Commun. Korean Math. Soc. **31** (2016), No. 4, pp. 667–682
http://dx.doi.org/10.4134/CKMS.c150206
pISSN: 1225-1763 / eISSN: 2234-3024

THE MINIMAL POLYNOMIAL OF $\cos(2\pi/n)$

Yusuf Z. Gürtaş

Abstract. In this article we show a recursive method to compute the coefficients of the minimal polynomial of $\cos(2\pi/n)$ explicitly for $n \geq 3$. The recursion is not on n but on the coefficient index. Namely, for a given n, we show how to compute e_i of the minimal polynomial $\sum_{i=0}^{d}(-1)^i e_i x^{d-i}$ for $i \geq 2$ with initial data $e_0 = 1, e_1 = \mu(n)/2$, where $\mu(n)$ is the Möbius function.

1. Introduction

Finding the minimal polynomial of $\cos(2\pi/n)$ is an old problem due to its connection to the cyclotomic polynomials. Recall that the unique irreducible polynomial with integer coefficients having $e^{2\pi i/n}$ as one of its roots is called the nth cyclotomic polynomial $\Phi_n(x)$. It's well known that the other roots of $\Phi_n(x)$ are $e^{2k\pi i/n}$ where $1 \leq k < n$ and $(k, n) = 1$. Therefore

$$\Phi_n(x) = \prod_{\substack{k<n \\ (k,n)=1}} \left(x - e^{2k\pi i/n}\right). \tag{1.1}$$

It follows from (1.1) that the degree of $\Phi_n(x)$ is $\phi(n)$, Euler's totient function. Therefore $e^{2k\pi i/n}$ is an algebraic integer of degree $\phi(n)$ for $1 \leq k < n$ and $(k, n) = 1$. It follows that $e^{2k\pi i/n} + e^{-2k\pi i/n} = 2\cos(2k\pi/n)$ is an algebraic integer of degree $\phi(n)/2$ as shown by D. H. Lehmer in 1933 ([5]). In other words it satisfies a monic irreducible polynomial $f_n(x)$ of degree d with integer coefficients, where $d = \phi(n)/2$. Therefore $\cos(2\pi k/n)$ is an algebraic number since it satisfies the monic irreducible polynomial $\frac{1}{2^d} f_n(2x)$ with rational coefficients, which is called the minimal polynomial of $\cos(2\pi k/n)$. K. W. Wegner gave a short list of $f_n(2x)$ in 1957 and 1959 ([10, 11]). In 1993 W. Watkins and J. Zeitlin found some identities satisfied by the minimal polynomial of $\cos(2k\pi/n)$ using Chebyshev polynomials of the first kind ([9]). D. Surowski and P. McCombs reproved those identities using a different method and gave an explicit

Received November 5, 2015; Revised March 21, 2016.
2010 *Mathematics Subject Classification.* 11B83.
Key words and phrases. minimal polynomial, cyclotomic polynomial, algebraic number, Ramanujan sum, cosine.

formula for the minimal polynomial of $\cos(2\pi/p)$, where p is prime, in 2003, [7]. S. Beslin and V. De Angelis also gave an explicit formula for the minimal polynomial of $\cos(2\pi/p)$ as well as $\sin(2\pi/p)$, where p is prime, in 2004, [1].

In this article we show a method to compute the coefficients of the minimal polynomial of $\cos(2\pi/n)$ explicitly for all $n \geq 3$. The method is recursive but recursion is not on n. For a given n, we show how to compute the coefficients e_i of the minimal polynomial $\sum_{i=0}^{d}(-1)^i e_i x^{d-i}$ of $\cos(2\pi/n)$ for $i \geq 2$ with initial data $e_0 = 1, e_1 = \mu(n)/2$, where $\mu(n)$ is the Möbius function. The method uses power sum functions and Ramanujan sums, [3], pg 97. Lemma 2.1 shows how these two functions are related. The third section establishes the recursion on the coefficients of the minimal polynomial of $\cos(2\pi/n)$, which is demonstrated for $n = 66$ as an example. There are also two theorems for some special cases. One shows the connection between the cases of q and $2q$ where q is odd. The other shows that the minimal polynomial is an even function when $n = 4k$.

2. Main section

Let $n \geq 3$. Define

$$S_n = \{\, k \mid (k,n) = 1, 1 \leq k < n\} \quad \text{and} \qquad (2.1)$$
$$S_{n/2} = \{\, k \mid (k,n) = 1, 1 \leq k < n/2\}.$$

It's a well known fact that $|S_n| = \phi(n)$ and $\left|S_{n/2}\right| = \phi(n)/2$. The other roots of the minimal polynomial of $\cos(2\pi/n)$ are $\cos(2\pi k/n)$ for $k \in S_{n/2}$ as shown in [9]. Therefore the minimal polynomial of $\cos(2\pi/n)$ is given as

$$\prod_{k \in S_{n/2}} (x - \cos(2\pi k/n)). \qquad (2.2)$$

If the minimal polynomial of $2\cos(2\pi k/n)$ is $f_n(x)$, then (2.2) is $\frac{1}{2^d} f_n(2x)$, where $d = \phi(n)/2$. In order to avoid rational coefficients we will work on the coefficients of $f_n(2x)$, which will be denoted from this point on by $\Psi_n(x)$. Namely we will be computing the coefficients of

$$\Psi_n(x) = \prod_{k \in S_{n/2}} 2(x - \cos(2\pi k/n)). \qquad (2.3)$$

Let $1, k_2, \ldots, k_d$ be the elements of $S_{n/2}$ in increasing order and $r_1, r_2, \ldots, r_d$ be the corresponding roots in (2.3). Namely, assume

$$\Psi_n(x) = \prod_{k=1}^{d} 2(x - r_k).$$

Recall the definition of the elementary symmetric polynomials:

$$\begin{aligned} e_0(x_1,\dots,x_m) &= 1, \\ e_1(x_1,\dots,x_m) &= x_1+x_2+\cdots+x_m, \\ e_2(x_1,\dots,x_m) &= \sum_{1\le i<j\le m} x_i x_j, \\ &\vdots \\ e_m(x_1,\dots,x_m) &= x_1x_2\cdots x_m. \end{aligned} \tag{2.4}$$

Also define the k^{th} *power sum* function as

$$p_k(x_1,\dots,x_m) = \sum_{i=1}^{m} x_i^k = x_1^k + x_2^k + \cdots + x_m^k.$$

It's possible to write the elementary symmetric polynomials e_n in terms of power sum functions p_k, [6], as

$$e_n = \frac{1}{n!}\begin{vmatrix} p_1 & 1 & 0 & \cdots & & \\ p_2 & p_1 & 2 & 0 & \cdots \\ \vdots & & \ddots & \ddots & \\ p_{n-1} & p_{n-2} & \cdots & p_1 & n-1 \\ p_n & p_{n-1} & \cdots & p_2 & p_1 \end{vmatrix}. \tag{2.5}$$

Now, since

$$\Psi_n(x) = \prod_{k=1}^{d} 2(x-r_k) = 2^d \sum_{i=0}^{d} (-1)^i e_i(r_1,\dots,r_d)x^{d-i}$$

all we have to do is compute e_i for $1 \le i \le d$, which comes down to determining $p_k(r_1,\dots,r_d)$ for $1 \le k \le d$ thanks to (2.5).

Recall Ramanujan's trigonometric sum

$$c_n(m) = \sum_{k\in S_n} e^{2\pi i k m/n}. \tag{2.6}$$

It's not difficult to show that (2.6) reduces to

$$c_n(m) = \sum_{k\in S_n} \cos\frac{2\pi k m}{n}, \tag{2.7}$$

(see [8], pg 99 for a proof). Here we observe that $(n,k)=1$ for $1 \le k < n$ is equivalent to $(n, n-k) = 1$. Therefore both $\cos(2\pi km/n)$ and $\cos(2\pi(n-k)m/n)$ appear in the sum (2.7) because $k \in S_n$ and $n-k \in S_n$. Since

$$\cos(2\pi(n-k)/n) = \cos(2\pi - 2\pi k/n) = \cos(-2\pi k/n) = \cos(2\pi k/n) \tag{2.8}$$

(2.7) can be rewritten as

$$c_n(m) = \sum_{k\in S_n} \cos\frac{2\pi km}{n} = 2\sum_{k\in S_{n/2}} \cos\frac{2\pi km}{n}. \tag{2.9}$$

On the other hand we also have

$$c_n(m) = \sum_{k|d} k\mu(n/k), \tag{2.10}$$

where $d=$gcd(n,m) and μ is the Möbius function, (see [3], pg 99 for a proof). For example setting $m=1$ in (2.10) and using (2.9) we obtain

$$c_n(1) = \sum_{k|1} k\mu(n/k) = \mu(n) = \sum_{k\in S_n} \cos\frac{2\pi k}{n} = 2\sum_{k=1}^{d} r_k. \tag{2.11}$$

Thus, we can conclude that

$$p_1(r_1,\dots,r_d) = e_1(r_1,\dots,r_d) = \frac{1}{2}\mu(n). \tag{2.12}$$

If we let $\theta_k = 2\pi k/n$ we can write

$$c_n(m) = 2\sum_{k\in S_{n/2}} \cos(m\theta_k) = 2\sum_{k\in S_{n/2}} T_m\left(\cos\theta_k\right) = 2\sum_{k=1}^{d} T_m\left(r_k\right), \tag{2.13}$$

where $T_m(x)$ is the Chebyshev polynomial of the first kind. There are several equivalent definitions of $T_m(x)$. The one that we will use here is

$$T_m(x) = \frac{m}{2}\sum_{j=0}^{\lfloor m/2\rfloor} (-1)^j \frac{(m-j-1)!}{(m-2j)!j!}\,(2x)^{m-2j}, \tag{2.14}$$

which can be found in [2]. Now we can write (2.13) as

(2.15)

$$\begin{aligned}\frac{1}{2}\,c_n(m) &= \sum_{k=1}^{d}\sum_{j=0}^{\lfloor m/2\rfloor} (-1)^j m\,2^{m-2j-1}\frac{(m-j-1)!}{(m-2j)!j!}\,r_k^{m-2j} \\ &= 2^{m-1}\sum_{k=1}^{d} r_k^m + \sum_{j=1}^{\lfloor m/2\rfloor} (-1)^j m\,2^{m-2j-1}\frac{(m-j-1)!}{(m-2j)!j!}\,\sum_{k=1}^{d} r_k^{m-2j}\end{aligned}$$

by releasing the $j=0$ term. Using the definition of $p_k(r_1,\dots,r_d)$ and dropping the variables $r_1,\dots,r_d$ (2.15) can be rewritten as

$$\frac{1}{2}\,c_n(m) = 2^{m-1}p_m + \sum_{j=1}^{\lfloor m/2\rfloor} (-1)^j m\,2^{m-2j-1}\frac{(m-j-1)!}{(m-2j)!j!}\,p_{m-2j}.$$

Solving the last equation for p_m yields

$$p_m = \frac{1}{2^m} c_n(m) - \sum_{j=1}^{\lfloor m/2 \rfloor} (-1)^j m\, 2^{-2j} \frac{(m-j-1)!}{(m-2j)!j!} p_{m-2j}, \tag{2.16}$$

which is a recursive definition for p_m. The following lemma shows how to express p_m explicitly in terms of the Ramanujan sums. Recall that $c_n(1) = \mu(n)$. Also note that (2.10) doesn't make sense for $m = 0$ but we will extend the definition to $m = 0$ as $c_n(0) = d$ for convenience even though (2.9) suggests that $c_n(0) = 2d$.

Lemma 2.1. *The power sum function p_m defined on variables $r_1, \ldots, r_d$ can be written in terms of the Ramanujan sums $c_n(m)$ as*

$$p_m(r_1, \ldots, r_d) = \frac{1}{2^m} \sum_{j=0}^{\lfloor m/2 \rfloor} \binom{m}{j} c_n(m-2j). \tag{2.17}$$

Proof. We'll prove the lemma using induction on m. If we set $m = 0$, then (2.17) gives $p_0 = c_n(0) = d$, which agrees with the definition of p_0. If we let $m = 1$, then (2.17) gives

$$p_1(r_1, \ldots, r_d) = \frac{1}{2} c_n(1),$$

which is in agreement with (2.12). If $m = 2$, then (2.17) yields

$$p_2(r_1, \ldots, r_d) = \frac{1}{4} c_n(2) + \frac{1}{4} 2c_n(0) = \frac{1}{4} c_n(2) + \frac{d}{2} \tag{2.18}$$

and (2.16) yields

$$\begin{aligned} p_2 &= \frac{1}{4} c_n(2) - (-1)2 \cdot 2^{-2} \frac{(2-1-1)!}{(2-2)!1!} p_0 \\ &= \frac{1}{4} c_n(2) + \frac{1}{2} p_0 = \frac{1}{4} c_n(2) + \frac{d}{2}, \end{aligned}$$

because $p_0 = d$. We also need to check $m = 3$, which gives

$$p_3(r_1, \ldots, r_d) = \frac{1}{8} c_n(3) + \frac{1}{8} 3c_n(1) = \frac{1}{8} c_n(3) + \frac{3}{8}\mu(n) \tag{2.19}$$

in (2.17) and

$$\begin{aligned} p_3 &= \frac{1}{2^3} c_n(3) - (-1)3 \cdot 2^{-2} \frac{(3-1-1)!}{(3-2)!1!} p_1 \\ &= \frac{1}{8} c_n(3) + \frac{3}{4} p_1 = \frac{1}{8} c_n(3) + \frac{3}{8} \mu(n) \end{aligned}$$

in (2.16). Assume now $m \geq 4$ and (2.17) is true for integers less than m. Substituting p_{m-2j} in (2.16) using the induction assumption yields:

(2.20)

$$p_m = \frac{1}{2^m} c_n(m) - \sum_{j=1}^{\lfloor m/2 \rfloor} (-1)^j m\, 2^{-2j} \frac{(m-j-1)!}{(m-2j)!j!} \frac{1}{2^{m-2j}} \sum_{i=0}^{\lfloor (m-2j)/2 \rfloor} \binom{m-2j}{i} c_n(m-2j-2i)$$
$$= \frac{1}{2^m} c_n(m) + \sum_{j=1}^{\lfloor m/2 \rfloor} \frac{(m-j-1)!}{(m-2j)!j!} \frac{(-1)^{j+1} m}{2^m} \sum_{i=0}^{\lfloor m/2 \rfloor - j} \binom{m-2j}{i} c_n(m-2j-2i).$$

We need to make sure that the coefficients in (2.17) and (2.20) match. Clearly the coefficient of $c_n(m)$ is $1/2^m$ in both. Let $t = j + i$ and let's compute the coefficient of $c_n(m-2t)$ for a fixed value of t where $0 < t \leq \lfloor m/2 \rfloor$ in (2.20). This can be achieved through a summation where j runs from 1 to t and i is replaced by $t - j$, namely $c_n(m-2t)$ with its coefficient is

$$\sum_{j=1}^{t} \frac{(m-j-1)!}{(m-2j)!j!} \frac{(-1)^{j+1} m}{2^m} \binom{m-2j}{t-j} c_n(m-2t). \tag{2.21}$$

Simplifying the coefficients in (2.21) further we obtain

$$\frac{(m-j-1)!}{(m-2j)!j!} \frac{(-1)^{j+1} m}{2^m} \binom{m-2j}{t-j}$$
$$= \frac{(m-j-1)!}{(m-2j)!j!} \frac{(-1)^{j+1} m}{2^m} \frac{(m-2j)!}{(t-j)!(m-t-j)!}$$
$$= \frac{(m-j-1)!}{(t-j)!(m-t-j)!j!} \frac{(-1)^{j+1} m}{2^m}.$$

Now, the task comes down to showing the equality

$$\sum_{j=1}^{t} \frac{(m-j-1)!}{(t-j)!(m-t-j)!j!} \frac{(-1)^{j+1} m}{2^m} = \frac{1}{2^m} \binom{m}{t}$$

for $0 < t \leq \lfloor m/2 \rfloor$ for a given $m \geq 4$ using (2.17), in other words, showing that

$$\sum_{j=1}^{t} \frac{(-1)^{j+1} m (m-j-1)!}{j!(t-j)!(m-t-j)!} = \binom{m}{t}. \tag{2.22}$$

We will proceed by equating the denominators on the left. The common denominator is $t!(m-t)!$ as we can see from the right hand side.

$$\sum_{j=1}^{t} \binom{t}{j} \binom{m-t}{j} \frac{(-1)^{j+1} m (m-j-1)! j!}{t!(m-t)!} = \binom{m}{t}. \tag{2.23}$$

Canceling the denominators and dividing by m results in

$$\sum_{j=1}^{t} (-1)^{j+1} \binom{t}{j} \binom{m-t}{j} (m-j-1)! j! = (m-1)!. \tag{2.24}$$

Finally dividing by $(m-1)!$ yields

$$\sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\binom{m-t}{j}\binom{m-1}{j}^{-1}=1. \tag{2.25}$$

Now, we can simplify two of the combination terms and write them as a product:

$$\binom{m-t}{j}\binom{m-1}{j}^{-1}=\prod_{i=1}^{j}\frac{m-t-i+1}{m-i}.$$

Then (2.25) becomes

$$\sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=1}^{j}\frac{m-t-i+1}{m-i}=1. \tag{2.26}$$

Next, we multiply and divide the left hand side by $\prod_{i=j+1}^{t}(m-i)$ and then multiply both sides of the equation by $\prod_{i=1}^{t}(m-i)$. The result is

$$\sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=1}^{j}(m-t-i+1)\prod_{i=j+1}^{t}(m-i)=\prod_{i=1}^{t}(m-i). \tag{2.27}$$

If $t=1$, then both sides of (2.27) are equal to $m-1$. Let's assume now $1<t$. Note that for every value of j the first product on the left hand side produces $(m-t)$ when $i=1$. Therefore we can cancel out $(m-t)$ from both sides of (2.27) and adjust the indices accordingly to get

$$\sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=2}^{j}(m-t-i+1)\prod_{i=j+1}^{t}(m-i)=\prod_{i=1}^{t-1}(m-i). \tag{2.28}$$

Combining the two products into one on the left hand side and adjusting the index i after that yields

$$\begin{aligned}\sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=j+1}^{t+j-1}(m-i)&=\prod_{i=1}^{t-1}(m-i),\\ \sum_{j=1}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=1}^{t-1}(m-i-j)&=\prod_{i=1}^{t-1}(m-i).\end{aligned} \tag{2.29}$$

We can move the product on the right hand side to the left and write the result as

$$\sum_{j=0}^{t}(-1)^{j+1}\binom{t}{j}\prod_{i=1}^{t-1}(m-i-j)=0. \tag{2.30}$$

Now the task is showing the equality in (2.30). Combining the first two terms on the left hand side of (2.30) gives

$$-\prod_{i=1}^{t-1}(m-i)+t\prod_{i=1}^{t-1}(m-i-1)=(-1+t)(m-t-1)\prod_{i=2}^{t-1}(m-i). \tag{2.31}$$

Adding the $j=2$ term of (2.30) to the sum in (2.31) yields

$$\begin{aligned}(-1+t)(m-t-1)\prod_{i=2}^{t-1}(m-i)-\binom{t}{2}\prod_{i=1}^{t-1}(m-i-2)\\ =\left(-1+t-\binom{t}{2}\right)(m-t-1)(m-t-2)\prod_{i=3}^{t-1}(m-i)\\ =\left(\sum_{j=0}^{2}(-1)^{j+1}\binom{t}{j}\right)\left(\prod_{i=1}^{2}(m-t-i)\right)\left(\prod_{i=3}^{t-1}(m-i)\right).\end{aligned} \tag{2.32}$$

Suppose that combining the first k terms on the left hand side of (2.30) is given by

$$\left(\sum_{j=0}^{k-1}(-1)^{j+1}\binom{t}{j}\right)\left(\prod_{i=1}^{k-1}(m-t-i)\right)\left(\prod_{i=k}^{t-1}(m-i)\right). \tag{2.33}$$

If we add the $j=k$ term of (2.30) to the sum in (2.33) we obtain

$$\begin{aligned}\left(\sum_{j=0}^{k-1}(-1)^{j+1}\binom{t}{j}\right)\left(\prod_{i=1}^{k-1}(m-t-i)\right)\left(\prod_{i=k}^{t-1}(m-i)\right)\\ +(-1)^{k+1}\binom{t}{k}\prod_{i=1}^{t-1}(m-i-k).\end{aligned} \tag{2.34}$$

The common factors of (2.34) are

$$\left(\prod_{i=1}^{k-1}(m-t-i)\right)\left(\prod_{i=k+1}^{t-1}(m-i)\right) \tag{2.35}$$

and factoring them out of (2.34) leaves

$$\left(\sum_{j=0}^{k-1}(-1)^{j+1}\binom{t}{j}\right)(m-k)+(-1)^{k+1}\binom{t}{k}(m-t), \tag{2.36}$$

which can be rewritten as

$$(-1)^{k}\binom{t-1}{k-1}(m-k)+(-1)^{k+1}\binom{t}{k}(m-t) \tag{2.37}$$

using Lemma 2.3. Equating the denominators in (2.37) and simplifying the result we obtain

$$\begin{aligned}
&\frac{k(-1)^k(t-1)!(m-k)}{k!(t-k)!}+\frac{(-1)^{k+1}t!(m-t)}{k!(t-k)!}\\
&=\frac{(-1)^{k+1}(t-1)![\,-k(m-k)+t(m-t)\,]}{k!(t-k)!}\\
&=\frac{(-1)^{k+1}(t-1)!(t-k)(m-k-t)}{k!(t-k)!}\\
&=(-1)^{k+1}\binom{t-1}{k}(m-k-t)\\
&=\left(\sum_{j=0}^{k}(-1)^{j+1}\binom{t}{j}\right)(m-t-k)
\end{aligned}$$

using Lemma 2.3 once again. Now, putting this result and (2.35) together yields

$$\left(\sum_{j=0}^{k}(-1)^{j+1}\binom{t}{j}\right)\left(\prod_{i=1}^{k}(m-t-i)\right)\left(\prod_{i=k+1}^{t-1}(m-i)\right), \tag{2.38}$$

which finishes the induction. If we set now $k=t$ in the summation in (2.38) we get 0 using Lemma 2.2 and this proves the equality in (2.30). □

Lemma 2.2. *For $t>0$ we have*

$$\sum_{j=0}^{t}(-1)^{j+1}\binom{t}{j}=0.$$

Proof. The binomial expansion of $(x+y)^t$ is

$$(x+y)^t=\sum_{j=0}^{t}\binom{t}{j}x^{t-j}y^j. \tag{2.39}$$

Substitute $x=1, y=-1$ in (2.39) and multiply the result by -1. □

Lemma 2.3. *For $0\le k\le t$ we have*

$$\sum_{j=0}^{k}(-1)^{j+1}\binom{t}{j}=(-1)^{k+1}\binom{t-1}{k}. \tag{2.40}$$

Proof. If $k=0$, then both sides of (2.40) are equal to -1. If $k=t$, then the result follows from Lemma 2.2. Suppose now $0<k<t$ and (2.40) is true.

Then

$$\begin{aligned}\sum_{j=0}^{k+1}(-1)^{j+1}\binom{t}{j} &= \sum_{j=0}^{k}(-1)^{j+1}\binom{t}{j} + (-1)^k\binom{t}{k+1}\\ &= (-1)^{k+1}\binom{t-1}{k} + (-1)^k\binom{t}{k+1}\\ &= (-1)^{k+2}\binom{t-1}{k+1}\end{aligned} \tag{2.41}$$

using the inductive hypotheses and the definition of the entries of Pascal triangle. □

3. Results and examples

Using (2.12) we can conclude that the first two terms are

$$2^d\left(x^d - \frac{1}{2}\mu(n)x^{d-1}\right) = 2^d x^d - 2^{d-1}\mu(n)x^{d-1}. \tag{3.1}$$

Let's write the rest of the terms of $\Psi_n(x)$ as

$$2^d\sum_{i=2}^{d}(-1)^i e_i x^{d-i},$$

where e_i are as defined in (2.5) in terms of power sum functions. Lemma 2.1 tells us how to compute the power sum functions in terms of the Ramanujan sums.

Remark 3.1. Note that the matrix whose determinant yields e_d, call it M_d, carries the information for all the coefficients of $\Psi_n(x)$ starting with the term of degree $d-2$. However, computing the determinant of M_d will be eventually time consuming as n gets large. Therefore we need a way to avoid it. The following Theorem allows us to define the coefficients of $\Psi_n(x)$ recursively using the leading two coefficients as the input. More precisely:

Theorem 3.2. *Let $\Psi_n(x) = 2^d\sum_{i=0}^{d}(-1)^i e_i x^{d-i}$, where $e_0 = 1$ and $e_1 = \frac{\mu(n)}{2}$. Assume $n > 4, n \neq 6$. Then*

$$e_i = \frac{1}{i}\sum_{j=1}^{i}(-1)^{j-1}p_j e_{i-j} \tag{3.2}$$

for $i = 2, 3, \ldots, d$.

Proof. The assumption on n is just to make sure that the degree is at least 2. Let

$$M_i = \begin{pmatrix} p_1 & 1 & 0 & 0 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & 0 & 0 & \cdots & 0 \\ p_3 & p_2 & p_1 & 3 & 0 & \cdots & 0 \\ p_4 & p_3 & p_2 & p_1 & 4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & 0 \\ p_{i-1} & p_{i-2} & p_{i-3} & p_{i-4} & \cdots & p_1 & i-1 \\ p_i & p_{i-1} & p_{i-2} & p_{i-3} & \cdots & p_2 & p_1 \end{pmatrix}$$

for $2 \leq i \leq d$ and define $M_0 = 1, M_1 = p_1$. It will suffice to show that

$$|M_i| = \sum_{j=1}^{i} (-1)^{j-1} p_j \frac{(i-1)!}{(i-j)!} |M_{i-j}| \tag{3.3}$$

for $2 \leq i \leq d$ since $|M_i| = i! e_i$ by (2.5) and substituting this in (3.3) yields

$$\begin{aligned} i! e_i &= \sum_{j=1}^{i} (-1)^{j-1} p_j \frac{(i-1)!}{(i-j)!} |M_{i-j}| \\ &= \sum_{j=1}^{i} (-1)^{j-1} p_j \frac{(i-1)!}{(i-j)!} (i-j)! e_{i-j} \end{aligned}$$

$$i! e_i = \sum_{j=1}^{i} (-1)^{j-1} p_j (i-1)! e_{i-j} \tag{3.4}$$

and solving (3.4) for e_i gives (3.2). Now, we will prove (3.3). Let $i = 2$. Then

$$|M_2| = \left| \begin{bmatrix} p_1 & 1 \\ p_2 & p_1 \end{bmatrix} \right| = p_1^2 - p_2$$

and (3.3) gives

$$\begin{aligned} |M_2| &= \sum_{j=1}^{2} (-1)^{j-1} p_j \frac{(2-1)!}{(2-j)!} |M_{2-j}| \\ &= p_1 |M_1| - p_2 |M_0| = p_1^2 - p_2. \end{aligned}$$

Assume now $2 < i \leq d$. To find the determinant of M_i we will expand it on the last column:

$$|M_i| = p_1 |M_{i-1}| - (i-1) |M_{i-1,\, i}|, \tag{3.5}$$

where $M_{i-1,\,i}$ is the minor of M_i obtained by deleting row $i-1$ and column i :

$$M_{i-1,\,i} = \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ p_3 & p_2 & p_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{i-2} & p_{i-3} & p_{i-4} & \cdots & i-2 \\ p_i & p_{i-1} & p_{i-2} & \cdots & p_2 \end{pmatrix}.$$

Expanding on the last column again we find

$$|M_{i-1,\,i}| = p_2\,|M_{i-2}| - (i-2)\left|(M_{i-1,\,i})_{i-2,\,i-1}\right|,$$

where $(M_{i-1,\,i})_{i-2,\,i-1}$ is the minor of $M_{i-1,\,i}$ obtained by deleting row $i-2$ and column $i-1$:

$$(M_{i-1,\,i})_{i-2,\,i-1} = \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ p_3 & p_2 & p_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{i-3} & p_{i-4} & p_{i-5} & \cdots & i-3 \\ p_i & p_{i-1} & p_{i-2} & \cdots & p_3 \end{pmatrix}.$$

Continuing this way and substituting our findings in (3.5) we obtain

$$\begin{aligned} |M_i| &= p_1\,|M_{i-1}| - (i-1)p_2\,|M_{i-2}| + (i-1)(i-2)p_3\,|M_{i-3}| - \cdots \\ &\quad + (-1)^{i-3}(i-1)\cdots 3\cdot p_{i-2}\,|M_2| + (-1)^{i-2}(i-1)!p_{i-1}\,|M_1| \\ &\quad + (-1)^{i-1}(i-1)!p_i \cdot 1, \end{aligned} \tag{3.6}$$

which is the same as the expression in (3.3). The last two matrices in this sequence are

$$\begin{pmatrix} p_1 & 1 & 0 \\ p_2 & p_1 & 2 \\ p_i & p_{i-1} & p_{i-2} \end{pmatrix}, \quad \begin{pmatrix} p_1 & 1 \\ p_i & p_{i-1} \end{pmatrix}.$$

□

Another way of expressing $c_n(m)$ is

$$c_n(m) = \mu(u_m)\frac{\phi(n)}{\phi(u_m)}, \text{ where } u_m = \frac{n}{\gcd(n,m)}, \tag{3.7}$$

(see [4], page 238, for a proof). The example that follows will make use of this formula.

Example 3.3. Let $n = 66$. Then $\phi(n) = 20$ and $d = 10$. We have defined $e_0 = 1, e_1 = \frac{1}{2}\mu(n) = -\frac{1}{2}$. Recall that $c_n(0) = d = 10, c_n(1) = \mu(n) = -1$, and $p_1 = e_1 = \frac{1}{2}\mu(n) = -\frac{1}{2}$. Now, what we need is p_i and $c_n(i)$ for $2 \leq i \leq 10$. Using (3.7) we obtain

$$c_n(2) = 1,\ c_n(3) = 2,\ c_n(4) = 1,\ c_n(5) = -1,$$
$$c_n(6) = -2, c_n(7) = -1,\ c_n(8) = 1,\ c_n(9) = 2,\ c_n(10) = 1$$

and using (2.17) we compute p_i as

$$p_2 = \frac{21}{4},\ p_3 = -\frac{1}{8},\ p_4 = \frac{65}{16},\ p_5 = -\frac{1}{2},\ p_6 = \frac{219}{64},$$
$$p_7 = -\frac{1}{128},\ p_8 = \frac{769}{256},\ p_9 = -\frac{1}{512},\ p_{10} = \frac{2771}{1024}.$$

Now we can compute e_i for $2 \leq i \leq 10$ using (3.2):

$$e_2 = \frac{1}{2}(p_1e_1 - p_2e_0) = \frac{1}{2}\left(\frac{1}{4} - \frac{21}{4}\right) = -\frac{5}{2},$$
$$e_3 = \frac{1}{3}(p_1e_2 - p_2e_1 + p_3e_0) = \frac{1}{3}\left(\frac{1}{2}\cdot\frac{5}{2} + \frac{21}{4}\cdot\frac{1}{2} - \frac{1}{8}\right) = \frac{5}{4},$$
$$e_4 = \frac{1}{4}(p_1e_3 - p_2e_2 + p_3e_1 - p_4e_0) = \frac{1}{4}\left(-\frac{1}{2}\cdot\frac{5}{4} + \frac{21}{4}\cdot\frac{5}{2} + \frac{1}{8}\cdot\frac{1}{2} - \frac{65}{16}\right) = \frac{17}{8}.$$

Further computation yields

$$e_5 = -\frac{17}{16},\ e_6 = -\frac{43}{64},\ e_7 = \frac{43}{128},\ e_8 = \frac{3}{64},\ e_9 = -\frac{3}{128},\ e_{10} = \frac{1}{1024}.$$

Therefore

$$\Psi_n(x) = 2^{10}\Big(x^{10} + \frac{1}{2}x^9 - \frac{5}{2}x^8 - \frac{5}{4}x^7 + \frac{17}{8}x^6 + \frac{17}{16}x^5$$
$$-\frac{43}{64}x^4 - \frac{43}{128}x^3 + \frac{3}{64}x^2 + \frac{3}{128}x + \frac{1}{1024}\Big),$$

and $\Psi_{66}(x) = 1024x^{10} + 512x^9 - 2560x^8 - 1280x^7 + 2176x^6 + 1088x^5$
$- 688x^4 - 344x^3 + 48x^2 + 24x + 1.$

Next, we will show the relation between $\Psi_q(x)$ and $\Psi_{2q}(x)$ when q is odd. First, we note that $\phi(q) = \phi(2q)$ for $q \geq 3$ in that case. Therefore both polynomials have the same degree.

Theorem 3.4. *Let q be an odd integer. If $\Psi_q(x) = 2^d \sum_{i=0}^{d}(-1)^i e_i x^{d-i}$ and $\Psi_{2q}(x) = 2^d \sum_{i=0}^{d}(-1)^i e'_i x^{d-i}$, then $e_i = e'_i$ for $i-$ even and $e_i = -e'_i$ for $i-$ odd.*

Proof. The claim is trivially true when $q = 1$ because $\Psi_1(x) = 2x - 2$ and $\Psi_2(x) = 2x + 2$. Assume now $q \geq 3$. First of all $e_0 = e'_0 = 1$. If $\mu(q) = 0$, then $\mu(2q) = 0$, otherwise $\mu(q) = -\mu(2q)$ because $2q$ has one more prime among its factors that q doesn't have. In either case we have $e_1 = -e'_1$. Next, we will compute p_i and p'_i for $2 \leq i \leq d$. Suppose i is odd. According to (2.17) we need to compute $c_q(j)$ and $c_{2q}(j)$ for $j = i, i-2, i-4, \ldots, 1$. Note that

$$\frac{2q}{\gcd(2q,j)} = 2\frac{q}{\gcd(q,j)}$$

because both q and j are odd. Therefore we have

$$c_q(j) = \mu(u_j)\frac{\phi(q)}{\phi(u_j)}, \text{ where } u_j = \frac{q}{\gcd(q,j)} \quad \text{and}$$
$$c_{2q}(j) = \mu(v_j)\frac{\phi(2q)}{\phi(v_j)} = \mu(2u_j)\frac{\phi(2q)}{\phi(2u_j)}, \text{ because } v_j = \frac{2q}{\gcd(2q,j)} = 2u_j.$$

Using $\phi(q) = \phi(2q), \phi(u_j) = \phi(2u_j)$, because both q and u_j are odd numbers greater than or equal to 3, and $\mu(2u_j) = -\mu(u_j)$, for the same reason used for $\mu(q) = -\mu(2q)$ earlier, we conclude that $c_q(j) = -c_{2q}(j)$. Therefore $p_i = -p'_i$ when i is odd using (2.17). Suppose now i is even. We need to compute $c_q(j)$ and $c_{2q}(j)$ for $j = i, i-2, i-4, \ldots, 2$. This time we have

$$\frac{2q}{\gcd(2q,j)} = \frac{2q}{2\gcd(q,j)} = \frac{q}{\gcd(q,j)}$$

because q is odd and j is even. Therefore

$$c_q(j) = \mu(u_j)\frac{\phi(q)}{\phi(u_j)}, \text{ where } u_j = \frac{q}{\gcd(q,j)} \quad \text{and}$$
$$c_{2q}(j) = \mu(v_j)\frac{\phi(2q)}{\phi(v_j)} = \mu(u_j)\frac{\phi(2q)}{\phi(u_j)}, \text{ because } v_j = \frac{2q}{\gcd(2q,j)} = u_j.$$

Therefore $p_i = p'_i$ when i is even, using (2.17), because $\phi(q) = \phi(2q)$. Now we will prove the theorem using induction on i in e_i. The initial step is true as mentioned above: $e_0 = e'_0$ and $e_1 = -e'_1$. Suppose $e_j = -e'_j$ for $j-$ odd with $3 \leq j < i$ and $e_j = e'_j$ for $j-$ even with $2 \leq j < i$. Suppose i is odd. Then in each term of the recursive expansion of e_i given in (3.2) exactly one of the two multiplicands is negative of the respective element with prime. Namely,

$$e_i = \frac{1}{i}\sum_{j=1}^{i}(-1)^{j-1}p_j e_{i-j} = \frac{1}{i}\left(p_1 e_{i-1} - p_2 e_{i-2} + \cdots - p_{i-1}e_1 + p_i e_0\right)$$
$$= \frac{1}{i}\left((-p'_1)e'_{i-1} - p'_2(-e'_{i-2}) + \cdots - p'_{i-1}(-e'_1) + (-p'_i)e'_0\right) = -e'_i$$

using induction assumption and $p_1 = e_1, p'_1 = e'_1$. Using the same reasoning we get

$$e_i = \frac{1}{i}\sum_{j=1}^{i}(-1)^{j-1}p_j e_{i-j} = \frac{1}{i}\left(p_1 e_{i-1} - p_2 e_{i-2} + \cdots - p_{i-1}e_1 + p_i e_0\right)$$
$$= \frac{1}{i}\left((-p'_1)(-e'_{i-1}) - p'_2(e'_{i-2}) + \cdots - (-p'_{i-1})(-e'_1) + p'_i e'_0\right) = e'_i$$

for $i-$ even by realizing that each term of the recursive expansion of e_i this time has two multiplicands of the same sign when we replace them by those that have prime. This finishes the proof. □

Example 3.5.

$$\Psi_{27}(x) = 512\,x^9 - 1152\,x^7 + 864\,x^5 - 240\,x^3 + 18\,x + 1,$$
$$\Psi_{54}(x) = 512\,x^9 - 1152\,x^7 + 864\,x^5 - 240\,x^3 + 18\,x - 1.$$

Example 3.6.

$$\Psi_{21}(x) = 64\,x^6 - 32\,x^5 - 96\,x^4 + 48\,x^3 + 32\,x^2 - 16\,x + 1,$$
$$\Psi_{42}(x) = 64\,x^6 + 32\,x^5 - 96\,x^4 - 48\,x^3 + 32\,x^2 + 16\,x + 1.$$

Corollary 3.7. *Let q be an odd integer. Then*

$$\Psi_{2q}(x) = (-1)^d \Psi_q(-x),$$

where d is the degree of $\Psi_q(x)$.

Proof. The claim is true for $q = 1$ because $(-1)^1\Psi_1(-x) = -(2(-x) - 2)$, which is equal to $\Psi_2(x) = 2x + 2$. If $q \geq 3$, then $\phi(q) = \phi(2q)$ as noted before Theorem 3.4 because q is odd. Therefore the leading term of both $\Psi_q(x)$ and $\Psi_{2q}(x)$ is $2^d x^d$. First, let's suppose that d is even. Then by Theorem 3.4 the coefficients of all even degree terms of $\Psi_{2q}(x)$ agree with those of $\Psi_q(x)$. Also, the coefficients of all odd degree terms of $\Psi_{2q}(x)$ are opposites of those of $\Psi_q(x)$. Another way of saying this is $\Psi_{2q}(x) = \Psi_q(-x)$. Suppose now d is odd. Since the leading coefficients are the same the coefficients of all odd degree terms of $\Psi_{2q}(x)$ agree with those of $\Psi_q(x)$. Likewise the coefficients of all even degree terms of $\Psi_{2q}(x)$ are opposites of those of $\Psi_q(x)$. We can write this fact as $\Psi_{2q}(x) = -\Psi_q(-x)$. □

Theorem 3.8. *Let $n > 4$. If n is divisible by 4, then $\Psi_n(x)$ is a polynomial consisting of even powers of x only.*

Proof. Let $n = 4m$. First, we will show that p_{2k+1} vanish for $k \geq 0$. Clearly $p_1 = \mu(n)/2 = 0$ by (2.12) and $p_{2k+1} = 0$ for $k > 0$ will follow once we show that $c_n(j) = 0$ for odd values of $j > 1$ because of (2.17) and the fact that $c_n(1) = \mu(n) = 0$ by (2.11). According to (3.7)

$$c_n(j) = \mu(u_j)\frac{\phi(n)}{\phi(u_j)}, \text{ where } u_j = \frac{4m}{\gcd(4m, j)}.$$

If $\gcd(4m, j) = 1$, then $u_j = 4m$ and $\mu(u_j) = 0$, which yields $c_n(j) = 0$. Suppose $\gcd(4m, j) \neq 1$. Since j is odd $\gcd(4m, j)$ can not be even and because of that $\gcd(4m, j) \nmid 4$, which means u_j is divisible by 4. Therefore $\mu(u_j) = 0$. Thus $c_n(j) = 0$ for odd values of j and our claim that $p_{2k+1} = 0$ follows. Now we will prove the theorem by showing that $e_{2k+1} = 0$ for $k \geq 0$ because $\Psi_n(x) = 2^d \sum_{i=0}^{d} (-1)^i e_i x^{d-i}$ and $d = \phi(n)/2$ is even. In order to see that d is even it suffices to show that $4 \,|\, \phi(n)$ which follows from the fact that

$\phi(4m) = 2\phi(2m)$ and evenness of $\phi(2m)$ because of the assumption $2m \geq 4$. We will use induction to achieve that. The first step is $e_1 = 0$, which follows from $e_1 = p_1$ by definition. Suppose that $e_j = 0$ for $j = 3, 5, \ldots, 2k-1$. Then according to (3.2)

$$\begin{aligned} e_{2k+1} &= \frac{1}{2k+1} \sum_{j=1}^{2k+1} (-1)^{j-1} p_j e_{2k+1-j} \\ &= \frac{1}{2k+1} \left(p_1 e_{2k} - p_2 e_{2k-1} + p_3 e_{2k-2} - \cdots - p_{2k} e_1 + p_{2k+1} e_0 \right). \end{aligned}$$

The terms with plus sign in the expansion above all vanish because we showed earlier that $p_j = 0$ for $j = 1, 3, 5, \ldots, 2k+1$ and the terms with minus sign also vanish because of our induction assumption and $e_1 = 0$. □

Example 3.9.

$$\Psi_{60}(x) = 256\,x^8 - 448\,x^6 + 224\,x^4 - 32\,x^2 + 1,$$

$$\Psi_{72}(x) = 4096\,x^{12} - 12288\,x^{10} + 13824\,x^8 - 7168\,x^6 + 1680\,x^4 - 144\,x^2 + 1.$$

Acknowledgment. This work was partially supported by PSC-CUNY Research Award.

References

[1] S. Beslin and V. De Angelis, *The minimal polynomials of* $\sin(2\pi/p)$ *and* $\cos(2\pi/p)$, Math. Mag. **77** (2004), no. 2, 146–149.
[2] P. Borwein and T. Erdélyi, *Polynomials and Polynomial Inequalities*, Springer-Verlag, NY, Inc., 1995.
[3] E. Grosswald, *Topics from the Theory of Numbers*, The Macmillan Company, NY, 1966.
[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fourth Ed. Oxford University Press, London. 1975.
[5] D. H. Lehmer, *A Note on Trigonometric Algebraic Numbers*, Amer. Math. Monthly **40** (1933), no. 3, 165–166.
[6] I. G. Macdonald, *Symmetric functions and Hall polynomials*, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1979.
[7] D. Surowski and P. McCombs, *Homogeneous polynomials and the minimal polynomial of* $\cos(2\pi/n)$, Missouri J. Math. Sci. **15** (2003), no. 1, 4–14.
[8] C. R. Wall, *Selected Topics in Elementary Number Theory*, University of South Carolina Press, Columbia, S.C., 1974.
[9] W. Watkins and J. Zeitlin, *The Minimal Polynomial of* $\cos(2\pi/n)$, The American Mathematical Monthly **100** (1993), no. 5, 471–474.
[10] K. W. Wegner, *Trigonometric values that are algebraic numbers*, The Mathematics Teacher **50** (1957), no. 8, 557–561.
[11] ———, *Equations with trigonometric values as roots*, Amer. Math. Monthly **66** (1959), no. 1, 52–53.

Yusuf Z. Gürtaş
Department of Mathematics and Computer Sciences
Queensborough Community College, CUNY
222-05 56th Avenue Bayside, NY 11364, USA
E-mail address: ygurtas@qcc.cuny.edu