ROOTS OF UNITY AND CIRCULAR SUBSETS WITHOUT CONSECUTIVE ELEMENTS

John Konvalina
Department of Mathematics and Computer Science, University of Nebraska at Omaha, Omaha, NE 68182
(*Submitted March, 1994*)

1. INTRODUCTION

Recall that the n^{th} roots of unity are the roots of the polynomial $x^n - 1$. Also, they have a geometrical interpretation in terms of the vertices of a regular polygon with n sides inscribed in the unit circle. Now consider the polynomial of degree n with the property that each of its roots is the sum of an n^{th} root of unity and its square. That is, let U_n denote the set of n^{th} roots of unity and consider the polynomial

$$P_n(x) = \prod_{\zeta \in U_n} (x - (\zeta + \zeta^2)).$$

What are the coefficients of $P_n(x)$? *A priori* the coefficients are complex numbers. However, we will show they are actually integers. In fact, we will prove the unexpected result that the absolute value of the coefficient of x^k has a combinatorial interpretation in terms of the number of k-subsets of n objects arranged in a circle with no two selected objects being consecutive. The sum of the coefficients is expressed in terms of Lucas numbers.

2. COMBINATORIAL IDENTITIES

Before proving the theorem, we will state some known combinatorial identities. We assume throughout the paper that $n > 0$. It is well known that the number of k-subsets without consecutive elements chosen from n objects arranged in a circle is (see Riordan [3], p. 198)

$$\frac{n}{n-k}\binom{n-k}{k}.$$

The generating function of this sequence has the following closed form:

$$\sum_{k=0}^{[\frac{n}{2}]} \frac{n}{n-k}\binom{n-k}{k} x^k = \left(\frac{1+\sqrt{1+4x}}{2}\right)^n + \left(\frac{1-\sqrt{1+4x}}{2}\right)^n. \tag{1}$$

When $x = -1$ we obtain the following identity [since $\frac{1}{2}(1 \pm \sqrt{-3})$ are sixth roots of unity]:

$$\sum_{k=0}^{[\frac{n}{2}]} \frac{n}{n-k}\binom{n-k}{k}(-1)^k = \begin{cases} 2(-1)^n & \text{if } n \equiv 0 \pmod 3, \\ (-1)^{n-1} & \text{if } n \not\equiv 0 \pmod 3. \end{cases} \tag{2}$$

The following identity will also be used:

$$\sum_{k=0}^{[\frac{n}{2}]} \binom{n-k}{k}(-1)^k = \frac{(-1)^{[\frac{n}{3}]} + (-1)^{[\frac{n+1}{3}]}}{2}. \tag{3}$$

References for these combinatorial identities include Graham, Knuth, & Patashnik [2], pp. 178-79 and 204, or Riordan [4], pp. 75-77, or Gould [1], Identities 1.64, 1.68, and 1.75.

3. THE THEOREM

Theorem: The roots of the polynomial

$$P_n(x) = x^n + (-1)^n - \sum_{k=0}^{[\frac{n}{2}]} \frac{n}{n-k}\binom{n-k}{k} x^k \tag{4}$$

are precisely the n complex numbers (not necessarily distinct) of the form $\zeta+\zeta^2$, where ζ ranges over U_n the n^{th} roots of unity. That is,

$$\prod_{\zeta\in U_n}(x-(\zeta+\zeta^2)) = x^n + (-1)^n - \sum_{k=0}^{[\frac{n}{2}]} \frac{n}{n-k}\binom{n-k}{k} x^k .$$

Proof: Let ζ denote any n^{th} root of unity. Then $x=\zeta+\zeta^2$ is a root of $P_n(x)$ of and only if

$$\sum_{k=0}^{[\frac{n}{2}]} \frac{n}{n-k}\binom{n-k}{k}(\zeta+\zeta^2)^k = (\zeta+\zeta^2)^n + (-1)^n = (1+\zeta)^n + (-1)^n. \tag{5}$$

But (5) follows immediately from (1) since $1+4(\zeta+\zeta^2) = (2\zeta+1)^2$ *and* $\zeta^n = 1$. Hence, if the n complex numbers, $\zeta+\zeta^2$, are distinct as ζ ranges over U_n, then all roots of $P_n(x)$ have been determined.

To complete the proof, we will show all the roots are distinct except when $n\equiv 0 \pmod 3$. In that case, $x=-1$ will be a double root. To verify this, first observe that by (2) and (4) $x=-1$ is a root of $P_n(x)$ if and only if $n\equiv 0 \pmod 3$. Now the derivative of $P_n(x)$ is

$$P_n'(x) = nx^{n-1} - n\sum_{k=0}^{[\frac{n-2}{2}]}\binom{n-2-k}{k}x^k . \tag{6}$$

So $x=-1$ is a root of $P_n'(x)$ if and only if

$$\sum_{k=0}^{[\frac{n-2}{2}]}\binom{n-2-k}{k}(-1)^k = (-1)^{n-1}. \tag{7}$$

But, if $n\equiv 0 \pmod 3$, then (7) follows immediately from (3) with n replaced by $n-2$ and noting that [since $(-1)^{n/3} = (-1)^n$]

$$(-1)^{[\frac{n-2}{3}]} = (-1)^{\frac{n-3}{3}} = (-1)^{n-1}.$$

Thus, $x=-1$ is at least a double root of $P_n(x)$ when $n\equiv 0 \pmod 3$. Finally, we will show $x=-1$ is in fact a double root. First, however, a lemma to determine when the sum of two n^{th} roots of unity is equal to -1.

Lemma: Let ζ_n denote the primitive n^{th} root of unity $\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$. Suppose $0\le j<k<n$. Then, for some j and k, $\zeta_n^j+\zeta_n^k=-1$ if and only if $n=3j$ and $k=2j$.

Proof: If $n=3j$ and $k=2j$, then $\zeta_{3j}^j+\zeta_{3j}^{2j}$ is a sum of the primitive cube roots of unity and, hence, is equal to -1. Conversely, suppose the sum of the two n^{th} roots of unity is equal to -1. Equating real and imaginary parts, we obtain $\cos\frac{2\pi}{n}j+\cos\frac{2\pi}{n}k=-1$ and $\sin\frac{2\pi}{n}j+\sin\frac{2\pi}{n}k=0$. Now solve for $\cos\frac{2\pi}{n}k$ and $\sin\frac{2\pi}{n}k$:

$$\cos\frac{2\pi}{n}k=-1-\cos\frac{2\pi}{n}j \tag{8}$$

and

$$\sin\frac{2\pi}{n}k=-\sin\frac{2\pi}{n}j. \tag{9}$$

Next, square both sides of (8) and (9), then add to obtain $\cos\left(\frac{2\pi}{n}j\right)=-\frac{1}{2}$. Similarly, solving the original equations for $\cos\frac{2\pi}{n}j$ and $\sin\frac{2\pi}{n}j$, we obtain $\cos\left(\frac{2\pi}{n}k\right)=-\frac{1}{2}$. Since $0\le j<k<n$, we must have $\frac{2\pi}{n}j=\frac{2\pi}{3}$ and $\frac{2\pi}{n}k=\frac{4\pi}{3}$. Hence, $n=3j$ and $3k=2n$. Therefore, $n=3j$ and $k=2j$, and the lemma is proved.

Now we return to the proof of the theorem to determine when the roots of $P_n(x)$ will not be distinct. Suppose $0\le j<k<n$ and two roots are the same. Then

$$\zeta_n^j+\zeta_n^{2j}=\zeta_n^k+\zeta_n^{2k} \tag{10}$$

Hence, $\zeta_n^j-\zeta_n^k=\zeta_n^{2k}-\zeta_n^{2j}=(\zeta_n^k-\zeta_n^j)(\zeta_n^k+\zeta_n^j)$. So we must have

$$\zeta_n^j+\zeta_n^k=-1. \tag{11}$$

Therefore, by the lemma, ζ_n^j and ζ_n^k are the primitive cube roots of unity. Since the square of one primitive cube root of unity is the other primitive cube root, the root $x=-1$ will occur exactly twice in $\zeta+\zeta^2$ as ζ ranges over the n^{th} roots of unity for $n\equiv 0 \pmod 3$.

Corollary: $P_n(1)=\begin{cases}-L_n & \text{if } n \text{ is odd,}\\ -L_n+2 & \text{if } n \text{ is even,}\end{cases}$ where L_n is the n^{th} Lucas number.

Proof: It is well known that $\sum_{k\ge 0}\frac{n}{n-k}\binom{n-k}{k}=L_n$, where L_n is the n^{th} Lucas number.

REFERENCES

1. H. W. Gould. *Combinatorial Identities.* Morgantown, WV, 1972.
2. R. L. Graham, D. E. Knuth, & O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science.* Reading, MA: Addison-Wesley, 1989.
3. J. Riordan. *An Introduction to Combinatorial Analysis.* New York: Wiley, 1958.
4. J. Riordan. *Combinatorial Identities.* New York: Wiley, 1968.

AMS Classification Number: 05A15

❖❖❖