α được gọi là *argument* của z và kí hiệu là $\arg(z)$. Chú ý rằng môđun của một số phức là xác định duy nhất và argument của một số phức là xác định sai khác một bội nguyên lần của 2π, tức là $r(\cos\alpha + i\sin\alpha) = r'(\cos\alpha' + i\sin\alpha')$ nếu và chỉ nếu $r = r'$ và $\alpha = \alpha' + 2k\pi$ với $k \in \mathbb{Z}$.

Với mỗi số phức $z = a+bi$, rõ ràng $|z| = \sqrt{a^2+b^2} = |\overline{z}|$. Hơn nữa, với $z_1, z_2 \in \mathbb{C}$ ta có $|z_1|.|z_2| = |z_1|.|z_2|$ và $|z_1+z_2| \leqslant |z_1| + |z_2|$.

1.1.4 Chú ý. Cho $z = r(\cos\varphi + i\sin\varphi)$ và $z' = r'(\cos\varphi' + i\sin\varphi')$ là hai số phức. Khi đó $zz' = rr'\big(\cos(\varphi+\varphi') + i\sin(\varphi+\varphi')\big)$ và nếu $z' \neq 0$ thì $\frac{z}{z'} = \frac{r}{r'}\big(\cos(\varphi-\varphi') + i\sin(\varphi-\varphi')\big)$. Từ đây ta có thể nâng lên lũy thừa bằng công thức sau (gọi là công thức Moirve):

$$z^n = r^n(\cos n\varphi + i\sin n\varphi).$$

1.1.5 Định nghĩa. Số phức u là một *căn bậc* n của số phức z nếu $u^n = z$.

Chú ý rằng mỗi số phức $z = r(\cos\varphi + i\sin\varphi)$ khác 0 đều có đúng n căn bậc n, đó là

$$\omega_k = \sqrt[n]{r}(\cos\frac{\varphi + k2\pi}{n} + i\sin\frac{\varphi + k2\pi}{n}), k = 0, 1, \ldots, n-1.$$

Đặc biệt, có đúng n căn bậc n của đơn vị, đó là

$$\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1.$$

1.2 Khái niệm đa thức

Trong suốt tiết này, luôn giả thiết K là một trong các trường $\mathbb{C}, \mathbb{R}, \mathbb{Q}$.

1.2.1 Định nghĩa. Một biểu thức dạng $f(x) = a_n x^n + \ldots + a_0$ trong đó $a_i \in K$ với mọi i được gọi là một *đa thức* của ẩn x (hay biến x) với hệ số trong K. Nếu $a_n \neq 0$ thì a_n được gọi là *hệ số cao nhất* của $f(x)$ và số tự nhiên n được gọi là *bậc* của $f(x)$, kí hiệu là $\deg f(x)$. Nếu $a_n = 1$ thì $f(x)$ được gọi là *đa thức dạng chuẩn* (monic polynomial).

Chú ý rằng hai đa thức $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$ là bằng nhau nếu và chỉ nếu $a_i = b_i$ với mọi i. Ta chỉ định nghĩa bậc cho những đa thức khác 0, còn ta quy ước đa thức 0 là không có bậc. Kí hiệu $K[x]$ là tập các đa thức ẩn x với hệ số trong K. Với $f(x) = \sum a_i x^i$ và $g(x) = \sum b_i x^i$, định nghĩa $f(x) + g(x) = \sum(a_i + b_i)x^i$ và $f(x)g(x) = \sum c_k x^k$, trong đó $c_k = \sum_{i+j=k} a_i b_j$. Rõ ràng nếu $f(x) \neq 0$ và $f(x)g(x) = f(x)h(x)$ thì $g(x) = h(x)$. Hơn nữa ta có

$$\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$$
$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

1.2.2 Định nghĩa. Cho $f(x), g(x) \in K[x]$. Nếu $f(x) = q(x)g(x)$ với $q(x) \in K[x]$ thì ta nói rằng $g(x)$ là *ước* của $f(x)$ hay $f(x)$ là *bội* của $g(x)$ và ta viết $g(x)|f(x)$. Tập các bội của $g(x)$ được kí hiệu là (g).

Ta có ngay các tính chất đơn giản sau đây.

1.2.3 Bổ đề. *Các phát biểu sau là đúng.*
(i) Với $a \in K$ và k là số tự nhiên ta có $(x-a)|(x^k - a^k)$.
(ii) Nếu $f(x) \in K[x]$ và $a \in K$ thì tồn tại $q(x) \in K[x]$ sao cho

$$f(x) = q(x)(x-a) + f(a).$$

Định lí sau đây, gọi là Định lí chia với dư, đóng một vai trò rất quan trọng trong lí thuyết đa thức.

1.2.4 Định lý. *Cho $f(x), g(x) \in K[x]$, trong đó $g(x) \neq 0$. Khi đó tồn tại duy nhất một cặp đa thức $q(x), r(x) \in K[x]$ sao cho*

$$f(x) = g(x)q(x) + r(x), \text{ với } r(x) = 0 \text{ hoặc } \deg r(x) < \deg g(x).$$

Chứng minh. Trước hết ta chứng minh tính duy nhất. Giả sử

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

trong đó $r(x), r_1(x)$ bằng 0 hoặc có bậc nhỏ hơn bậc của $g(x)$. Khi đó

$$g(x)(q(x) - q_1(x)) = r_1(x) - r(x).$$

Nếu $r(x) \neq r_1(x)$ thì

$$\deg(r - r_1) = \deg\big(g(q - q_1)\big) = \deg g + \deg(q - q_1).$$

Điều này mâu thuẫn vì

$$\deg(r - r_1) \leqslant \max\{\deg r, \deg r_1\} < \deg g \leqslant \deg g + \deg(q - q_1).$$

Do vậy, $r_1(x) = r(x)$. Suy ra $g(x)(q(x) - q_1(x)) = 0$. Vì $g(x) \neq 0$ nên $q(x) - q_1(x) = 0$, tức là $q(x) = q_1(x)$.

Bây giờ ta chứng minh sự tồn tại. Nếu $\deg f(x) < \deg g(x)$ thì ta chọn $q(x) = 0$ và $r(x) = f(x)$. Giả sử $\deg f(x) \geq \deg g(x)$. Viết $f(x) = a_m x^m + \ldots + a_0$ và $g(x) = b_n x^n + \ldots + b_0$ với $a_m, b_n \neq 0$ và $n \leqslant m$. Chọn $h(x) = \dfrac{a_m}{b_n} x^{m-n}$. Đặt $f_1(x) = f(x) - g(x)h(x)$. Khi đó $f_1(x) = 0$ hoặc $f_1(x)$ có bậc thực sự bé hơn bậc của $f(x)$. Trong trường hợp $f_1(x) = 0$, ta tìm được dư của phép chia $f(x)$ cho $g(x)$ là $r(x) = 0$ và thương là $q(x) = h(x)$. Nếu $f_1(x) \neq 0$ thì ta tiếp tục làm tương tự với $f_1(x)$ và ta được đa thức $f_2(x)$. Cứ tiếp tục quá trình trên ta được dãy đa thức $f_1(x), f_2(x), \ldots$, nếu chúng đều khác 0 thì chúng có bậc giảm dần. Vì thế sau hữu hạn bước ta được một đa thức có bậc bé hơn bậc của $g(x)$ và đó chính là đa thức dư $r(x)$. Nếu một đa thức của dãy bằng 0 thì dư $r(x) = 0$. Thế vào rồi nhóm lại ta tìm được $q(x)$. □

Trong định lý trên, $q(x)$ được gọi là *thương* và $r(x)$ được gọi là *dư* của phép chia $f(x)$ cho $g(x)$. Nếu dư của phép chia $f(x)$ cho $g(x)$ là 0 thì tồn tại $q(x) \in K[x]$ sao cho $f(x) = g(x)q(x)$. Trong trường hợp này ta nói rằng $f(x)$ *chia hết cho* $g(x)$ hay $g(x)$ là *ước* của $f(x)$.

1.2.5 Định nghĩa. Với mỗi $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ và $\alpha \in \mathbb{C}$, đặt $f(\alpha) = a_n \alpha^n + \ldots + a_1 \alpha + a_0$. Nếu $f(\alpha) = 0$ thì ta nói α là một *nghiệm* của đa thức $f(x)$ hay là nghiệm của phương trình $f(x) = 0$.

1.2.6 Hệ quả. *Phần tử $a \in K$ là nghiệm của đa thức $f(x) \in K[x]$ nếu và chỉ nếu tồn tại đa thức $g(x) \in K[x]$ sao cho $f(x) = (x - a)g(x)$.*

Giả sử $a \in K$. Ta nói a là *nghiệm bội k* của $f(x)$ nếu $f(x)$ chia hết cho $(x - a)^k$ nhưng $f(x)$ không chia hết cho $(x - a)^{k+1}$. Nếu $k = 1$ thì a được gọi là *nghiệm đơn*. Nếu $k = 2$ thì a được gọi là *nghiệm kép*.

Từ Hệ quả trên ta có kết quả sau đây.

1.2.7 Hệ quả. *Cho* $a_1, a_2, \ldots, a_r \in K$ *là những nghiệm phân biệt của* $f(x) \in K[x]$. *Giả sử* a_i *là nghiệm bội* k_i *của* $f(x)$ *với* $i = 1, 2, \ldots, r$. *Khi đó* $f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_r)^{k_r}u(x)$, *trong đó* $u(x) \in K[x]$ *và* $u(a_i) \neq 0$ *với mọi* $i = 1, \ldots, r$.

1.2.8 Hệ quả. *Cho* $0 \neq f(x) \in K[x]$ *là đa thức. Khi đó số nghiệm của* $f(x)$, *mỗi nghiệm tính với số bội của nó, không vượt quá bậc của* $f(x)$.

Chứng minh. Giả sử $a_1, \ldots, a_r$ là các nghiệm của $f(x)$ với số bội lần lượt là $k_1, \ldots, k_r$. Theo Hệ quả 1.2.7, tồn tại $g(x) \in K[x]$ sao cho

$$f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\ldots(x-a_r)^{k_r}g(x).$$

Vì thế $\deg f(x) = \deg g(x) + \sum_{i=1}^{r} k_i \geq \sum_{i=1}^{r} k_i$, điều cần chứng minh. □

1.2.9 Hệ quả. *Cho* $f(x), g(x) \in K[x]$, *trong đó* $\deg f, \deg g \leqslant n$. *Nếu* $f(x)$ *và* $g(x)$ *có giá trị bằng nhau tại* $n+1$ *phần tử khác nhau của* K *thì* $f(x) = g(x)$.

Chứng minh. Đặt $h(x) = f(x) - g(x)$. Theo giả thiết, $h(x)$ có ít nhất $n+1$ nghiệm phân biệt. Nếu $h(x) \neq 0$ thì

$$\deg h(x) \leqslant \max\{\deg f(x), \deg g(x)\} \leqslant n.$$

Vì thế, theo Hệ quả 1.2.8, $h(x)$ có nhiều nhất n nghiệm. Điều này là vô lí. Vậy $h(x) = 0$ và do đó $f(x) = g(x)$. □

1.2.10 Định nghĩa. Một đa thức dạng chuẩn $d(x) \in K[x]$ được gọi là *ước chung lớn nhất* của $f(x), g(x) \in K[x]$ nếu $d(x)$ là một ước chung của $f(x)$ và $g(x)$, và nếu $h(x)$ là một ước chung của $f(x)$ và $g(x)$ thì $h(x)$ là ước của $d(x)$. Ta kí hiệu ước chung lớn nhất của $f(x)$ và $g(x)$ là $\gcd(f(x), g(x))$. Nếu $\gcd(f(x), g(x)) = 1$ thì ta nói $f(x)$ và $g(x)$ là *nguyên tố cùng nhau*.

Với $0 \neq d(x) \in K[x]$, kí hiệu $d^*(x) = d(x)/a_n$ trong đó a_n là hệ số cao nhất của $d(x)$. Chú ý rằng $d^*(x)$ là đa thức dạng chuẩn. Để tìm ước chung lớn nhất ta có thuật toán sau:

1.2.11 Mệnh đề. *(Thuật toán Euclid tìm ước chung lớn nhất). Giả sử $f, g \in K[x]$ và $g \neq 0$. Khi đó tồn tại một số tự nhiên k sao cho khi thực hiện liên tiếp các phép chia ta có*

$$\begin{cases} f = gq + r, \ r \neq 0, degr < \deg g \\ g = rq_1 + r_1, \ r_1 \neq 0, \deg r_1 < \deg r \\ r = r_1q_2 + r_2, \ r_2 \neq 0, \deg r_2 < \deg r_1 \\ \ldots\ldots \\ r_{k-2} = r_{k-1}q_k + r_k, \ r_k \neq 0, \deg r_k < \deg r_{k-1} \\ r_{k-1} = r_kq_{k+1}. \end{cases}$$

Trong trường hợp này, r_k^* là ước chung lớn nhất của f và g.

Chứng minh. Chia f cho g ta được dư r. Nếu $r \neq 0$ thì chia g cho r ta được dư r_1. Nếu $r_1 \neq 0$ thì chia r cho r_1 ta được dư r_2. Quá trình trên phải dừng sau một số hữu hạn bước vì dãy giảm các số tự nhiên $\deg g > \deg r > \deg r_1 > \ldots$ không thể kéo dài vô hạn. Xét từ đẳng thức cuối ngược trở lên ta suy ra r_k là một ước chung của f và g. Giả sử $t(x)$ là một ước chung của f và g. Xét từ đẳng thức trên cùng trở xuống ta suy ra $t(x)$ là ước của $r_k(x)$. Vì thế r_k^* là ước chung lớn nhất của f và g. □

1.2.12 Hệ quả. *Giả sử $f(x), g(x) \in K[x]$ và $d(x) = \gcd(f(x), g(x))$. Khi đó tồn tại $u(x), v(x) \in K[x]$ sao cho*

$$d(x) = f(x)u(x) + g(x)v(x).$$

Chứng minh. Trong các phép chia liên tiếp ở thuật toán Euclid tìm ước chung lớn nhất, $d(x) = r_k^*(x) = r_k(x)/a_n$, trong đó a_n là hệ số cao nhất

của $r_k(x)$. Đặt $u_1(x) = 1, v_1(x) = -q_k(x)$, từ đẳng thức giáp cuối ta có

$$d(x) = \frac{1}{a_n}\big(r_{k-2}(x)u_1(x) + r_{k-1}(x)v_1(x)\big).$$

Thay $r_{k-1}(x)$ từ đẳng thức trước giáp cuối ta được

$$r_{k-1}(x) = r_{k-3}(x) - r_{k-2}(x)q_{k-1}(x).$$

Vì thế ta có $d(x) = \frac{1}{a_n}\big(r_{k-3}(x)u_2(x) + r_{k-2}(x)v_2(x)\big)$, trong đó $u_2(x) = v_1(x)$ và $v_2(x) = u_1(x) - v_1(x)q_{k-1}(x)$. Cứ tiếp tục đi từ dưới lên đến đẳng thức đầu tiên ta có kết quả. □

1.2.13 Hệ quả. *Cho* $p(x), f(x), g(x) \in K[x]$. *Nếu* $\gcd(p(x), f(x)) = 1$ *và* $p(x)|f(x)g(x)$ *thì* $p(x)|g(x)$.

Chứng minh. Theo giả thiết, $1 = p(x)a(x) + f(x)b(x)$. Suy ra

$$g(x) = p(x)a(x)g(x) + f(x)b(x)g(x).$$

Do $p(x)$ là ước của đa thức ở vế phải nên $p(x)|g(x)$. □

Chương 2

Một số tính chất cơ sở của đa thức chia đường tròn

2.1 Công thức nghịch chuyển Mobius

2.1.1 Định nghĩa. *Hàm Mobius* $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ được định nghĩa như sau: Đặt $\mu(1) = 1$. Cho $n > 1$. Nếu d^2 không là ước của n với mọi số tự nhiên $d > 1$ thì ta đặt $\mu(n) = (-1)^k$, trong đó k là số các ước nguyên tố của n. Nếu có số tự nhiên $d > 1$ sao cho d^2 là ước của n thì ta đặt $\mu(n) = 0$.

Từ định nghĩa trên ta có $\mu(6) = (-1)^2 = 1$, $\mu(9) = 0$, $\mu(12) = 0$. Hiển nhiên μ là hàm nhân, tức là $\mu(mn) = \mu(m)\mu(n)$ với mọi số nguyên dương m, n nguyên tố cùng nhau. Sau đây là một số tính chất của hàm Mobius.

2.1.2 Mệnh đề. *Cho n là số nguyên dương. Khi đó*

a) Nếu $n = 1$ thì $\sum_{d|n} \mu(d) = 1$.

b) Nếu $n \geq 2$ thì $\sum_{d|n} \mu(d) = 0$.

Chứng minh. a) Với $n = 1$ thì ước dương duy nhất của n là 1. Do đó, theo định nghĩa hàm Mobius ta có $\sum_{d|n} \mu(d) = \mu(1) = 1$.

b) Cho $n \geq 2$. Ta đặt T là tích tất cả các số nguyên tố p là *ước* của n, tức là $T = \prod_{p|n} p$. Chú ý rằng nếu q là ước của n có chứa thừa số bình phương thì $\mu(q) = 0$. Do đó ta có thể bỏ những chỉ số q như thế ra khỏi tổng. Do đó ta có

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

Gọi p là một *ước* nguyên tố bất kỳ của T. Chú ý rằng mỗi ước của T là một ước d của T/p hoặc là pd với d là ước của T/p. Vì thế, từ tính chất hàm nhân của μ ta có

$$\begin{aligned}\sum_{d|T} \mu(d) = \sum_{d|\frac{T}{p}} (\mu(d) + \mu(pd)) &= \sum_{d|\frac{T}{p}} (\mu(d) + \mu(p)\mu(d)) \\ &= \sum_{d|\frac{T}{p}} (\mu(d) + (-1)^1 \mu(d)) \\ &= \sum_{d|\frac{T}{p}} (\mu(d) - \mu(d)) = 0.\end{aligned}$$

Ta có điều phải chứng minh. □

Một kết quả quen biết trong số học nói rằng nếu f là hàm nhân thì $F(n) = \sum_{d|n} f(d)$. Từ Mệnh đề 2.1.2, ta có một kết quả quan trọng của hàm Mobius, đó là công thức *nghịch chuyển hàm Mobius* sau đây.

2.1.3 Mệnh đề. *Kí hiệu $\mathbb{Z}^+$ là tập các số nguyên dương. Cho hai hàm $F, f : \mathbb{Z}^+ \to \mathbb{Z}^+$ sao cho $F(n) = \sum_{d|n} f(d)$. Khi đó ta có*

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

Chứng minh. Theo giả thiết ta có

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

Vì mọi ước t của n/d đều là ước của n nên ta có

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

Dễ thấy rằng với hai ước t và d của n ta có d là ước của n/t khi và chỉ khi t là ước của n/d. Do vậy ta có

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

Theo mệnh đề 2.1.2, nếu $n/t = 1$ tức là $t = n$ thì $\sum_{d|\frac{n}{t}} \mu(d) = 1$ và nếu $n/t \geq 2$ thì $\sum_{d|\frac{n}{t}} \mu(d) = 0$. Vì vậy ta có

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

mệnh đề được chứng minh. □

2.1.4 Mệnh đề. *Giả sử $F, f : \mathbb{Z}^+ \to \mathbb{Z}^+$ là hai hàm thỏa mãn điều kiện $F(n) = \prod_{d|n} f(d)$. Khi đó ta có $f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$.*

Chứng minh. Chứng minh của mệnh đề này tương tự như chứng minh của Mệnh đề 2.1.3, trong đó mỗi tổng được thay bằng tích và mỗi phép nhân liên quan đến hàm μ được thay bởi lũy thừa của hàm đó.

Giả sử t là ước của n/d. Theo giả thiết ta có $F(n/d) = \prod_{t|\frac{n}{d}} f(t)$. Suy ra

$$\prod_{d|n} F(n/d)^{\mu(d)} = \prod_{d|n} \left(\prod_{t|\frac{n}{d}} f(t) \right)^{\mu(d)}.$$

Vì mọi ước t của n/d đều là ước của n nên ta có

$$\prod_{d|n} F(n/d)^{\mu(d)} = \prod_{d|n} \left(\prod_{t|\frac{n}{d}} f(t) \right)^{\mu(d)} = \prod_{t|n} f(t)^{\sum_{d|n, t|\frac{n}{d}} \mu(d)}.$$

Chú ý rằng nếu d và t đều là ước của n thì d là ước của n/t khi và chỉ khi t là ước của n/d. Do vậy ta có

$$\prod_{d|n} F(n/d)^{\mu(d)} = \prod_{d|n} \left(\prod_{t|\frac{n}{d}} f(t) \right)^{\mu(d)} = \prod_{t|n} f(t)^{\sum_{d|n, t|\frac{n}{d}} \mu(d)} = \prod_{t|n} f(t)^{\sum_{d|\frac{n}{t}} \mu(d)}.$$

Vì thế theo Mệnh đề 2.1.2, nếu $n/t = 1$ tức là $t = n$ thì $\sum_{d|\frac{n}{t}} \mu(d) = 1$, và nếu $n/t \geq 2$ thì $\sum_{d|\frac{n}{t}} \mu(d) = 0$. Do đó

$$\begin{aligned} \prod_{d|n} F(n/d)^{\mu(d)} &= \prod_{d|n} \left(\prod_{t|\frac{n}{d}} f(t) \right)^{\mu(d)} \\ &= \prod_{t|n} f(t)^{\sum_{d|n, t|\frac{n}{d}} \mu(d)} \\ &= \prod_{t|n} f(t)^{\sum_{d|\frac{n}{t}} \mu(d)} = f(n), \end{aligned}$$

mệnh đề được chứng minh. □

2.2 Căn nguyên thủy bậc n của đơn vị

2.2.1 Định nghĩa. Cho n là một số nguyên dương và ϵ là một căn bậc n của đơn vị. Khi đó số nguyên dương nhỏ nhất k sao cho $\epsilon^k = 1$ được gọi là *cấp* của ϵ và được kí hiệu là $\mathrm{ord}(\epsilon)$.

2.2.2 Ví dụ. Các căn bậc 4 của đơn vị là $1, -1, i, -i$. Cấp của 1 là 1, cấp của -1 là 2, cấp của i là 4, cấp của $-i$ là 4.

2.2.3 Bổ đề. *Cho n là số nguyên dương và ϵ là căn bậc n của đơn vị. Khi đó $\epsilon^k = 1$ nếu và chỉ nếu $\mathrm{ord}(\epsilon)$ là ước của k, với mọi số nguyên k. Đặc biệt cấp của ϵ luôn là ước của n.*

Chứng minh. Đặt $d = \mathrm{ord}(\epsilon)$. Giả sử $\epsilon^k = 1$. Ta cần chứng minh d là ước của k. Theo định lí chia với dư ta có $k = dq + r$, trong đó $q, r \in \mathbb{Z}$ và $0 \leqslant r < d$. Suy ra

$$1 = \epsilon^k = \epsilon^{qd+r} = (\epsilon^d)^q.\epsilon^r = \epsilon^r.$$

Vì d là số nguyên dương bé nhất có tính chất $\epsilon^d = 1$ nên ta có $r = 0$. Do đó d là ước của k. Ngược lại, giả sử d là ước của k. Ta cần chứng minh $\epsilon^k = 1$. Viết $k = dq$, trong đó $q \in \mathbb{Z}$. Ta có $\epsilon^k = (\epsilon^d)^q = 1$. □

2.2.4 Hệ quả. *Cho n là số nguyên dương và ϵ là một căn bậc n của đơn vị. Giả sử $d = \mathrm{ord}(\epsilon)$. Khi đó $\epsilon^k = \epsilon^t$ nếu và chỉ nếu $k \equiv t (\mathrm{mod}\ d)$ với mọi số nguyên k, t.*

Chứng minh. Cho $\epsilon^k = \epsilon^t$. Cần chứng minh $k - t$ chia hết cho r. Ta có $\epsilon^{k-t} = 1$. Theo Bổ đề 2.2.3, $k - t$ là bội của d. Ngược lại, nếu $k - t$ là bội của d thì $\epsilon^{k-t} = 1$ và do đó $\epsilon^k = \epsilon^d$. □

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

2.2.6 Ví dụ. a) Các căn bậc 3 của đơn vị là

$$\epsilon_0 = 1, \epsilon_1 = -\frac{1}{2} + \frac{i\sqrt{3}}{2}, \epsilon_2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}.$$

Ta có $\mathrm{ord}(\epsilon_0) = 1, \mathrm{ord}(\epsilon_1) = 3, \mathrm{ord}(\epsilon_2) = 3$. Vì thế các căn nguyên thủy bậc 3 của đơn vị là ϵ_1 và ϵ_2.

b) Trong các căn bậc 4 của đơn vị: $1, -1, i, -i$, các số $i, -i$ là các căn nguyên thủy bậc 4 của đơn vị.

2.2.7 Chú ý. Nếu ϵ là một căn bậc n của đơn vị và $d = \mathrm{ord}(\epsilon)$ thì ϵ là căn nguyên thuỷ bậc d của đơn vị.

2.2.8 Bổ đề. *Cho ϵ là căn nguyên thuỷ bậc n của đơn vị. Khi đó tập các căn bậc n của đơn vị là $\{\epsilon, \epsilon^2, \epsilon^3, \ldots, \epsilon^n\}$.*

Chứng minh. Với mọi số dương k ta có $(\epsilon^k)^n = 1$. Vì thế ϵ^k là một căn bậc n của đơn vị. Theo định nghĩa căn nguyên thuỷ bậc n của đơn vị, những số $\epsilon, \epsilon^2, \epsilon^3, \ldots, \epsilon^n$ là đôi một khác nhau. Chú ý rằng có đúng n căn bậc n của của đơn vị, vì thế ta có điều phải chứng minh. □

2.2.9 Bổ đề. *Cho n, k là hai số nguyên dương và ϵ là một căn nguyên thuỷ bậc n của đơn vị. Khi đó ϵ^k là một căn nguyên thuỷ bậc n của đơn vị khi và chỉ khi* $\gcd(k, n) = 1$

Chứng minh. Đặt $d = \mathrm{ord}(\epsilon^k)$. Khi đó $(\epsilon^k)^d = 1$, tức là $\epsilon^{kd} = 1$. Do ϵ là căn nguyên thủy bậc n của đơn vị nên theo Bổ đề 2.2.3, $\mathrm{ord}(\epsilon) = n$ là ước của kd. Nếu $\gcd(k, n) = 1$ thì n phải là ước của d. Theo Bổ đề 2.2.3, d luôn là ước của n. Dó đó $d = n$, tức là ϵ^k là căn nguyên thuỷ bậc n của đơn vị.

Ngược lại, giả sử $\gcd(k, n) \neq 1$. Khi đó $\dfrac{n}{\gcd(k, n)} < n$ và $(\epsilon^k)^{\frac{n}{\gcd(k,n)}} = 1$. Do vậy $d < n$, tức là ϵ^k không là căn nguyên thuỷ bậc n của đơn vị. □

2.2.10 Định nghĩa. *Hàm Euler* $\varphi : \mathbb{N}^+ \to \mathbb{N}$ được định nghĩa như sau: $\varphi(1) = 1$. Cho $n > 1$. Khi đó $\varphi(n)$ là số các số tự nhiên nhỏ hơn n và nguyên tố cùng nhau với n.

Chẳng hạn, $\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2$.

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

Chứng minh. Đặt $\epsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$, trong đó $k = 0, 1, \ldots, n-1$. Ta chỉ cần chứng ϵ_k là căn nguyên thủy bậc n của đơn vị nếu và chỉ nếu

$\gcd(k,n)=1$ với mọi $k=0,\ldots,n-1$. Giả sử ϵ_k là căn nguyên thủy bậc n của đơn vị. Khi đó $\mathrm{ord}(\epsilon_k)=n$. Giả sử $\gcd(k,n)=d>1$. Ta có

$$\epsilon_k^{n/d}=(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n})^{n/d}=\cos\frac{2k\pi}{d}+i\sin\frac{2k\pi}{d}=1.$$

Điều này là vô lí. Vậy $d=1$. Ngược lại, cho $\gcd(k,n)=1$. Gọi t là cấp của ϵ_k, tức t là số nguyên dương bé nhất để $\epsilon_k^t=1$. Ta có

$$\epsilon_k^t=\cos\frac{2kt\pi}{n}+i\sin\frac{2kt\pi}{n}=1.$$

Suy ra $\dfrac{2kt\pi}{n}=m2\pi$ với m là một số nguyên. Do đó kt là bội của n. Vì $\gcd(k,n)=1$ nên t là bội của n. Suy ra $t=n$, tức là $\mathrm{ord}(\epsilon_k)=n$. □

2.2.12 Ví dụ. Do $\varphi(3)=2$, có 2 căn nguyên thuỷ bậc 3 của đơn vị, đó là

$$\epsilon_1=-\frac{1}{2}+i\frac{\sqrt{3}}{2};\epsilon_2=-\frac{1}{2}-i\frac{\sqrt{3}}{2}.$$

Có $\varphi(4)=2$ căn nguyên thuỷ bậc 4 của đơn vị là i và $-i$.

2.3 Tính chất cơ sở của đa thức chia đường tròn

2.3.1 Định nghĩa. Cho n là số nguyên dương. *Đa thức chia đường tròn thứ* n là đa thức dạng chuẩn (tức là có hệ số cao nhất bằng 1) và có đúng $\varphi(n)$ nghiệm là các căn nguyên thủy bậc n của đơn vị. Ta kí hiệu đa thức chia đường tròn thứ n là $\Phi_n(x)$. Như vậy $\Phi_n(x)$ có bậc $\varphi(n)$ và

$$\Phi_n(x)=\prod_{\substack{\epsilon^n=1\\ \mathrm{ord}(\epsilon)=n}}(x-\epsilon).$$

2.3.2 Ví dụ. Các căn bậc 3 của đơn vị là

$$\epsilon_k=\cos\frac{2k\pi}{3}+i\sin\frac{2k\pi}{3},k=0,1,2.$$

Các căn nguyên thuỷ bậc 3 của đơn vị là $\epsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}; \epsilon_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$. Do đó đa thức chia đường tròn thứ ba là

$$\Phi_3(x) = (x + (\frac{1}{2} - i\frac{\sqrt{3}}{2}))(x + (\frac{1}{2} + i\frac{\sqrt{3}}{2})) = x^2 + x + 1.$$

Các căn bậc 4 của đơn vị là

$$\epsilon_k = \cos\frac{2k\pi}{4} + i\sin\frac{2k\pi}{4}, k = 0, 1, 2, 3.$$

Các căn nguyên thuỷ bậc 4 của đơn vị là $\epsilon_1 = i$ và $\epsilon_3 = -i$. Đa thức chia đường tròn thứ tư là

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

2.3.3 Định lý. *Cho n là số nguyên dương. Khi đó*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Chứng minh. Để chứng minh đẳng thức trên, ta chỉ cần chứng minh hai đa thức $x^n - 1$ và $\prod_{d|n} \Phi_d(x)$ đều có dạng chuẩn, đều không có nghiệm bội, và có cùng tập nghiệm. Theo định nghĩa, mỗi $\Phi_d(x)$ là một đa thức dạng chuẩn. Vì thế đa thức phía bên phải có dạng chuẩn. Do đó hai đa thức ở hai vế đều có dạng chuẩn. Chú ý rằng một đa thức có nghiệm bội nếu và chỉ nếu đa thức đó và đạo hàm của nó phải có nghiệm chung. Vì thế $x^n - 1$ không có nghiệm bội (các nghiệm của $x^n - 1$ đều khác 0, trong khi đó đạo hàm của nó là nx^{n-1} chỉ có duy nhất nghiệm bằng 0). Với mỗi ước d của n, các nghiệm của $\Phi_d(x)$ đều là nghiệm của $x^d - 1$ và do đó nó không có nghiệm bội. Giả sử d và d' là hai ước khác nhau của n. Khi đó mỗi nghiệm của $\Phi_d(x)$ có cấp là d, trong khi đó mỗi nghiệm của $\Phi_{d'}(x)$ có cấp là d'. Vì thế, các nghiệm của đa thức $\prod_{d|n} \Phi_d(x)$ đều là nghiệm đơn. Giả sử ϵ là nghiệm của $x^n - 1$. Gọi d là cấp của ϵ. Khi đó $\epsilon^d = 1$ và d là số nguyên

dương bé nhất có tính chất này. Vì thế ϵ là căn nguyên thuỷ bậc d của đơn vị. Suy ra ϵ là nghiệm của đa thức của $\Phi_d(x)$. Ngược lại, cho d là ước của n và ϵ là nghiệm của $\Phi_d(x)$. Khi đó $\epsilon^d = 1$. Suy ra $\epsilon^n = 1$ tức ϵ là nghiệm của đa thức $x^n - 1$. □

2.3.4 Bổ đề. *Giả sử* $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_1x + a_0$ *và* $g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ *là hai đa thức với hệ số hữu tỉ. Nếu các hệ số của* fg *đều là số nguyên thì các hệ số của* f *và* g *cũng nguyên.*

Chứng minh. Bằng cách quy đồng mẫu số, ta có thể chọn được m và n là hai số nguyên dương nhỏ nhất để tất cả các hệ số của hai đa thức $mf(x)$ và $ng(x)$ là các số nguyên. Đặt $A_i = ma_i$ với $i = 0, \ldots, m-1$ và $B_i = nb_i$ với $i = 0, \ldots, n-1$. Đặt $A_m = m$ và $B_n = n$. Khi đó

$$mnf(x)g(x) = A_mB_nx^{m+n} + ... + A_0B_0.$$

Do $f(x)g(x) \in \mathbb{Z}[x]$ nên tất cả các hệ số của $mnf(x)g(x)$ đều chia hết cho mn. Giả sử rằng $mn > 1$. Gọi p là một ước nguyên tố của mn. Khi đó tồn tại một số nguyên $i \in \{0, ..., m\}$ sao cho p không là ước của hệ số A_i của mf. Thật vậy, nếu p không là ước của m thì p không là ước của hệ số cao nhất A_m của mf; còn nếu p là ước của m thì p là ước của A_i với mọi $i \in \{0, ..., m\}$ và do đó $\dfrac{A_i}{p} = \dfrac{m}{p}a_i \in \mathbb{Z}$, điều này là mâu thuẫn với giả thiết m là số nguyên dương nhỏ nhất có tính chất các hệ số của mf đều là số nguyên. Tương tự, tồn tại một số nguyên $j \in 0, ..., n$ sao cho p không là ước của hệ số B_j của đa thức ng. Gọi i_0 và j_0 tương ứng là số nguyên lớn nhất trong các số i và j thỏa mãn tính chất p không là ước của A_i và p không là ước của B_j. Khi đó hệ số của $x^{i_0+j_0}$ trong đa thức $mnf(x)g(x)$ là $A_{i_0}B_{j_0} + pt$ trong đó t là số nguyên. Rõ ràng hệ số này nó không là bội của p. Vì các hệ số của fg đều nguyên nên các hệ số của $mnfg$ đều chia hết cho mn và do đó đều chia hết cho p, điều này là vô lí. Vậy $mn = 1$. Suy ra f, g có các hệ số đều nguyên. □

2.3.5 Hệ quả. *Với mỗi số nguyên dương n, các hệ số của đa thức chia đường tròn $\Phi_n(x)$ đều là số nguyên, tức là $\Phi_n(x) \in \mathbb{Z}[x]$.*

Chứng minh. Ta chứng minh hệ quả này bằng phương pháp quy nạp theo n. Khẳng định này đúng với $n = 1$ vì $\Phi_1(x) = x - 1$. Giả sử khẳng định trên đúng với mọi $k < n$. Khi đó từ Định lý 2.3.3 ta có được:

$$\Phi_n(x) = \frac{x^n - 1}{\prod\limits_{d|n, d\neq n} \Phi_d(x)}.$$

Đặt $f(x) = \Phi_n(x)$ và $g(x) = \prod\limits_{d|n, d\neq n} \Phi_d(x)$. Theo giả thiết quy nạp, các hệ số của đa thức $\Phi_d(x)$ đều là số nguyên với mọi ước d của n với $d \neq n$. Do đó $g(x)$ có các hệ số đều nguyên. Suy ra $f(x)$ có các hệ số hữu tỷ. Vì $x^n - 1 = f(x)g(x)$ là đa thức với hệ số nguyên, trong đó $f(x)$ và $g(x)$ có hệ số cao nhất bằng 1 và có các hệ số đều nguyên nên theo Bổ đề 2.3.4, các đa thức f và g đều có hệ số nguyên. Đặc biệt $f(x) = \Phi_n(x)$ có các hệ số đều là số nguyên. □

2.3.6 Hệ quả. *Cho n là số nguyên dương. Khi đó*

$$\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Chứng minh. Kết quả này suy ra ngay từ các Mệnh đề 2.1.4 và 2.3.3. Thật vậy, với mỗi số tự nhiên x, đặt $F_x, f_x : \mathbb{Z}^+ \to \mathbb{Z}^+$ là các hàm xác định bởi $F_x(n) = x^n - 1$ và $f_x(n) = \Phi_n(x)$. Theo Định lý 2.3.3 ta có $F_x(n) = \prod_{d|n} f_x(d)$. Do đó theo Định lý 2.1.4 ta có $f_x(n) = \prod\limits_{d|n} F_x\left(\frac{n}{d}\right)^{\mu(d)}$. Nghĩa là với mọi số tự nhiên x ta có

$$\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Như vậy, hai đa thức ở hai vế của đẳng thức trên có bậc là $\varphi(n)$ và nhận giá trị bằng nhau tại mọi số tự nhiên x. Lại chú ý thêm rằng hai đa thức

này có bậc $\varphi(n)$ nên nhận giá trị bằng nhau tại không quá $\varphi(n)$ điểm. Do đó chúng là hai đa thức bằng nhau. □

2.3.7 Bổ đề. *Cho p là số nguyên tố và n là số nguyên dương. Khi đó*

a) Nếu $p|n$ thì $\Phi_{pn}(x) = \Phi_n(x^p)$.

b) Nếu p không là ước của n thì $\Phi_{pn}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$.

Chứng minh. Trước hết, giả sử $p|n$. Kí hiệu $I_{p,n}$ là tập các ước d của pn sao cho d không là ước của n. Theo Hệ quả 2.3.6 ta có

$$\begin{aligned}\Phi_{pn}(x) &= \prod_{d|pn}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}\\ &= \left(\prod_{d|n}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}\right)\left(\prod_{d\in I_{p,n}}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}\right)\\ &= \Phi_n(x^p)\prod_{d\in I_{p,n}}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}.\end{aligned}$$

Lấy $d \in I_{p,n}$. Khi đó $d|pn$ và d không là ước của n. Viết $d = p^k m, n = p^t l$ với m, l không chia hết cho p. Vì $d|pn$ nên $p^k m|p^{t+1}l$. Suy ra $k \le t+1$ và $m|l$. Do d không là ước của n và $m|l$ nên $k > t$. Do $p|n$ nên $t > 0$. Suy ra $k \ge 2$, tức là $p^2|d$ nên $\mu(d) = 0$. Do vậy $\prod\limits_{d\in I_{p,n}}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)} = 1$ và do đó $\Phi_{pn}(x) = \Phi_n(x^p)$.

Ngược lại, giả sử p không là ước của n. Theo Hệ quả 2.3.6 ta có:

$$\begin{aligned}\Phi_{pn}(x) = \prod_{d|pn}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)} &= \left(\prod_{d|n}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}\right)\left(\prod_{d|n}\left(x^{\frac{pn}{pd}}-1\right)^{\mu(pd)}\right)\\ &= \left(\prod_{d|n}\left(x^{\frac{pn}{d}}-1\right)^{\mu(d)}\right)\left(\prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{-\mu(d)}\right)\\ &= \frac{\Phi_n(x^p)}{\Phi_n(x)}.\end{aligned}$$

Từ đây ta suy ra điều phải chứng minh. □

2.3.8 Hệ quả. *Cho p là số nguyên tố và n, k là các số nguyên dương.*

a) Nếu $p|n$ thì $\Phi_{p^k n}(x) = \Phi_n\left(x^{p^k}\right)$.

b) Nếu p không là ước của n thì $\Phi_{p^k n}(x) = \dfrac{\Phi_n\left(x^{p^k}\right)}{\Phi_n\left(x^{p^{k-1}}\right)}$.

Chứng minh. Theo Bổ đề 2.3.7, ta có

$$\Phi_{p^k n}(x) = \Phi_{p^{k-1} n}(x^p) = \Phi_{p^{k-2} n}\left(x^{p^2}\right) = ... = \Phi_{pn}\left(x^{p^{k-1}}\right).$$

Vì thế, cũng theo Bổ đề 2.3.7, nếu $p|n$ thì $\Phi_{pn}\left(x^{p^{k-1}}\right) = \Phi_n\left(x^{p^k}\right)$ và nếu p không là ước của n thì $\Phi_{pn}\left(x^{p^{k-1}}\right) = \dfrac{\Phi_n\left(x^{p^k}\right)}{\Phi_n\left(x^{p^{k-1}}\right)}$, hệ quả đã được chứng minh. □

Cho $f(x) = a_n x^n + \ldots + a_1 x + a_0$ và $g(x) = b_n x^n + \ldots + b_1 x + b_0 \in \mathbb{Z}[x]$. Nếu $a_i \equiv b_i \pmod p$, với mọi $i = 0, 1, \ldots, n$ thì ta nói $f(x)$ và $g(x)$ *đồng dư với nhau theo modulo* p và ta viết $f(x) \equiv g(x) \pmod p$.

2.3.9 Bổ đề. *Cho p là số nguyên tố và $k \geq 2$ là một số tự nhiên. Giả sử đa thức $x^n - 1$ có nghiệm bội k modulo p, nghĩa là tồn tại $a \in \mathbb{Z}$ và $f(x) \in \mathbb{Z}[x]$ sao cho $x^n - 1 \equiv (x-a)^k f(x) \pmod p$. Khi đó $p|n$.*

Chứng minh. Rõ ràng p không là ước của a. Thay $y = x - a$, ta có:

$$(y+a)^n - 1 \equiv y^k f(y+a) \pmod p.$$

So sánh các hệ số, chúng ta thấy rằng các hệ số bậc nhất của y ở vế bên phải là bằng 0. Theo định lý nhị thức, hệ số bậc nhất của y ở vế bên trái là bằng na^{n-1}. Chính vì vậy ta có $na^{n-1} \equiv 0(modp)$, do đó $p|na^{n-1}$. Nhưng p không là ước của a nên p không là ước của a^{n-1}, vì vậy $p|n$. Bổ đề đã được chứng minh. □

2.3.10 Hệ quả. *Cho n là số nguyên dương và $d < n$ là một ước của n. Cho x là số nguyên. Giả sử rằng p là một ước nguyên tố chung của $\Phi_n(x)$ và $\Phi_d(x)$. Khi đó $p|n$.*

Chứng minh. Theo Định lý 2.3.3 ta có $X^n - 1 = \prod_{t|n} \Phi_t(X)$. Do $d|n$ và $n > d$ nên $X^n - 1$ chia hết cho $\Phi_n(x)\Phi_d(x)$. Do $\Phi_n(x) = 0 \pmod p$ theo giả thiết nên $\Phi_n(X) \equiv (X - x)f(X) \pmod p$. Chứng minh tương tự ta được $\Phi_d(X) \equiv (X - x)g(X) \pmod p$. Suy ra $X^n - 1$ nhận x làm nghiệm bội $k \geq 2$. Do đó theo Bổ đề 2.3.9 ta có $p|n$. □

2.3.11 Định lý. *Cho n là số nguyên dương và $x \in \mathbb{Z}$. Giả sử p là một ước nguyên tố của $\Phi_n(x)$. Khi đó $p \equiv 1 \pmod n$ hoặc $p|n$*

Chứng minh. Giả sử p là một ước nguyên tố của $\Phi_n(x)$. Do $p|\Phi_n(x)$ và $\Phi_n(x)|x^n - 1$ nên $p|x^n - 1$. Do đó p không là ước của x. Vì thế theo Định lí Fermat bé ta có $x^{p-1} \equiv 1 \pmod p$. Do đó ta có thể chọn được số nguyên dương k bé nhất thoả mãn $x^k \equiv 1 \pmod p$. Vì $p|x^n - 1$ ta suy ra $x^n \equiv 1 \pmod p$. Viết $n = kq + r$ với $0 \leqslant r < k$. Khi đó $1 \equiv x^n = (x^k)^q x^r \equiv x^r \pmod p$. Từ cách chọn k ta có $r = 0$. Do đó $k|n$. Viết $p - 1 = kt + s$, trong đó $0 \leqslant s < k$. Khi đó $1 \equiv x^{p-1} = (x^k)^t x^s \equiv x^s \pmod p$. Từ cách chọn k ta có $s = 0$, tức là $k|(p - 1)$. Nếu $k = n$ thì $n|p - 1$. Do đó $p \equiv 1 \pmod n$. Giả sử $k < n$. Vì $0 \equiv x^k - 1 = \prod_{d|k} \Phi_d(x) \pmod p$ nên tồn tại một ước d của k sao cho $p|\Phi_d(x)$. Do $d|k$, $k|n$ và $d < n$ nên theo Hệ quả 2.3.10 ta có $p|n$. □

2.3.12 Hệ quả. *Cho p là một số nguyên tố và $x \in \mathbb{Z}$. Giả sử q là ước nguyên tố của $1 + x + ... + x^{p-1}$. Khi đó $q \equiv 1 \pmod p$ hoặc $q = p$.*

Chứng minh. Ta có

$$1 + x + ... + x^{p-1} = \frac{x^p - 1}{x - 1} = \frac{x^p - 1}{\Phi_1(x)}.$$

Chú ý rằng trong các căn bậc p của đơn vị

$$\epsilon_k = \cos\frac{2k\pi}{p} + i\sin\frac{2k\pi}{p}, k = 0, \ldots, p-1,$$

các căn ϵ_k với $(k,p) = 1$ là các căn nguyên thuỷ. Vì p là số nguyên tố nên $(k,p) = 1$ với mọi $k = 1, \ldots, p-1$. Do đó, ϵ_k với $k = 1, \ldots p-1$ là các căn nguyên thủy bậc p của đơn vị. Vì thế

$$\Phi_p(x) = \prod_{k=1}^{p-1}(x - \epsilon_k) = \frac{x^p - 1}{x - 1}.$$

Suy ra $x^p - 1 = \Phi_p(x)(x-1)$ và do đó $1 + x + ... + x^{p-1} = \Phi_p(x)$. Theo giả thiết ta có $q|\Phi_p(x)$. Vì thế áp dụng Định lý 2.3.11 ta có $q \equiv 1 \pmod p$ hoặc $q|p$, tức là $q \equiv 1 \pmod p$ hoặc $q = p$ (do p, q là nguyên tố). □

2.3.13 Bổ đề. *Cho a và b là hai số nguyên dương và $x \in \mathbb{Z}$. Khi đó*

$$\gcd\left(x^a - 1, x^b - 1\right) = \left|x^{\gcd(a,b)} - 1\right|.$$

Chứng minh. Đặt $T = \gcd\left(x^a - 1, x^b - 1\right)$ và $t = \gcd(a,b)$. Từ giả thiết $x^t - 1|x^a - 1$ và $x^t - 1|x^b - 1$ ta suy ra $x^t - 1|T$. Rõ ràng, $\gcd(x,T) = 1$. Vì thế $x^{\varphi(T)} \equiv 1 \pmod T$, trong đó φ là hàm Euler. Do đó tồn tại số nguyên dương d bé nhất sao cho $x^d \equiv 1 \pmod T$. Do đó $T|x^d - 1$. Vì $x^a \equiv x^b \equiv 1 \,(\mathrm{mod} T)$ nên ta có $d|a$ và $d|b$. Do đó $d|t$. Vì vậy $x^d - 1|x^t - 1$. Vì thế $T|x^t - 1$. Suy ra $T = |x^t - 1|$, ta có kết quả. □

2.3.14 Định lý. *Cho a và b là hai số nguyên dương và tồn tại một số nguyên x sao cho $\gcd(\Phi_a(x), \Phi_b(x)) > 1$. Khi đó $\frac{a}{b}$ là luỹ thừa với số mũ nguyên của một số nguyên tố, nghĩa là $\frac{a}{b} = p^k$ với p là số nguyên tố và k là một số nguyên.*

Chứng minh. Vì $\gcd(\Phi_a(x), \Phi_b(x)) > 1$ nên tồn tại một ước nguyên tố chung p của $\Phi_a(x)$ và $\Phi_b(x)$. Ta chứng minh rằng $\frac{a}{b}$ phải là một luỹ thừa

của p. Viết $a = p^{\alpha}A$ và $b = p^{\beta}B$ với α, β là các số nguyên không âm và A, B là các số nguyên dương không chia hết cho p. Ta sẽ chỉ ra rằng $A = B$. Thật vậy, vì $p|\Phi_a(x)$ và $\Phi_a(x)|x^a - 1$ nên $p|x_a - 1$, do đó p không là ước của x. Trước tiên ta chứng minh $p|\Phi_A(x)$. Điều này là hiển nhiên nếu $\alpha = 0$. Nếu $\alpha > 1$ thì theo Hệ quả 2.3.8 ta có $0 \equiv \Phi_a(x) = \dfrac{\Phi_A\left(x^{p^{\alpha}}\right)}{\Phi_a\left(x^{p^{\alpha-1}}\right)} (\mathrm{mod} p)$. Vì thế $\Phi_A\left(x^{p^{\alpha}}\right) \equiv 0 (\mathrm{mod} p)$. Nhưng $x^{p^{\alpha}} \equiv x.x^{p^{\alpha}-1}$ và từ $p^{\alpha} - 1$ chia hết cho $p - 1$ nên theo công thức *Hàm Euler* ta suy ra được $x^{p^{\alpha}-1} \equiv 1 (\mathrm{mod} p)$ nên $x.x^{p^{\alpha}-1} \equiv x.1 (\mathrm{mod} p)$ và do đó $x^{p^{\alpha}} \equiv x (\mathrm{mod} p)$. Vì vậy

$$0 \equiv \Phi_A\left(x^{p^{\alpha}}\right) \equiv \Phi_A(x) (\mathrm{mod} p).$$

Vì vậy $p|\Phi_A(x)$. Tương tự chứng minh, ta cũng có được kết quả $p|\Phi_B(x)$. Không mất tính tổng quát, ta có thể giả thiết $A > B$. Đặt $t = \gcd(A, B)$. Khi đó $t < A$. Vì $p|\Phi_A(x)$ và $\Phi_A(x)|x^A - 1$, $p|\Phi_B(x)$ và $\Phi_B(x)|x^B - 1$ nên $p|\gcd\left(x^A - 1, x^B - 1\right)$. Theo Bổ đề 2.3.13 ta có $\gcd\left(x^A - 1, x^B - 1\right) = |x^t - 1|$, vì thế $p|x^t - 1$. Suy ra $0 \equiv x^t - 1 = \prod_{d|t} \Phi_d(x) (\mathrm{mod} p)$, do đó tồn tại một ước d của t sao cho $p|\Phi_d(x)$. Vì $d|t$, $t|A$, $d < A$ và $p|\Phi_A(x)$, nên theo Hệ quả 2.3.10 ta có $p|A$, điều này là mâu thuẫn với điều giả sử ban đầu p không là ước của A. Do đó $A = B$, vì vậy $\dfrac{a}{b} = p^{\alpha-\beta}$. □

2.4 Một số ứng dụng của đa thức chia đường tròn

Một ứng dụng phổ biến của đa thức chia đường tròn là chứng minh Định lý *Dirichlet*

2.4.1 Định lý. *(Dirichlet). Cho n là số nguyên dương. Khi đó tồn tại vô số số nguyên tố p sao cho* $p \equiv 1 (\mathrm{mod} n)$

Chứng minh. Với $n = 1$, kết quả hiển nhiên đúng. Cho $n > 1$. Giả sử chỉ tồn tại hữu hạn số nguyên tố p sao cho $p \equiv 1 (\mathrm{mod} n)$. Đặt T_1 là tích của

các số nguyên tố p có tính chất $p \equiv 1(\mod n)$ và T_2 là tích của tất cả các ước nguyên tố của n. Đặt $T = T_1T_2$. Do $n > 1$ nên $T - 2 > 1$ và vì thế $T > 1$. Đặt k là một số nguyên dương đủ lớn sao cho $\Phi_n\left(T^k\right) > 1$ (với $\Phi_n(X)$ là đa thức dạng chuẩn có bậc $\Phi(n) \geq 1$ nên k tồn tại). Lấy q là một ước nguyên tố của $\Phi_n\left(T^k\right)$. Vì q là ước của $T^{kn} - 1$ nên q không là ước của T, vì thế q không là ước của T_1 và q không là ước của T_2 nên $q \not\equiv 1 (\mathrm{mod} n)$ và q không là ước của n. Điều này là mâu thuẫn với Định lý 2.3.11. □

Một ứng dụng khác rất hay của đa thức chia đường tròn là giải quyết các bài tập trong các đề thi học sinh giỏi Quốc tế.

2.4.2 Bài toán. *(Đề thi học sinh giỏi Quốc tế 2002) Giả sử $p_1, p_2, ..., p_n$ là các số nguyên tố phân biệt lớn hơn 3. Chứng minh rằng $2^{p_1p_2\cdots p_n} + 1$ có ít nhất 4^n ước.*

Để giải quyết bài toán 2.4.2, ta sẽ chứng minh một bài toán tổng quát hơn. Cụ thể, với giả thiết như trong bài toán 2.4.2 ta chứng minh được $2^{p_1p_2\cdots p_n} + 1$ có ít nhất $2^{2^{n-1}}$ ước. Rõ ràng $2^{2^{n-1}} > 4^n$ (khi n đủ lớn). Do đó Bài tập 2.4.2 là trường hợp đặc biệt của bài toán sau:

2.4.3 Bài toán. *Đặt $p_1, p_2, ..., p_n$ là các số nguyên tố phân biệt lớn hơn 3. Chứng minh rằng $2^{p_1p_2\cdots p_n} + 1$ có ít nhất $2^{2^{n-1}}$ ước.*

Chứng minh. Ta chứng minh rằng $2^{p_1p_2\cdots p_n} + 1$ có ít nhất 2^{n-1} ước đôi một nguyên tố cùng nhau và do đó ta suy ra $2^{p_1p_2\cdots p_n} + 1$ có ít nhất 2^{n-1} ước nguyên tố phân biệt. Theo Định lý 2.3.3 ta có:

$$\left(2^{p_1p_2\cdots p_n} - 1\right)\left(2^{p_1p_2\cdots p_n} + 1\right) = 2^{2p_1p_2\cdots p_n} - 1 = \prod_{d \mid 2p_1p_2\cdots p_n} \Phi_d(2)$$

Đặt $A = \{d \mid d \text{ là ước của } 2p_1 \dots p_n\}$ và

$$B = \{d \in A \mid d \text{ là ước của } \ p_1 \dots p_n\}$$
$$C = \{2d \mid d \text{ là ước của } p_1 \dots p_n\}.$$

Ta thấy $B \cup C = A$ và $B \cap C = \emptyset$. Do đó

$$\begin{aligned}\prod_{d|2p_1p_2\dots p_n} \Phi_d(2) &= \left(\prod_{d|p_1p_2\dots p_n} \Phi_d(2)\right)\left(\prod_{k|p_1p_2\dots p_n} \Phi_{2k}(2)\right)\\ &= \prod_{d\in B} \Phi_d(2) \prod_{d\in C} \Phi_d(2)\\ &= \prod_{d|p_1\dots p_n} \Phi_d(2) \prod_{2d'|p_1\dots p_n} \Phi_{2d'}(2)\\ &= (2^{p_1p_2\dots p_n} - 1)\left(\prod_{k|p_1p_2\dots p_n} \Phi_{2k}(2)\right).\end{aligned}$$

Do vậy

$$2^{p_1p_2\dots p_n} + 1 = \prod_{k|p_1p_2\dots p_n} \Phi_{2k}(2).$$

Do đó có bao nhiêu ước của $p_1 \dots p_n$ thì tích ở vế bên phải của đẳng thức trên có bấy nhiêu nhân tử. Chú ý rằng mỗi ước m của $p_1 \dots p_n$ là tích của các phần tử trong một tập con của tập $\{p_1, \dots, p_n\}$. Vì thế, số các ước của $p_1 \dots p_n$ chính là số tập con của tập $\{p_1, \dots, p_n\}$. Vì tập này có 2^n tập con nên $p_1 \dots p_n$ có 2^n ước khác nhau, mỗi ước đều là tích của hữu hạn số nguyên tố phân biệt trong tập $\{p_1, \dots, p_n\}$.

Gọi E là tập các ước d của $p_1 \dots p_n$ sao cho d là tích của một số chẵn thừa số nguyên tố và F là tập các ước d của $p_1 \dots p_n$ sao cho d là tích của một số lẻ thừa số nguyên tố. Khi đó E và F có số phần tử như nhau, mỗi tập có 2^{n-1} phần tử. Cho $a \neq b$, $a, b \in E$. Giả sử $\Phi_a(2)$ và $\Phi_b(2)$ không nguyên tố cùng nhau. Theo Định lý 2.3.14 ta suy ra $\dfrac{a}{b}$ là luỹ thừa nguyên

của một số nguyên tố. Nhưng vì a và b đều là tích của một số chẵn thừa số nguyên tố phân biệt nên điều này là không thể. Vì thế $\Phi_a(2)$ và $\Phi_b(2)$ là hai ước nguyên tố cùng nhau của $2^{p_1p_2\ldots p_n}+1$ với mọi $a, b \in E$ với $a \neq b$. Do E có 2^{n-1} phần tử nên ta có kết quả. □

2.4.4 Bài toán. *(Đề thi học sinh giỏi Quốc tế 2006) Tìm tất cả các cặp số nguyên (x, y) thoả mãn phương trình*

$$\frac{x^7-1}{x-1} = y^5 - 1.$$

Lời giải: Phương trình đã cho tương đương với

$$1 + x + ... + x^6 = (y-1)(1 + y + ... + y^4).$$

Từ Hệ quả 2.3.12 ta biết rằng mọi ước nguyên tố p của $1+x+...+x^6$ đều thoả mãn $p = 7$ hoặc $p \equiv 1 \pmod 7$. Nếu p nguyên tố và $p|1+x+...+x^6$ thì $p = 7$ hoặc $p \equiv 1 \pmod 7$ (Theo Hệ quả 2.3.12). Lấy d là một ước của $1 + x + ... + x^6$. Viết $d = p_1^{\alpha_1} \ldots p_k^{\alpha_r}$ với p_i là số nguyên tố, $\alpha_i \in \mathbb{N}$. Do $d|1+x+...+x^6$ nên $p_i|1+x+...+x^6$. Do đó $p_i = 7$ hoặc $p_i \equiv 1 \pmod 7$ với mọi $i = 1, \ldots, k$. Suy ra d chia hết cho 7 hoặc $d \equiv 1 \pmod 7$, tức là tất cả các ước của $1+x+...+x^6$ hoặc chia hết cho 7, hoặc đồng dư 1 modulo 7. Như vậy, $(y-1) \equiv 0 \pmod 7$ hoặc $(y-1) \equiv 1 \pmod 7$. Đó là $y \equiv 1 \pmod 7$ hoặc $y \equiv 2 \pmod 7$. Nếu $y \equiv 1 \pmod 7$ thì $1 + y + ... + y^4 \equiv 5 \pmod 7$ và do đó $1+y+...+y^4$ là ước của $1+x+...+x^6$ nhưng không đồng dư với $0 \pmod 7$ và không đồng dư với $1 \pmod 7$. Điều này là mâu thuẫn. Nếu $y \equiv 2 \pmod 7$ thì $1+y+...+y^4 \equiv 31 \equiv 3 \pmod 7$ và do đó $1+y+...+y^4$ không đồng dư với 0 hoặc 1 theo $\pmod 7$. Điều này cũng mâu thuẫn. Do vậy, phương trình này không có nghiệm nguyên.

Chương 3

Tính bất khả quy

3.1 Đa thức bất khả quy

Cho K là trường con của trường số phức $\mathbb{C}$ (chẳng hạn $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)

3.1.1 Định nghĩa. Một đa thức $f(x) \in K[x]$ được gọi là *bất khả quy* nếu $\deg f(x) > 0$ và $f(x)$ không phân tích được thành tích của hai đa thức có bậc bé hơn. Nếu $\deg f(x) > 0$ và $f(x)$ là tích của hai đa thức có bậc bé hơn thì ta nói $f(x)$ là *khả quy*.

3.1.2 Ví dụ. Cho $f(x) \in K[x]$ và $a \in K$. Khi đó

(i) Nếu $\deg f(x) = 1$ thì $f(x)$ luôn bất khả quy.

(ii) $f(x)$ là bất khả quy nếu và chỉ nếu $f(x + a)$ là bất khả quy.

(iii) Nếu $\deg f(x) > 1$ và $f(x)$ có nghiệm trong K thì $f(x)$ khả quy.

(iv) Nếu $\deg f(x)$ là 2 hoặc 3 thì $f(x)$ là bất khả quy nếu và chỉ nếu nó không có nghiệm trong K.

Tiếp theo, chúng ta định nghĩa khái niệm đa thức bất khả quy của một phần tử đại số. Trước hết, ta cần kết quả sau.

3.1.3 Định nghĩa. Cho $a \in \mathbb{C}$. Ta nói a là *phần tử đại số trên* K nếu tồn tại một đa thức $0 \neq f(x) \in K[x]$ nhận a làm nghiệm. Nếu a không đại số trên K thì ta nói a là *siêu việt* trên K.

3.1.4 Định lý. *Cho $a \in \mathbb{C}$ là phần tử đại số trên K. Khi đó tồn tại duy nhất một đa thức $p(x) \in K[x]$ bất khả quy dạng chuẩn nhận a làm nghiệm, và mọi đa thức $g(x) \in K[x]$ nhận a làm nghiệm đều là bội của $p(x)$.*

Chứng minh. Vì a là nghiệm của một đa thức khác 0 với hệ số trong K nên chọn được đa thức khác 0 với hệ số trong K có bậc bé nhất nhận a làm nghiệm. Gọi $p(x) \in K[x]$ là dạng chuẩn của đa thức này. Khi đó a là nghiệm của $p(x)$. Ta chứng minh $p(x)$ bất khả quy. Giả sử $p(x)$ không bất khả quy. Khi đó $p(x)$ phân tích được thành tích của hai đa thức trong $K[x]$ với bậc bé hơn, và do đó một trong hai đa thức này phải nhận a làm nghiệm, điều này là mâu thuẫn với cách chọn $p(x)$. Giả sử $g(x) \in K[x]$ nhận a làm nghiệm. Nếu $p(x)$ không là ước của $g(x)$ thì vì $p(x)$ bất khả quy nên $\gcd(g(x), p(x)) = 1$, do đó $1 = p(x)q(x) + g(x)h(x)$ với $q(x), h(x) \in K[x]$. Thay $x = a$ vào cả hai vế ta được $1 = 0$, điều này là vô lí. Vậy $g(x)$ chia hết cho $p(x)$. Giả sử $q(x) \in K[x]$ cũng là đa thức bất khả quy dạng chuẩn nhận a làm nghiệm. Theo chứng minh trên, $q(x)$ là bội của $p(x)$. Viết $q(x) = p(x)k(x)$. Vì $q(x)$ bất khả quy nên $k(x) = b \in K$. Do đó $q(x) = bp(x)$. Đồng nhất hệ số cao nhất của hai vế với chú ý rằng $q(x)$ và $p(x)$ đều có dạng chuẩn, ta suy ra $b = 1$. Vì thế $p(x) = q(x)$. □

3.1.5 Định nghĩa. Đa thức $p(x) \in K[x]$ bất khả quy dạng chuẩn xác định như trong mệnh đề trên được gọi là *đa thức bất khả quy* của a.

3.1.6 Ví dụ. Đa thức $x^3 - 7 \in \mathbb{Q}[x]$ là đa thức bất khả quy của $\sqrt[3]{7} \in \mathbb{R}$; đa thức $x^2 + 1 \in \mathbb{R}[x]$ là đa thức bất khả quy của $i \in \mathbb{C}$.

Tiếp theo, Định lí 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 này là duy nhất nếu không kể đến thứ tự các thừa số. Kết quả sau đây là một sự tương tự của định lí này đối với đa thức.

3.1.7 Định lý. *Mỗi đa thức dạng chuẩn bậc dương 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 phần tử.*

Chứng minh. Trước hết, chúng 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 nên sự phân tích bất khả quy của $f(x)$ là $f(x) = f(x)$, kết quả đúng cho trường hợp $d = 1$. Cho $d > 1$ và giả sử kết quả đã đúng cho các đa thức có 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 $g(x), h(x)$ đều có bậc bé hơn bậc của $f(x)$. Đặt $g^*(x) = g(x)/a_k$ với a_k là hệ số cao nhất của $g(x)$. Khi đó ta có $f(x) = g^*(x)(a_k h(x))$. Đồng nhất hệ số cao nhất ở hai vế ta được $1 = a_k b_t$, trong đó b_t là hệ số cao nhất của $h(x)$. Đặt $h^*(x) = a_k h(x)$. Khi đó $f(x) = g^*(x)h^*(x)$ với $g^*(x), h^*(x)$ 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 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 quy nạp theo n rằng $n = m$ và sau một phép hoán vị ta có $p_i(x) = q_i(x)$ với mọi $i = 1, ..., n$. Cho $n = 1$. Khi đó ta có $p_1(x) = q_1(x)q_2(x)...q_m(x)$. Suy ra

$$p_1(x)|q_1(x)q_2(x)...q_m(x).$$

Do $p_1(x)$ là bất khả quy nên $p_1(x)$ là ước của một nhân tử $q_i(x)$ nào đó. Không mất tính tổng quát ta có thể giả thiết $p_1(x)|q_1(x)$. Biểu diễn $q_1(x) = p_1(x)t_1(x)$. Vì $q_1(x)$ bất khả quy nên $t_1(x) = a \in K$. Đồng nhất hệ số cao nhất của hai vế của đẳng thức $q_1(x) = ap_1(x)$ với chú ý

rằng $p_1(x)$ và $q_1(x)$ là dạng chuẩn, ta có $1 = 1.a$. Suy ra $a = 1$ và do đó $p_1(x) = q_1(x)$. Nếu $m > 1$ thì $1 = q_2(x)...q_m(x)$, điều này là vô lí. Vậy kết quả đúng cho $n = 1$.

Cho $n > 1$. Vì $p_1(x)|q_1(x)q_2(x)...q_m(x)$ và $p_1(x)$ là bất khả quy nên không mất tính tổng quát ta có thể giả thiết $p_1(x)|q_1(x)$. Lại do $q_1(x)$ là bất khả quy và $p_1(x), q_1(x)$ đều có dạng chuẩn nên tương tự như lập luận trên ta có $p_1(x) = q_1(x)$. Giản ước cả hai vế cho $p_1(x)$ ta được

$$p_2(x)p_3(x)...p_n(x) = q_2(x)q_3(x)...q_m(x).$$

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

3.2 Tính bất khả quy của đa thức chia đường tròn

Đa thức chia đường tròn $\Phi_n(x)$ luôn là đa thức bất khả quy với mọi số nguyên dương n. Đây là một kết quả cơ sở của lí thuyết số. Chứng minh tính bất khả quy của đa thức chia đường tròn có một lịch sử khá dài.

Với n nguyên tố, tính bất khả quy của đa thức chia đường tròn $\Phi_n(x)$ lần đầu tiên được chứng minh bởi C. F. Gauss [Gau] năm 1801. Hơn 40 năm sau, năm 1845, L. Kronecker [K] đã đưa ra một chứng minh đơn giản hơn. Ngay sau đó, T. Schonemann [Sch] năm 1846 và F. Eidenstein [E] năm 1850 đã đưa ra hai chứng minh đơn giản hơn nữa. Cho đến bây giờ, chứng minh của Eidenstein [E] vẫn là chứng minh chuẩn mực nhất. Với n tùy ý (không nhất thiết nguyên tố), tính bất khả quy của đa thức chia đường tròn $\Phi_n(x)$ lần đầu tiên được chứng minh bởi L. Kronecker [K2] vào năm 1854. Các chứng minh đơn giản hơn được đưa ra bởi R. Dedekind [D] năm 1857, E. Landau năm 1929 và I. Schur năm 1929. Cho đến nay, chứng minh của Dedekind [D] vẫn là chứng minh chuẩn mực nhất.

Mục đích của tiết này là đưa ra một số chứng minh cổ điển cho tính bất khả quy của đa thức chia đường tròn $\Phi_n(x)$ khi n nguyên tố. Do giới hạn về khuôn khổ một luận văn thạc sĩ nên tác giả luận văn xin phép không trình bày chứng minh tính bất khả quy cho đa thức chia đường tròn $\Phi_n(x)$ khi n bất kì.

Nhắc lại rằng một đa thức $f(x_1, \ldots, x_k)$ được gọi là đa thức *đối xứng* nếu $f(x_1, \ldots, x_k) = f(x_{\delta(1)}, \ldots, x_{\delta(k)})$ với mọi hoán vị δ của tập hợp k phần tử $\{1, 2, \ldots, k\}$. Chẳng hạn, $x^2 + 3xy + y^2$ là đa thức đối xứng, $2x^3 + 2y^3 + 2z^3 + xyz + xy + xz + yz$ là đa thức đối xứng. Với n biến $x_1, \ldots, x_n$, các đa thức sau là đối xứng và ta gọi là *các đa thức đối xứng cơ bản*

$$\begin{aligned}
\delta_1 &= \sum_{i=1}^{n} x_i = x_1 + \ldots + x_n \\
\delta_2 &= \sum_{1 \leqslant i < j \leqslant n} x_i x_j = x_1x_2 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n \\
&\ldots\ldots \\
\delta_n &= x_1 \ldots x_n.
\end{aligned}$$

Bổ đề sau đây, còn gọi là \Định lí cơ bản của đa thức đối xứng" là một kết quả quan trọng về đa thức đối xứng.

3.2.1 Bổ đề. *Kí hiệu $A = \mathbb{Z}$ hoặc $A = \mathbb{Q}$. Cho $f(x_1, \ldots, x_n)$ là đa thức đối xứng với hệ số trong A. Khi đó tồn tại đa thức $g(x_1, \ldots, x_n)$ với các hệ số trong A sao cho $f(x_1, \ldots, x_n) = g(\delta_1, \ldots, \delta_n)$.*

3.2.2 Định lý. *Cho p là số nguyên tố. Khi đó đa thức chia đường tròn $\Phi_p(x)$ là bất khả quy.*

Chứng minh. (Chứng minh của Gauss năm 1801) Với $p = 2$ ta có $\Phi_2(x) = x + 1$ là đa thức bất khả quy. Giả sử p là số nguyên tố lẻ. Trước tiên, đặt $f(x)$ là một đa thức dạng chuẩn bất kỳ với hệ số hữu tỉ có các nghiệm

$r_1, \ldots, r_m$, ta có $f(x) = (x - r_1) \ldots (x - r_m)$. Gọi $g(x)$ là đa thức dạng chuẩn mà các nghiệm là các luỹ thừa bậc k của các nghiệm của $f(x)$. Khi đó $g(x) = (x - r_1^k) \ldots (x - r_m^k)$. Vì thế các hệ số của $g(x)$ là các đa thức đối xứng của $r_1^k, \ldots, r_m^k$ và do đó các hệ số của $g(x)$ cũng là các đa thức đối xứng của $r_1, \ldots, r_m$. Theo công thức Viet, mỗi đa thức đối xứng cơ bản của $r_1, \ldots, r_m$ đều được biểu diễn theo các hệ số của $f(x)$ thông qua các phép toán cộng, trừ, nhân, chia (cho phần tử khác 0). Vì thế, theo Bổ đề 3.2.1, các hệ số của $g(x)$ được biểu diễn theo các hệ số của $f(x)$ thông qua các phép toán cộng, trừ, nhân, chia. Vì tổng, hiệu, tích, thương của hai số hữu tỷ lại là số hữu tỷ nên các hệ số của $g(x)$ đều là số hữu tỉ.

Tiếp theo, gọi $\varphi(x_1, x_2, ...)$ là một đa thức với hệ số nguyên và ϵ là một căn nguyên thuỷ bậc p của đơn vị. Thay $x_i = \epsilon^{k_i}$ với $i = 1, \ldots,$ ta có

$$\varphi(\epsilon^{k_1}, \epsilon^{k_2}, ...) = A_0 + A_1\epsilon + ... + A_{p-1}\epsilon^{p-1}$$

với $A_0, ..., A_{p-1}$ là các số nguyên nào đó. Vì thế với mọi t ta có

$$\varphi(\epsilon^{tk_1}, \epsilon^{tk_2}, ...) = A_0 + A_1\epsilon^t + ... + A_{p-1}\epsilon^{(p-1)t}.$$

Đặc biệt, ta có $\varphi(1, 1, ...) = \varphi(\epsilon^{pk_1}, \epsilon^{pk_2}, ...) = A_0 + A_1 + ... + A_{p-1}$và $\varphi(\epsilon^{k_1}, \epsilon^{k_2}, ...) + \varphi(\epsilon^{2k_1}, \epsilon^{2k_2}, ...) + ... + \varphi(\epsilon^{pk_1}, \epsilon^{pk_2}, ...) = pA_0$, và do đó tổng này chia hết cho p.

Bây giờ ta chứng minh $\Phi_p(x)$ bất khả quy. Giả sử $\Phi_p(x)$ không bất khả quy. Khi đó $\Phi_p(x) = f(x)g(x)$ với $f(x)$ và $g(x)$ là các đa thức dạng chuẩn bậc dương và có hệ số hữu tỷ. Đặt $\deg f(x) = d$. Vì $f(x)$ và $g(x)$ có hệ số cao nhất bằng 1 và tích $\Phi_p(x) = f(x)g(x)$ là đa thức với hệ số nguyên nên theo Bổ đề 2.3.4 ta suy ra $f(x), g(x) \in \mathbb{Z}[x]$. Viết $f(x) = x^d + a_{d-1}x^{d-1} + ... + a_1x + a_0$. Kí hiệu Ω là tập các căn nguyên thuỷ bậc p của đơn vị, F là tập các nghiệm của $f(x)$ và G là tập các nghiệm của $g(x)$. Khi đó $F \cup G = \Omega$ và $F \cap G = \emptyset$. Kí hiệu F' là tập các nghịch

đảo của các phần tử của F và G' là tập các nghịch đảo các phần tử của G. Khi đó, tương tự ta có $F' \cup G' = \Omega$ và $F' \cap G' = \emptyset$. Kí hiệu $f^*(x)$ là đa thức dạng chuẩn mà các nghiệm của nó là các phần tử của F'. Khi đó

$$f^*(x) = x^d + \left(\frac{a_1}{a_0}\right) x^{d-1} + ... + \left(\frac{a_{d-1}}{a_0}\right) x + \left(\frac{1}{a_0}\right).$$

Ta xét 4 trường hợp sau:

(i) Trường hợp 1: $F' = F$. Khi đó $f^*(x) = f(x)$. Trong trường hợp này, các nghiệm của $f(x)$ xuất hiện thành từng cặp với nhau, do đó $f(x)$ là tích của $d/2$ nhân tử, mỗi nhân tử có dạng $(x-\epsilon)(x-\epsilon^{-1}) = x^2-(\epsilon+\epsilon^{-1})x+1$, chú ý rằng $x^2-(\epsilon+\epsilon^{-1})x+1$ là số dương với mọi số thực x. Kí hiệu F_k là tập các luỹ thừa bậc k của các phần tử của F và $f_k(x)$ là đa thức dạng chuẩn mà các nghiệm của nó là các phần tử của F_k với mỗi $k = 1, \ldots, p-1$. Khi đó $f_k(x)$ cũng có tính chất giống như tính chất của $f(x)$, nghĩa là nó là tích của những đa thức của biến x mà mỗi đa thức đều nhận giá trị dương với mọi số thực x. Đặt $q_k = f_k(1)$ với $k = 1, ..., p-1$. Khi đó $q_1, ..., q_{p-1}$ là các số hữu tỷ dương. Theo lập luận trên, mỗi đa thức $f_k(x)$ đều có các hệ số nguyên, vì thế $q_1, ..., q_{p-1}$ là các số nguyên dương. Nếu $\varphi(x_1, ..., x_d) = (1-x_1)...(1-x_d)$ thì $q_k = \varphi(\epsilon_1^k, ..., \epsilon_d^k)$ với $k = 1, ..., p-1$. Chú ý rằng $F = \{\epsilon_1, ..., \epsilon_d\}$ và $\varphi(\epsilon_1^p, ..., \epsilon_d^p) = \varphi(1, ..., 1) = 0$, do đó từ đẳng thức thứ hai ở trên ta thấy rằng $q_1 + ... + q_{p-1}$ chia hết cho p. Nhận xét rằng $f_1(x)...f_{p-1}(x) = \Phi_p(x)^d$ vì mỗi căn nguyên thuỷ bậc p của đơn vị là nghiệm bội d của đa thức ở vế bên trái của đẳng thức này. Do đó khi thay $x = 1$ ta có được $q_1, ..., q_{p-1} = p^d$. Vì p là số nguyên tố và $d < p-1$ nên trong các số nguyên $q_1, ..., q_{p-1}$, luôn tồn tại g số (với $g > 0$) bằng 1 và các số còn lại đều là luỹ thừa của p, tức là $q_1 + ... + q_{p-1} \equiv g (\mathrm{mod} p)$. Chú ý rằng $1 < 0 < g < p$ nên $q_1 + ... + q_{p-1}$ chắc chắn không chia hết cho p, điều này là mâu thuẫn với khẳng định $q_1 + ... + q_{p-1}$ chia hết cho p ở trên.

(ii) Trường hợp 2: $F \neq F'$ và $T = F \cap F' \neq \emptyset$. Gọi $t(x)$ là đa thức dạng

chuẩn mà nghiệm của nó là các phần tử của T. Khi đó $t(x)$ là *ước chung lớn nhất* của $f(x)$ và $f^*(x)$. Do đó, với lập luận của trường hợp 1 ta suy ra $t(x)$ có ít nhất một hệ số không là số hữu tỷ. Vì $f(x)$ và $f^*(x)$ là các đa thức có các hệ số hữu tỷ nên theo thuật toán tìm ước chung lớn nhất, $t(x)$ phải có hệ số hữu tỷ. Điều này là mâu thuẫn.

(iii) Trường hợp 3: $G \cap G' \neq \emptyset$. Lập luận tương tự như trong trường hợp 1 hoặc trường hợp 2 đối với $g(x)$ ta cũng tìm ra mâu thuẫn tương tự.

(iv) Trường hợp 4: $g = F'$ và $F = G'$. Khi đó ta có

$$\begin{aligned}\Phi_p(x) &= f(x)f'(x)\\ &= (x^d + a_{d-1}x^{d-1} + ... + a_1x + a_0)(x^d + \frac{a_1}{a_0}x^{d-1} + ... + \frac{a_{d-1}}{a_0}x + \frac{1}{a_0}).\end{aligned}$$

Thay $x = 1$ vào ta có được $a_0p = (1 + a_{d-1} + ... + a_0)^2$. Chú ý rằng $f^*(x)$ có các hệ số nguyên. Vì vậy $a_0 = \pm 1$, điều này là vô lí. □

Chứng minh. (Chứng minh của Kronecker năm 1845). Trước tiên chúng ta chứng minh Bổ đề sau: Cho $f(x)$ là một đa thức bất kỳ với hệ số nguyên và ϵ là căn nguyên thuỷ bậc p của đơn vị. Khi đó $f(\epsilon)...f(\epsilon^{p-1})$ và $f(1)$ là hai số nguyên và

$$f(\epsilon)...f(\epsilon^{p-1}) \equiv f(1)^{p-1}(\mathrm{mod} p).$$

Để chứng minh tích $f(\epsilon)...f(\epsilon^{p-1})$ là một số nguyên, ta quan sát thấy rằng $f(\epsilon)...f(\epsilon^{p-1})$ là một đa thức đối xứng của $\{\epsilon, ..., \epsilon^{p-1}\}$. Kí hiệu $r(x)$ là đa thức dạng chuẩn có các nghiệm $\{\epsilon, ..., \epsilon^{p-1}\}$. Khi đó, theo Bổ đề 3.2.1, $f(\epsilon)...f(\epsilon^{p-1})$ là một đa thức hệ số nguyên theo các hệ số của đa thức $r(x)$. Chú ý rằng $r(x)$ chính là đa thức chia đường tròn

$$r(x) = \Phi_p(x) = x^{p-1} + ... + 1.$$

Bây giờ ta chứng minh đồng dư thức ở trên. Đặt $g(x) = f(x)...f(x^{p-1}) = \sum_n A_n x^n$ và xét tổng $\sum_{i=0}^{p-1} g(\epsilon^i)$. Biểu thức thứ nhất của $g(x)$ cho giá trị

là tổng $f(1)^{p-1} + (p-1)f(\epsilon)\dots f(\epsilon^{p-1})$, trong khi đó biểu thức thứ hai của $g(x)$ cho giá trị $\sum_n A_n p$ với tổng chạy trên các bội n của p. Do đó $f(1)^{p-1} + (p-1)f(\epsilon)\dots f(\epsilon^{p-1}) \equiv 0(\mathrm{mod}p)$, Bổ đề được trực tiếp suy ra.

Bây giờ giả sử rằng $\Phi_p(x)$ không bất khả quy. Khi đó $\Phi_p(x) = f(x)g(x)$ là tích của hai đa thức có bậc dương. Chú ý rằng cả hai đa thức $f(x)$ và $g(x)$ đều có hệ số nguyên. Vì thế $p = \Phi_p(1) = f(1)g(1)$ và do đó một trong hai thừa số $f(1)$ hoặc $g(1)$ phải bằng ± 1. Giả sử rằng $f(1) = \pm 1$. Vì ϵ^k là một nghiệm của $\Phi_p(x)$ với mọi k nên $f(\epsilon^k) = 0$ với $k \pm 0(\mathrm{mod}p)$. Mặt khác ta lại có $f(1)^{p-1} \equiv 1(\mathrm{mod}p)$, điều này mâu thuẫn. □

Chứng minh. (Chứng minh của Schonemann năm 1846) Chúng ta có thể kiểm tra được tiêu chuẩn bất khả quy sau đây: Cho $f(x) \in \mathbb{Z}[x]$ là đa thức bậc k. Nếu tồn tại số nguyên tố p và số nguyên a sao cho $f(x) = (x-a)^k + pg(x)$ với $g(x) \in \mathbb{Z}[x]$ thỏa mãn $g(a)$ không chia hết cho p, thì $f(x)$ là đa thức bất khả quy trên $\mathbb{Q}$. Kí hiệu $C_p^i = \dfrac{p!}{(p-i)!i!}$ là số tổ hợp chập i của p phần tử. Vì p là số nguyên tố nên C_p^i là bội của p với mọi $i = 1, \dots, p-1$. Vì thế ta có $x^p - 1 \equiv (x-1)^p(\mathrm{mod}p)$. Suy ra $\Phi_p(x) = \dfrac{x^p - 1}{x-1} \equiv (x-1)^{p-1}(\mathrm{mod}p)$. Vì vậy thì $\Phi_p(x) = x^{p-1} + \dots + 1$. Do đó $\Phi_p(1) = p$ và vì thế $\Phi_p(x)$ thoả mãn giả thiết của tiêu chuẩn bất khả quy ở trên. □

Chứng minh. (Chứng minh của Eisenstein năm 1850). Chúng ta có thể kiểm tra được tiêu chuẩn bất khả quy sau đây, gọi là *tiêu chuẩn Eisenstein*. Cho $f(x) = c_k x^k + \dots + c_0 \in \mathbb{Z}[x]$ là một đa thức và p là số nguyên tố sao cho hệ số cao nhất c_k không chia hết cho p, các hệ số khác $c_{k-1}, \dots, c_0$ đều chia hết cho p và hệ số tự do c_0 không chia hết cho p^2. Khi đó $f(x)$ là đa thức bất khả quy trên $\mathbb{Q}$. Bây giờ ta áp dụng tiêu chuẩn này để chứng minh tính bất khả quy của đa thức chia đường tròn $\Phi_p(x)$. Rõ ràng đa thức này

là bất khả quy khi và chỉ khi $\Phi_p(x+1)$ là bất khả quy. Ta có

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + a_{p-2}x^{p-2} + ... + a_1 x + p.$$

Rõ ràng các hệ số của $\Phi_p(x+1)$ thỏa mãn giả thiết của tiêu chuẩn Eidenstein đối với số nguyên tố p này. Vì thế $\Phi_p(x)$ bất khả quy trên $\mathbb{Q}$. □

3.2.3 Chú ý. Tiêu chuẩn bất khả quy của Schonemann và cách chứng minh của Schonemann về tính bất khả quy của đa thức $\Phi_p(x)$ bây giờ ít được nhớ đến, còn tiêu chuẩn bất khả quy của Eisenstein và cách chứng minh của Eisenstein về tính bất khả quy của đa thức $\Phi_p(x)$ rất nổi tiếng, đã trở thành chứng minh chuẩn mực cho đến tận ngày nay. Nhưng trong thực tế thì tiêu chuẩn và cách chứng minh của cả hai ông là tương đương nhau. Khẳng định này được D. A. Cox đưa ra trong một hội nghị năm 2011 về Toán học và Lịch sử Toán.

KẾT LUẬN

Trong luận văn này, chúng tôi đã trình bày các nội dung sau đây về đa thức chia đường tròn:

- Trình bày khái niệm đa thức chia đường tròn $\Phi_n(x)$ và một số tính chất cơ sở của đa thức chia đường tròn. Chứng tôi chứng minh công thức $x^n - 1 = \prod_{d|n} \Phi_d(x)$ và từ đó suy ra $\Phi_n(x) \in \mathbb{Z}[x]$, đồng thời chỉ ra rằng nếu $x \in \mathbb{Z}$ và p là một ước nguyên tố của $\Phi_n(x)$ thì $p \equiv 1 \pmod{n}$ hoặc $p|n$.

- Trình bày một số ứng dụng của đa thức chia đường tròn. Chúng tôi sử dụng các tính chất của đa thức chia dường tròn để chứng minh một Định lý của Dirichlet và giải quyết một số bài toán thi học sinh giỏi toán quốc tế liên quan đến phương trình nghiệm nguyên và đánh giá số ước của một số tự nhiên.

- Đưa ra một số phương pháp xét tính bất khả quy của đa thức chia đường tròn $\Phi_p(x)$ với p là số nguyên tố như phương pháp của Gauss 1801, phương pháp của Kronecker năm 1845, phương pháp của Schonemann năm 1846, và phương pháp của Eisenstein năm 1850.

Tài liệu tham khảo

[D] R. Dedekind, *Beweis făur die Irreduktibilităat der Kreisteilungsgleichung*, J. reine angew. Math., **54** (1857), 27-30

[E] F. G. Eisenstein, *Uber die Irreductibilitat und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhangt*, J. reine angew. Math., **39** (1850), 160-179.

[Gau] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801 (Bản dịch sang tiếng Đức bởi H. Maser, xuất bản bởi AMS 2006).

[Ge] Y. Ge, *Elementary Properties of Cyclotomic Polynomials*, Preprint (PDF from drchristiansalas.org.uk, from it-hiroshima.ac.jp)

[K] L. Kronecker, *Beweis dass făur jede Primzahl p die Gleichung* $1 + x + \ldots + x^{p-1} = 0$ *irreductibel ist*, J. reine angew. Math., **29** (1845), 280.

[K2] L. Kronecker, *Memoire sur les facteures irreductibles de L'expression* $x^n - 1$, J. Math. Pure et Appls, **19** (1854), 177-192.

[Sc] A. Schinzel, *Polynomials with special regards to reducibility*, Cambridge University Press (2000).

[Sch] T. Schoenemann, *Von denjenigen Moduln welche potenzen von primzahlen sind*, J. reine angew. Math., **32** (1846), 93-105.

[W1] S. H. Weintraub, *Galois Theory*, Springer Verlag, New York (2009), second edition.

[W2] S. H. Weintraub, *Several proofs of the irreducibility of the cyclotomic polynomial*, Preprint (PDF from lehigh.edu.)