J. Chosun Natural Sci.
Vol. 7, No. 4 (2014) pp. 283 − 285
http://dx.doi.org/10.13160/ricns.2014.7.4.283

Irreducibility of Certain Quadrinomials

Seon-Hong Kim†

Abstract

We investigate irreducibility of the quadrinomial

$$F_m(x) = x^{2m} - x^{m+1} - x^{m-1} - 1,$$

where m is an even integer ≥ 2 using only basic techniques that can be often used in many classes of polynomials.

Key words : Polynomial, Quadrinomial, Irreducibility

1. Introduction

A polynomial $f(x) \in \mathbb{Z}[x]$ is called irreducible over $\mathbb{Z}$ if $f(x) \not\equiv \pm 1$ and whenever $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$,

$$g(x) \equiv \pm 1 \text{ or } h(x) \equiv \pm 1.$$

In the theory of polynomials, we often encounter with the question of deciding whether a given polynomial is irreducible over $\mathbb{Z}$ or not. A simple criterion which would give this information is desirable. However, no such criterion that apply to all polynomials has been found; but many irreducibility criteria have been obtained for some particular classes of polynomials.

Kim [1] considered the quadrinomial

$$F_m(x) = x^{2m} - x^{m+1} - x^{m-1} - 1,\ m \geq 2.$$

He showed that the unique positive zero of $F_m(x)$ leads to analogues of $2\binom{2n}{k}$ (k even) by using hypergeometric functions, and their minimal polynomials are related to Chebyshev polynomials. He also considered the irreducibility of $F_m(x)$ and obtained the following proposition.

Proposition 1 Let m be an integer ≥ 2.

(a) If m is odd, then $F_m(x)$ is irreducible over $\mathbb{Z}$.

(b) If m is even, then $F_m(x)/(1+x^2)$ is irreducible over $\mathbb{Z}$. More precisely,

(i) if 4 does not divide m, then

$$\begin{aligned} G(x) := G_m(x) = F_m(x)/(1+x^2) \\ = -1 + x^2 - x^4 + \cdots + x^{m-4} - x^{m-2} - x^{m-1} \\ + x^m - x^{m+2} + \cdots + x^{2m-2} \end{aligned}$$

is irreducible over $\mathbb{Z}$,

(ii) if 4 divides m, then

$$\begin{aligned} H(x) := H_m(x) = F_m(x)/(1+x^2) \\ = -1 + x^2 - x^4 + \cdots - x^{m-4} + x^{m-2} - x^{m-1} \\ - x^m + x^{m+2} + \cdots + x^{2m-2} \end{aligned}$$

is irreducible over $\mathbb{Z}$.

The main idea for the proof of Proposition 1 was due to deep theory for quadrinomial by Mills[2]. In Secton 2 of this paper, we prove (b) of Proposition 1 in another way using only basic techniques that can be often used in many classes of polynomials.

2. Proof

In this section, we only prove (i) of (b) of Proposition 1. The (ii) of (b) can be proved in the same way. Suppose that $G(x) = \Omega(x)\Psi(x)$, where $\Omega(x), \Psi(x) \in \mathbb{Z}[x]$, $r = \deg \Omega$ and $s = \deg \Psi$. Write

Department of Mathematics, Sookmyung Women's University, Seoul 140-742, Korea

†Corresponding author : shkim17@sookmyung.ac.kr

(Received : December 3, 2014, Revised : December 15, 2014, Accepted : December 25, 2014)

$$G_1(x) := x^r \Omega\left(\frac{1}{x}\right)\Psi(x) = \sum_{k=0}^{2m-2} c_k x^k$$
$$G_2(x) := x^{2m-2} G_1\left(\frac{1}{x}\right) = x^s \Psi\left(\frac{1}{x}\right)\Omega(x) = \sum_{k=0}^{2m-2} c_k x^{2m-2-k}.$$

Then

$$\begin{aligned}
G_1(x)\,G_2(x) &= \Omega(x)\Psi(x)\left(x^{2m-2}\Omega\left(\frac{1}{x}\right)\Psi\left(\frac{1}{x}\right)\right) \\
&= G(x)x^{2m-2}G\left(\frac{1}{x}\right) \\
&= (-1+x^2-x^4+\cdots+x^{m-4}-x^{m-2}-x^{m-1} \\
&\quad +x^m-x^{m+2}+\cdots+x^{2m-2}) \\
&\quad (1-x^2+x^4-\cdots-x^{m-4}+x^{m-2}-x^{m-1} \\
&\quad -x^m+x^{m+2}+\cdots-x^{2m-2}) \\
&= -1+2x^2-3x^4+4x^6-\cdots+(-1)^{t/2+1}(t/2+1)x^t \\
&\quad +\cdots-(m-1)x^{2m-4}+(m+1)x^{2m-2}-(m-1)x^{2m} \\
&\quad +(m-2)x^{2m+2}-\cdots+2x^{4m-6}-x^{4m-4}. \qquad (1)
\end{aligned}$$

Comparing coefficients in (1) gives

$$\sum_{k=0}^{l} c_k c_{2m-2-l+k} = \begin{cases} 0, & l \text{ odd}, \\ -\left(\dfrac{l}{2}+1\right), & l=4t, \\ \dfrac{1}{2}+1, & l=4t+2, \end{cases} \qquad (2)$$

where $t \geq 0$. In particular,

$$c_0 c_{2m-2} = -1 \qquad (3)$$
$$c_0 c_{2m-3} + c_1 c_{2m-2} = 0 \qquad (4)$$

and

$$c_0^2 + c_1^2 + \cdots + c_{2m-2}^2 = m+1 \quad (\text{coefficient of } x^{2m-2}). \qquad (5)$$

So $G_1(x)$ and $G_2(x)$ have at most $m+1$ non-zero terms. In fact $G_1(x)$ and $G_2(x)$ have exactly $m+1$ non-zero terms, since if $|c_k| = 2$ for some k, $k \neq 0,\ 2m-2$. Then

$$c_0^2 + c_1^2 + \cdots + c_{k-1}^2 + c_{k+1}^2 + \cdots + c_{2m-2}^2 = m-3.$$

So there are at most $m-2$ non-zero terms in $G_1(x)$ and $G_2(x)$. Then $G_1(x)G_2(x)$ has at most $2m-4$ non-zero terms. But $G(x)x^{2m-2}G(1/x)$ has $2m-1$ non-zero terms by (1), which is a contradiction. Hence $G_1(x)$ and $G_2(x)$ have exactly $m+1$ non-zero terms, and all of them are 1 or -1. First without loss of generality we may assume that $c_0 = -1$ and $c_{2m-2} = 1$ from (3). By (4), we see that $c_1 = c_{2m-3}$. Then we have three cases, i.e. either $c_1 = c_{2m-3} = 1$ or $c_1 = c_{2m-3} = -1$ or $c_1 = c_{2m-3} = 0$.

Suppose that $c_1 = c_{2m-3} = 1$. Then, by the case $l=2$ in (2), either $c_2 = 1,\ c_{2m-4} = 0$ or $c_2 = 0,\ c_{2m-4} = -1$. Now the each case has two cases again so that we have two possibilities: either

$$\begin{aligned} &c_1 = 1,\ c_2 = 1,\ c_3 = -1,\ c_4 = -1,\ c_5 = 1 \\ &c_{2m-3} = 1,\ c_{2m-4} = 0,\ c_{2m-5} = 0,\ c_{2m-6} = 1, \\ &c_{2m-7} = 1 \end{aligned} \qquad (6)$$

or

$$\begin{aligned} &c_1 = 1,\ c_2 = 0,\ c_3 = 0,\ c_4 = -1,\ c_5 = 1 \\ &c_{2m-3} = 1,\ c_{2m-4} = -1,\ c_{2m-5} = -1,\ c_{2m-6} = 1, \\ &c_{2m-7} = 1 \end{aligned} \qquad (7)$$

The above patterns continue on. In fact, (6) is obtained by

$$c_k - c_{2m-2-l+k} = \begin{cases} -2, & l=4t, \\ 0, & l=4t+1, \\ 1, & l=4t+2, \\ -1, & l=4t+3, \end{cases}$$

where $t \geq 0$, and (7) is similarly obtained. So this is not the case, since there are non-zero terms more than $m+1$. By the same method above, we can also show that $c_1 = c_{2m-3} = -1$ is also not the case. Hence the only case is

$$c_1 = c_{2m-3} = 0.$$

Then, by the case l odd in (2), we observe that $c_k =$, $c_{2m-2-l-k}$ where k is odd. On the other hand, if l is even in (2), then we see that the c_k (k even) and $c_{m-1} = -1$ are exactly the same as the coefficients of $G(x)$ by comparing the number of non-zero terms. In fact, $c_{m-1} = 1$ or -1. Suppose that $c_{m-1} = 1$. Obviously

$$G_1(x)\,G_2(x) \neq G(x)x^{2m-2}G(1/x).$$

So $c_{m-1} = -1$. Hence $G(x) = G_1(x)$. Thus

$$x^r \Omega\left(\frac{1}{x}\right)\Psi(x) = G_1(x) = \Omega(x)\,\Psi(x)$$

which means $\Omega(x)$ is a self-reciprocal polynomial. If $c_0 = 1$ and $c_{2m-2} = -1$, then by the same method above, $\Psi(x)$ is a self-reciprocal polynomial. Hence at least one of $\Omega(x)$ and $\Psi(x)$ is a self-reciprocal polynomial. If the both are self-reciprocal, then so is $G(x)$, which is a contradiction. So only one of them is self-reciprocal. Then $G(x)$ has more than one non-reciprocal irreducible factors (not necessarily distinct). Let $u(x)$ be one of them. Then $w(x) = x^{\deg u} u(1/x)$ is also non-reciprocal irreducible factor. If $w(x) \mid G(x)$, then we consider $\Omega(x)$ and $\Psi(x)$ such that

$$G(x) = \Omega(x)\Psi(x), \quad u(x) \nmid \Psi(x),$$
$$w(x) \nmid \Omega(x).$$

If α is a root of $u(x)$, then

$$\Omega(x) = 0 \text{ and } \Omega\left(\frac{1}{\alpha}\right) \neq 0$$

so that $\Omega(x)$ is a non-reciprocal polynomial. Similarly, $\Psi(x)$ is non-reciprocal. Hence this is a contradiction. In all

$$G(x) = -1 + x^2 - x^4 + \cdots - x^{m-2} - x^{m-1} + x^m$$
$$- x^{m+2} + \cdots + x^{2m-2}$$

is irreducible over $\mathbb{Z}$.

References

[1] S. H. Kim, “The analogues of some binomial coefficients”, Indian J. Pure Ap. Mat., Vol. 34, pp. 1771-1784, 2003.

[2] W. H. Mills, “The factorization of certain quadrinomials”, Math. Scand., Vol. 57, pp. 44-50, 1985.