New relation for the coefficients of cyclotomic polynomials

Hajime Kaneko
Institute of Mathematics, University of Tsukuba
Research Core for Mathematical Sciences, University of Tsukuba

概 要

本稿では, 秋山茂樹氏との共同研究論文 [1] の内容について解説をする (証明は省略). 本研究において, 円分多項式の係数に関する新しい種類の合同式が得られた. 円分多項式の係数に関する Lehmer の予想など, 本研究の周辺の研究も含めて紹介する.

1 序論

正整数 n に対して, n 次の円分多項式を

$$\Phi_n(x) = \prod_{\substack{0<d<n \\ (d,n)=1}} \left(x - \exp\left(\frac{2\pi d i}{n}\right)\right) \tag{1.1}$$

により記す. ただし $i = \sqrt{-1}$ である. 本稿では, 円分多項式を $x = 0$ および $x = 1$ で Taylor 展開する際に現れる係数を調べる. 本節では, $x = 0$ における展開について, 知られている性質を紹介する. さて,

$$\Phi_n(x) = \sum_{m=0}^{\phi(n)} c(n;m) x^m$$

とおく. ただし, ϕ は Euler の totient 関数である. $n \leq 104$ のとき, 円分多項式 $\Phi_n(x)$ の係数 $c(n;m)$ には $-1, 0, 1$ しか現れない. ところが $n = 105$ のとき, $c(105, 7) = -2$ が現れる. 鈴木 治郎氏 [17] は, 任意の整数 a に対して, $c(n;m) = a$ となる n, m が存在することを示した. また, n を固定する. このとき, $\Phi_n(x)$ の係数の最大絶対値

$$A_n := \max\{|c(n;m)| \mid 0 \leq m \leq \phi(n)\}$$

も研究されている. Erdős[5] は, ある正定数 C が存在して, 以下が成立することを示した. 無限に多くの n に対して,

$$A_n > \exp\left(\exp\left(\frac{C \log n}{\log\log n}\right)\right). \tag{1.2}$$

さらに, Vaughan[18] は $C = \log 2$ に対して, (1.2) が成立することを示した. 一方, Bateman[2] は $n \to \infty$ のとき,

$$A_n < \exp\left(\exp\left(\log 2 + o(1)\right) \cdot \frac{\log n}{\log\log n}\right)$$

であることを示した. 特に, Vaughan の定数 $C = \log 2$ は最善である.

2 $x = 1$ における円分多項式の Taylor 展開

円分多項式 $\Phi_n(x)$ の $x = 1$ における Taylor 展開の係数を考察するための研究動機を述べる. 本瀬 香氏 [11, 12] は, $\Phi_n(x)$ が $x > 1$ において単調増加であることを証明しようと試みた. 単調増加性の証明は, 本瀬 香氏が和書 [19, 20] で述べている[1]. ここでは, その証明を記載する.

命題 2.1. n を任意の正の整数とする. このとき, 任意の $j = 1, 2, \ldots, \phi(n)$ に対して, $\Phi_n^{(j)}(1) > 0$ である. 特に, $\Phi_n(x)$ は $x > 1$ において単調増加である.

Proof. $\Phi_1(x) = x - 1$ および $\Phi_2(x) = x + 1$ に対しては, 命題が成立することを容易に確認できる. 以下, $n \geq 3$ とする. すると,

$$\begin{aligned}\Phi_n(x) &= \prod_{\substack{0<d<n/2\\(d,n)=1}} \left(x - \exp\left(\frac{2\pi d i}{n}\right)\right)\left(x - \exp\left(\frac{2\pi (n-d) i}{n}\right)\right)\\ &= \prod_{\substack{0<d<n/2\\(d,n)=1}} \left(x^2 - 2\cos\left(\frac{2\pi d}{n}\right)x + 1\right) \qquad (2.1)\end{aligned}$$

である. ここで, $-2 < b < 2$ を満たす任意の実数 b に対して,

$$(x+1)^2 + b(x+1) + 1 = x^2 + (b+2)x + b + 2$$

の係数はすべて正であることに注意する. よって, 式 (2.1) の積を展開すると,

$$\Phi_n(x+1) = \sum_{j=0}^{\phi(n)} \frac{\Phi_n^{(j)}(1)}{j!} x^j$$

の係数はすべて正であることがわかる. よって, 命題が示された. □

円分多項式の微分 $\Phi_n^{(j)}(1)$ に関する明示公式は, 古くから研究されてきた. ただし, ここでは便宜上 $j = 0$ の場合も含めて考察する. 以降, 本稿では単純化のために $n \geq 3$ の場合のみを考える. Lebesque[8] は,

$$\Phi_n(1) = \exp(\Lambda(n)) = \begin{cases} p & (n = p^e, p \text{は素数}, e \text{は正整数}),\\ 1 & (otherwise)\end{cases}$$

[1] 参考文献 [20] では, イギリスの人が証明を注意した, と記述されている.

であることを証明した．ただし，Λ は von Mangoldt 関数である．$j \geq 1$ のときには，Hölder[7](c.f. [3, Lemma 10]) が

$$\Phi_n'(1) = \frac{1}{2}\phi(n)\Phi_n(1)(> 0)$$

であることを証明した．

補足 2.2. $\Phi_n(x)$ の $[1,\infty)$ における単調増加性は，実は $\Phi_n'(1) > 0$ から従う．実際，Gauss-Lucas theorem より $\Phi_n'(z)$ の任意の零点は，$\Phi_n(z)$ の零点の凸閉包に属する．$n \geq 3$ および式 (1.1) より，$\Phi_n(z)$ は右半平面

$$\{z = a + bi \mid a \geq 1\}$$

上に零点を持たない．したがって，$\Phi_n'(z)$ は $[1,\infty)$ 上に零点を持たない．特に，$\Phi_n'(1) > 0$ から $\Phi_n'(a) > 0$ が任意の実数 $a \geq 1$ に対して成立する．

$j \geq 2$ のとき，$\Phi_n^{(j)}(1)/\Phi_n(1)$ に対する明示式が Lehmer によって考察された．証明には対数微分法が用いられる．j が小さいときの具体例に対して，数値実験により観察される現象がある．この現象について秋山茂樹氏からセミナーで説明を受けたことが，本研究の始まりである．

さて，Lehmer の明示式を紹介する準備のために，Jordan の totient 関数を導入する．$\mu(n)$ を Möbius 関数とする．このとき，正整数 k に対して $J_k(n) = \sum_{d|n} \mu(n/d)d^k$ とおく．すると，

$$J_k(n) = n^k \prod_{p|n}\left(1 - \frac{1}{p^k}\right)$$

であることに注意する．ただし，p は n を割り切る素数を動くとする．定義により $\phi(n) = J_1(n)$ である．よって Jordan の totient 関数は Euler の totient 関数の一般化である．

補足 2.3. Jordan は，$\mathbb{Z}/n\mathbb{Z}$ 上の一般線型群 $GL_k(\mathbb{Z}/n\mathbb{Z})$ における元の個数の明示公式に totient 関数を用いた．この公式は以下のように表される:

$$\text{Card } (GL_k(\mathbb{Z}/n\mathbb{Z})) = n^{k(k-1)/2}\prod_{j=1}^{k} J_j(n).$$

定理 2.4 (Lehmer[9])**.** $\ell \geq 2$ とする．$h = \lfloor(\ell+1)/2\rfloor$ とする．すると，有理係数多項式 $F_\ell(Y, X_1, X_2, \ldots, X_h)$ が存在して，以下を満たす: 正整数 n が $\phi(n) \geq \ell$ を満たせば，

$$\frac{\Phi_n^{(\ell)}(1)}{\Phi_n(1)} = F_\ell(\phi(n), J_2(n), J_4(n), \ldots, J_{2h}(n)).$$

定理 2.4 における多項式 F_ℓ が一意的に定まるかどうかは証明が与えられていない．数論的関数 $\phi, J_2, J_4, \ldots, J_{2h}$ の代数的独立性を証明できれば，多項式 F_ℓ の一意性は保証できる．以下，F_ℓ は Lehmer の証明により構成されたものを用いる．

さて, 定理 2.4 の具体例を挙げる:

$$\begin{aligned}
\frac{\Phi_n^{(2)}(1)}{\Phi_n(1)} =& \frac{J_2(n)}{12} + \frac{\phi(n)^2}{4} - \frac{\phi(n)}{2},\\
\frac{\Phi_n^{(3)}(1)}{\Phi_n(1)} =& \frac{(\phi(n)-2)(J_2(n)+\phi(n)(\phi(n)-4))}{8},\\
\frac{\Phi_n^{(4)}(1)}{\Phi_n(1)} =& \frac{1}{240}\Big(30J_2(n)\phi(n)^2 - 180J_2(n)\phi(n) + 5J_2(n)^2 + 220J_2(n) - 2J_4(n)\\
&+ 15\phi(n)^4 - 180\phi(n)^3 + 660\phi(n)^2 - 720\phi(n)\Big),\\
\frac{\Phi_n^{(5)}(1)}{\Phi_n(1)(\phi(n)-4)} =& \frac{1}{96}\Big(3\phi(n)^4 - 48\phi(n)^3 + 10J_2(n)\phi(n)^2 + 228\phi(n)^2\\
&- 80J_2(n)\phi(n) - 288\phi(n) + 5J_2(n)^2 + 100J_2(n) - 2J_4(n)\Big).
\end{aligned}$$

さて, $\Phi_n^{(3)}(1)/\Phi_n(1)$ および $\Phi_n^{(5)}(1)/\Phi_n(1)$ がそれぞれ $\phi(n)-2$ および $\phi(n)-4$ で割り切れていることに着目する. この観察が, 本稿の主結果である関係式と関連がある.

Lehmer は, Stirling 数や Bernoulli 数を用いて, 定理 2.4 における多項式 $F_\ell(Y, X_1, X_2, \ldots, X_h)$ 具体的表示を与えた. また, [13, 6, 10, 14] が関連文献である.

改めて,

$$\Phi_n(x+1) =: \sum_{h=0}^{\phi(n)} b_n(h)x^h$$

とおく. ただし, $b_n(h) = \Phi_n^{(h)}(1)/h!(\in \mathbb{Z})$ である. Lehmer[9] は定理 2.4 以外に, $b_n(h)$ に関する命題を, 証明なしで述べている. 実数 R および正整数 ℓ に対して,

$$R^{[\ell]} := R(R-1)\cdots(R-\ell+1)$$

とおく. また, 正整数 r に対して, $t_r := J_r(n)/(2r)$ とおく. さらに, ベルヌーイ数 B_m $(m \geq 0)$ を

$$\frac{te^t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

により定義する. このとき, Lehmer は

$$\frac{b_n(h)}{\Phi_n(1)} = t_1^{[h]} + 2\sum_{\ell=1}^{\infty} B_{2\ell}\binom{h}{2\ell}(t_1-\ell)^{[h-2\ell]}\Omega_\ell \tag{2.2}$$

であると主張した. ただし, Ω_ℓ については, 最初の数項

$$\begin{aligned}
\Omega_1 &= t_2,\\
\Omega_2 &= t_4 - 5t_2^{[2]},\\
\Omega_3 &= t_6 - 7t_4(t_2-1) + \frac{35}{3}t_2^{[3]} + \frac{14}{3}t_2,\\
\Omega_4 &= t_8 - \frac{20}{3}t_6(t_2-1) - \frac{7}{3}t_4^{[2]} + \frac{70}{3}t_4(t_2-1)^{[2]}\\
&\qquad - \frac{175}{9}t_2^{[4]} + \frac{10}{3}t_6 - \frac{280}{9}t_2^{[2]} + \frac{290}{9}t_2
\end{aligned}$$

が書かれているだけで, 具体的な定義は書かれていない.

さて, 式 (2.2) において, h が奇数 $2k+1$ である場合を考える. 等式

$$\frac{b_n(2k+1)}{\Phi_n(1)} = t_1^{[2k+1]} + 2\sum_{\ell=1}^{k} B_{2\ell}\binom{2k+1}{2\ell}(t_1-\ell)^{[2k+1-2\ell]}\Omega_\ell$$

において, 右辺の有限和はそれぞれ $t_1 - k = J_1(n)/2 - k = (\phi(n)-2k)/2$ で割り切ることができる. ここで, $2k+1-2\ell$ は決して 0 にはならないことに注意する.

さて, 式 (2.2) が成立すると仮定する. さらに, Ω_ℓ が t_2 などの多項式で書けると仮定すれば, 以下の予想が成立する:

予想 2.5. k を非負整数とする. すると, 定理 2.4 における多項式 $F_{2k+1}(Y, X_1, X_2, \ldots, X_h)$ は $Y - 2k$ で割り切れる. つまり, $\Phi_n^{(2k+1)}(1)/\Phi_n(1)$ を $\phi(n), J_2(n), J_4(n), \ldots, J_{2h}(n)$ の多項式として表示するとき, その多項式は $\phi(n) - 2k$ で割り切ることができる.

次の節では, 多項式としての整除性ではなく, 整数として $\Phi_n^{(2k+1)}(1)/\Phi_n(1)$ が $\phi(n)-2k$ で割り切れるかどうかを考察する. なお, 予想 2.5 を, 京都大学数理解析研究所の本研究集会において紹介した. その後に松坂俊輝氏から, 予想を証明したとの報告を受けた.

3 主結果

次の定理は, 整数としての整除性に関する結果である.

定理 3.1. (i) $2\Phi_n'''(1)$ は $\phi(n)-2$ で割り切れる. さらに, $\phi(n)$ が 4 で割り切れるならば, $\Phi_n'''(1)$ は $\phi(n)-2$ で割り切れる.
(ii) $k \geq 2$ とする. すると, $\Phi_n^{(2k+1)}(1)$ は $\phi(n)-2k$ で割り切れる.

具体的な k に対して, 例えば $k \leq 15$ の場合, 定理 3.1 の結果は直接証明できる. 定理 2.4 における多項式 F_{2k+1} を具体的に求めればよい. このとき, Jordan の totient 関数に関する合同式を用いる. この合同式は単独で興味深いために, 本稿で紹介する. $\lambda(m)$ を Carmichael の lambda 関数とする. つまり, $\mathbb{Z}/m\mathbb{Z}$(c.f. [4, 13]) の単元群を $(\mathbb{Z}/m\mathbb{Z})^\times$ とすると,

$$\lambda(m) = \min\{h \geq 1 \mid \text{任意の } a \in (\mathbb{Z}/m\mathbb{Z})^\times \text{ に対し, } a^h = 1\}$$

により定義される．なお, $\lambda(m)$ の具体的な値は, 以下に述べる方法により具体的に計算をすることができる．m の素因数分解を $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ とする．ただし, $p_1, p_2, \ldots, p_r$ は互いに異なる素数であり, $e_1, e_2, \ldots, e_r$ は正整数とする．すると, 中国剰余定理より,

$$\lambda(m) = \mathrm{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r}))$$

である．ただし, lcm は最小公倍数を表す．さて, p を奇素数とすると, 任意の正整数 e に対して $(\mathbb{Z}/p^e\mathbb{Z})^\times$ は巡回群である．よって $\lambda(p^e) = \phi(p^e)$ である．一方, e が 2 以上の整数のとき,

$$(\mathbb{Z}/2^e\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{e-2}\mathbb{Z}$$

である．特に,

$$\lambda(2^e) = \begin{cases} 1 & e = 1, \\ 2 & e = 2, \\ 2^{e-2} & e \geq 3 \end{cases}$$

が成立する．

命題 3.2. $k \geq 3$ とし, $n \geq k+2$ とする．すると,

$$J_k(n) \equiv 0 \pmod{\prod_{\lambda(p^e)\|k} p^e} \tag{3.1}$$

が成立する．一方, $M > \prod_{\lambda(p^e)\|k} p^e$ をみたす整数 M と正整数 n_0 を任意に選ぶ．すると, $n \geq n_0$ となる整数 n で, 以下を満たすものが存在する:

$$J_k(n) \not\equiv 0 \pmod{M}.$$

上記の意味で, 合同式 (3.1) は最善である．

例えば, $k = 1$ のときを考察する．$n \geq 3$ のとき, 合同式 (3.1) は

$$J_1(n) = \phi(n) \equiv 0 \pmod{2}$$

という有名な関係式を表す．さらなる具体例を表すため, $\prod_{\lambda(p^e)\|k} p^e$ の表を以下に記載する．なお, [16] も参照.

k	奇数	2	4	6	8	10	12	14	16	18	20
$\prod_{\lambda(p^e)\|k} p^e$	2	24	240	504	480	264	65520	24	16320	28728	13200

一般の k に対する定理 3.1 は, 円分多項式の係数に関する関係式から導かれる．まず, $n \geq 3$ のとき, $\Phi_n(x)$ は (偶数次数の) 自己相反多項式であることに注意する．すなわち, $x^{\phi(n)}\Phi_n(x^{-1}) = \Phi_n(x)$ である．よって, $y = x + x^{-1}$ とおくと, ある $g(y) \in \mathbb{Z}[y]$ が存在して, $\Phi_n(x) = x^{\phi(n)/2}g(y)$ が成立する．さて,

$$\Phi_n(x+1) =: \sum_{h=0}^{\phi(n)} b(h)x^h, \quad g(y+2) =: \sum_{\ell=0}^{\phi(n)/2} a(\ell)y^\ell$$

とおく．すると, 以下が成立する:

命題 3.3. $0 \le h \le \phi(n)$ を満たす任意の h に対して,

$$b(h) = \sum_{\ell=0}^{\lfloor h/2 \rfloor} \binom{\phi(n)/2 - \ell}{h - 2\ell} a(\ell) \tag{3.2}$$

が成立する.

ζ_n を 1 の原始 n 乗根の一つとする. 命題 3.3 は, $\zeta_n + \zeta_n^{-1} - 2$ の最小多項式の係数を用いて $\Phi_n^{(h)}(1)$ を表示したものである. なお, 式 (3.2) における 2 項係数を調べることにより, 定理 3.1 は証明することができる. 実は, 円分多項式のみならず, 一般の自己相反多項式に対して定理 3.1 および命題 3.3 の一般化が成立するので, 次節で紹介する.

補足 3.4. h が奇数 $2k+1 (k \ge 2)$ のとき, (3.2) の 2 項係数における $h - 2\ell = 2k + 1 - 2\ell$ は決して 0 にはならない. このことにより, $\Phi_n^{(2k+1)}(1)$ は $\phi(n) - 2k$ で割り切れる. 一方, h が偶数のとき, $h - 2\ell = 0$ となる場合があるため, 整除関係が成立しない.

4 自己相反多項式の係数の関係式

論文 [1] の投稿時点では, 組み合わせ論を用いた少し複雑な議論により, 命題 3.3 を証明していた. レフェリーコメントをもとに, 一般の自己相反多項式に対する関係式に発展させることができた. このことにより, 関係式がより鮮明となった. その結果, 秋山茂樹氏が現在のシンプルな証明を思いつくに至った.

さて, $f(x) \in \mathbb{Z}[x]$ を次数が偶数 $2q (\ge 2)$ の自己相反多項式とする. すると, $x^{2q} f(x^{-1}) = f(x)$ である. また, $y = x + x^{-1}$ とおくと, ある $g(y) \in \mathbb{Z}[y]$ が存在して, $f(x) = x^q g(y)$ が成立する. さて,

$$f(x+1) =: \sum_{h=0}^{2q} \beta(h) x^h, \quad g(y+2) =: \sum_{\ell=0}^{q} \alpha(\ell) y^\ell$$

とおく. ただし, $\beta(2q) = \alpha(q)$ である. すると, 以下が成立する:

命題 4.1. $0 \le h \le 2q$ を満たす任意の h に対して,

$$\beta(h) = \sum_{\ell=0}^{\lfloor h/2 \rfloor} \binom{q - \ell}{h - 2\ell} \alpha(\ell) \tag{4.1}$$

が成立する.

命題 4.1 において 2 項係数を注意深く調べると, 以下の関係式を導くことができる:

命題 4.2. (i) $2f'''(1)$ は $2q - 2$ で割り切れる. さらに, q が偶数ならば, $f'''(1)$ は $2q - 2$ で割り切れる.
(ii) $k \ge 2$ とする. すると, $f^{(2k+1)}(1)$ は $2q - 2k$ で割り切れる.

補足 4.3. 命題と同様の手法が, [15] の Proposition 2 において渋川 元樹氏により導入されている. また, [15] では超幾何関数の応用により, 更なる関係式が導き出されている.

謝辞

Pieter Moree 氏と Michel Marcus 氏に, 貴重なコメントおよび参考文献についてお知らせいただき, 感謝申し上げます. 渋川 元樹氏には, 和書 [19, 20] に関する貴重な情報等のご提供, 感謝申し上げます. 本研究は JSPS 科研費 (19K03439) の助成を受けたものです.

参考文献

[1] S. Akiyama, H. Kaneko, Curious congruences for cyclotomic polynomials, Res. Number Theory **8** (2022), no. 4, Paper No. 102, 10 pp.

[2] P. T. Bateman, Note on the coefficients of the cyclotomic polynomial, Bull. Amer. Math. Soc. **55** (1949), 1180–1181.

[3] B. Bzdęga, A. Herrera-Poyatos, P. Moree, Cyclotomic polynomials at roots of unity. Acta Arith. **184** (2018), no. 3, 215–230.

[4] R. D. Carmichael, Note on a new number theory function. Bull. Amer. Math. Soc. 16 (1910), no. 5, 232–238.

[5] P. Erdős, On the coefficients of the cyclotomic polynomial, Portugal. Math. **8** (1949), 63–71.

[6] A. Herrera-Poyatos, P. Moree, Coefficients and higher order derivatives of cyclotomic polynomials: Old and new. Expo. Math. **39** (2021), no. 3, 309–343.

[7] O. Hölder, Zur theorie der Kreisteilungsgleichung $k_m(x) = 0$, Prace Mat. Fiz **43** (1936), 13–23.

[8] V.-A. Lebesgue, Démonstration de l'irréductibilité de l'équation aux racines primitives de l'unité, Journal de mathématiques pures et appliquées 2 e série, tome 4 (1859), p. 105–110.

[9] D. H. Lehmer, Some properties of the cyclotomic polynomial. J. Math. Anal. Appl. **15** (1966), 105–117.

[10] P. Moree, S. S. Eddin, A. Sedunova, Y. Suzuki, Jordan totient quotients, J. Number Th. **209** (2020), 147–166.

[11] K. Motose, On values of cyclotomic polynomials. VII. Bull. Fac. Sci. Technol. Hirosaki Univ. **7** (2004), no. 1, 1–8.

[12] K. Motose, Ramanujan's sums and cyclotomic polynomials. Math. J. Okayama Univ. **47** (2005), 65–74.

[13] J. Sándor, B. Crstici, Handbook of number theory. II. Kluwer Academic Publishers, Dordrecht, 2004.

[14] C. Sanna, A survey on coefficients of cyclotomic polynomials, Expo. Math. **40** (2022), no. 3, 469–494.

[15] G. Shibukawa, New identities for some symmetric polynomials, and a higher order analogue of the Fibonacci and Lucas numbers, Fibonacci Quart. **58** (2020), no. 5, 200–221.

[16] N.J.A. Sloane, Entry A079612 in The On-Line Encyclopedia of Integer Sequences, OEIS Foundation Inc. (2022), http://oeis.org/A079612

[17] J. Suzuki, On coefficients of cyclotomic polynomials, Proc. Japan Acad. Ser. A Math. Sci. **63** (1987), no. 7, 279–280.

[18] R. C. Vaughan, Bounds for the coefficients of cyclotomic polynomials, Michigan Math. J. **21** (1974), 289–295 (1975).

[19] 本瀬 香, 円分多項式・有限群の指標, 弘前大学出版会, 2006 年.

[20] 本瀬 香, 三角形の独り言, 弘前大学出版会, 2017 年.