円分多項式の係数

金沢光則

平成 11 年 11 月 1 日

1 はじめに

数学科の 3 年生の自主ゼミで、van der Waerden を読んでいて、素体上の円分多項式が出てきた。それが標数に依らないと書いてあり、係数が 0, 1, -1 しかないんじゃないかという話になった。探してみたら Φ_{105} の係数に 2 が現れるとある。また、Φ_n $(n = 1, 2, \cdots, 100)$ の係数には 0, 1, -1 しか現れないそうである。それじゃあ、$105 = 3 \times 5 \times 7$ だから、$n = pq$ (p, q は異なる素数) なら成り立つんじゃないかと言う話になった。
ここでは、$\Phi_{pq}(x)$, $\Phi_{2^k pq}(x)$ に現れる係数が 0, 1, -1 であることを示し、Φ_n $(n = 1, 2, \cdots, 104)$ について成り立つことを見る。

2 円分多項式

2.1 定義

n を正の整数とするとき、x の方程式 $x^n = 1$ の根を 1 の累乗根という。$\zeta = e^{2\pi\sqrt{-1}/n} = \cos\dfrac{2\pi}{n} + \sqrt{-1}\sin\dfrac{2\pi}{n}$ と置くとき、$1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$ が累乗根の全体である。
ある数 t が $t^n = 1$ をみたすとしても、n の真に n より小さい正の約数 d に対して、$t^d = 1$ となるかも知れない。そうならないとき、t を原始的と呼ぶ。
これら原始 n 乗根全体を根に持つ $\mathbb{Q}$ 上の既約多項式を円分多項式と呼び、$\Phi_n(x)$ で表す。
以下、p, q は、異なる素数を表すとする。

2.2 基本公式

$x^n = 1$ となる根は、n のある約数に関して原始的であり、原始的であるような約数は 1 つしかないから

$$x^n - 1 = \Pi_{d \mid n} \Phi_d(x)$$

が成り立つ。これから次が成り立つ。

$$\Phi_n(x) = \frac{x^n - 1}{\Pi_{d \mid n,\ d \neq n} \Phi_d(x)}$$

特に、p を素数とすると、約数は 1, p しかないから、

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

この係数はすべて 1 である。

3　いくつかの公式

必要となるいくつかの公式をあげる。

3.1　Φ_{p^n}

n を正の整数とする。このとき、

$$\begin{aligned}
\Phi_{p^n}(x) &= \frac{x^{p^n}-1}{\Phi_1\Phi_p\Phi_{p^2}\cdots\Phi_{p^{n-1}}} \\
&= \frac{x^{p^{n-1}}-1}{\Phi_1\Phi_p\Phi_{p^2}\cdots\Phi_{p^{n-2}}}\frac{x^{p^n}-1}{(x^{p^{n-1}}-1)\Phi_{p^{n-1}}} \\
&= \Phi_{p^{n-1}}(x)\frac{\Phi_p(x^{p^{n-1}})}{\Phi_{p^{n-1}}(x)} \\
&= \Phi_p(x^{p^{n-1}})
\end{aligned}$$

3.2　$\Phi_{p^nq^m}(x)$

n, m を正の整数とする。このとき、

$$\begin{aligned}
\Phi_{p^nq^m}(x) &= \frac{x^{p^nq^m}-1}{\prod_{d\mid p^nq^m,\ d\neq p^nq^m}\Phi_d} \\
&= \frac{x^{p^nq^m}-1}{(\prod_{d\mid p^{n-1}q^m}\Phi_d)\times(\prod_{d\mid q^m,\ d\neq q^m}\Phi_{p^nd})} \\
&= \frac{x^{p^nq^m}-1}{(x^{p^{n-1}q^m}-1)\times(\prod_{d\mid q^m,\ d\neq q^m}\Phi_{p^nd})} \\
&= \frac{\Phi_p(x^{p^{n-1}q^m})}{\prod_{d\mid q^m,\ d\neq q^m}\Phi_{p^nd}} \\
&= \frac{\Phi_p(x^{p^{n-1}q^m})}{\prod_{k=0}^{m-1}\Phi_{p^nq^k}}
\end{aligned}$$

$m=1$ のときは、

$$\Phi_{p^nq}(x)=\frac{\Phi_p(x^{p^{n-1}q})}{\Phi_{p^n}(x)}=\frac{\Phi_p(x^{p^{n-1}q})}{\Phi_p(x^{p^{n-1}})}$$

$m>1$ のときは、

$$\begin{aligned}
\frac{\Phi_{p^nq^m}(x)}{\Phi_{p^nq^{m-1}}(x)} &= \frac{\Phi_p(x^{p^{n-1}q^m})}{\prod_{k=0}^{m-1}\Phi_{p^nq^k}}\times\frac{\prod_{k=0}^{m-2}\Phi_{p^nq^k}}{\Phi_p(x^{p^{n-1}q^{m-1}})} \\
&= \frac{\Phi_p(x^{p^{n-1}q^m})}{\Phi_{p^nq^{m-1}}(x)}\times\frac{1}{\Phi_p(x^{p^{n-1}q^{m-1}})}
\end{aligned}$$

より、

$$\Phi_{p^nq^m}(x)=\frac{\Phi_p(x^{p^{n-1}q^m})}{\Phi_p(x^{p^{n-1}q^{m-1}})}$$

これは、$m=1$ のときも成り立つ。

4　円分多項式に現れる係数

$\Phi_{p^n}(x)=\Phi_p(x^{p^{n-1}})$ ゆえ、円分多項式 $\Phi_{p^n}(x)$ に現れる係数は、0 または 1 である。

$$\Phi_{p^nq^m}(x)=\frac{\Phi_p(x^{p^{n-1}q^m})}{\Phi_p(x^{p^{n-1}q^{m-1}})}$$

において、$t=x^{p^{n-1}q^{m-1}}$ とおくと、

$$\Phi_{p^nq^m}(x)=\frac{\Phi_p(t^q)}{\Phi_p(t)}=\Phi_{pq}(t)$$

ゆえ、$\Phi_{p^nq^m}(x)$ に現れる係数が $0,\ 1,\ -1$ のいずれかであることを示すためには、$n=1,\ m=1$ の場合を示せば十分であることがわかる。

4.1　$\Phi_{pq}(x)$ の係数

$$\begin{aligned}\Phi_{pq}(x)-1 &= \frac{\Phi_p(x^q)}{\Phi_p(x)}-1\\ &= \frac{(x^q)^{p-1}+(x^q)^{p-2}+\cdots+(x^q)+1}{x^{p-1}+x^{p-2}+\cdots+x+1}-1\\ &= \frac{\{(x^q)^{p-1}+(x^q)^{p-2}+\cdots+(x^q)+1\}(x-1)}{x^p-1}-1\\ &= \frac{\{(x^q)^{p-1}+(x^q)^{p-2}+\cdots+(x^q)+1-(x^{p-1}+x^{p-2}+\cdots+x+1)\}(x-1)}{x^p-1}\end{aligned}$$

よって、定数項を除けば、

$$(x^q)^{p-1}+(x^q)^{p-2}+\cdots+(x^q)+1-(x^{p-1}+x^{p-2}+\cdots+x+1)$$

が x^p-1 で割り切れ、かつ商の係数が 0 または 1 であることを示せばよい。定数項については、$x=0$ を代入すれば分かるように 1 である。
$(x^q)^{p-1},\ (x^q)^{p-2},\ \cdots,\ (x^q),\ 1$ に現れる x の指数 $0,\ q,\ 2q,\ 3q,\ \cdots,\ (p-1)q$ は p を法としてすべて異なる。$(x^q)^k$ の指数を $ap+b$ と表しておく。(ここで a は商、b は余り。) このとき、同じあまりを持つ $x^{p-1}+x^{p-2}+\cdots+x+1$ の中の項 x^b がただ一つ存在し、

$$\begin{aligned}x^{ap+b}-x^b &= x^b(x^{ap}-1)\\ &= x^b\{(x^p)^a-1\}\\ &= x^b(x^p-1)\{(x^p)^{a-1}+(x^p)^{a-2}+\cdots+(x^p)+1\}\end{aligned}$$

従って、x^p-1 で割り切れ、商は

$$x^b\{(x^p)^{a-1}+(x^p)^{a-2}+\cdots+(x^p)+1\}$$

となる。特に、指数は p を法として b であるから、他の $x^{ap+b'}-x^{b'}$ から生じた商の中に現れる項とは同じ指数を持たない。
$\Phi_{pq}(x)$ は、これらの商の和として現れるから、$\Phi_{pq}(x)$ の係数は $0,\ 1,\ -1$ のいずれかである。

4.2 $\Phi_{2^k pq}(x)$

ここでは、さらに 2, p, q を互いに異なる素数とする。まず $k=1$ のときの式を求める。

$$\begin{aligned}
\Phi_{2pq}(x) &= \frac{x^{2pq}-1}{\Phi_1\Phi_2\Phi_p\Phi_{2p}\Phi_q\Phi_{2q}\Phi_{pq}} \\
&= \frac{(x^{pq}-1)(x^{pq}+1)}{(\Phi_1\Phi_p\Phi_q)\times(\Phi_{pq})\times(\Phi_2\Phi_{2p}\Phi_{2q})} \\
&= \frac{\Phi_{pq}\times(x^{pq}+1)}{(\Phi_{pq})\times(\Phi_2\Phi_{2p}\Phi_{2q})} \\
&= \frac{x^{pq}+1}{\Phi_2\Phi_{2p}\Phi_{2q}} \\
&= \frac{(x^{pq}+1)}{(x+1)}\frac{\Phi_2(x)}{\Phi_2(x^p)}\frac{\Phi_2(x)}{\Phi_2(x^q)} \\
&= \frac{(x^{pq}+1)(x+1)^2}{(x+1)(x^p+1)(x^q+1)} \\
&= \frac{\{(-x)^{pq}-1\}\{(-x)-1\}^2}{\{(-x)-1\}\{(-x)^p-1\}\{(-x)^q-1\}} \\
&= \frac{((-x)^{pq}-1)}{\Phi_1(-x)\Phi_p(-x)\Phi_q(-x)} \\
&= \Phi_{pq}(-x)
\end{aligned}$$

次に一般の k について計算する。

$$\frac{\Phi_{2^k pq}}{\Phi_{2^{k-1}pq}} = \frac{x^{2^k pq}-1}{x^{2^{k-1}pq}-1}\frac{1}{\Phi_{2^k}\Phi_{2^k p}\Phi_{2^k q}\Phi_{2^{k-1}pq}}$$

従って、

$$\begin{aligned}
\Phi_{2^k pq} &= \frac{x^{2^k pq}-1}{(x^{2^{k-1}pq}-1)\Phi_2(x^{2^{k-1}})\Phi_2(x^{2^{k-1}p})\Phi_2(2^{x^{k-1}q})} \\
&= \frac{(x^{2^{k-1}pq})^2-1}{(x^{2^{k-1}pq}-1)(x^{2^{k-1}}+1)(x^{2^{k-1}p}+1)(x^{2^{k-1}q}+1)} \\
&= \frac{x^{2^{k-1}pq}+1}{(x^{2^{k-1}}+1)(x^{2^{k-1}p}+1)(x^{2^{k-1}q}+1)} \\
&= \frac{(-x^{2^{k-1}})^{pq}-1}{((-x^{2^{k-1}})-1)((-x^{2^{k-1}})^p-1)((-x^{2^{k-1}})^q-1)} \\
&= \frac{(-x^{2^{k-1}})^{pq}-1}{\Phi_1(-x^{2^{k-1}})\Phi_p(-x^{2^{k-1}})\Phi_q(-x^{2^{k-1}})} \\
&= \Phi_{pq}(-x^{2^{k-1}})
\end{aligned}$$

よって、$\Phi_{2^k pq}(x)$ の係数も 0, 1, -1 のいずれかである。
これから、もし $\Phi_n(x)$ の係数に 0, 1, -1 以外の数が出てくるとすれば、その最小数 n は、2 を含まない 3 つの互いに異なる奇素数の積を因数に持つ。
実際、mathematica で計算すると $\Phi_{3\cdot5\cdot7}(x) = 1+x+x^2-x^5-x^6-2x^7-x^8-x^9+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}-x^{20}-x^{22}-x^{24}-x^{26}-x^{28}+x^{31}+x^{32}+x^{33}+x^{34}+x^{35}+x^{36}-x^{39}-x^{40}-2x^{41}-x^{42}-x^{43}+x^{46}+x^{47}+x^{48}$ である。この次の候補は $\Phi_{3\cdot5\cdot11}$ で、係数に 2 が (1 0個) 現れるが、その次の候補 $\Phi_{3\cdot7\cdot11}$ には係数に 0, 1, -1 しか現れない。

円分多項式の係数2

金沢光則

平成11 年 11 月 3 日

1 はじめに

「円分多項式の係数」では、係数が $0, 1, -1$ となる場合について調べた。そこで係数に 2 がでてくる例をあげたが、このような場合でも、係数の絶対値を上から押さえられないだろうか。

2 $\Phi_n(x)$ の係数の絶対値を押さえるある方法

2.1 $\Phi_n(x^{p^k})$ の分解

p を素数、k を正の整数、n を p を素因数に持たない正の整数とする。このとき、

$$\Phi_n(x^{p^k}) = \Phi_n(x) \times \Phi_{np}(x) \times \Phi_{p^2n}(x) \times \cdots \times \Phi_{p^kn}(x)$$

が成り立つ。

n の原始 n 乗根全体を $\zeta_1, \zeta_2, \ldots, \zeta_l$ とするとき、

$$\Phi_n(x^{p^k}) = \prod_{i=1} (x^{p^k} - \zeta_i)$$

である。この式=0 の解を ξ で表すと、

$$(\xi^{p^k})^n = (\zeta_i)^n = 1(\text{となる } i \text{ が存在する})$$

ので ξ は 1 の p^kn 乗根である。しかし、だからといって 1 の原始 p^kn 乗根とは言えない。
そこで、$\xi^{p^md} = 1$ とする。ただし、$m = 0, 1, 2, ..., k$, $d|n$ とする。このとき、

$$(\xi^{p^md})^{p^{k-m}} = 1^{p^{k-m}} = 1$$

となり、また一方で、

$$(\xi^{p^md})^{p^{k-m}} = \xi^{p^md \times p^{k-m}} = \xi^{p^kd} = (\xi^{p^k})^d = (\zeta_i)^d$$

となる i が存在するので、ζ_i の原始性から $d = n$ となる。
これから、ξ は、1 の原始 n 乗根, 原始 pn 乗根,..., 原始 p^kn 乗根のいずれかである。
逆に、ξ を原始 p^mn 乗根とすると、$(\xi^{p^k})^n = 1$ ゆえ、ξ^{p^k} は 1 の n 乗根であるが、$(\xi^{p^k})^d \neq 1$ $(d|n, d \neq n)$ ゆえ、ξ^{p^k} は 1 の原始 n 乗根である。従って、$\Phi_n(x^{p^k}) = 0$ の根となり成り立つことが分かる。

2.2 $\Phi_{p^k n}(x)$ のみたす式

p を素数、k を正の整数、n を p と素な自然数とする。この時次が成り立つ。

$$\Phi_{p^k n}(x) = \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}$$

上の結果から、次の計算が成り立つからである。

$$\begin{aligned}
\Phi_{p^k n}(x) &= \frac{x^{p^k n}-1}{\prod_{d|p^k n, d\neq p^k n}\Phi_d(x)} \\
&= \frac{x^{p^k n}-1}{(\prod_{d|n}\Phi_d(x))(\prod_{d|n}\Phi_{pd}(x))\cdots(\prod_{d|n,d\neq n}\Phi_{p^k d}(x))} \\
&= \frac{x^{p^k n}-1}{(\prod_{d|n,d\neq n}\prod_{i=0}^{k}\Phi_{p^i d}(x))\times(\prod_{i=0}^{k-1}\Phi_{p^i n}(x))} \\
&= \frac{x^{p^k n}-1}{(\prod_{d|n,d\neq n}\Phi_d(x^{p^k}))\times(\Phi_n(x^{p^{k-1}}))} \\
&= \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}
\end{aligned}$$

2.3 係数の評価

p, q, r を互いに異なる素数とする。

$$\begin{aligned}
\Phi_{pqr}(x)\times\Phi_p(x^{qr}) &= \frac{\Phi_{pr}(x^q)}{\Phi_{pr}(x)}\times\Phi_p(x^{qr}) \\
&= \Phi_{pr}(x^q)\times\frac{\Phi_p(x)}{\Phi_p(x^r)}\times\Phi_p(x^{qr}) \\
&= \Phi_{pr}(x^q)\times\frac{\Phi_p(x^{qr})}{\Phi_p(x^r)}\times\Phi_p(x) \\
&= \Phi_{pr}(x^q)\times\Phi_{pq}(x^r)\times\Phi_p(x)
\end{aligned}$$

よって、

$$\Phi_{pqr}(x)\times(x^{pqr}-1) = \Phi_{pr}(x^q)\times\Phi_{pq}(x^r)\times\Phi_p(x)\times\Phi_1(x^{qr})$$

ここで、$\Phi_{pqr}(x)$ は $(p-1)(q-1)(r-1)$ 次の多項式ゆえ、左辺の係数は、$\Phi_{pqr}(x)$ に現れる係数が、“2 度” づつ現れるだけなので、右辺に現れる係数で評価することができる。
右辺は、高々$(p-1)(r-1)+1$ 項、高々$(p-1)(q-1)+1$ 項、p 項、2 項の多項式で、それらの係数は 0, 1, -1 のいずれかであるから、係数の絶対値は $((p-1)(q-1)+1)p2$ で押さえられる。
$p=3$, $q=5$, $r=7$ のときを考えると、$\Phi_{105}(x)$ の係数の絶対値は 54 で押さえられることになる。実際には、係数の最大値は 2 なので、残念ながらこの評価はかなり緩い。

参考文献

[1] B. L. van der Waerden, 演習現代代数学, 東京図書

[2] 渡辺敬一・草場公邦, すうがくぶっくす　代数の世界, 朝倉書店

[3] 金沢光則, 円分多項式の係数