MATH. SCAND. 2 (1954), 327–333

CONGRUENCE PROPERTIES OF TCHEBYCHEFF POLYNOMIALS

THØGER BANG

The Tchebycheff polynomials appear in the theory of numbers only as a special case of the recurring sequences which have been treated extensively by Lucas [4], Lehmer [3] and many others. However, it may be justified to consider them separately, since this can be done in a simple way, and they have important applications, as is also shown by Rankin in the preceding article [5]. The following is based on notes, made by the author in connection with a popular lecture [1] in which, among other things, the Lucas test for the Mersenne primes was discussed. It is usual in the study of recurring sequences to consider two interacting sequences; we shall here give a self-contained treatment of only the primary sequence $T_n(x)$ (for the definition of $T_n(x)$ see (1) below). From the properties of this sequence, it would be easy to deduce the properties of the other sequence $F_n(x)$ by means of a few of the formulas which connect $F_n(x)$ and $T_n(x)$. (See formulas (3)–(9) of Rankin [5]; the polynomials $F_n(x)$ are naturally dominating in the article of Rankin, since they occur in the powers of a second order matrix, formula (12).) In the present paper, we shall use rather few formulas, and this will make it easier to emphasize certain points, in particular the formula (3) below. The rank r which we use (the notation is in accordance with Lehmer [3]) differs from the order n used by Rankin. Indeed, n is uniquely determined by r, but the converse is not true since $n = r/(r, 2)$ (where (a, b) denotes the greatest common divisor of a and b).

We put $x = \cos v$, where x and v are complex numbers. Then $e^{\pm iv} = x \pm (x^2-1)^{\frac{1}{2}}$, and by inserting this in $\cos nv = \frac{1}{2}(e^{i|n|v} + e^{-i|n|v})$, where n is an integer, we get

$$\cos nv = \sum_{j \text{ even}} \binom{|n|}{j} (x^2-1)^{j/2} x^{|n|-j} = T_n(x) \tag{1}$$

(the non-vanishing terms in the sum result from $0 \leqq j \leqq |n|$). The

Received November 11, 1954.

polynomial $T_n(x)$ defined by (1) is the n'th Tchebycheff polynomial; obviously, it is of degree $|n|$, and the coefficients are integers. We have $T_{-n}(x) = T_n(x)$ and $T_0(x) = 1$. Furthermore, $T_1(x) = x$ and $T_2(x) = 2x^2 - 1$.

The formula

$$\{\cos(m+n)v - 1\}\{\cos(m-n)v - 1\} = \{\cos mv - \cos nv\}^2$$

yields

$$\{T_{m+n}(x) - 1\}\{T_{m-n}(x) - 1\} = \{T_m(x) - T_n(x)\}^2 , \tag{2}$$

and the formula $\cos m(nt) = \cos(mn)t$ yields

$$T_m(T_n(x)) = T_{mn}(x) . \tag{3}$$

In the sequel p is a fixed odd prime. The symbol of congruence $\equiv$ means congruence modulo p, and by "residue class" (or short "residue") we mean residue class modulo p.

For an integer x, or rather a residue x, we define the rank $r = r_x$ to be the least positive integer r for which $T_r(x) \equiv 1$ (when there exists such a finite r; later we shall prove, that this is the case for all x). We have $r_1 = 1$ and $r_{-1} = 2$ for all p.

In the following lemma x is a fixed residue, and we write T_n for $T_n(x)$. As usual, $[\alpha]$ denotes the largest integer not exceeding α.

LEMMA 1. *If x is of rank r, then the residues $T_0 = 1, T_1, T_2, \ldots, T_{[r/2]}$ are all different. They determine the sequence of residues T_n, where n runs through all integers, since $T_{r-n} \equiv T_n$ and $T_{r+n} \equiv T_n$. In particular, $T_n \equiv 1$ if and only if r divides n.*

For, if $m > n$ are two arbitrary of the numbers $0, 1, \ldots, [r/2]$, then it follows from the definition of r that the left side of (2) is $\not\equiv 0$, which proves the first part of the lemma. If we put $m = r-n$ in (2), the left side will be $\equiv 0$, which proves that $T_{r-n} \equiv T_n$, and, since $T_n = T_{-n}$, the rest of the lemma follows.

LEMMA 2. *There exist at most $1 + [n/2]$ residues x whose ranks divide the positive number n, that is, for which $T_n(x) \equiv 1$.*

In fact, from (2) it follows that

$$\{T_n(x) - 1\}\{T_2(x) - 1\} = \{T_{(n+2)/2}(x) - T_{(n-2)/2}(x)\}^2 \qquad \text{for } n \text{ even},$$

$$\{T_n(x) - 1\}\{T_1(x) - 1\} = \{T_{(n+1)/2}(x) - T_{(n-1)/2}(x)\}^2 \qquad \text{for } n \text{ odd},$$

and in each of these formulas the right side is the square of a polynomial of degree $1 + [n/2]$, which proves the lemma.

LEMMA 3. *If x is of rank r, then the residues mentioned in the beginning of Lemma 1 are all the residues whose ranks divide r. The rank of $T_j(x)$ is $r/(r,j)$. For $r > 2$, there exist exactly $\frac{1}{2}\varphi(r)$ different residues of rank r, while for $r = 1$ or 2 there exists only one residue of rank r.*

From (3) and Lemma 1 we have $T_r(T_j(x)) = T_{rj}(x) \equiv 1$. Hence the rank of $T_j(x)$ divides r. However, Lemma 2 states that there cannot be more than those $1 + [r/2]$ different residues, whose ranks divide r. The rank of $T_j(x)$ is (Lemma 1) the least positive integer m for which r divides mj, and this is $m = r/(r,j)$. Hence, the residues of rank r are the residues $T_j(x)$, where r and j are relatively prime; and, for $r > 2$, there exist exactly $\frac{1}{2}\varphi(r)$ such residues among $T_0, T_1, \ldots, T_{[r/2]}$. As $T_2(x) = 2x^2 - 1 \equiv 1$ gives $x \equiv \pm 1$, these two residues are the only ones for which r divides 2, and here $r_1 = 1$ and $r_{-1} = 2$. Thus the lemma is completely proved.

LEMMA 4. *If there exist $1 + [n/2]$ residues x that are solutions of the congruence $T_n(x) \equiv 1$, where n is a positive integer, then at least one of those residues is of rank n.*

To prove the lemma, let us consider the positive function $\psi(d)$ defined by $\psi(d) = \frac{1}{2}\varphi(d)$ when $d > 2$, $\psi(1) = 1$ and $\psi(2) = 1$. If there exists an x of rank r, then the total number of residues of rank r equals $\psi(r)$ (Lemma 3). Hence, the total number of solutions of the congruence $T_n(x) \equiv 1$ is $\Sigma\psi(r)$, where r runs through the possible ranks. These are divisors of n. Since an elementary calculation shows that $\Sigma\psi(d) = 1 + [n/2]$, when the sum is taken over all divisors d of n, all those divisors, in particular n itself, must occur as rank for some x. This proves the lemma.

LEMMA 5. *If x is of rank r and y is of rank s, where r and s are relatively prime, and if there exists a z such that $z^2 \equiv (x^2-1)(y^2-1)$, then there exists a residue of rank rs.*

This lemma is not needed in the sequel, but it gives certain information that will be of interest in a later connection.

To prove the lemma, we remark that the formula which expresses $\cos(u \pm v)$ in terms of $\cos u$ and $\cos v$, together with the trigonometric formula which was used to obtain (2), gives the following identity (valid for all complex x and y):

$$\{T_j\left(xy + \left((x^2-1)(y^2-1)\right)^{\frac{1}{2}}\right) - 1\}\{T_j\left(xy - \left((x^2-1)(y^2-1)\right)^{\frac{1}{2}}\right) - 1\} = \{T_j(x) - T_j(y)\}^2 .$$

The right side is a polynomial, and hence, after multiplication in the left side, all the square-roots will occur in even powers. These powers are, for the given x, y, and z, congruent to the same powers of z, such that

$$\{T_j(xy+z) - 1\}\{T_j(xy-z) - 1\} \equiv \{T_j(x) - T_j(y)\}^2 .$$

This quantity can only be $\equiv 0$ if $T_j(x)$ and $T_j(y)$ are congruent, which implies that they are of the same rank. Their common rank divides r and s and is therefore 1, from which it follows that rs divides j. On the other hand, if rs divides j, then $T_j(x) \equiv T_j(y) \equiv 1$. The least positive integer, for which the left side is $\equiv 0$, will thus be $j = rs$, which proves that at least one of the residues $xy \pm z$ is of rank rs.

Up to now the lemmas and their proofs are valid if, instead of residue classes, we consider elements of an arbitrary integral domain. From now on, it will be essential that we consider residues modulo the odd prime p.

LEMMA 6. *For all* x,

$$T_p(x) \equiv T_1(x) .$$

This may be called "*The theorem of Fermat for Tchebycheff polynomials*". The proof is immediate taking $n = p$ in (1). All the occurring binomial coefficients

$$\binom{p}{j}$$

are divisible by p, except for $j = 0$, and we have $T_p(x) \equiv x^p \equiv x = T_1(x)$.

LEMMA 7. *Any* x *has a rank dividing* $p+1$ *or* $p-1$. *The two cases occur simultaneously for* $x \equiv \pm 1$, *but for no other residue. The first case occurs for* $(p+3)/2$ *residues, and there exists a residue of rank* $p+1$. *The second case occurs for* $(p+1)/2$ *residues, and there exists a residue of rank* $p-1$.

From (2) and Lemma 6 we get

$$\{T_{p+1}(x) - 1\}\{T_{p-1}(x) - 1\} = \{T_p(x) - T_1(x)\}^2 \equiv 0 ,$$

which proves the first part of the lemma. The rank divides $p+1$ and $p-1$ simultaneously if it divides $(p+1, p-1) = 2$, and this occurs only for $x \equiv \pm 1$, which proves the second part. Lemma 2 states that the first case occurs for at most $(p+3)/2$ residues, and the second case occurs for at most $(p+1)/2$ residues; the total number of residues is p, and hence the numbers are exactly $(p+3)/2$ and $(p+1)/2$. The existence of residues of rank $p \pm 1$ follows then from Lemma 4.

The main content of Lemma 7 and the preceding lemmas can be expressed more lucidly in the following theorem:

THEOREM. *There exists a one-to-one correspondence between the residue classes modulo p and the p different real values of* $\cos(2\pi h/(p+1))$ *and* $\cos(2\pi k/(p-1))$ *(where h and k are arbitrary integers), such that when x corresponds to $\alpha = \cos\xi$, then $T_j(x)$ corresponds to $T_j(\alpha) = \cos j\xi$ for every integer j. The rank of the residue x is equal to the least positive denominator d, when ξ is written in the form $\xi = 2\pi n/d$, where n and d are integers.*

Indeed, choose a residue y of rank $p+1$, and let it correspond to $\cos\eta$ with $\eta = 2\pi/(p+1)$, and choose a residue z of rank $p-1$, and let it correspond to $\cos\zeta$ with $\zeta = 2\pi/(p-1)$. Then the remainder of the proof is straightforward, and we omit it.

The residues $x \equiv \pm 1$ (whether they are determined from y or from z) correspond to $\cos\xi = \pm 1$. The residue 0 corresponds to $\cos(\pi/2) = 0$. It is easy to see that, for $p > 3$, $(p+1)/2$ corresponds to $\frac{1}{2} = \cos(2\pi/6)$, and $(p-1)/2$ corresponds to $-\frac{1}{2} = \cos(2\pi/3)$; while, for all residues other than those mentioned, the liberty in the choice of y and z gives rise to more than one value of the corresponding real number $\cos\xi$.

The p real numbers $\alpha = \cos\xi$ are the p roots of the equation $T_p(\alpha) = T_1(\alpha)$, or, expressed in another way, ξ is a root of $\cos p\xi = \cos\xi$. The group of permutations of the numbers α corresponding to different choices of y and z is the same as the group of permutations of the roots of $T_p(\alpha) = T_1(\alpha)$, considered as an equation over the rational field.

The following remark is important for the applications of the theory: *The rank of x divides $p+1$ if and only if x^2-1 is a quadratic non-residue modulo p, or if $x \equiv \pm 1$.* This is immediate by taking $n = p+1$ in (1); then p will divide all the occurring binomial coefficients except for $j = 0$ and $j = p+1$, such that

$$T_{p+1}(x) - 1 \equiv (x^2-1)^{(p+1)/2} + x^{p+1} - 1 \equiv (x^2-1)\left((x^2-1)^{(p-1)/2} + 1\right),$$

which gives the desired result.

From this remark, it follows that r_x divides $p-1$ if and only if x^2-1 is a quadratic residue, or if $x \equiv \pm 1$. We observe, that this classification of the residues shows that the condition of Lemma 5 (about the existence of a z, such that $z^2 \equiv (x^2-1)(y^2-1)$) is satisfied, if and only if the ranks of x and y both divide $p+1$ or both divide $p-1$. By using this, it would be possible to prove the existence of residues of rank $p \pm 1$ (mentioned in Lemma 7) without the use of Lemma 4.

Lemma 7 together with the supplementary remark states how often x^2-1 is a quadratic residue, and how often it is not. Thus, as a corollary, we get the number of times a quadratic residue succeeds a quadratic

residue, and the number of times a quadratic residue succeeds a quadratic non-residue, etc. (for these numbers see for instance Hasse [2, p. 150]).

The Lucas test for the Mersenne primes may in a natural way be stated by means of $T_n(x)$. From the properties mentioned above follows:

A necessary and sufficient condition in order that $M = 2^n - 1$ *(with* $n > 2$*) be a prime, is that* M *divides* $T_{2^{n-2}}(x)$*, where* x *is* 2*, or, more generally, where* x *is an arbitrary* $T_j(2)$*, with* j *odd, for example* $x = T_3(2) = 26$.

Since the proof can be performed by the same method as in Lehmer [3] (the sequences considered there are equal to $2T_n$), we shall omit the proof.

Our study of the polynomials $T_n(x)$ has been based on the formulas (1), (2), and (3), where, of course, (2) and (3) can be derived from (1). But formula (3) has in itself interesting properties. Besides its obvious significance for the multiplicative properties of the rank, it also implies that the polynomials $T_m(x)$ and $T_n(x)$ commute in the sense

$$P_m\big(P_n(x)\big) = P_n\big(P_m(x)\big)\,. \tag{4}$$

Here we have written $P_n(x)$ instead of $T_n(x)$, and $P_n(x)$ shall now denote a polynomial of degree n, not necessarily a Tchebycheff polynomial.

It is obvious that (3), and hence (4), is satisfied by

$$P_n(x) = L^{-1}\big(T_n\big(L(x)\big)\big)\,, \tag{5}$$

where $L(x)$ is a polynomial of first degree and $L^{-1}(x)$ is its inverse function. But (3) is also satisfied by the monomials $P_n(x) = x^n$, and more generally by

$$P_n(x) = L^{-1}\big(\{L(x)\}^n\big)\,. \tag{6}$$

Now it is interesting to remark that if a sequence of polynomials $P_1(x), P_2(x), \ldots, P_q(x)$ $(q > 2)$ satisfies (4), then it must be of the type (5) or of the type (6). This follows from two statements, both of which can be proved by elementary calculations on the coefficients of the polynomials involved: 1° If $P_2\big(P_3(x)\big) = P_3\big(P_2(x)\big)$, then $P_2(x)$ is of type (5) or (6); 2° to a given $P_2(x)$ there exists at most one $P_n(x)$ of degree n, such that the two polynomials satisfy (4). Both $P_n(x) = x^n$ and $P_n(x) = T_n(x)$ satisfy the Fermat congruence $P_p(x) \equiv P_1(x) \pmod p$, and this congruence is not spoiled by the transformation in (5) or (6) by means of a rational function $L(x) = ax + b$, if p does not divide a. Hence we have:

If a sequence of polynomials with rational coefficients $P_1(x), P_2(x), \ldots,$

$P_n(x), \ldots$, where $P_n(x)$ is of degree n, satisfies (4), *then the polynomials are of type* (5) *or* (6). *In particular, the Fermat congruence $P_p(x) \equiv P_1(x) \pmod{p}$ is satisfied for all p, except those which divide the numerator in a, where $L(x) = ax+b$.*

REFERENCES

1. Th. Bang, *Store Primtal*, Nordisk Mat. Tidskr. 2 (1954), 157–168.
2. H. Hasse, *Vorlesungen über Zahlentheorie* (Die Grundlehren der mathematischen Wissenschaften 59), Berlin · Göttingen · Heidelberg, 1950.
3. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. 31 (1930), 419–448.
4. E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.
5. R. A. Rankin, *Chebyshev polynomials and the modulary group of level p*. Math. Scand. 2 (1954), 315–326.

UNIVERSITY OF COPENHAGEN, DENMARK