International Journal of Pure and Applied Mathematics
Volume 44 No. 2 2008, 195-204

ON THE MINIMAL POLYNOMIAL OF $\zeta_n + \zeta_n^{-1}$

Nancy Colwell[1 §], Josua Illian[2]

[1]Department of Mathematical Sciences
Saginaw Valley State University
7400 Bag Road, University Center, MI 48710, USA
e-mail: nccolwel@svsu.edu

[2]Department of Mathematics
Purdue University
West Lafayette, IN 47907, USA
e-mail: jillian@purdue.edu

Abstract: Let ζ_n be a primitive n-th root of unity. It is well known that the minimal polynomial of ζ_n over $\mathbb{Q}$ can be found recursively using the relation

$$x^n - 1 = \prod_{d|n} g_d \,,$$

where g_d denotes the minimal polynomial of ζ_d over $\mathbb{Q}$. In this note we describe a polynomial Ω_n that plays a similar role for $\zeta_n + \zeta_n^{-1}$. That is,

$$\Omega_n = \prod_{\substack{d|n \\ d>2}} f_d \,,$$

where f_d denotes the minimal polynomial of $\zeta_d + \zeta_d^{-1}$. Furthermore, if n is a prime, $f_n = \Omega_n$.

AMS Subject Classification: 12E10, 11R18
Key Words: cyclotomic polynomials, roots of unity

1. Introduction

Let ζ_n be a primitive n-th root of unity. We can take $\zeta_n = e^{\frac{2\pi}{n}i}$. It is well

Received: January 27, 2008

§Correspondence author

known that $\mathbb{Q}(\zeta_n)$ is a cyclic extension of $\mathbb{Q}$ of degree $\phi(n)$ over $\mathbb{Q}$, where $\phi(n)$ is the Euler ϕ function, the number of positive integers less than n that are relatively prime to n. The minimal polynomial for ζ_n over $\mathbb{Q}$ is well known for the case where n is a prime power. In general, since $\zeta_n^n = 1$, the minimal polynomial must divide $x^n - 1$. And for $n > 1$, it must also divide $\frac{x^n-1}{x-1} = x^n + x^{n-1} + \cdots + x + 1$. If n is prime, $\frac{x^n-1}{x-1}$ is the minimal polynomial of ζ_n. In general, the minimal polynomial of ζ_n can be found recursively using the following relation: Let g_m denote the minimal polynomial of ζ_m. Then

$$x^n - 1 = \prod_{d|n} g_d \,.$$

The Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group of units in $(\mathbb{Z}/n\mathbb{Z})$. For each j in $(\mathbb{Z}/n\mathbb{Z})^*$ there is a unique $\mathbb{Q}$-automorphism σ_j such that $\sigma_j(\zeta_n) = \zeta_n^j$. The automorphism of order 2 is the mapping that sends ζ_n to ζ_n^{-1}. The fixed field of this automorphism is a real extension of $\mathbb{Q}$, generated by $\zeta_n + \zeta_n^{-1}$, with degree $\frac{\phi(n)}{2}$ over $\mathbb{Q}$ (see for example [1, Chapter V, Section 8]).

In this note we describe explicitly for $n > 2$ a polynomial Ω_n such that $\zeta_n + \zeta_n^{-1}$ is a root of Ω_n, and therefore the minimal polynomial of $\zeta_n + \zeta_n^{-1}$ must divide Ω_n. If n is prime, the minimal polynomial of $\zeta_n + \zeta_n^{-1}$ is equal to Ω_n. Furthermore, letting f_m denote the minimal polynomial of $\zeta_m + \zeta_m^{-1}$, we have the relation

$$\Omega_n = \prod_{\substack{d|n \\ d>2}} f_d \,.$$

2. Notation, Definitions, and Background

Throughout this note n is a natural number greater than 2. ζ_n denotes a primitive n-th root of unity. We will frequently use the following well-known identities:

$$\sum_{j=0}^{n-1} \zeta_n^j = 0 \tag{1}$$

and for any integer k,

$$\zeta_n^k \text{ is a primitive } d\text{-th root of unity, where } d = \frac{n}{\gcd(n,k)}. \tag{2}$$

If $d|n$, $d > 1$ we also have

$$\sum_{j=0}^{n-1} \zeta_d^j = \sum_{q=0}^{\frac{n}{d}-1} \sum_{k=0}^{d-1} \zeta_d^{qd+k} = \frac{n}{d} \sum_{k=0}^{d-1} \zeta_d^k \,,$$

giving us:

$$\text{If } d|n,\ d > 1 \sum_{j=0}^{n-1} \zeta_d^j = 0 \,. \tag{3}$$

Furthermore, if d is odd and n is even, $\frac{n}{d}$ is even, and

$$\sum_{\substack{j=0 \\ j \text{ even}}}^{n-2} \zeta_d^j = \sum_{\substack{q=0 \\ q \text{ even}}}^{\frac{n}{d}-2} \left(\sum_{\substack{k=0 \\ k \text{ even}}}^{d-1} \zeta_d^{qd+k} \right) + \sum_{\substack{q=1 \\ q \text{ odd}}}^{\frac{n}{d}-1} \left(\sum_{\substack{k=1 \\ k \text{ odd}}}^{d-2} \zeta_d^{qd+k} \right)$$

$$= \frac{n}{2d} \sum_{\substack{k=0 \\ k \text{ even}}}^{d-1} \zeta_d^k + \frac{n}{2d} \sum_{\substack{k=1 \\ k \text{ odd}}}^{d-2} \zeta_d^k = \frac{n}{2d} \sum_{k=0}^{d-1} \zeta_d^k = 0 \,.$$

The case for summing over odd powers of ζ_d is handled similarly, which gives us:

$$\text{If } d|n,\ d > 1,\ d \text{ odd and } n \text{ even, } \sum_{\substack{j=0 \\ j \text{ even}}}^{n-2} \zeta_d^j = \sum_{\substack{j=1 \\ j \text{ odd}}}^{n-1} \zeta_d^j = 0 \,. \tag{4}$$

Finally:

$$\text{if } n \text{ is even, } \sum_{\substack{j=0 \\ j \text{ even}}}^{n-2} \zeta_n^j = \sum_{\substack{j=1 \\ j \text{ odd}}}^{n-1} \zeta_n^j = 0 \,. \tag{5}$$

To see this last equation, note that

$$\sum_{\substack{j=0 \\ j \text{ even}}}^{n-2} \zeta_n^j = \sum_{k=0}^{\frac{n-2}{2}} \zeta_n^{2k} = \sum_{k=0}^{\frac{n}{2}-1} \left(\zeta_n^2\right)^k = 0,$$

because ζ_n^2 is a primitive $\frac{n}{2}$ root of unity. Consequently, by equation (1), $\sum_{\substack{j=1 \\ j \text{ odd}}}^{n-1} \zeta_n^j = 0$ as well.

Now let $z_n = \zeta_n + \zeta_n^{-1}$. For $j \geq 0$, we define $z_n^{(j)}$ as follows.

$$z_n^{(j)} = \begin{cases} \zeta_n^j + \zeta_n^{-j}, \text{ for } j > 0 \,, \\ 1, \text{ for } j = 0 \,. \end{cases}$$

Remark. For any natural number k,

$$z_n^k = \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) \zeta_n^{k-i} \zeta_n^{-i} = \sum_{i=0}^{k} \left(\begin{array}{c} k \\ i \end{array} \right) \zeta_n^{k-2i}.$$

Since $\left(\begin{array}{c} k \\ i \end{array} \right) = \left(\begin{array}{c} k \\ k-i \end{array} \right)$ and $k-2(k-i) = -(k-2i)$, we can write the above sum as

$$\sum_{i=0}^{\frac{k-1}{2}} \left(\begin{array}{c} k \\ i \end{array} \right) \left(\zeta_n^{k-2i} + \zeta_n^{-(k-2i)} \right), \text{ if } k \text{ is odd,}$$

and as

$$\sum_{i=0}^{\frac{k}{2}-1} \left(\begin{array}{c} k \\ i \end{array} \right) \left(\zeta_n^{k-2i} + \zeta_n^{-(k-2i)} \right) + \left(\begin{array}{c} k \\ \frac{k}{2} \end{array} \right), \text{ if } k \text{ is even.}$$

In either case we get:

$$z_n^k = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \left(\begin{array}{c} k \\ i \end{array} \right) z_n^{(k-2i)} = \sum_{\substack{j=0 \\ j \equiv k, \bmod 2}}^{k} \left(\begin{array}{c} k \\ \frac{k-j}{2} \end{array} \right) z_n^{(j)}. \tag{6}$$

Also, using (1) and (3) and the fact that $\zeta_d^{-1} = \zeta_d^{n-1}$, we obtain for odd n, if $d|n$, $d > 1$,

$$\sum_{j=0}^{\frac{n-1}{2}} z_d^{(j)} = 0. \tag{7}$$

For even n, if $d|n$,

$$\sum_{\substack{j=0 \\ j \equiv \frac{n}{2}-1, \\ \bmod 2}}^{\frac{n}{2}-1} z_d^{(j)} = \sum_{\substack{j=0 \\ j \equiv \frac{n}{2}-1, \\ \bmod 2}}^{n-1} \zeta_d^{(j)}.$$

If d is odd, $d > 1$, this sum is 0 by (4). If d is even, $d > 2$,

$$\sum_{\substack{j=0 \\ j \equiv \frac{n}{2}-1, \\ \bmod 2}}^{n-1} \zeta_d^{(j)} = \frac{n}{d} \left(\sum_{\substack{k=0 \\ k \equiv \frac{n}{2}-1, \\ \bmod 2}}^{d-1} \zeta_d^{(k)} \right),$$

which is equal to 0 by (5). So in either case, we have, for n even, if $d|n$, $d > 2$,

$$\sum_{\substack{j=0 \\ j \equiv \frac{n}{2}-1, \\ \mod 2}}^{\frac{n}{2}-1} z_d^{(j)} = 0\,. \tag{8}$$

We are now ready to define the polynomials Ω_n and show that they satisfy the properties claimed in the introduction.

3. The Polynomials

In this section we use the following notation throughout. n is an integer greater than 2. For fixed n, set $m = m(n) = \lfloor \frac{n-1}{2} \rfloor$. For $k = 0 \cdots m$, we define the coefficients $C_k(n)$ to be:

$$C_k(n) = \begin{cases} 0 & \text{if } n \text{ is even and } k \not\equiv m \bmod 2\,, \\ (-1)^{\lfloor \frac{m-k}{2} \rfloor} \begin{pmatrix} \lfloor \frac{m+k}{2} \rfloor \\ k \end{pmatrix} & \text{otherwise}\,. \end{cases}$$

Then the polynomial Ω_n is defined to be

$$\Omega_n(x) = \sum_{k=1}^{m} C_k(n) x^k.$$

Example. $\Omega_{19} = x^9 + x^8 - 8x^7 - 7x^6 + 21x^5 + 15x^4 - 20x^3 - 10x^2 + 5x + 1$.

Theorem 1. *Let Ω_n be the polynomial defined above. Let f_n denote the minimal polynomial of z_n over $\mathbb{Q}$. Then the following holds.*

1. $\Omega_n(z_n^{(j)}) = 0$ *for all* $j = 1 \cdots \lfloor \frac{n-1}{2} \rfloor$.
2. $\Omega_n = \prod_{\substack{d|n \\ d>2}} f_d$.
3. $\Omega_n = f_n$ *if n is a prime larger than 2.*

Both 2 and 3 follow directly from 1. 2 follows from 1 because if d divides n, $z_d = z_n^{\left(\frac{n}{d}\right)}$, so f_d must also divide Ω_n. So $\prod_{\substack{d|n \\ d>2}} f_d$ divides Ω_n. By comparing degrees we see that they are equal. 3 can be seen from the fact that the degree of $\mathbb{Q}(z_n)/\mathbb{Q}$ is $\frac{n-1}{2}$ if n is a prime larger than 2.

Before proving part 1 of Theorem 1, we need a few properties of the coefficients $C_k(n)$. First note that if n is even and $k \equiv m \bmod 2$, or if n is odd and $k \not\equiv m \bmod 2$,

$$C_k(n) = C_k(n-1)\,. \tag{9}$$

We will also use the following properties of binary coefficients, which can be easily checked. For all natural numbers r and t with $0 < r < t$,

$$\binom{t}{r} = \binom{t-1}{r-1} + \binom{t-1}{r}\,. \tag{10}$$

And for natural numbers r, t and m, with $r \le t \le \frac{m}{2}$,

$$\binom{m-r}{m-2r}\binom{m-2r}{t-r} = \binom{m-r}{t}\binom{t}{r}\,. \tag{11}$$

Finally, we will need the following proposition.

Proposition 2. *For n odd, and for all j, $0 \le j \le m = \left\lfloor \frac{n-1}{2} \right\rfloor$,*

$$\sum_{\substack{k=j \\ k\equiv j, \bmod 2}}^{m} C_k(n)\binom{k}{\frac{k-j}{2}} = 1\,.$$

Proof. Case 1. $j \equiv m \bmod 2$. In this case

$$\sum_{\substack{k=j \\ k\equiv j, \bmod 2}}^{m} C_k(n)\binom{k}{\frac{k-j}{2}} = \sum_{\substack{k=j \\ k\equiv j, \bmod 2}}^{m} (-1)^{\frac{m-k}{2}}\binom{\frac{m+k}{2}}{k} \times \binom{k}{\frac{k-j}{2}} = \sum_{r=0}^{\frac{m-j}{2}} (-1)^r \binom{m-r}{m-2r}\binom{m-2r}{\frac{m-j}{2}-r}.$$

The last equality comes from letting $r = \frac{m-k}{2}$. Using (11) and setting $t = \frac{m-j}{2}$, the above sum becomes $\sum_{r=0}^{t} (-1)^r \binom{t}{r}\binom{m-r}{t}$. So we need to show that, for all $m \ge 1$, and all $t \le \left\lfloor \frac{m}{2} \right\rfloor$, this sum is equal to 1. We use induction on m, the case $m = 1$ being trivial.

Assume $\sum_{r=0}^{t} (-1)^r \binom{t}{r}\binom{(m-1)-r}{t} = 1$, for all t, $0 \le t \le \left\lfloor \frac{(m-1)}{2} \right\rfloor$. If $t = 0$, the sum is trivial. And if $t = 1$, the sum becomes

$$(-1)^0\binom{1}{0}\binom{m}{1} + (-1)^1\binom{1}{1}\binom{m-1}{1} = m - (m-1) = 1.$$

Now assume $1 < t \le \lfloor \frac{m}{2} \rfloor$. Then

$$\sum_{r=0}^{t} (-1)^r \binom{t}{r} \binom{m-r}{t} = (-1)^0 \binom{t}{0} \binom{m}{t} + \left[\sum_{r=1}^{t-1} (-1)^r \binom{t}{r} \binom{m-r}{t} \right] + (-1)^t \binom{t}{t} \binom{m-t}{t}.$$

Using (10), we get

$$\begin{aligned}
&\binom{m}{t} \\
&+ \left(\sum_{r=1}^{t-1} (-1)^r \left[\binom{t-1}{r-1} + \binom{t-1}{r} \right] \binom{m-r}{t} \right) + (-1)^t \binom{t}{t} \binom{m-t}{t} \\
&= \binom{m}{t} + \sum_{r=1}^{t-1} \left[(-1)^r \binom{t-1}{r-1} \binom{m-r}{t} + (-1)^r \binom{t-1}{r} \binom{m-r}{t} \right] \\
&\quad + (-1)^t \binom{t}{t} \binom{m-t}{t} = (-1)^0 \binom{t-1}{0} \binom{m}{t} \\
&\quad + (-1)^1 \binom{t-1}{0} \binom{m-1}{t} + (-1)^1 \binom{t-1}{1} \binom{m-1}{t} \\
&\quad + (-1)^2 \binom{t-1}{1} \binom{m-2}{t} + \cdots + (-1)^{t-1} \binom{t-1}{t-2} \binom{m-(t-1)}{t} \\
&\quad + (-1)^{t-1} \binom{t-1}{t-1} \binom{m-(t-1)}{t} + (-1)^t \binom{t-1}{t-1} \binom{m-1}{t} \\
&= \sum_{r=0}^{t-1} \left[(-1)^r \binom{t-1}{r} \binom{m-r}{t} + (-1)^{r+1} \binom{t-1}{r} \binom{m-(r+1)}{t} \right] \\
&\quad = \sum_{r=0}^{t-1} (-1)^r \binom{t-1}{r} \left[\binom{m-r}{t} - \binom{m-r-1}{t} \right] \\
&\quad\quad = \sum_{r=0}^{t-1} (-1)^r \binom{t-1}{r} \binom{m-1-r}{t-1},
\end{aligned}$$

which is 1 by induction, since we have $t-1 \le \lfloor \frac{m}{2} \rfloor - 1 \le \lfloor \frac{m-1}{2} \rfloor$. This completes the proof of the case where $j \equiv m \bmod 2$.

Case 2. $j \equiv m - 1 \bmod 2$. Since n is odd, for $k \not\equiv m \bmod 2$, by (9),

$C_k(n) = C_k(n-1) = C_k(n-2)$. So

$$\sum_{\substack{k=j \\ k\equiv j, \bmod 2}}^{m} C_k(n) \binom{k}{\frac{k-j}{2}} = \sum_{\substack{k=j \\ k\equiv j, \bmod 2}}^{m-1} C_k(n-2) \binom{k}{\frac{k-j}{2}}.$$

Since $m(n) - 1 = \frac{n-1}{2} - 1 = \frac{(n-2)-1}{2} = m(n-2)$, this sum is equal to 1 by Case 1. □

We can now prove the first part of Theorem 1. Recall that $\Omega_n = \sum_{k=0}^{m} C_k(n)x^k$, where $m = \lfloor \frac{n-1}{2} \rfloor$. We want to show that $\Omega_n(z_n^{(j)}) = 0$, for all $j = 1 \cdots m$. Since ζ_n^j is a primitive d^{th} root of unity, where $d = \frac{n}{\gcd(n,j)}$, we only need to show that $\Omega_d(z_d) = 0$ for all divisors d of n, where $d > 2$.

$$\Omega_n(z_d) = \sum_{k=0}^{m} C_k(n) z_d^k = \sum_{k=0}^{m} C_k(n) \left(\sum_{\substack{j=0 \\ j\equiv k, \\ \bmod 2}}^{k} \binom{k}{\frac{k-j}{2}} z_d^{(j)} \right)$$

by (6). This can be rewritten as

$$\sum_{j=0}^{m} \left(\sum_{\substack{k=j \\ k\equiv j, \\ \bmod 2}}^{m} C_k(n) \binom{k}{\frac{k-j}{2}} \right) z_d^{(j)}.$$

If n is odd, by Proposition 2, this sum is $\sum_{j=0}^{m} z_d^{(j)}$, which is 0 by (7). If n is even, $C_k(n) = 0$ whenever $k \not\equiv m \bmod 2$, so the coefficients of $z_d^{(j)}$ are 0 for $j \equiv m-1 \bmod 2$. For $j \equiv m \bmod 2$, by (9), $C_k(n) = C_k(n-1)$, so the coefficients of $z_d^{(j)}$ are 1 by Proposition 2. So, if n is even, $\Omega_n(z_d) = \sum_{\substack{j=0 \\ j\equiv m, \bmod 2}}^{m} z_d^{(j)}$, where $m = \frac{n}{2} - 1$. This is 0 by (8), and we are done.

4. The Coefficients and Pascal's Triangle

There is an interesting pattern that can be seen in the coefficients of the polynomial Ω_n that can be followed in Pascal's triangle. A table of the coefficients $C_k(n)$, n odd, for $n = 3$ to $n = 25$ is shown in Table 1 (the coefficients are

n	$k=$ 12	11	10	9	8	7	6	5	4	3	2	1	0
3												1	1
5											1	1	-1
7										1	1	-2	-1
9									1	1	-3	-2	1
11								1	1	-4	-3	3	1
13							1	1	-5	-4	6	3	-1
15						1	1	-6	-5	10	6	-4	-1
17					1	1	-7	-6	15	10	-10	-4	1
19				1	1	-8	-7	21	15	-20	-10	5	1
21			1	1	-9	-8	28	21	-35	-20	15	5	-1
23		1	1	-10	-9	36	28	–56	-35	35	15	-6	-1
25	1	1	-11	-10	45	36	-84	–56	70	35	-21	-6	1

Table 1: The coefficient of x^k in Ω_n

						1							
					1		1						
				1		2		1					
			1		3		3		1				
		1		4		6		4		1			
	1		5		10		10		5		1		
1		6		15		20		15		**- 6**		**1**	
	1		7		21		35		**35**		**- 21**		7		1
		1		8		28		**- 56**		**70**		56		28		8		1
			1		9		**36**		**- 84**		126		126		84		36		9		1
		1		**- 10**		**45**		120		210		252		210		120		45		10		1	
	1		**- 11**		55		165		330		462		462		330		165		55		11		1
1		12		66		220		494		792		924		792		495		220		66		12		1

$$\Omega_{25} = x^{12}+x^{11}-11x^{10}-10x^9+45x^8$$
$$+36x^7-84x^6-56x^5+70x^4+35x^3-21x^2-6x+1$$

Table 2: Pascal's triangle with coefficients of Ω_{25}

either 0, or the same as $n-1$ or $n+1$, for even n). Since $C_k(n)$ is defined from binomial coefficients for all odd n, for a fixed power k, the coefficients (in absolute value) of x^k in Ω_n for any n, are to be found along the $k+1$ diagonal

of Pascal's triangle. But if we look at the coefficients from Ω_n for a fixed n, one can see a different, yet also clear pattern emerging. The coefficients follow a stair step pattern across the triangle. The leading coefficient of Ω_n can be found in the left-most entry of the $\frac{n+1}{2}$ line of the triangle; the leading coefficient is always a positive 1. The next coefficient can be found by moving up to the right, then the next by moving right and changing sign. Then the pattern continues until we run out of triangle. To illustrate, Table 2 shows Pascal's triangle with coefficients of Ω_{25} highlighted in bold with the appropriate signs inserted.

References

[1] T. Hungerford, *Algebra*, Graduate Texts in Mathematics, Springer-Verlag, **73** (1974).