MODIFIED DICKSON POLYNOMIALS

Piero Filipponi

Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142 Rome, Italy

e-mail: filippo@fub.it

(*Submitted April 1995*)

1. INTRODUCTION AND PRELIMINARIES

The aim of this paper is to extend the previous work [1] by considering the polynomials

$$Z_n(y) \stackrel{\text{def}}{=} \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j}\binom{n-j}{j} y^{\lfloor n/2 \rfloor - j} \quad (n \geq 1) \tag{1.1}$$

in the indeterminate y, where the symbol $\lfloor \cdot \rfloor$ denotes the greatest integer function. It can be seen that

$$Z_n(y) = \begin{cases} p_n(y^{1/2}, 1) & (n \text{ even}), \\ y^{-1/2} p_n(y^{1/2}, 1) & (n \text{ odd and } y \neq 0), \end{cases} \tag{1.2}$$

where $p_n(y, 1)$ are the *Dickson polynomials* in y with the parameter $c = 1$ (e.g., see (1.1) of [1]). Because of the relation (1.2), the quantities $Z_n(y)$ will be referred to as *modified Dickson polynomials*. Information on theoretical aspects and practical applications of (usual) Dickson polynomials can be found through the exhaustive list of references reported in [1], where an extension of them has been studied.

In this article we are concerned with modified Dickson polynomials taken at nonnegative integers. In fact, it is the purpose of this article to establish basic properties of the elements of the sequences of integers $\{Z_n(k)\}_0^\infty$ $(k = 0, 1, 2, \ldots)$. More precisely, in Section 2 closed-form expressions for $Z_n(k)$ are found which, for $k = 2, 3$, and 4, give rise to three supposedly new combinatorial identities. Several identities involving $Z_n(k)$ are exhibited in Section 3, while some congruence properties of these numbers are established in Section 4.

To obtain the results presented in Sections 2 and 3, we make use of the main properties of the generalized Fibonacci numbers $U_n(x)$ and the generalized Lucas numbers $V_n(x)$ (e.g., see [2], [8]) defined by

$$U_n(x) = xU_{n-1}(x) + U_{n-2}(x), \quad [U_0(x) = 0, U_1(x) = 1], \tag{1.3}$$

$$V_n(x) = xV_{n-1}(x) + V_{n-2}(x), \quad [V_0(x) = 2, V_1(x) = x], \tag{1.4}$$

where x is an arbitrary (possibly complex) quantity. Recall that closed-form expressions (Binet forms) for $U_n(x)$ and $V_n(x)$ are

$$\begin{cases} U_n(x) = (\alpha_x^n - \beta_x^n) / \Delta_x, \\ V_n(x) = \alpha_x^n + \beta_x^n, \end{cases} \tag{1.5}$$

where

$$\begin{cases} \Delta_x = \sqrt{x^2 + 4}, \\ \alpha_x = (x + \Delta_x) / 2, \\ \beta_x = (x - \Delta_x) / 2. \end{cases} \tag{1.6}$$

As an illustration, the numbers $Z_n(k)$ are displayed in Table 1 for the first few values of k and n. From (1.1), we can observe that $Z_0(k)$ yields the indeterminate form $0/0$. For the sake of completeness, we assume that

$$Z_0(k) \stackrel{\text{def}}{=} 2 \ \forall k. \tag{1.7}$$

It can be checked readily that all the results established throughout the paper are consistent with the assumption (1.7).

TABLE 1. The Numbers $Z_n(k)$ for $0 \le n, k \le 8$

$n \backslash k$	0	1	2	3	4	5	6	7	8
0	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1
2	−2	−1	0	1	2	3	4	5	6
3	−3	−2	−1	0	1	2	3	4	5
4	2	−1	−2	−1	2	7	14	23	34
5	5	1	−1	−1	1	5	11	19	29
6	−2	2	0	−2	2	18	52	110	198
7	−7	1	1	−1	1	13	41	91	169
8	2	−1	2	−1	2	47	194	527	1154

2. CLOSED-FORM EXPRESSIONS FOR $Z_n(k)$

The following identity (see [3]) plays a crucial role in the proofs of the results established in this article.

$$Z_n(\Delta_x^2) = \begin{cases} V_n(x) & (n \text{ even}), \\ U_n(x) & (n \text{ odd}). \end{cases} \tag{2.1}$$

As particular cases of (2.1), we have

$$Z_n(5) = \begin{cases} V_n(1) = L_n & (n \text{ even}), \\ U_n(1) = F_n & (n \text{ odd}), \end{cases} \tag{2.2}$$

where F_n and L_n are the n^{th} Fibonacci and Lucas numbers, respectively, and

$$Z_n(8) = \begin{cases} V_n(2) = Q_n & (n \text{ even}), \\ U_n(2) = P_n & (n \text{ odd}), \end{cases} \tag{2.3}$$

where P_n and Q_n are the n^{th} Pell and Pell-Lucas numbers, respectively (e.g., see [6]).

2.1 Results

A closed-form expression for $Z_n(k)$ which is valid for all k can be obtained readily from (2.1), (1.5), and (1.6). Namely, we get

$$Z_n(k) = \begin{cases} V_n(\sqrt{k-4}) & (n \text{ even}), \\ U_n(\sqrt{k-4}) & (n \text{ odd}). \end{cases} \tag{2.4}$$

It is worth mentioning that using (2.4) along with an interesting result established by Melham and Shannon [9, (5.1)-(5.3)] allows us to state that the terms of $\{Z_n(k)\}$ are generated by the powers of the 2-by-2 matrix $\mathbf{M}_k$ defined as

$$\mathbf{M}_k = \begin{bmatrix} k-2 & \sqrt{k-4} \\ \sqrt{k-4} & 2 \end{bmatrix}. \tag{2.5}$$

More precisely, it can be seen that the lower-right entry of $\mathbf{M}_k^n$ equals $k^{\lfloor n/2 \rfloor} Z_{n-1}(k)$.

As we shall see in the following, for $k = 1, 2, 3$, and 4, the corresponding value of $Z_n(k)$ is periodic, and (2.4) produces some interesting combinatorial identities. The proofs of these results are given in subsection 2.2.

The trivial case $k = 0$ is treated here only for the sake of completeness. This can be solved readily on the basis of the usual convention (e.g., see [10, p. 147])

$$0^h = \begin{cases} 1, & \text{if } h = 0, \\ 0, & \text{if } h > 0. \end{cases} \tag{2.6}$$

In fact, from (1.1) and (2.6), we have

$$Z_n(0) = \frac{n}{n - \lfloor n/2 \rfloor} \binom{n - \lfloor n/2 \rfloor}{\lfloor n/2 \rfloor} (-1)^{\lfloor n/2 \rfloor} = \begin{cases} 2(-1)^{n/2} & (n \text{ even}), \\ n(-1)^{(n-1)/2} & (n \text{ odd}). \end{cases} \tag{2.7}$$

The case $k = 1$ gives rise to a particularly interesting combinatorial identity. Its solution (credited to Hardy, 1924), which is reported in [10, p. 77], contains several misprints. In [4] we proved that

$$Z_n(1) = \begin{cases} 2(-1)^n, & \text{if } n \equiv 0 \pmod 3, \\ (-1)^{n+1}, & \text{otherwise.} \end{cases} \tag{2.8}$$

In this article we give a simpler proof of (2.8) which is obtained by using the Binet forms for $U_n(x)$ and $V_n(x)$, and certain trigonometric identities. For $2 \le k \le 4$, we get the identities

$$Z_n(2) = \begin{cases} -2, & \text{if } n \equiv 4, \\ -1, & \text{if } n \equiv \pm 3, \\ 0, & \text{if } n \equiv \pm 2 \pmod 8, \\ 1, & \text{if } n \equiv \pm 1, \\ 2, & \text{if } n \equiv 0, \end{cases} \tag{2.9}$$

$$Z_n(3) = \begin{cases} -2, & \text{if } n \equiv 6, \\ -1, & \text{if } n \equiv \pm 4 \text{ or } \pm 5, \\ 0, & \text{if } n \equiv \pm 3 \qquad \pmod{12} \\ 1, & \text{if } n \equiv \pm 1 \text{ or } \pm 2, \\ 2, & \text{if } n \equiv 0, \end{cases} \tag{2.10}$$

and

$$Z_n(4) = \begin{cases} 1 & (n \text{ odd}), \\ 2 & (n \text{ even}). \end{cases} \tag{2.11}$$

2.2 Proofs

The proofs of (2.8)-(2.11) are similar so that, for the sake of brevity, we prove only (2.8) and (2.9).

Proof of (2.8): Denoting the imaginary unit by i, from (2.4) write

$$Z_n(1) = \begin{cases} V_n(i\sqrt{3}) & (n \text{ even}), \\ U_n(i\sqrt{3}) & (n \text{ odd}), \end{cases} \tag{2.12}$$

whence, on using the Binet forms (1.5),

$$\begin{aligned} Z_n(1) &= [(i\sqrt{3}+1)/2]^n + (-1)^n[(i\sqrt{3}-1)/2]^n \\ &= \cos\frac{n\pi}{3} + i\sin\frac{n\pi}{3} + (-1)^n\left[\cos\frac{2n\pi}{3} + i\sin\frac{2n\pi}{3}\right]. \end{aligned} \tag{2.13}$$

Using (2.13) along with the trigonometric identities

$$\sin\frac{n\pi}{3} = (-1)^{n+1}\sin\frac{2n\pi}{3} \tag{2.14}$$

and

$$\cos\frac{n\pi}{3} = \begin{cases} (-1)^n, & \text{if } 3|n, \\ (-1)^{n+1}/2, & \text{otherwise}, \end{cases} \tag{2.15}$$

yields identity (2.8). Q.E.D.

Proof of (2.9): From (2.4) write

$$Z_n(2) = \begin{cases} V_n(i\sqrt{2}) & (n \text{ even}), \\ U_n(i\sqrt{2}) & (n \text{ odd}), \end{cases} \tag{2.16}$$

whence, on using (1.5),

$$\begin{aligned} Z_n(2) &= \begin{cases} [(i\sqrt{2}+\sqrt{2})/2]^n + [(i\sqrt{2}-\sqrt{2})/2]^n & (n \text{ even}), \\ \dfrac{1}{\sqrt{2}}\{[(i\sqrt{2}+\sqrt{2})/2]^n - [(i\sqrt{2}-\sqrt{2})/2]^n\} & (n \text{ odd}), \end{cases} \\ &= \begin{cases} \cos\dfrac{n\pi}{4} + i\sin\dfrac{n\pi}{4} + \cos\dfrac{3n\pi}{4} + i\sin\dfrac{3n\pi}{4} & (n \text{ even}), \\ \dfrac{1}{\sqrt{2}}\left[\cos\dfrac{n\pi}{4} + i\sin\dfrac{n\pi}{4} - \cos\dfrac{3n\pi}{4} - i\sin\dfrac{3n\pi}{4}\right] & (n \text{ odd}). \end{cases} \end{aligned} \tag{2.17}$$

Using (2.17) along with the trigonometric identities

$$\sin\frac{n\pi}{4} = (-1)^{n+1}\sin\frac{3n\pi}{4} \tag{2.18}$$

and

$$\cos\frac{n\pi}{4} = (-1)^n \cos\frac{3n\pi}{4} = \begin{cases} -1, & \text{if } n \equiv 4, \\ -1/\sqrt{2}, & \text{if } n \equiv \pm 3, \\ 0, & \text{if } n \equiv \pm 2 \pmod 8, \\ 1/\sqrt{2}, & \text{if } n \equiv \pm 1, \\ 1, & \text{if } n \equiv 0, \end{cases} \tag{2.19}$$

yields identity (2.9). Q.E.D.

3. SOME IDENTITIES INVOLVING $Z_n(k)$

Some simple identities involving the numbers $Z_n(k)$ (or simply Z_n if no misunderstanding can arise) are exhibited in this section. Most of the proofs are left as an exercise for the interested reader. First, we get the recurrences

$$Z_{n+1} - Z_n = \begin{cases} -Z_{n-1} & (n \text{ even}), \\ Z_{n+2} & (n \text{ odd}). \end{cases} \tag{3.1}$$

Then, we observe that, for n even, identity (3.1) is a special case (namely, $m = 1$) of the more general identity

$$Z_{n+m} + Z_{n-m} = \begin{cases} kZ_nZ_m, & \text{if } n \text{ and } m \text{ are odd}, \\ Z_nZ_m, & \text{otherwise}, \end{cases} \tag{3.2}$$

which can be proved by using (2.4) and the identities (3)-(8) of [7, p. 94]. It is worth noting that letting n be a suitable function of m in (3.2) yields

$$Z_nZ_{n-1} = Z_{2n-1} + 1 \quad (n = m+1), \tag{3.3}$$

$$Z_{2n} = \begin{cases} Z_n^2 - 2 & (n \text{ even}) \\ kZ_n^2 - 2 & (n \text{ odd}) \end{cases} \quad (n = m), \tag{3.4}$$

$$\begin{aligned} Z_{3n} &= Z_n(Z_{2n} - 1) \quad (n = 2m) \\ &= \begin{cases} Z_n^3 - 3Z_n & (n \text{ even}) \\ kZ_n^3 - 3Z_n & (n \text{ odd}) \end{cases} \quad [\text{from } (3.4)]. \end{aligned} \tag{3.5}$$

More generally, for $h = 1, 2, 3, \ldots$, we get the multiplication formula

$$Z_{hn} = \sum_{j=0}^{\lfloor h/2 \rfloor} (-1)^j \frac{h}{h-j}\binom{h-j}{j}\begin{bmatrix} \cdot Z_n^{h-2j} & (n \text{ even}), \\ \cdot Z_n^{h-2j}k^{\lfloor h/2 \rfloor - j} & (n \text{ odd}). \end{bmatrix} \tag{3.6}$$

Induction on h provides the required proof. Observe that, for n even, Z_{hn} and the Dickson polynomial $p_h(Z_n, 1)$ coincide, whereas, for n odd and h even, $Z_{hn}(k) = Z_h(kZ_n^2(k))$.

The Simson formula analog for the sequence $\{Z_n(k)\}$ is

$$Z_n^2 - Z_{n-1}Z_{n+1} = \frac{(-1)^n(k-1)Z_{2n} + 2}{k} + \begin{bmatrix} 1 & (n \text{ even}) \\ 2-k & (n \text{ odd}). \end{bmatrix} \tag{3.7}$$

Properties of the matrix $\mathbf{M}_k$ [see (2.5)] are useful tools for discovering combinatorial identities involving Z_n. For example, denoting by $\mathbf{I}$ the 2-by-2 identity matrix, we can expand the identity (see (5.8) of [9])

$$[k(\mathbf{M}_k - \mathbf{I})]^n = \mathbf{M}_k^{2n}, \tag{3.8}$$

and equate the lower-right entries on both sides to obtain

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}k^{\lfloor j/2\rfloor}Z_{j-1} = (-1)^n Z_{2n-1}. \tag{3.9}$$

Remark: The assumption $Z_{-1} = 1\,\forall k$ is implied by the definition $\mathbf{M}_k^0 = \mathbf{I}$. The same result can be obtained by using (3.1) and (1.7).

Analogously, after noting that $\mathbf{M}_k^{-1} = \mathbf{I} - \mathbf{M}_k / k$, we can expand the identity $\mathbf{M}_k^n\mathbf{M}_k^{-h} = \mathbf{M}_k^{n-h}$ to get the relation

$$\sum_{j=0}^{h}(-1)^j\binom{h}{j}k^{\lfloor (n-j)/2\rfloor}Z_{n+j-1} = k^{\lfloor (n-h)/2\rfloor}Z_{n-h-1} \quad (n \ge h) \tag{3.10}$$

which, for $n = h$, reduces to

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}k^{\lfloor (n-j)/2\rfloor}Z_{n+j-1} = 1. \tag{3.11}$$

Let us conclude this section by stating the summation identity:

$$S_N(k) \stackrel{\text{def}}{=} \sum_{n=1}^{N} Z_n = \frac{Z_{N+2} + Z_{N+1} - Z_N - Z_{N-1}}{k-4} - 1 \quad (k \ne 4) \tag{3.12}$$

$$= \begin{cases} (Z_{N+2} - 2Z_{N-1})/(k-4) - 1 & (N \text{ even}) \\ (2Z_{N+2} - Z_{N-1})/(k-4) - 1 & (N \text{ odd}) \end{cases} \quad \text{[from (3.1)]}. \tag{3.12'}$$

Remarks:

(i) Assumption (1.7) is needed to get the obvious result $S_1(k) = Z_1 = 1$.

(ii) $$S_N(4) = \begin{cases} 3N/2 & (N \text{ even}) \\ (3N-1)/2 & (N \text{ odd}) \end{cases} \quad \text{[from (2.11)]}. \tag{3.13}$$

Proof of (3.12): First, consider N odd, and rewrite $S_N(k)$ as

$$\begin{aligned} S_N(k) &= \sum_{j=1}^{(N+1)/2} Z_{2j-1} + \sum_{j=1}^{(N-1)/2} Z_{2j} \\ &= \sum_{j=1}^{(N+1)/2} U_{2j-1}(\sqrt{k-4}) + \sum_{j=1}^{(N-1)/2} V_{2j}(\sqrt{k-4}) \quad \text{[from (2.4)]}. \end{aligned} \tag{3.14}$$

By using the Binet forms (1.3) and (1.4), and the geometric series formula, it can be readily seen that

$$\sum_{j=1}^{h} U_{2j-1}(x) = [U_{2h+1}(x) - U_{2h-1}(x)]/x^2 \tag{3.15}$$

and

$$\sum_{j=1}^{h} V_{2j}(x) = [V_{2h+2}(x) - V_{2h}(x) - x^2] / x^2, \tag{3.16}$$

whence, invoking (2.4) again, (3.14) reduces to (3.12). The proof for N even is analogous to that for N odd, and is omitted. Q.E.D.

4. CONGRUENCE PROPERTIES OF $Z_n(k)$

In this section we show some basic congruence properties of the numbers $Z_n(k)$. For reasons of space, only Proposition 2 is proved in detail. We have established the following:

$$Z_n(k) \equiv 0 \pmod 2 \text{ if } \begin{cases} n \equiv 0 \pmod 2 & (k \text{ even}) \\ n \equiv 0 \pmod 3 & (k \text{ odd}). \end{cases} \tag{4.1}$$

From (1.1), we clearly have that

$$Z_n(k) \equiv Z_n(0) \pmod k \quad (k \geq 1), \tag{4.2}$$

where $Z_0(k)$ is given by (2.7). From (4.2), (2.7), and (3.4), one can readily see that

$$\frac{Z_n(k) - Z_n(0)}{k} = \frac{Z_n(k) - 2}{k} = Z_{n/2}^2(k) \quad [n \equiv 2 \pmod 4]. \tag{4.3}$$

Observe that (4.2) and (2.7) imply the congruence

$$Z_k(k) \equiv 0 \pmod k \quad (k \text{ odd}). \tag{4.4}$$

From (4.4) and (2.4), one immediately gets the following (supposedly known) result.

Proposition 1: If m is an odd integer and $h = m^2 + 4$, then $U_h(m)$ is divisible by h.

Finally, let us state the following proposition.

Proposition 2: If p is an odd prime, then

$$Z_p(k) \equiv (k / p) \pmod p, \tag{4.5}$$

where (k / p) denotes the Legendre symbol.

It is worth noting that (2.4) and (4.5) constitute a simple proof of a well-known congruence property of the generalized Fibonacci numbers $U_n(s)$ (s an arbitrary integer) defined by (1.3). In fact, we get

$$U_p(s) \equiv (s^2 + 4 / p) \pmod p. \tag{4.6}$$

Proof of Proposition 2: That $\binom{n-j}{j} \equiv 0 \pmod{n-j}$ if $j \geq 1$ and $\gcd(n, j) = 1$ is a well-known fact (e.g., see Lemma 1 of [5]). Consequently, from (1.1), we have

$$Z_p(k) \equiv k^{(p-1)/2} \pmod p, \tag{4.7}$$

whence

$$Z_p(k) \equiv 0 \pmod p \text{ if } k \equiv 0 \pmod p. \tag{4.8}$$

If $k \not\equiv 0 \pmod p$, by Fermat's little theorem we have the congruence $k^{p-1} \equiv 1 \pmod p$, whence we can write

$$(k^{(p-1)/2}+1)(k^{(p-1)/2}-1) \equiv 0 \pmod p. \tag{4.9}$$

Let $a\,(b)$ be the first (second) factor on the left-hand side of (4.9). Since $p \geq 3$ by definition, either a or b (not both) is divisible by p. If k is a quadratic residue (q.r.) $(\text{mod } p)$ [i.e., if there exists z such that $k \equiv z^2 \pmod p$], then, by Fermat's little theorem, we have $k^{(p-1)/2} \equiv z^{2(p-1)/2} \equiv 1$ $(\text{mod } p)$, that is, $b \equiv 0 \pmod p$. If k is not a q.r. $(\text{mod } p)$, then we necessarily have $a \equiv 0 \pmod p$. Therefore, from (4.7), we can write

$$Z_p(k) \equiv \begin{cases} 1 \pmod p & \text{if } k \text{ is a q.r. } (\text{mod } p), \\ -1 \pmod p & \text{otherwise.} \end{cases} \tag{4.10}$$

Congruences (4.8) and (4.10) prove the proposition. Q.E.D.

ACKNOWLEDGMENT

This work has been carried out in the framework of an agreement between the Italian PT Administration (Istituto Superiore PT) and the Fondazione Ugo Bordoni.

REFERENCES

1. P. Filipponi, R. Menicocci, & A. F. Horadam. "Extended Dickson Polynomials." *The Fibonacci Quarterly* **32.5** (1994):455-64.
2. P. Filipponi & A. F. Horadam. "Derivative Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers* **4**:99-108. Dordrecht: Kluwer, 1991.
3. P. Filipponi. "Waring's Formula, the Binomial Formula, and Generalized Fibonacci Matrices." *The Fibonacci Quarterly* **30.3** (1992):225-31.
4. P. Filipponi & S. Mascella. "On a Combinatorial Quantity Involved in a Fibonacci Identity." Technical Report 3T00995. Rome: Fondazione Ugo Bordoni, 1995.
5. P. Filipponi. "Incomplete Fibonacci and Lucas Numbers." *Rend. Circ. Mat. Palermo*, Series 2, **45.1** (1996):37-56.
6. A. F. Horadam & Bro. J. M. Mahon. "Pell and Pell-Lucas Polynomials." *The Fibonacci Quarterly* **23.1** (1985):7-20.
7. D. Jarden. *Recurring Sequences*. Jerusalem: Riveon Lematematika, 1973.
8. R. S. Melham & A. G. Shannon. "Inverse Trigonometric and Hyperbolic Summation Formulas Involving Generalized Fibonacci Numbers." *The Fibonacci Quarterly* **33.1** (1995):32-40.
9. R. S. Melham & A. G. Shannon. "Some Summation Identities Using Generalized *Q*-Matrices." *The Fibonacci Quarterly* **33.1** (1995):64-73.
10. J. Riordan. *Combinatorial Identities*. New York: Wiley, 1968.

AMS Classification Numbers: 11B39, 05A19, 11A07

❖❖❖