Far East Journal of Mathematical Sciences (FJMS)

Published Online: June 2015
http://dx.doi.org/10.17654/FJMSJul2015_573_582
Volume 97, Number 5, 2015, Pages 573-582 **ISSN: 0972-0871**

CYCLOTOMIC POLYNOMIALS OF THE SECOND KIND. PART 2

Javier Gomez-Calderon

Department of Mathematics
The Pennsylvania State University
New Kensington, Pennsylvania 15068
U. S. A.
e-mail: jxg11@psu.edu

Abstract

In this paper, we continue our work in [3]. For a primitive dth root of unity ς_d, we define the polynomial

$$R_d(x) = \prod_{(i,d)=1}^{[(d-1)/2]} (x - \varsigma_d^i - \varsigma_d^{-i})$$

and then show that

$$\prod_{2<e|d} R_e(x) = \begin{cases} f_{\frac{d-1}{2}}(x) + f_{\frac{d-3}{2}}(x) & \text{if } d \text{ is odd} > 3, \\ f_{\frac{d-2}{2}}(x) & \text{if } d \text{ is even} > 2, \end{cases}$$

where $f_d(x)$ denotes the well-known Dickson polynomial of the second kind. For an odd prime p, we also show that $Q(\varsigma_{p^n} + \varsigma_{p^n}^{-1}) \cap B = Z[\varsigma_{p^n} + \varsigma_{p^n}^{-1}]$, where B denotes the ring of algebraic integers.

Received: February 20, 2015; Accepted: April 2, 2015
2010 Mathematics Subject Classification: 11Txx, 11T06.
Keywords and phrases: Dickson and cyclotomic polynomials.
Communicated by K. K. Azad

Introduction

Let $g_d(x)$ and $f_d(x)$ denote the Dickson polynomials of the first and second kind, respectively, defined by

$$g_d(x) = \sum_{i=0}^{[d/2]} \frac{d}{d-i}\binom{d-i}{i}(-1)^i x^{d-2i}$$

and

$$f_d(x) = \sum_{i=0}^{[d/2]} \binom{d-i}{i}(-1)^i x^{d-2i}$$

where [ ] denotes the greatest integer function. Dickson polynomials have been extensively studied by many authors and an excellent survey of their properties has been written by Lidl et al. in [5]. Further related results can also be found in [1-3] and [4].

Alternatively we can also define $g_d(x)$ by

$$g_d(x) = xg_{d-1}(x) - g_{d-2}(x),$$

where $g_0(x) = 2$ and $g_1(x) = x$. Similarly, we can define $f_d(x)$ by

$$f_d(x) = xf_{d-1}(x) - f_{d-2}(x),$$

where $f_0(x) = 1$ and $f_1(x) = x$. Hence, there are functional equations for both $g_d(x)$ and $f_d(x)$ given by the following lemma.

Lemmata

Lemma 1.

(a) $$f_d(x) = \begin{cases} \dfrac{u^{d+1} - u^{-d-1}}{u - u^{-1}} & \text{if } x = u + u^{-1} \neq \pm 2, \\ d+1 & \text{if } x = \pm 2 \text{ and } d \text{ is even}, \\ \pm(d+1) & \text{if } x = \pm 2 \text{ and } d \text{ is odd}, \end{cases}$$

(b) $g_d(x) = u^d + u^{-d}$ *if* $x = u + u^{-1}$.

Proof. A proof of part (a) can be found in [3, Lemma 1]. For (b) we consider the formal power series

$$p(z) = g_0(x) + g_1(x)z + g_2(x)z^2 + g_3(x)z^3 + \cdots.$$

Then

$$(1 - xz + z^2)\,p(z) = g_0(x) + g_1(x)z - xg_0(x) + \sum_{n=2}^{\infty}(g_n(x) - xg_{n-1}(x) + g_{n-2}(x))z^n$$

$$p(z) = \frac{2 - xz}{z^2 - xz + 1} = \left(\frac{2 - xu_1}{u_1 - u_2}\right)\left(\frac{1}{z - u_1}\right) + \left(\frac{2 - xu_2}{u_2 - u_1}\right)\left(\frac{1}{z - u_2}\right),$$

where $z^2 - xz + 1 = (z - u_1)(z - u_2)$. Hence,

$$p(z) = \frac{1}{1 - u_2 z} + \frac{1}{1 - u_1 z} = \sum_{n=0}^{\infty}(u_2^n + u_1^n)z^n.$$

Therefore, $g_d(x) = u^d + u^{-d}$ if $x = u + u^{-1}$.

Lemma 2. $f_d(x) = \prod_{i=1}^{d}(x - \varsigma_{2d+2}^{i} - \varsigma_{2d+2}^{-i})$.

Proof. See [3, Lemma 2].

Corollary. $f_d(x) = \prod_{2<e|(2d+2)} R_e(x)$, *where* $R_n(x) = \prod_{(i,n)=1}^{[(n-1)/2]}(x - \varsigma_n^i - \varsigma_n^{-i})$ *for* $n > 2$.

For the purpose of completeness we also define $R_1(x) = x - 2$ and $R_2(x) = x + 2$.

Lemma 3. *The minimum polynomial of* $\varsigma_d + \varsigma_d^{-1}$ *over Q is* $R_d(x)$.

Proof. See [3, Lemma 3].

Lemma 4.

(a) $f_{\frac{d-1}{2}}(x) + f_{\frac{d-3}{2}}(x) = \prod_{2<e|d} R_e(x)$ *if d is odd* > 1

(b) $f_{\frac{d-2}{2}}(x) = \prod_{2<e|d} R_e(x)$ *if d is even* > 2

(c) $R_{2d}(x) = (-1)^{\phi(d)} R_d(-x)$ *if d is odd.*

(d) $\prod_{i=1}^{n} R_{p^i}(-x) = \pm\left(\prod_{i=1}^{n} R_{p^i}(x) - 2 f_{\frac{p^n-1}{2}}(x) \right)$ *if p is an odd prime.*

(e) $\varsigma_{p^n}^{k} + \varsigma_{p^n}^{-k}$ *is unit in* $B \cap Q(\varsigma_{p^n} + \varsigma_{p^n}^{-1})$, *where B denotes the ring of algebraic integers and p does not divide k.*

Proof. (a)

$$
\begin{aligned}
& f_{\frac{d-1}{2}}(\varsigma_d^i + \varsigma_d^{-i}) + f_{\frac{d-3}{2}}(\varsigma_d^i + \varsigma_d^{-i}) \\
&= \frac{\varsigma_d^{i(d+1)/2} - \varsigma_d^{-i(d+1)/2} + \varsigma_d^{i(d-1)/2} - \varsigma_d^{-i(d-1)/2}}{\varsigma_d^i - \varsigma_d^{-i}} \\
&= \frac{(\varsigma_d^i + 1)(\varsigma_d^{i(d-1)/2} - \varsigma_d^{-i(d+1)/2})}{\varsigma_d^i - \varsigma_d^{-i}} \\
&= 0,
\end{aligned}
$$

where $\varsigma_d^i + \varsigma_d^{-i} \neq \varsigma_d^j + \varsigma_d^{-j}$ for all $i \neq j, 1 \leq i, j \leq \frac{d-1}{2} = \deg\left(f_{\frac{d-1}{2}}(x) \right)$.

Hence,

$$
f_{\frac{d-1}{2}}(x) + f_{\frac{d-3}{2}}(x) = \prod_{i=1}^{[(d-1)/2]} (x - \varsigma_d^i - \varsigma_d^{-i}) = \prod_{2<e|d} R_e(x).
$$

(b) $f_{\frac{d-2}{2}}(x) = \prod_{2<e|d} R_e(x)$ by Lemma 2.

(c)

$$R_{2d}(x) = \prod_{(i,2d)=1}^{[(2d-1)/2]} (x - \varsigma_{2d}^{i} - \varsigma_{2d}^{-i})$$

$$= (-1)^{\phi(d)/2} \prod_{(i,d)=1}^{(d-1)/2} (-x - \varsigma_{d}^{i} - \varsigma_{d}^{-i}) = (-1)^{\phi(d)/2} R_d(-x)$$

(d) Combine (a) and (c).

(e) $N(\varsigma_{p^n}^{k} + \varsigma_{p^n}^{-k}) = R_{p^n}(0)$. On the other hand, $\prod_{i=1}^{n} R_{p^i}(0) = f_{\frac{p^n-1}{2}}(0) + f_{\frac{p^n-3}{2}}(0) = \pm 1$. Therefore, $R_{p^n}(0) = \pm 1$.

Lemma 5. *Let p denote an odd prime. Then* $2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1}$ *divides* $2 - \varsigma_{p^n}^{k} - \varsigma_{p^n}^{-k}$ *in* $Z[\varsigma_{p^n} - \varsigma_{p^n}^{-1}]$ *for all integers n and* $k \geq 1$.

Proof. $g_k(1 + 1^{-1}) = 1^k + 1^{-k} = 2$. Hence, $(x-2)h(x) = g_k(x) - 2$ for some polynomial $h(x) \in Z[x]$. Therefore, $(\varsigma_{p^n} + \varsigma_{p^n}^{-1} - 2)h(\varsigma_{p^n} + \varsigma_{p^n}^{-1}) = g_k(\varsigma_{p^n} + \varsigma_{p^n}^{-1}) - 2 = \varsigma_{p^n}^{k} + \varsigma_{p^n}^{-k} - 2$.

Main Results

Theorem 1. *disc*$(\varsigma_{p^n} + \varsigma_{p^n}^{-1})$ *divides* $p^{n\phi(p^n)/2}$.

Proof. $f_{p^n-1}(x) = \prod_{i=1}^{n} R_{p^i}(x) \prod_{i=1}^{n} R_{2p^i}(x) = \frac{u^{p^n} - u^{-p^n}}{u - u^{-1}}$, where $x = u + u^{-1}$.

Hence,

$$f'_{p^n-1}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})$$

$$=R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n}R_{2p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})$$

$$=\pm R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n}R_{p^i}(-\varsigma_{p^n}-\varsigma_{p^n}^{-1})$$

$$=\pm R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})$$

$$\left(\prod_{i=1}^{n}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})+2f_{\frac{p^n-1}{2}}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\right)$$

$$=\pm R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\left(-2\left(\frac{\varsigma_{p^n}^{\frac{p^n+1}{2}}-\varsigma_{p^n}^{-\frac{p^n+1}{2}}}{\varsigma_{p^n}-\varsigma_{p^n}^{-1}}\right)\right)$$

$$=\mp R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\left(\frac{2}{\varsigma_{p^n}^{\frac{p^n+1}{2}}+\varsigma_{p^n}^{-\frac{p^n+1}{2}}}\right). \qquad (1)$$

On the other hand, $f_{p^n-1}(x)=\dfrac{u^{p^n}-u^{-p^n}}{u-u^{-1}}=\dfrac{u^{2p^n}-1}{u^{p^n+1}-u^{p^n-1}}$, where $x=u+u^{-1}$. Hence, differentiating and then evaluating,

$f'_{p^n-1}(x)=$

$$\frac{(u^{p^n+1}-u^{p^n-1})(2p^n u^{p^n-1})-(u^{2p^n}-1)((p^n+1)u^{p^n}-(p^n-1)u^{p^n-2})}{(u^{p^n+1}-u^{p^n-1})^2}$$

$$\cdot\frac{u}{u-u^{-1}}$$

$$f'_{p^n-1}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})=\frac{(\varsigma_{p^n}-\varsigma_{p^n}^{-1})(2p^n\varsigma_{p^n}^{-1})}{(\varsigma_{p^n}-\varsigma_{p^n}^{-1})^2}\cdot\frac{\varsigma_{p^n}}{\varsigma_{p^n}-\varsigma_{p^n}^{-1}}$$

$$=\frac{2p^n}{(\varsigma_{p^n}-\varsigma_{p^n}^{-1})^2}. \tag{2}$$

Combining (1) and (2),

$$\frac{2p^n}{(\varsigma_{p^n}-\varsigma_{p^n}^{-1})^2}=\mp R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\left(\frac{2}{\varsigma_{p^n}^{\frac{p^n+1}{2}}+\varsigma_{p^n}^{-\frac{p^n+1}{2}}}\right)$$

$$\left(\varsigma_{p^n}^{\frac{p^n+1}{2}}+\varsigma_{p^n}^{-\frac{p^n+1}{2}}\right)p^n$$

$$=\mp R'_{p^n}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})(\varsigma_{p^n}-\varsigma_{p^n}^{-1})^2$$

Taking norms,

$$(\pm 1)(p^n)^{\phi(p^n)/2}=\pm disc(\varsigma_{p^n}+\varsigma_{p^n}^{-1})N(\alpha)$$

where $\alpha=\prod_{i=1}^{n-1}R_{p^i}(\varsigma_{p^n}+\varsigma_{p^n}^{-1})(\varsigma_{p^n}-\varsigma_{p^n}^{-1})^2$ is an algebraic integer and so $N(\alpha)\in Z$.

Theorem 2. *Let B denote the ring of algebraic integers. Then $Z[\varsigma_{p^n} + \varsigma_{p^n}^{-1}] = B \cap Q(\varsigma_{p^n} + \varsigma_{p^n}^{-1})$ for all odd prime p and integer $n \geq 1$.*

Proof. Since $Z[\varsigma_{p^n} + \varsigma_{p^n}^{-1}] = Z[2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1}]$, it will be enough if we show that $Z[2 - \varsigma_{p^n} + \varsigma_{p^n}^{-1}] = B \cap Q(\varsigma_{p^n} + \varsigma_{p^n}^{-1})$. If $p^n = 3$, then $\varsigma_3 + \varsigma_3^{-1} = -1$ and the result is trivial. It is also clear that $disc(\varsigma_{p^n} + \varsigma_{p^n}^{-1}) = disc(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})$ and that $Z[2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1}] \subseteq B \cap Q(\varsigma_{p^n} + \varsigma_{p^n}^{-1}) = S$. Assume that $Z[2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1}] \neq S$. So, assume that there is an element β in S of the form

$$\beta = \frac{m_i(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})^i + m_{i+1}(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})^{i+1} + \cdots + m_{\phi(p^n)/2-1}(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})^{\phi(p^n)/2-1}}{p},$$

where $m_i \in Z$ is not divisible by p. Then

$$\frac{p\beta}{(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})^{i+1}}$$

$$= \frac{m_i}{2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1}} + m_{i+1} + \cdots + m_{\phi(p^n)/2-1}(2 - \varsigma_{p^n} - \varsigma_{p^n}^{-1})^{\phi(p^n)/2-i-2}. \quad (1)$$

On the other hand,

$$f_{\frac{p^n-1}{2}}(2) + f_{\frac{p^n-3}{2}}(2) = \prod_{i=1}^{n} R_{p^i}(2)$$

$$\frac{p^n - 1}{2} + 1 + \frac{p^n - 3}{2} + 1 = \prod_{i=1}^{n-1} R_{p^i}(2) \prod_{(k,\ p^n)=1}^{(p^n-1)/2} (2 - \varsigma_{p^n}^{k} - \varsigma_{p^n}^{-k})$$

$$\frac{p^n}{(2-\varsigma_{p^n}-\varsigma_{p^n}^{-1})^{\phi(p^n)/2}} = \prod_{i=1}^{n-1} R_{p^i}(2)\alpha,$$

where by Lemma 5,

$$\alpha = \frac{\prod_{(k,\ p^n)=1}^{(p^n-1)/2}(2-\varsigma_{p^n}^{k}-\varsigma_{p^n}^{-k})}{(2-\varsigma_{p^n}-\varsigma_{p^n}^{-1})^{\phi(p^n)/2}} \in Z[\varsigma_{p^n}+\varsigma_{p^n}^{-1}]$$

Now, $R_p(2) = f_{p-1}(2) = p$ and $p^n = f_{\frac{p^n-1}{2}}(2) + f_{\frac{p^n-3}{2}}(2) = \prod_{i=1}^{n} R_{p^i}(2)$.

So, one easily sees that $R_{p^k}(2) = p$ for all k.

Therefore,

$$\frac{p}{(2-\varsigma_{p^n}-\varsigma_{p^n}^{-1})^{\phi(p^n)/2}} = \alpha \in Z[\varsigma_{p^n}+\varsigma_{p^n}^{-1}]. \tag{2}$$

Hence, combining (1) and (2),

$$\frac{m_i}{2-\varsigma_{p^n}-\varsigma_{p^n}^{-1}} = \lambda \in Z[\varsigma_{p^n}+\varsigma_{p^n}^{-1}].$$

Taking norms,

$$N(m_i) = N(2-\varsigma_{p^n}-\varsigma_{p^n}^{-1})N(\lambda)$$

$$m_i^{(\phi(p^n)-1)/2} = R_{p^n}(2)N(\lambda) = pN(\lambda),$$

where $N(\lambda) \in Z$. Since this last result provides a contradiction, then $Z[2-\varsigma_{p^n}-\varsigma_{p^n}^{-1}] = S$.

References

[1] M. Bhargava and M. Zieve, Factoring Dickson polynomials over finite fields, Finite Fields Appl. 5 (1999), 103-111.

[2] W. S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. 3 (1997), 84-96.

[3] J. Gomez-Calderon and A. Perriello, Cyclotomic polynomials of the second kind, Far East J. Math. Sci. (FJMS) 30(2) (2008), 211-219.

[4] R. Matthews, Permutations polynomials in one and several variables, Ph.D. Thesis, University of Tasmania, Hobart, 1982.

[5] R. Lidl, G. L. Mullen and G. Turnwald, Dickson polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman, London, Harlow, Essex, 1993.