PRIME POWERS OF ZEROS OF MONIC POLYNOMIALS WITH INTEGER COEFFICIENTS

Garry J. Tee
Department of Mathematics, University of Auckland, Auckland, New Zealand
(*Submitted December 1992*)

1. INTRODUCTION

For a monic polynomial with integer coefficients $x^d - a_1 x^{d-1} - \cdots - a_d$, the sum S_k of the k^{th} powers of the zeros is an integer, for positive integer k. For prime p, $S_p \equiv a_1 \pmod p$; and hence, if $a_1 = 0$ then $p | S_p$. If $a_d = \pm 1$, then similar congruences hold for sums of negative powers of the zeros. Illustrations are given for various types of Chebyshev polynomials with integer argument.

2. SYMMETRIC FUNCTIONS OF ROOTS

Consider the monic polynomial equation with complex (or real) coefficients

$$x^d - a_1 d^{d-1} - a_2 x^{d-2} - \cdots - a_d = 0. \tag{1}$$

The roots of equation (1) will be denoted by $\alpha, \beta, \gamma, \ldots, \psi, \omega$, and those symmetric functions of the roots that are called *sigma functions* will be denoted thus:

$$\begin{aligned}
&\Sigma\alpha \overset{\text{def}}{=} \alpha + \beta + \cdots + \omega, \\
&\Sigma\alpha\beta \overset{\text{def}}{=} \alpha\beta + \alpha\gamma + \cdots + \alpha\omega + \beta\gamma + \cdots + \beta\omega + \cdots + \psi\omega, \\
&\Sigma\alpha^3\beta^2 \overset{\text{def}}{=} \alpha^3\beta^2 + \alpha^3\gamma^2 + \cdots + \alpha^3\omega^2 + \beta^3\gamma^2 + \cdots + \beta^3\omega^2 + \cdots + \psi^3\omega^2 \\
&\qquad + \beta^3\alpha^2 + \gamma^3\alpha^2 + \cdots + \omega^3\alpha^2 + \gamma^3\beta^2 + \cdots + \omega^3\beta^2 + \cdots + \omega^3\psi^2, \\
&\qquad\qquad \textit{et cetera}.
\end{aligned} \tag{2}$$

The sigma functions $\Sigma\alpha, \Sigma\alpha\beta, \Sigma\alpha\beta\gamma, \ldots, \Sigma\alpha\beta\gamma\ldots\omega$ are called the *elementary symmetric functions* of $\alpha, \beta, \gamma, \ldots, \omega$, and Vieta's Rule expresses them in terms of the coefficients of the polynomial (1):

$$\begin{aligned}
&\Sigma\alpha = a_1, \quad \Sigma\alpha\beta = -a_2, \quad \Sigma\alpha\beta\gamma = a_3, \\
&\ldots, \ \Sigma\alpha\beta\gamma\ldots\omega = \alpha\beta\gamma\ldots\omega = (-1)^{d-1} a_d.
\end{aligned} \tag{3}$$

Each symmetric polynomial with integer coefficients can be expressed as a polynomial in the elementary symmetric functions, with integer coefficients ([1], p. 67).

Therefore, if all coefficients $a_1, \ldots, a_d$ of the monic polynomial (1) are integers (positive, negative, or zero), each symmetric polynomial [in the roots of (1)] with integer coefficients has integer value. In particular, each sigma function then has integer value.

For integer k, denote the sum of the k^{th} powers of the roots as

$$S_k \overset{\text{def}}{=} \Sigma\alpha^k = \alpha^k + \beta^k + \cdots + \omega^k, \tag{4}$$

which is a sigma function if $k > 0$. The initial values $S_1, S_2, \ldots, S_d$ may be computed successively by Newton's Rule:

$$S_k = a_1 S_{k-1} + a_2 S_{k-2} + \cdots + a_{k-2} S_2 + a_{k-1} S_1 + k \cdot a_k \quad (k = 1, 2, \ldots, d), \tag{5}$$

and for $k > d$, Newton's Rule becomes the recurrence relation

$$S_k = a_1 S_{k-1} + a_2 S_{k-2} + \cdots + a_d S_{k-d} \quad (k = d+1, d+2, d+3, \ldots), \tag{6}$$

by which $S_{d+1}, S_{d+2}, S_{d+3}, \ldots$ may be computed successively.

If the coefficients $a_1, \ldots, a_d$ are integers, then S_k has integer value for all positive integers k, by the general result cited above for symmetric polynomials with integer coefficients. But for the S_k, it is simpler to note [from (5)] that $S_1 = a_1$, and the result then follows from (5) and (6) by induction on k.

From Newton's Rule, the sums of powers of roots can be expressed in terms of the coefficients of the monic polynomial (1). For example,

$$\begin{aligned}
&S_1 = a_1, \quad S_2 = a_1^2 + 2a_2, \quad S_3 = a_1^3 + 3(a_1 a_2 + a_3),\\
&S_4 = a_1^4 + 4a_1^2 a_2 + 4a_1 a_3 + 2a_2^2 + 4a_4,\\
&S_5 = a_1^5 + 5(a_1^3 a_2 + a_1^2 a_3 + a_1(a_2^2 + a_4) + a_2 a_3 + a_5),\\
&S_6 = a_1^6 + 6a_1^4 a_2 + 6a_1^3 a_3 + a_1^2(9a_2^2 + 6a_4) + a_1(12a_2 a_3 + 6a_5)\\
&\qquad + 2a_2^3 + 18a_2 a_4 + 3a_3^2 + 6a_6,\\
&S_7 = a_1^7 + 7(a_1^5 a_2 + a_1^4 a_3 + a_1^3(2a_2^2 + a_4) + a_1^2(3a_2 a_3 + a_5)\\
&\qquad + a_1(a_2^3 + 2a_2 a_4 + a_3^2 + a_6) + a_2^2 a_3 + a_2 a_5 + a_3 a_4 + a_7),
\end{aligned} \tag{7}$$

where a_j is taken as 0 if $j > d$.

Waring's formula (of 1762) expresses S_k explicitly ([1], p. 72) in terms of the coefficients of the monic polynomial (1):

$$S_k = \sum \frac{k \cdot (r_1 + r_2 + \cdots + r_d - 1)!}{r_1! r_2! \ldots r_d!} a_1^{r_1} a_2^{r_2} \ldots a_d^{r_d}, \tag{8}$$

where the sum extends over all sets of nonnegative integers $r_1, r_2, \ldots, r_d$ for which

$$r_1 + 2r_2 + 3r_3 + \cdots + dr_d = k. \tag{9}$$

The expressions (7) for $S_1, \ldots, S_7$ suggest that S_k has some interesting divisibility properties for prime k.

3. DIVISIBILITY OF SUMS OF PRIME POWERS OF ROOTS

Hereinafter, the polynomial coefficients $a_1, \ldots, a_d$ are taken to be integers, except where otherwise stated.

Theorem 1: For all primes p, $S_p \equiv a_1 \pmod{p}$.

Proof: If all roots are integers, then by Fermat's Little Theorem,

$$S_p = \alpha^p + \beta^p + \cdots + \omega^p \equiv \alpha + \beta + \cdots + \omega \equiv a_1 \pmod{p}. \tag{10}$$

In the general case, when the roots are algebraic numbers, expand S_1^k by the Multinomial Theorem:

$$S_1^k = (\alpha+\beta+\gamma+\cdots+\omega)^k$$
$$= \alpha^k+\beta^k+\gamma^k+\cdots+\omega^k + \sum_{q+\cdots+v=k} \frac{k!}{q!r!s!\ldots v!} \sum \alpha^q\beta^r\gamma^s\ldots\omega^v, \tag{11}$$

where at least two of the indices q, r, ..., v are positive integers, and the others equal zero. This may be rewritten as:

$$a_1^k = S_k + \sum_{q+\cdots+v=k} \frac{k!}{q!r!s!\ldots v!} \sum \alpha^q\beta^r\gamma^s\ldots\omega^v. \tag{12}$$

Each multinomial coefficient is an integer; hence, the denominator $q!r!s! \ldots v!$ divides the numerator $k! = k(k-1)!$. Every factor in the denominator is strictly less than k; and hence, if k is prime the denominator and k are coprime, so the denominator must then divide the other factor $(k-1)!$ in the numerator. Therefore, if k is prime then each such multinomial coefficient is an integer multiple of k.

But we have seen that, if all coefficients $a_1, \ldots, a_d$ are integers, then each of the sigma functions in (12) has integer value. Thus, if k is any prime p, then it follows from (12) that

$$a_1^p = S_p + pF_p, \tag{13}$$

where F_p is an integer* which depends on p (and also on $a_1, a_2, \ldots, a_d$). Therefore,

$$S_p \equiv a_1^p \equiv a_1 \pmod{p}, \tag{14}$$

by Fermat's Little Theorem. □

Corollary 1.1: If p is prime, then $p|S_p \Leftrightarrow p|a_1$.

Corollary 1.2: If $a_1 = \pm 1$, then S_p is not a multiple of p for any prime p.

Corollary 1.3: If $a_1 = \pm q^e$, where q is prime and $e \geq 1$, then q is the only prime p for which $p|S_p$.

It was shown above that, if k is prime, then each such multinomial coefficient is an integer multiple of k. However, the converse does not hold. For example, $k!/(1!)^k = k(k-1)!$ for all $k \geq 2$; $k!/(2!(1!)^{k-1}) = k \times ((k-1)(k-2)\ldots 3)$ for all $k \geq 3$; $8!/(2!)^4 = 8 \times (7 \times 5 \times 3^2)$, and so on.

Theorem 2: S_p is an integer multiple of p for all primes p, if and only if $a_1 = 0$.

Proof: If $a_1 = 0$, then equation (13) reduces to $S_p = -pF_p$, and hence $p|S_p$.**

If $p|S_p$ then (by Theorem 1, Corollary 1), $p|a_1$ and, if this holds for infinitely many primes p, then $a_1 = 0$. □

The converse does not hold, since examples exist with $k|S_k$ where k is composite. For example (see [2]), take $d = 3$ with roots 1, 1, –2 (with $\sum \alpha = a_1 = 0$), for which the characteristic

* The proof given in Theorem 1 of [2] for this result is valid only for the case in which all roots $\alpha, \beta, \ldots$ are integers.

** This is Theorem 2 in [2].

polynomial is $(x-1)^2(x+2) = x^3 - 3x + 2$ and $S_k = 2 + (-2)^k$. In this case, $S_6 = 66$ so that $6|S_6$, and 6 is composite.

Lemma: If $a_d = \pm 1$, then S_k has integer values for all integers k—positive, zero, and negative.

Proof: For general complex coefficients $a_1, \ldots, a_d$, if $a_d \neq 0$, then $\alpha\beta\gamma \ldots \omega = (-1)^{d-1} a_d \neq 0$, so that no root equals 0; hence, S_0 exists:

$$S_0 = \alpha^0 + \beta^0 + \cdots + \omega^0 = 1 + 1 + \cdots + 1 = d. \tag{15}$$

The monic polynomial equation inverse to (1),

$$z^d + \frac{a_{d-1}}{a_d} z^{d-1} + \frac{a_{d-2}}{a_d} z^{d-2} + \cdots + \frac{a_1}{a_d} z - \frac{1}{a_d} = 0, \tag{16}$$

has roots $\alpha^{-1}, \beta^{-1}, \ldots, \omega^{-1}$, including multiplicity. Accordingly, for $k \leq -1$, S_k can be constructed by Newton's Rule from the coefficients in (16), similarly to (5) and (6).

If all coefficients $a_1, \ldots, a_d$ in (1) are integers and $a_d = \pm 1$, then all coefficients of the monic polynomial (16) are integers. It follows as in (5) and (6) that S_k has integer value for all integers $k \leq -1$. Combining these results with the previous result for $k \geq 1$, we get that S_k has integer value for all integers k. □

Theorem 3: If p is prime, $S_{-p} \equiv -a_{d-1} \pmod{p}$ if $a_d = 1$, and $S_{-p} \equiv a_{d-1} \pmod{p}$ if $a_d = -1$.

Proof: Apply Theorem 1 to the inverse polynomial equation (13), which is now

$$\begin{cases} z^d + a_{d-1}z^{d-1} + a_{d-2}z^{d-2} + \cdots + a_1 z - 1 = 0 & \text{if } a_d = +1, \\ z^d - a_{d-1}z^{d-1} - a_{d-2}z^{d-2} - \cdots - a_1 z + 1 = 0 & \text{if } a_d = -1. \end{cases} \quad \square \tag{17}$$

Note that this result holds for a more general polynomial with integer coefficients, with leading term $-a_0 x^d$ rather than x^d as in (1).

Corollary 3.1: If $a_d = \pm 1$ and p is prime, then $p|S_{-p} \Leftrightarrow p|a_{d-1}$.

Corollary 3.2: If $a_d = \pm 1$ and $a_{d-1} = \pm 1$, then S_{-p} is not a multiple of p for any prime p.

Corollary 3.3: If $a_d = \pm 1$ and $a_1 = \pm 1$ and $a_{d-1} = \pm 1$, then, for all primes p, $p \nmid S_p$ and $p \nmid S_{-p}$.

Corollary 3.4 If $a_d = \pm 1$ and $a_{d-1} = \pm q^f$, where q is prime and $f \geq 1$, then q is the only prime p for which $p|S_{-p}$.

Corollary 3.5: If $a_d = \pm 1$ and $a_1 = \pm q^e$ and $a_{d-1} = \pm q^f$, where q is prime and $e \geq 1$ and $f \geq 1$, then q is the only prime p for which $p|S_p$, and also q is the only prime p for which $p|S_{-p}$.

Corollary 3.6: If $a_d = \pm 1$, then there is no prime p that divides both S_p and S_{-p} if and only if a_1 and a_{d-1} are coprime.

Corollary 3.7: If $a_d = \pm 1$ and if a_1 and a_{d-1} have the same set of prime divisors and if p is prime, then $p|S_p \Leftrightarrow p|a_1 \Leftrightarrow p|a_{d-1} \Leftrightarrow p|S_{-p}$.

Note that a_1 and a_{d-1} may have different signs, and they may have different exponents for their prime factors.

Theorem 4: If $a_d = \pm 1$, then S_{-p} is an integer multiple of p for all primes p if and only if $a_{d-1} = 0$.

Proof: Apply Theorem 2 to the inverse polynomial (17). □

Theorem 5: For all polynomial equations of the form

$$x^d - a_2 x^{d-2} - a_3 x^{d-3} - \cdots - a_{d-3} x^3 - a_{d-2} x^2 \pm 1 = 0, \tag{18}$$

with integer coefficients, both S_p and S_{-p} are integer multiples of p for all primes p.

Proof: By Theorem 2, $p | S_p$ since $a_1 = 0$, and by Theorem 4, $p | S_{-p}$ since $a_d = \pm 1$ and $a_{d-1} = 0$. □

4. APPLICATION TO CHEBYSHEV POLYNOMIALS

The Chebyshev polynomials of the first kind are defined by the initial values:

$$T_0(y) \stackrel{\text{def}}{=} 1, \quad T_1(y) \stackrel{\text{def}}{=} y; \tag{19}$$

with the recurrence relation

$$T_n(y) = 2yT_{n-1}(y) - T_{n-2}(y), \quad (n = 2, 3, \ldots). \tag{20}$$

In terms of the modified Chebyshev polynomial of the first kind,

$$C_n(z) \stackrel{\text{def}}{=} 2T_n\left(\frac{z}{2}\right), \tag{21}$$

the initial values are

$$C_0(z) \stackrel{\text{def}}{=} 2, \quad C_1(z) \stackrel{\text{def}}{=} z, \tag{22}$$

and the recurrence relation is

$$C_n(z) = zC_{n-1}(z) - C_{n-2}(z), \quad (n = 2, 3, \ldots). \tag{23}$$

The characteristic polynomial for $T_n(y)$ is

$$P(x) = x^2 - 2xy + 1. \tag{24}$$

In terms of the roots of the characteristic equation,

$$\alpha = y + \sqrt{y^2 - 1}, \quad \beta = y - \sqrt{y^2 - 1}, \tag{25}$$

(22) becomes

$$C_0(2y) = 2 = \alpha^0 + \beta^0 = S_0, \quad C_1(2y) = 2y = \alpha + \beta = S_1, \tag{26}$$

and it follows from (23) by induction on n that

$$C_k(2y) = 2T_k(y) = \alpha^k + \beta^k = S_k \quad (k = 0, 1, 2, \ldots). \tag{27}$$

Theorem 6: For integer j, $T_p(j) \equiv j \pmod{p}$ for all odd primes p, and $2T_p\left(j + \frac{1}{2}\right) \equiv (2j+1) \pmod{p}$ for all primes p.

Proof: If $m=2y$ is any integer, then it follows from (22) and (23) by induction on n that $S_k = C_k(m) = 2T_k\left(\frac{m}{2}\right)$ is an integer for all integers $k \geq 0$, and Theorem 1 shows that, for every prime p,

$$2T_p\left(\frac{m}{2}\right) = S_p \equiv m \pmod{p}. \tag{28}$$

Therefore, if $y = j$ is any integer and p is prime,

$$2T_p(j) \equiv 2j \pmod{p}; \tag{29}$$

and hence, for every integer j and every odd prime p,

$$T_p(j) \equiv j \pmod{p}. \tag{30}$$

For $p = 2$,

$$T_2(j) = 2j^2 - 1, \tag{31}$$

so that (30) holds only for odd j.

If $2y = m = 2j+1$ is odd, then, for every prime p, (28) becomes

$$2T_p\left(j + \frac{1}{2}\right) \equiv (2j+1) \pmod{p} \tag{32}$$

for all integers j. □

Theorem 7: For odd prime p, $T_p(j) \equiv j \pmod{jp}$ for all integers j except multiples of p, and if j is odd (and not a multiple of p) then $T_p(j) \equiv j \pmod{2jp}$.

Proof: For integer j and odd prime p,

$$T_p(j) = j + ep, \tag{33}$$

where e is an integer, in view of Theorem 6.

From the initial values (19), it follows from (20) by induction on n that $T_n(y) = 2^{n-1}y^n - \cdots$ is a polynomial in y of degree n with integer coefficients, and that $T_n(y)$ is an even polynomial in y if n is even and $T_n(y)$ is an odd polynomial in y if n is odd. Hence, if j is an integer and n is odd, then $j \mid T_n(j)$. Thus, for all odd primes p,

$$j + ep = T_p(j) = jb \tag{34}$$

for some integer b.

If j is an even integer then jb is even; and hence ep is even, so that $e = 2f$ for some integer f.

If j is an odd integer then $T_0(j)$ and $T_1(j)$ are odd [from (19)], and it follows from (20) by induction on n that $T_n(j)$ is odd for all $n \geq 0$. Thus, both j and $T_p(j)$ in (33) are odd; hence, ep is even, so that $e = 2f$.

Therefore, for all integers j and odd prime p,

$$j + 2fp = T_p(j) = jb, \tag{35}$$

so that, if j is not a multiple of p, then $j \mid (2f)$ and if j is also odd then $j \mid f$. □

Theorem 8: For prime $p \geq 5$ and odd integer m, $2T_p\left(\frac{m}{2}\right) \equiv m \pmod{2p}$, and if m is not a multiple of p then $2T_p\left(\frac{m}{2}\right) \equiv m \pmod{2mp}$.

Proof: From (22) we get $C_0(m) = 2$, which is even, and $C_1(m) = m$, which is odd; and from (23) we get $C_2(m) = m^2 - 2$, which is odd. It follows from (23), by induction on n, that $C_n(m)$ is even if and only if $3|n$. From (31),

$$C_p(m) = 2T_p\left(\frac{m}{2}\right) = m + ep, \tag{36}$$

where e is an integer; hence, for all primes $p \neq 3$, we must have ep even. Thus, for all odd integers m and for all primes $p \geq 5$, e must be even $e = 2f$; therefore,

$$2T_p\left(\frac{m}{2}\right) = m + 2fp \equiv m \pmod{2p} \quad (p \geq 5). \tag{37}$$

From the initial values (19), it follows from (23) by induction on n that $C_n(z) = z^n - \cdots$ is a monic polynomial in z of degree n with integer coefficients, and that $C_n(z)$ is an even polynomial in z if n is even and $C_n(z)$ is an odd polynomial in z if n is odd. Hence, if j is an integer and n is odd, then $j|C_n(j)$, so that for all odd primes p,

$$C_p(j) = jb, \tag{38}$$

where b is an integer, and if $j = m$ is an odd integer and $p \geq 5$, then

$$m + 2fp = C_p(m) = mb. \tag{39}$$

Therefore, if m is not a multiple of p, then $m|(2f)$, and since m is odd then $m|f$, so that

$$C_p(m) = 2T_p\left(\frac{m}{2}\right) \equiv m \pmod{2mp}. \;\square \tag{40}$$

REFERENCES

1. Leonard Eugene Dickson. *Elementary Theory of Equations*. New York: Wiley; London: Chapman & Hall, 1914.
2. B. H. Neumann & L. G. Wilson. "Some Sequences Like Fibonacci's." *The Fibonacci Quarterly* **17.1** (1979):80-83. (Rpt. in *Selected Works of B. H. Neumann and Hanna Neumann*, 6 vols [Winnipeg: The Charles Babbage Research Centre, 1988], **1**:131-34.)
3. B. H. Neumann & L. G. Wilson. "Corrigenda to 'Some Sequences Like Fibonacci's.'" *The Fibonacci Quarterly* **21.3** (1983):229. (Rpt. in *Selected Works of B. H. Neumann and Hanna Neumann*, 6 vols [Winnipeg: The Charles Babbage Research Centre, 1988], **1**:135.)

AMS Classification Numbers: 11A07, 11A41, 11C08

❖❖❖