On coefficients of Yablonskii-Vorob'ev polynomials

By Masanobu Kaneko and Hiroyuki Ochiai

(Received May 7, 2002)

Abstract. We give a formula for the coefficients of the Yablonskii-Vorob'ev polynomial. Also the reduction modulo a prime number of the polynomial is studied.

1. Introduction.

The object of study in the present article is a sequence of polynomials \( T_n(x) \in \mathbb{Z}[x] \) \((n = 0, 1, 2, \ldots)\), referred to as the Yablonskii-Vorob'ev polynomials, satisfying the recursion

\[
T_{n+1}(x)T_{n-1}(x) = xT_n(x)^2 + T_n(x)T''_n(x) - T'_n(x)^2,
\]

with the initial condition \( T_0(x) = 1, \ T_1(x) = x \). The first few are

\[
T_2(x) = x^3 - 1, \\
T_3(x) = x^6 - 5x^3 - 5, \\
T_4(x) = x^{10} - 15x^7 - 175x, \\
T_5(x) = x^{15} - 35x^{12} + 175x^9 - 1225x^6 - 12250x^3 + 6125.
\]

Note that we have adopted a normalization different from the usual one (see the remark at the end of Section 2).

Although it is not clear a priori that the recursion (1) gives a sequence of polynomials, we know it does indeed, the fact which is most naturally explained in the context of connection with rational solutions of the second Painlevé equation \( \text{(P}_II\text{)} \). (See, e.g., [1], [6] for this and related subjects.) Specifically, the logarithmic derivative \( y = T'_n(x)/T_n(x) - T'_{n-1}(x)/T_{n-1}(x) \) of the ratio \( T_n(x)/T_{n-1}(x) \) is a solution of

\[
\frac{dy}{dx^2} = 2y^3 - 4xy + 4n.
\]

As such, the Yablonskii-Vorob'ev polynomial can be thought of as a non-linear analogue of the classical special polynomials associated to linear differential equations. In this paper, we discuss some properties including explicit formulas and reductions modulo primes of coefficients of this “Painlevé special polynomial”. We note that, owing to the connection with Schur functions, such results also give a kind of information on certain character values of irreducible representations of symmetric groups.

2000 Mathematical Subject Classification. Primary 34M55; Secondary 33E17.

Key Words and Phrases. Yablonskii-Vorob'ev polynomial, Schur function, Painlevé equation.

Work in part supported by Grant-in-Aid for Exploratory Research No. 14654009, and Scientific Research No. 11440011(B)(2), Japan Society for the Promotion of Science.
Now we state our main results. Using the recursion (1), it is easy to see by induction that the polynomial $T_n(x)$ is monic of degree $n(n + 1)/2$ and has the following expansion:

$$T_n(x) = \sum_{j \geq 0} t_j(n)x^{3j + \delta}, \quad t_j(n) \in \mathbb{Z},$$

(2)

where $\delta = 1$ if $n \equiv 1 \mod 3$ and 0 otherwise. Set

$$\mu_n = \prod_{k=1}^{n} (2k - 1)!!.$$

The first theorem gives the coefficient of the term of the lowest degree (= the constant term if $n \equiv 0, 2 \mod 3$ and the term of degree 1 if $n \equiv 1 \mod 3$) of $T_n(x)$.

**Theorem 1.** We have

$$t_0(n) = \begin{cases} (-1)^{m} 3^{-(3m-1)m/2} \mu_n / (\mu_{m-1}^2 \mu_m), & \text{if } n = 3m - 1, \\ (-1)^{m} 3^{-(3m+1)m/2} \mu_n / (\mu_{m-1}^2 \mu_m^2), & \text{if } n = 3m, \\ (-1)^{m} 3^{-(3m+1)m/2} \mu_n / \mu_m^3, & \text{if } n = 3m + 1. \end{cases}$$

(3)

As for the higher coefficients, we show the following.

**Theorem 2.** For fixed $j$, the function $n \mapsto t_j(n)/t_0(n)$ extends to a polynomial function in $n$ depending on $n \mod 3$.

Several examples of the theorem will be given at the end of Section 3.

The next result concerns the reduction modulo a prime of the polynomial $T_n(x)$.

**Theorem 3.** For a prime number $p > 3$ and any non-negative integers $m$ and $n$, we have

$$T_{mp+n}(x) \equiv x^{d_p+n} T_n(x) \mod p,$$

where $d_n = n(n + 1)/2$, the degree of $T_n(x)$.

2. **Constant terms.**

To prove Theorem 1, we recall the determinant expression of the Yablonskii-Vorob’ev polynomial of Jacobi-Trudi type [2]. Define a family of polynomials $h_k(x) \in \mathbb{Q}[x]$ ($n = 0, 1, 2, \ldots$) by the generating function

$$e^{x^3}(1/3)x^3 = \sum_{k=0}^{\infty} h_k(x)x^k,$$

(4)

and set $h_{-1} = h_{-2} = \cdots = 0$. Writing the left-hand side as $e^{x^3/3}e^x$ and expanding this out, we see that the polynomial $h_k(x)$ is given by

$$h_k(x) = \sum_{i=0}^{[k/3]} \frac{1}{3^i i!(k - 3i)!} x^{k-3i},$$

(5)
where \( \lfloor k/3 \rfloor \) is the greatest integer which does not exceed \( k/3 \). In particular, the degree of \( h_k(x) \) is \( k \) and the leading coefficient is \( 1/k! \). Set
\[
\tau_n(x) = \det(h_{j-2i+n+1}(x))_{1 \leq i, j \leq n}.
\] (6)

The polynomial \( \tau_n(x) \) is known as the 2-core Schur polynomial attached to the staircase partition of depth \( n \). The degree of \( \tau_n(x) \) is at most \( d_n = n(n+1)/2 \) since the degree of \( h_k(x) \) is \( k \), but it turns out that it is exactly \( d_n \) and the coefficient of \( x^{d_n} \) in \( \tau_n(x) \) is given by \( \mu_n^{-1} = 1/\prod_{k=1}^{n}(2k-1)!! \), as the following lemma shows.

**LEMMA 4.** We have
\[
\det(1/(j - 2i + n + 1)!)_{1 \leq i, j \leq n} = \mu_n^{-1},
\]
where we understand \( 1!/l! = 0 \) if \( l < 0 \).

A proof is found in [5], Corollary 7.16.3 (formula 7.71) combined with Corollary 7.21.6.

The determinant formula for the Yablonskii-Vorob’ev polynomial [2] asserts that \( T_n(x) \) is a constant multiple of \( \tau_n(x) \):
\[
T_n(x) = \mu_n \tau_n(x).
\] (7)

**PROOF OF THEOREM 1.**

Suppose \( n = 3m - 1 \). Then \( t_0(n) \) is the constant term of \( T_n(x) \). From equations (7) and (6), we want to compute the determinant
\[
\tau_n(0) = \det(h_{j-2i+3m}(0))_{1 \leq i, j \leq 3m - 1}.
\]
The point is that this determinant splits into three blocks and we can calculate each block separately by using \textbf{Lemma 4}. Actually, noting from (5) that \( h_{3l}(0) = 1/(3^l l!) \) and \( h_{3l-1}(0) = h_{3l+1}(0) = 0 \), we proceed as follows:

1. For \( i = 3k \) with \( 1 \leq k \leq m - 1 \), the \( (i, j) \) entry \( h_{j-6k+3m}(0) \) is zero unless \( j = 3l \) with \( 1 \leq l \leq m - 1 \), in which case the value is \( h_{3(i-2k+m)}(0) = 1/(3^{l-2k+m}(l-2k+m))! \). Then, by \textbf{Lemma 4} the determinant of \( m-1 \) by \( m-1 \) matrix with these \( (k, l) \) entries is equal to \( 1/(3^{(m-1)/2} \mu_{m-1}). \)

2. For \( i = 3k-1 \) with \( 1 \leq k \leq m \), the \( (i, j) \) entry \( h_{j-6k+3m+2}(0) \) is zero unless \( j = 3l-2 \) with \( 1 \leq l \leq m \), in which case the value is \( h_{3(i-2k+m)}(0) = 1/(3^{l-2k+m}(l-2k+m))! \). Noting that this is equal to 0 for \( k = m \) and \( l < m \), and 1 for \( k = l = m \), we see that the \( m \) by \( m \) determinant is equal to the one in (1) as above, i.e., equal to \( 1/(3^{(m-1)/2} \mu_{m-1}). \)

3. Similarly, for \( i = 3k-2 \) with \( 1 \leq k \leq m \), the \( (i, j) \) entry \( h_{j-6k+3m+4}(0) \) is zero unless \( j = 3l-1 \) with \( 1 \leq l \leq m \). By \textbf{Lemma 4} the determinant of \( m \) by \( m \) matrix with entries \( 1/(3^{l-2k+m+1}(l-2k+m+1))! \) is equal to \( 1/(3^{(m+1)/2} \mu_{m}). \)

Combining the above three, we conclude \( \tau_{3m-1}(0) = \pm 1/(3^{(m-1)/2} \mu_{m-1}^2) \), the sign being the inversion number of the permutations of rows and columns, which, as is readily seen, is equal to \((-1)^m\). This establishes the formula in the case of \( n = 3m - 1 \).

The computation in the case when \( n = 3m \) is exactly the same and will be omitted. When \( n = 3m + 1 \), \( t_0(n) \) is not the constant term and the above computation does not work. But the following lemma allows us to reduce this case to the preceding two.
Lemma 5. We have
\[ T_{n-1}(x)T_{n+1}'(x) - T_n'(x)T_{n+1}(x) = (2n + 1)T_n(x)^2 \]
for all n.

See [6, p. 92] or [1, p. 188] for a proof. Putting \( n = 3m \) in the lemma and comparing the constant term of both sides, we obtain
\[ t_0(3m - 1)t_0(3m + 1) = (6m + 1)t_0(3m)^2. \] (8)

From this, we have
\[ t_0(3m + 1) = (6m + 1)t_0(3m)^2/t_0(3m - 1) \]
\[ = (-1)^m(6m + 1)3^{-3(m+1)/2}\mu_{3m}^2/(\mu_{3m-1}\mu_m^3) \]
\[ = (-1)^m 3^{-3(m+1)/2}\mu_{3m+1}/\mu_m^3, \]
which completes the proof of Theorem 1. \( \square \)

Remark 6. When \( n \equiv 0, 2 \mod 3 \), there is an alternative way to derive the formula in Theorem 1 from the hook-type formula of \( T_n(x) \) in [7] (the authors would like to thank Masatoshi Noumi for pointing out this). However, the case \( n \equiv 1 \mod 3 \) does not follow from the hook-type formula.

Remark 7. As mentioned in the introduction, the usual recursion for the Yablonskii-Vorob'ev polynomials is
\[ T_{n+1}(x)T_{n-1}(x) = xT_n(x)^2 - 4(T_n(x)T_n''(x) - T_n'(x))^2. \] (9)

If in general we start with the recursion
\[ T_{n+1}(x)T_{n-1}(x) = xT_n(x)^2 + a(T_n(x)T_n''(x) - T_n'(x))^2, \] (10)
a being a constant, and the same initial values \( T_0(x) = 1 \) and \( T_1(x) = x \), the formula for the lowest term in Theorem 1 changes only by a power of a, namely,
\[ t_0(n) = \begin{cases} 
(-1)^m(a/3)3^{(3m-1)/2}\mu_n/(\mu_{3m-1}\mu_m), & \text{if } n = 3m - 1, \\
(-1)^m(a/3)3^{(3m+1)/2}\mu_n/(\mu_{3m-1}\mu_m^3), & \text{if } n = 3m, \\
(-1)^m(a/3)3^{(3m+1)/2}\mu_n/\mu_m^3, & \text{if } n = 3m + 1.
\end{cases} \]

3. Higher coefficients.

For the proof of Theorem 2 it is convenient to use different symbols for \( t_j(n) \) according to the congruence classes of n modulo 3. Put
\[ a_j(m) = t_j(3m - 1), \quad b_j(m) = t_j(3m), \quad \text{and} \quad c_j(m) = t_j(3m + 1). \]

Also put
\[ \tilde{a}_j(m) = a_j(m)/a_0(m), \quad \tilde{b}_j(m) = b_j(m)/b_0(m), \quad \text{and} \quad \tilde{c}_j(m) = c_j(m)/c_0(m). \]
Proof of Theorem 2. First let \( n = 3m \). We substitute the expansion (2) into the recursion (1) and compare the coefficients of \( x^{3k+1} \) for \( k \geq 0 \) to obtain

\[
\sum_{i=0}^{k} c_i(m)a_{k-i}(m) = \sum_{i=0}^{k} b_i(m)b_{k-i}(m) + \sum_{i=1}^{k+1} 3i(3i-1)b_i(m)b_{k+1-i}(m)
- \sum_{i=1}^{k} 9ib_i(m)b_{k+1-i}(m).
\]

Dividing both sides by \( c_0(m)a_0(m) \), which is equal to \( (6m+1)b_0(m)^2 \) by (8), and separating the term with \( i = k + 1 \) in the middle sum on the right (the only place where \( b_{k+1}(m) \) appears), we obtain

\[
3(k+1)(3k+2)\tilde{b}_{k+1}(m) = (6m+1)\sum_{i=0}^{k} \tilde{c}_i(m)\tilde{a}_{k-i}(m) - \sum_{i=0}^{k} \tilde{b}_i(m)\tilde{b}_{k-i}(m)
+ 3\sum_{i=1}^{k} i(3k - 6i + 4)\tilde{b}_i(m)\tilde{b}_{k+1-i}(m)
\] (11)

for \( k \geq 0 \). Similarly, for \( n = 3m - 1 \) we obtain from the recursion (1)

\[
3(k+1)(3k+2)\tilde{a}_{k+1}(m) = -(6m-1)\sum_{i=0}^{k} \tilde{c}_i(m-1)\tilde{b}_{k-i}(m)
- \sum_{i=0}^{k} \tilde{a}_i(m)\tilde{a}_{k-i}(m) + 3\sum_{i=1}^{k} i(3k - 6i + 4)\tilde{a}_i(m)\tilde{a}_{k+1-i}(m)
\] (12)

for \( k \geq 0 \). Here, we have used the identity \( b_0(m)c_0(m - 1) = -(6m - 1)a_0(m)^2 \) which follows from Lemma 5 by putting \( n = 3m - 1 \) and comparing the constant terms of both sides. For \( n = 3m + 1 \), we compare the constant terms in the recursion (1) to get \( a_0(m+1)b_0(m) = -c_0(m)^2 \), and then with this we obtain as above (comparing the coefficients of \( x^{3k+3} \) in (1))

\[
(3k+1)(3k+4)\tilde{c}_{k+1}(m) = -\sum_{i=0}^{k+1} \tilde{a}_i(m+1)\tilde{b}_{k+1-i}(m) - \sum_{i=0}^{k} \tilde{c}_i(m)\tilde{c}_{k-i}(m)
+ \sum_{i=1}^{k} (3i + 1)(3k - 6i + 4)\tilde{c}_i(m)\tilde{c}_{k+1-i}(m)
\] (13)

for \( k \geq 0 \).

Now we prove Theorem 2 by induction on \( j \). For \( j = 0 \), the required property, which is equivalent to the statement that \( \tilde{a}_j(m), \tilde{b}_j(m), \) and \( \tilde{c}_j(m) \) are polynomials in \( m \), holds trivially. Suppose the property holds up to \( j \leq k \). Then equations (12) and (11) ensures respectively that both \( \tilde{a}_{k+1}(m) \) and \( \tilde{b}_{k+1}(m) \) are polynomials in \( m \). Then,
we conclude in turn by equation (13) that \( \tilde{c}_{k+1}(m) \) is also a polynomial in \( m \). This completes the proof of Theorem 2. \( \square \)

Equations (11), (12), and (13) allow us to compute explicitly the polynomials \( \tilde{a}_j(m) \), \( \tilde{b}_j(m) \), and \( \tilde{c}_j(m) \). First several examples are given below.

**Example 8.**

\[
\begin{align*}
\tilde{a}_1(m) &= -m, \\
\tilde{a}_2(m) &= -m(m - 1)/10, \\
\tilde{a}_3(m) &= (m + 1)m(m - 1)/210, \\
\tilde{a}_4(m) &= -(19m + 6)(m + 1)m(m - 1)/46200, \\
\tilde{a}_5(m) &= -(155m^2 - 572m - 48)(m + 1)m(m - 1)/21021000, \\
\tilde{b}_1(m) &= m, \\
\tilde{b}_2(m) &= -m(m + 1)/10, \\
\tilde{b}_3(m) &= -(m + 1)m(m - 1)/210, \\
\tilde{b}_4(m) &= -(19m - 6)(m + 1)m(m - 1)/46200, \\
\tilde{b}_5(m) &= (155m^2 + 572m - 48)(m + 1)m(m - 1)/21021000, \\
\tilde{c}_1(m) &= 0, \\
\tilde{c}_2(m) &= 3m(m + 1)/70, \\
\tilde{c}_3(m) &= -(m + 1)m/350, \\
\tilde{c}_4(m) &= -9(m + 2)(m + 1)m(m - 1)/200200, \\
\tilde{c}_5(m) &= 3(m + 2)(m + 1)m(m - 1)/3503500, \\
\tilde{c}_6(m) &= -(207m^2 + 207m + 50)(m + 2)(m + 1)m(m - 1)/4526522000, \\
\tilde{c}_7(m) &= 9(107m^2 + 107m + 4)(m + 2)(m + 1)m(m - 1)/348542194000.
\end{align*}
\]

**Remark 9.** (i) We can extend the recursion (1) to negative \( n \). Then by the symmetry we have \( T_{n-1}(x) = T_n(1/x) \). From this, we can deduce \( \tilde{b}_j(m) = \tilde{a}_j(-m) \) and \( \tilde{c}_j(m) = \tilde{c}_j(-m - 1) \).

(ii) As a polynomial in \( m \), \( \tilde{a}_{j+1}(m) \) is divisible by \( \tilde{a}_j(m) \) for \( j \leq 3 \), but this does not hold in general as the case \( j = 4 \) shows. Likewise, \( \tilde{c}_j(m) \) divides \( \tilde{a}_{j+1}(m) \) for \( 2 \leq j \leq 5 \) but not for \( j = 6 \).

(iii) The fact that \( \tilde{c}_1(m) = 0 \) was given in [6, Theorem 1].


Fix a prime number \( p > 3 \) once and for all. We first establish a special case of Theorem 3, namely for \( m = 1 \) and \( n = 0 \). Once having this, the general case will be proved rather easily.

**Proposition 10.** We have

\[
T_p(x) \equiv x^d_p \mod p.
\]

**Proof.** The key ingredient is again the determinant formula (7):

\[
T_p(x) = \mu_p \tau_p(x).
\]
Noting that $(2k - 1)!!$ is prime to $p$ if $k < (p + 1)/2$ and is divisible by $p$ exactly once if $(p + 1)/2 \leq k \leq p$, we find the exact power of $p$ which divides $\mu_p = \prod_{k=1}^{p} (2k - 1)!!$ is $p^{(p+1)/2}$. So, if we put $\mu'_p = p^{-(p+1)/2} \mu_p$, we have $\mu'_p \in \mathbb{Z}$ and
\[ T_p(x) = \mu'_p p^{(p+1)/2} \tau_p(x). \] (14)

We first show that the polynomial $p^{(p+1)/2} \tau_p(x)$ is realized as a determinant of a matrix with entries which have $p$-integral coefficients. To state this, we develop some notation. Let $\mathbb{Z}_p$ denote the local ring $\{b/a \in \mathbb{Q} \mid a, b \in \mathbb{Z}, (a, p) = 1\}$ which contains $\mathbb{Z}$ as a subring. The maximal ideal of $\mathbb{Z}_p$ generated by $p$ is denoted by $p$. Set $p[x] = \{\sum_{j \geq 0} r_j x^j \in \mathbb{Z}_p[x] \mid r_j \in p\}$. By “mod $p$” of an element in $\mathbb{Z}_p[x]$, we mean its image in the quotient ring $\mathbb{Z}_p[x]/p[x] \cong \mathbb{F}_p[x]$, where $\mathbb{F}_p$ is the field of $p$ elements.

Recall the polynomial $h_k(x)$ was defined by the generating function (4). Expanding $(d/d\lambda)e^{x^2+\lambda^3/3} = (x + \lambda^2)e^{x^2+\lambda^3/3}$ we obtain the recursion
\[(k + 1)h_{k+1}(x) = xh_k(x) + h_{k-2}(x) \quad \text{for} \quad k \geq 2,
\]
with $h_0 = 1$, $h_1 = x$, and $h_2 = x^2/2$. Multiplying both sides by $k!$ and setting $\tilde{h}_k(x) = k! h_k(x)$, we have
\[ \tilde{h}_{k+1}(x) = x \tilde{h}_k(x) + k(k - 1) \tilde{h}_{k-2}(x) \quad \text{for} \quad k \geq 2,
\]
with $\tilde{h}_0 = 1$, $\tilde{h}_1 = x$, $\tilde{h}_2 = x^2$. This implies inductively that $\tilde{h}_k(x)$ is a monic polynomial of degree $k$ with integral coefficients. In particular, we have
\[ h_k(x) \in \mathbb{Z}_p[x] \quad \text{if} \quad k < p \quad \text{and} \quad ph_k(x) \in \mathbb{Z}_p[x] \quad \text{if} \quad p \leq k < 2p. \] (15)

Now define a matrix $(a_{ij})_{1 \leq i, j \leq p}$ by
\[ a_{ij} = \begin{cases} h_{j-2i+p+1} & \text{if} \quad i > (p + 1)/2, \\ ph_{j-2i+p+1} & \text{if} \quad i \leq (p + 1)/2. \end{cases} \]
Then by (15) and (6), we have $a_{ij} \in \mathbb{Z}_p[x]$ and
\[ p^{(p+1)/2} \tau_p(x) = \det(a_{ij})_{1 \leq i, j \leq p}. \] (16)
To compute this determinant modulo $p$, it is convenient to consider instead a modified matrix $(c_{ij})_{1 \leq i, j \leq p}$ which is obtained from $(a_{ij})$ by a suitable permutation of rows: namely set
\[ c_{ij} = \begin{cases} a_{kj} & \text{if} \quad i = 2k - 1, \\ a_{k+(p+1)/2,j} & \text{if} \quad i = 2k. \end{cases} \]
The inversion number of this permutation is $\sum_{i=1}^{(p+1)/2} i = (p^2 - 1)/8$ and so
\[ \det(a_{ij}) = (-1)^{(p^2-1)/8} \det(c_{ij}). \] (17)

The following lemma supplies enough information for computing $\det(c_{ij})$ modulo $p$.

**Lemma 11.** (i) If $i > j$, then $c_{ij} \in p[x]$.
(ii) If $i$ is odd, then $c_{ii} \equiv -x^p \mod p$.
(iii) If $i$ is even, then $c_{ii} = 1$.  

Proof of Lemma. If \( i = 2k - 1 \), then \( k \leq (p + 1)/2 \) and \( c_{ij} = a_{kj} = ph_{j-2k+p+1} = ph_{j-(i-j)} \). By (15), this belongs to \( \mathbb{p}[x] \) if \( i > j \), while for \( i = j \) this is equal to \( ph_{p}(x) = \bar{h}_{p}(x)/(p-1)! \equiv -\bar{h}_{p}(x) \mod p \) by Wilson’s lemma. By (5), the coefficient of \( x^{p-3j} \) in \( \bar{h}_{p}(x) \) is \( p!/(3!(p-3i)) \), which is in \( \mathbb{p} \) for \( i \geq 1 \) and hence \( \bar{h}_{p}(x) \equiv x^{p} \mod p \). If \( i = 2k \), then \( c_{ij} = a_{k+(p+1)/2, j} = h_{j-2k} = h_{j-i} \). This is 0 if \( i > j \) and 1 if \( i = j \). \( \square \)

From (i) of the lemma, the matrix \( (c_{ij}) \) modulo \( p \) is upper-triangular, the diagonal entries of which are given by (ii) and (iii) of the lemma. We therefore have

\[
\det(c_{ij}) \equiv (-1)^{(p+1)/2}x^{p(p+1)/2} \mod p.
\]

Combining this with (17), (16) and (14), we have

\[
T_{p}(x) \equiv (-1)^{(p^{2}-1)/8+(p+1)/2} \frac{\mu_{p}}{\mu_{p}}x^{dp} \mod p.
\]

But we know that \( T_{p}(x) \) is a monic polynomial of degree \( dp \), hence the constant on the right should be congruent to 1 modulo \( p \) and we obtain the proposition. \( \square \)

Corollary 12. We have \( T_{p+1} \equiv x^{dp} \mod p \) and \( T_{p-1} \equiv x^{dp} \mod p \).

Proof. From Proposition 10 we have \( T'_{p}(x) \equiv 0 \mod p \) since \( dp = 0 \mod p \). Thus the recursion (1) reduces modulo \( p \) to \( T_{p+1}T_{p-1} = xT'_{p} \equiv x^{2dp} \). Since \( T_{p+1}(x) \) and \( T_{p-1}(x) \) are monic of degrees \( dp+1 \) and \( dp-1 \) respectively, and \( dp+1 + dp-1 = 2dp + 1 \), we get the formulas in the corollary. \( \square \)

Proof of Theorem 3. Set \( S_{n} = x^{-(d_{n}+p-d_{n})}T_{n+p} \mod p \). We know \( S_{0} = 1 \) and \( S_{1} = x \) by Proposition 10 and Corollary 12. Noting that \( S'_{n} = x^{-(d_{n}+p-d_{n})}T'_{n+p} \) and \( S''_{n} = x^{-(d_{n}+p-d_{n})}T''_{n+p} \) since \( d_{n+p} - d_{n} = p(p + 1 + 2n)/2 \equiv 0 \mod p \), we have the same recursion (1) for \( \{S_{n}\}_{n\geq0} \). Thus we conclude \( S_{n} \equiv T_{n} \mod p \) for all \( n \). Applying this inductively, we establish Theorem 3. \( \square \)

Corollary 13. We have \( T_{p+1-i} \equiv x^{dp_{i}-i-d_{i}}T_{i} \mod p \).

Proof. We use the relation \( T_{n-1}(x) = T_{n}(x) \) as indicated in Remark 9. Theorem 3 also holds for negative indices and we obtain

\[
T_{p-1-i} = T_{p+i}(x) \equiv x^{dp_{i}-i-d_{i}}T_{i}(x) = x^{dp_{i}-i-d_{i}}T_{i}(x).
\]

Finally, we briefly mention what happens in the case when \( p = 2 \) and 3.

Remark 14. Consider the general recursion [10] in Remark 7 with \( a \in \mathbb{Z} \). For \( p = 3 \), it is easy to see (using the fact that \( T_{n}(x) \) is “almost” a polynomial in \( x^{3} \)) that

\[
T_{n}(x) \equiv (x-a)^{d_{n}} \mod 3 \quad \text{if} \quad n \equiv 0, 2 \mod 3
\]

and

\[
T_{n}(x) \equiv x(x-a)^{d_{n}-1} \mod 3 \quad \text{if} \quad n \equiv 1 \mod 3.
\]

In contrast, it trivially holds that \( T_{n}(x) \equiv x^{d_{n}} \mod 2 \) if \( a \) is even, while for odd \( a \), numerical computation suggests that no periodic pattern for \( T_{n}(x) \mod 2 \) exists and that irreducible factors of arbitrary high degree occur as \( n \) gets bigger.
References


Masanobu Kaneko
Graduate School of Mathematics
Kyushu University
Fukuoka 812-8581
Japan
E-mail: mkaneko*math.kyushu-u.ac.jp

Hiroyuki Ochiai
Department of Mathematics
Tokyo Institute of Technology
Meguro
Tokyo 152-8551
Japan

Current address:
Department of Mathematics
Nagoya University
Nagoya 464-8602
Japan