EXTENDED DICKSON POLYNOMIALS

Piero Filipponi
Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142, Roma, Italy

Renato Menicocci
Fondazione Ugo Bordoni, Via B. Castiglione 59, I-00142, Roma, Italy

Alwyn F. Horadam
University of New England, Armidale, Australia 2351
(*Submitted May 1993*)

1. PRELIMINARIES

The polyomials $p_n(x,c)$ defined by

$$p_n(x,c)=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\binom{n-i}{i}(-c)^i x^{n-2i}\quad(n>0),\tag{1.1}$$

where $\lfloor\cdot\rfloor$ denotes the greatest integer function and x is an indeterminate, are commonly referred to as *Dickson polynomials* (e.g., see [6]). These polynomials have been studied in the past years, both from the point of view of their theoretical properties [2], [6], and [14], and from that of their practical applications [7], [9], [10]. and [13]. In particular, their relevance to public-key cryptosystems has been pointed out in [8], [11], [12], and [16]. As is shown, e.g., in [14], the coefficients of $p_n(x,c)$ are integers for any positive integer n and $c\in\mathbb{Z}$. It is also evident that

$$p_n(x,-1)=V_n(x),\tag{1.2}$$

where $V_n(x)=xV_{n-1}(x)+V_{n-2}(x)$ $[V_0(x)=2, V_1(x)=x]$ are the *Lucas polynomials* considered in [3] and [5]. In particular, we have

$$p_n(1,-1)=L_n,\tag{1.3}$$

where L_n is the n^{th} Lucas number.

In this paper, we consider the *extended Dickson polynomials* $p_n(x,c,U)$ defined in the next section.

2. INTRODUCTION AND DEFINITIONS

Let us define the extended Dickson polynomials $p_n(x,c,U)$ as the polynomials obtainable by replacing the upper range indicator in the sum (1.1) by a positive integer $U>\lfloor n/2\rfloor$. This paper is essentially dedicated to the study of the case $x=-c=1$.

By (1.1) we have

$$p_n(1,-1,U)\stackrel{\text{def}}{=}T_n(U)=\sum_{i=0}^{U}\frac{n}{n-i}\binom{n-i}{i}\quad(n>0).\tag{2.1}$$

If $\lfloor n/2\rfloor\le U\le n-1$, the sum (2.1) gives L_n as the binomial coefficient vanishes when $\lfloor n/2\rfloor+1\le i\le n-1$. For example, if $n=5$ (so $U=2,3,$ or 4), then $T_5(U)=L_5=11$. If $U\ge n$, the upper argument of the binomial coefficient becomes negative for $i\ge n+1$, and the (nonzero) value of the binomial coefficient can be obtained by (2.6). For $i = n$, the argument of the sum (2.1) assumes the indeterminate form $0 \cdot n / 0$ which will be settled in the sequel.

By (2.1) we can write

$$T_n(U) = L_n + H_n(k) \quad (k = U - n \geq 0), \tag{2.2}$$

where

$$H_n(k) = \sum_{i=n}^{n+k} \frac{n}{n-i}\binom{n-i}{i} = H_n(0) + \sum_{i=n+1}^{n+k} \frac{n}{n-i}\binom{n-i}{i} \quad (n > 0). \tag{2.3}$$

The quantity $H_n(0)$ in (2.3) is clearly given by the expression

$$H_n(0) = \sum_{i=n}^{n} \frac{n}{n-i}\binom{n-i}{i} \quad (n > 0), \tag{2.4}$$

which has the above said indeterminate form. In order to remove this obstacle, we use the combinatorial identities

$$\frac{h}{h-m}\binom{h-m}{m} = \binom{h-m}{m} + \binom{h-m-1}{m-1}, \tag{2.5}$$

$$\binom{-h}{m} = (-1)^m \binom{m+h-1}{h-1} = (-1)^m \binom{m+h-1}{m} \tag{2.6}$$

(available in [12], pp. 64 and 1, respectively), and rewrite (2.4) as

$$\begin{aligned} H_n(0) &= \sum_{i=n}^{n}\left[\binom{n-i}{i} + \binom{n-1-i}{i-1}\right] = \binom{0}{n} + \binom{-1}{n-1} \\ &= 0 + (-1)^{n-1}\binom{n-1}{n-1} = (-1)^{n-1} \quad (n > 0). \end{aligned} \tag{2.7}$$

For the sake of consistency, let us assume that the above result is valid also for $n = 0$, so

$$H_0(0) \stackrel{\text{def}}{=} (-1)^{-1} = -1. \tag{2.8}$$

On the basis of (2.3), (2.7), and (2.8), for given *nonnegative* integers n and k, let us define

$$H_n(k) \stackrel{\text{def}}{=} (-1)^{n-1} + \sum_{i=n+1}^{n+k} \frac{n}{n-i}\binom{n-i}{i} \quad (n, k \geq 0), \tag{2.9}$$

where the usual convention that

$$\sum_{i=a}^{b} f(i) = 0 \text{ for } b < a \tag{2.10}$$

has to be invoked for obtaining $H_0(0) = -1$.

The numbers $H_n(k)$ defined by (2.9) are the *companions* of the numbers

$$G_n(k) \stackrel{\text{def}}{=} \sum_{i=n}^{n+k}\binom{n-1-i}{i} = (-1)^n \sum_{j=0}^{k} (-1)^j \binom{n+2j}{j} \tag{2.11}$$

which have been thoroughly investigated in [4]. The numbers $G_n(k)$ arise from the incorrect use of a combinatorial formula for generating the Fibonacci numbers F_n, whereas the numbers $H_n(k)$

result from an analogous use of the combinatorial formula (2.1) which (under appropriate constraints on U) generates the Lucas numbers (compare (2.2) with [4, (1.7)]) and are the fruit of our mathematical curiosity. The principal aim of this paper is to give alternative expressions of the numbers $H_n(k)$ (Section 3), to find connections between these numbers and their companions $G_n(k)$, and to give a brief account of their properties (Sections 4 and 5). A glimpse of the application of the above argument to the Dickson polynomials (1.2) is caught in Section 6, where the polynomials $H_n(k,x)$ are considered.

3. THE NUMBERS $H_n(k)$

Letting $i=n+j$ in (2.9) yields

$$H_n(k)=(-1)^{n-1}+\sum_{j=1}^{k}\frac{n}{-j}\binom{-j}{n+j} \tag{3.1}$$

whence, by using the identity (2.6), we obtain the definition

$$H_n(k)=(-1)^{n-1}-(-1)^n\sum_{j=1}^{k}(-1)^j\frac{n}{j}\binom{n-1+2j}{j-1} \tag{3.2}$$

which can be rewritten as

$$H_n(k)=(-1)^{n-1}+(-1)^n\sum_{j=0}^{k-1}(-1)^j\frac{n}{j+1}\binom{n+1+2j}{j}. \tag{3.3}$$

By using (2.3), (2.5), and (2.6), the following equivalent definitions can be obtained, the proof of which are left as an exercise to the interested reader:

$$H_n(k)=(-1)^n\sum_{j=0}^{k}(-1)^j\left[\binom{n-1+2j}{j-1}-\binom{n-1+2j}{j}\right] \tag{3.4}$$

$$=(-1)^{n+1}\sum_{j=0}^{k-1}(-1)^j\binom{n+1+2j}{j}+(-1)^{n-1}\sum_{j=0}^{k}(-1)^j\binom{n-1+2j}{j}. \tag{3.5}$$

Definitions (3.4) and (3.5) show clearly that the numbers $H_n(k)$ are integers. Observe that $H_0(0)=-1$ results from (3.5) by invoking (2.10), and from (3.4) by assuming that

$$\binom{h}{-m}=0 \quad (m\geq 1,\ h \text{ arbitrary}) \quad [12, \text{p. } 2]. \tag{3.6}$$

Some particular cases, beyond $H_n(0)$ given by (2.7) and (2.8), are

$$H_n(1)=(-1)^n(n-1), \tag{3.7}$$

$$H_n(2)=(-1)^{n-1}(n^2+n+2)/2, \tag{3.8}$$

and

$$H_0(k)=-1\ \forall\ k, \tag{3.9}$$

which are readily obtainable by (3.2)–(3.5). The numbers $H_n(k)$ are shown in Table 1 for the first few values of n and k.

TABLE 1. The Numbers $H_n(k)$ for $0 \le n,\ k \le 5$

k \ n	0	1	2	3	4	5
0	−1	1	−1	1	−1	1
1	−1	0	1	−2	3	−4
2	−1	2	−4	7	−11	16
3	−1	−3	10	−21	37	−59
4	−1	11	−32	69	−128	216
5	−1	−31	100	−228	444	−785

4. SOME IDENTITIES INVOLVING THE NUMBERS $H_n(k)$ AND $G_n(k)$

First of all, we give a relation between the numbers $H_n(k)$ and their companions $G_n(k)$ [see (2.11)].

Proposition 1: $H_n(k) = G_{n-1}(k) + G_{n+1}(k-1) \quad (n, k \ge 0)$.

Proof: For $n, k \ge 1$, the above identity readily follows from the definitions (2.11) and (3.5). For n and/or $k = 0$, let us use the expressions of $G_{-n}(k)$ and $G_n(-k)$ established in [4, §4].

<u>Case 1</u>: $n \ge 1$ and $k = 0$.
By [4, (4.1)], (2.11), and (2.7), we get

$$G_{n-1}(0) + G_{n+1}(-1) = G_{n-1}(0) + 0 = (-1)^{n-1} = H_n(0).$$

<u>Case 2</u>: $n = 0$ and $k \ge 1$.
By [4, (4.9)] and (3.9), we get

$$G_{-1}(k) + G_1(k-1) = -[F_1 + G_1(k-1)] + G_1(k-1) = -1 = H_0(k).$$

<u>Case 3</u>: $n = k = 0$.
By [4, (4.1) and (4.8)] and (2.8), we get

$$G_{-1}(0) + G_1(-1) = G_{-1}(0) + 0 = -F_1 = -1 = H_0(0). \quad \square$$

Proposition 1 together with some properties of the numbers $G_n(k)$ found in [4] will play a crucial role in establishing several properties of the numbers $H_n(k)$. A further connection between $H_n(k)$ and $G_n(k)$ is stated in the following proposition.

Proposition 2: $H_n(k) = G_{n+2}(k-2) - G_{n-2}(k) \quad (n, k \ge 0)$.

Proof: By using the recurrence [4, (3.1)], namely,

$$G_{n+2}(k-1) = G_{n+1}(k) + G_n(k), \tag{4.1}$$

we can write

$$\begin{aligned} G_{n+2}(k-2) - G_{n-2}(k) &= G_{n+1}(k-1) + G_n(k-1) - G_{n-2}(k) \\ &= G_{n+1}(k-1) + G_n(k-1) - [G_n(k-1) - G_{n-1}(k)] \\ &= G_{n+1}(k-1) + G_{n-1}(k) = H_n(k) \quad \text{(by Proposition 1).} \quad \square \end{aligned}$$

Then, we establish a recurrence relation for the numbers $H_n(k)$.

Proposition 3: $H_{n+2}(k-1) = H_{n+1}(k) + H_n(k) \quad (k \geq 1)$.

Proof: $H_{n+1}(k) + H_n(k)$

$$= G_n(k) + G_{n+2}(k-1) + G_{n-1}(k) + G_{n+1}(k-1) \quad \text{(by Proposition 1)}$$
$$= G_n(k) + G_{n+3}(k-2) - G_{n+1}(k-1) + G_{n-1}(k) + G_{n+1}(k-1) \quad \text{[by (4.1)]}$$
$$= G_{n+3}(k-2) + [G_n(k) + G_{n-1}(k) - G_{n+1}(k-1)] + G_{n+1}(k-1).$$

Observing that the expression within square brackets vanishes in virtue of (4.1), we can write

$$H_{n+1}(k) + H_n(k) = G_{n+3}(k-2) + G_{n+1}(k-1) = H_{n+2}(k-1) \quad \text{(by Proposition 1)}. \ \square$$

As a direct consequence of Proposition 3, we can state the following proposition, the proof of which is omitted because of its triviality.

Proposition 4: $\sum_{n=s}^{s+2h-1} H_n(k) = \sum_{n=1}^{h} H_{2n+s}(k-1) \quad (k \geq 1)$.

Also, the curious identity

$$H_n(n) - H_n(n-1) = -\binom{3n-1}{2n} \quad (n \geq 1) \quad [\text{so } H_1(1) - H_1(0) = -1] \tag{4.2}$$

can be readily proved.

Proof of (4.2): By (3.3), we immediately obtain the recurrence relation

$$H_n(k+1) = H_n(k) + (-1)^{n+k} \frac{n}{k+1} \binom{n+1+2k}{k}. \tag{4.3}$$

Replace k by $n-1$ in (4.3) and use [12, (iii), p. 3] to obtain (4.2). $\square$

Let us conclude this section by proving a noteworthy property of the numbers $H_n(k)$.

Proposition 5: $R_n(h, k) \overset{\text{def}}{=} \sum_{i=0}^{h} \binom{h}{i} H_{n+i}(k) = \begin{cases} H_{n+2h}(k-h) & \text{if } k \geq h, \\ 0 & \text{if } k < h. \end{cases}$

Proof: Use Proposition 1 to write

$$R_n(h, k) = \sum_{i=0}^{h} \binom{h}{i} G_{n-1+i}(k) + \sum_{i=0}^{h} \binom{h}{i} G_{n+1+i}(k-1),$$

whence

$$R_n(h, k) = G_{n-1+2h}(k-h) + G_{n+1+2h}(k-1-h) \quad \text{(by [4, Proposition 3])}$$
$$= \begin{cases} H_{n+2h}(k-h) & \text{if } k \geq h \quad \text{(by Proposition 1)} \\ 0 & \text{if } k < h \quad (\text{since } G_n(-k) = 0 \ \forall \ n, \ [4, (4.1)]). \ \square \end{cases}$$

Remark: The proof of Proposition 5 in the case $k < h$ can also be obtained by using double induction (on k and m) to prove that

$$\sum_{i=0}^{k+m}\binom{k+m}{i}H_{n+i}(k)=0 \quad \text{if } m\geq 1. \tag{4.4}$$

This alternative and more direct proof is not difficult but it is rather lengthy and tedious, so it is omitted to save space.

5. SOME SIMPLE CONGRUENCE PROPERTIES OF $H_n(k)$

In this section we are concerned with some aspects of the parity of $H_n(k)$, and with a congruence property of these numbers that is valid for all prime values of the subscript n.

Proposition 6: $H_n(k)\equiv G_n(k) \pmod 2$.

Proof: By Proposition 1 and (4.1), we can write

$$\begin{aligned}H_n(k)&=G_{n-1}(k)+G_{n+1}(k-1)=G_{n-1}(k)+G_n(k)+G_{n-1}(k)\\&=G_n(k)+2G_{n-1}(k)\equiv G_n(k) \pmod 2. \quad \square\end{aligned}$$

The general solution of the problem of establishing the parity of $G_n(k)$ [and hence that of $H_n(k)$] seems to be rather difficult. On the basis of some partial results obtained in [4, §3.1], we show the solution for the particular cases $n=3$ and 2^h. Namely, we have

$$H_3(k) \text{ is even iff } k=2^h-3 \quad (h\geq 2) \tag{5.1}$$

and

$$H_{2^n}(k) \text{ is odd iff } 2^{2h+n-2}-2^n\leq k\leq 2^{2h+n-1}-2^n-1 \quad (n\geq 0;\ h\geq 1). \tag{5.2}$$

Proposition 7: If p is a prime and m is a nonnegative integer, then

(i) $H_p(mp)\equiv \sum_{j=0}^{m}(-1)^j C_j \pmod p$,

where $C_j=\frac{1}{j+1}\binom{2j}{j}$ is the j^{th} *Catalan number*, and

(ii) $H_p(k)\equiv H_p(mp) \pmod p$ if $mp+1\leq k\leq (m+1)p-1$.

Proof of Part (i): For $n=p$, consider the absolute value of the generic addend of the sum in (3.2), namely,

$$\frac{p}{j}\binom{p-1+2j}{j-1}\overset{\text{def}}{=}A_p(j) \quad (j=1,2,\ldots,k). \tag{5.3}$$

By virtue of the integrality of $H_n(k)$ [see Definition (3.4) or (3.5)] and the replacement of k by $k-1$ in the recurrence (4.3), it is readily seen that $A_p(j)$ is an integer. If $j\not\equiv 0 \pmod p$, this quantity is clearly divisible by p. If $p>2$, by (3.2) we can write

$$H_p(mp)\equiv 1+\sum_{\substack{i=1\\ i\equiv 0 \pmod p}}^{mp}(-1)^i A_p(i)=1+\sum_{j=1}^{m}(-1)^{jp}\frac{p}{jp}\binom{p-1+2jp}{jp-1}=$$

$$= 1 + \sum_{j=1}^{m} (-1)^j \frac{1}{j} \binom{2jp+p-1}{(j-1)p+p-1} \pmod{p}, \tag{5.4}$$

whence, by using Lucas' Theorem (e.g., see [1, Theorem 1.1]), we obtain

$$H_p(mp) \equiv 1 + \sum_{j=1}^{m} (-1)^j \frac{1}{j} \binom{2j}{j-1} = 1 + \sum_{j=1}^{m} (-1)^j \frac{1}{j+1} \binom{2j}{j} = \sum_{j=0}^{m} (-1)^j C_j \pmod{p}.$$

When $p = 2$, we have

$$H_2(2m) \equiv -1 + \sum_{j=1}^{m} C_j \pmod{2}. \tag{5.5}$$

Since $-1 \equiv 1 \pmod{2}$, the congruence (5.5) is clearly equivalent to (i).

Proof of Part (ii): For $mp+1 \le k \le (m+1)p-1$ [i.e., for $k \not\equiv 0 \pmod{p}$], rewrite (3.2) as

$$H_p(k) = (-1)^{p-1} - (-1)^p \sum_{j=1}^{mp} (-1)^j A_p(j) - (-1)^p \sum_{j=mp+1}^{k} (-1)^j A_p(j). \tag{5.6}$$

By (5.6), Proposition 7(i), and since $A_p(j) \equiv 0 \pmod{p}$ whenever $j \not\equiv 0 \pmod{p}$, we get the congruence

$$H_p(k) \equiv \sum_{j=0}^{m} (-1)^j C_j - 0 \equiv H_p(mp) \pmod{p}. \quad \square$$

Particular instances of Proposition 7 are:

$$H_p(k) \equiv 1 \pmod{p} \quad \text{if } 0 \le k \le p-1, \tag{5.7}$$

$$H_p(p) \equiv 0 \pmod{p}, \tag{5.8}$$

$$H_p(2p) \equiv 2 \pmod{p}, \tag{5.9}$$

$$H_p(3p) \equiv -3 \pmod{p}, \tag{5.10}$$

$$H_p(4p) \equiv 11 \pmod{p}, \tag{5.11}$$

and

$$H_p(5p) \equiv -31 \pmod{p}. \tag{5.12}$$

Proof of (5.7): Put $m = 0$ in Proposition 7(ii), thus getting the congruence $H_p(k) \equiv H_p(0) \pmod{p}$, if $1 \le k \le p-1$. Since $H_p(0) \equiv 1 \pmod{p}\ \forall\ p$ ($p = 2$ inclusive), the above congruence clearly can be rewritten as (5.7). $\square$

6. THE POLYNOMIALS $H_n(k, x)$

Let us consider the special Dickson polynomials $p_n(x, -1) = V_n(x)$ [see (1.2)]. Paralleling the argument of Section 2 leads us to define the polynomials [cf. (3.2)]

$$H_n(k, x) = \frac{(-1)^{n-1}}{x^n} \left[1 + \sum_{j=1}^{k} (-1)^j \frac{n}{j} \binom{n-1+2j}{j-1} \frac{1}{x^{2j}} \right] \quad (x \ne 0), \tag{6.1}$$

where x is a nonzero indeterminate. These polynomials are the companions of the polynomials

$$G_n(k,x)=\frac{(-1)^n}{x^{n+1}}\sum_{j=0}^{k}(-1)^j\binom{n+2j}{j}\frac{1}{x^{2j}}\quad(x\neq 0),\tag{6.2}$$

considered in [4, §5]. By using the identity (2.5), it can be readily proved that

$$H_n(k,x)=G_{n-1}(k,x)+G_{n+1}(k-1,x).\tag{6.3}$$

Observe that identity (6.3) generalizes Proposition 1.

We believe that the polynomials $H_n(k,x)$ are worthy of a deep investigation. Nevertheless, in this paper we confine ourselves to making nothing but a couple of observations on them.

Observation 1 [on the integrality of $H_n(k,x)$]

$H_n(k,x)$ is evidently an integer whenever x equals the reciprocal of an integer (say, $x=1/h$). This fact does not exclude the existence of irrational (or complex) values of x for which $H_n(k,x)$ is an integer. For example, if x equals any of the roots of the third-degree equation $hx^3-x^2+1=0$, then $H_1(1,x)=h$. Apart from the trivial case

$$H_0(k,x)=-1\ \forall\ k \text{ and } x,\tag{6.4}$$

the problem of the existence of *rational* values of $x\neq 1/h$ such that, for particular values of n and k, $H_n(k,x)$ in an integer in an open problem.

Observation 2 [on a limit concerning $H_n(k,x)$]

Consider the limit

$$\begin{aligned}\lim_{k\to\infty}H_n(k,x)&\overset{\text{def}}{=}H_n(\infty,x)\\&=\frac{(-1)^{n-1}}{x^n}\left[1+\sum_{j=1}^{\infty}(-1)^j\frac{n}{j}\binom{n-1+2j}{j-1}\frac{1}{x^{2j}}\right]\quad(x\neq 0)\quad[\text{by }(6.1)].\end{aligned}\tag{6.5}$$

The results presented in the sequel can be readily deduced from the analogous results on $G_n(k,x)$ established in [4, §5]. First, observe that by (6.1) we can write

$$H_n(\infty,-|x|)=(-1)^nH_n(\infty,|x|),\tag{6.6}$$

so, for the sake of brevity, we shall consider only positive values of x. Then, let us state the following two propositions concerning a closed-form expression and a recurrence relation for $H_n(\infty,x)$, respectively.

Proposition 8: If $x>2$, then $H_n(\infty,x)=-\left(\frac{x-\Delta}{2}\right)^n$, where $\Delta=\sqrt{x^2+4}$.

Proof: By (6.3) we have

$$H_n(\infty,x)=G_{n-1}(\infty,x)+G_{n+1}(\infty,x),\tag{6.7}$$

so that, by [4, (5.11)], namely,

$$G_n(\infty, x) = \frac{(x-\Delta)^n}{2^n \Delta} \quad (x > 2) \tag{6.8}$$

(although the above quantity unfortunately has been denoted in [4] by the symbol $H_n(x)$, it is only marginally related to the quantities denoted by $H_n(k)$ and $H_n(k, x)$ in this paper), we can write

$$H_n(\infty, x) = \frac{(x-\Delta)^{n-1}}{2^{n-1}\Delta} + \frac{(x-\Delta)^{n+1}}{2^{n+1}\Delta},$$

whence, after some simple manipulations, we obtain the desired result,

$$H_n(\infty, x) = -\left(\frac{x-\Delta}{2}\right)^n = -\Delta G_n(\infty, x).$$

We draw attention to the fact that, for $x < 2$, the series (6.5) diverges (see (6.7) and [4, (5.7)]), whereas nothing can be said when $x = 2$, although computer experiments suggest the conjecture $H_n(\infty, 2) \stackrel{c}{=} -(1-\sqrt{2})^n$. Observe that $1-\sqrt{2}$ is one of the roots of the characteristic equation for the Pell recurrence relation. □

We point out that, since

$$-1 < \frac{x-\Delta}{2} < 0 \quad (0 < x < \infty), \tag{6.9}$$

there do not exist real values of x for which $H_n(\infty, x)$ is an integer.

Proposition 9: The numbers $H_n(\infty, x)$ obey the second-order recurrence relation

$$H_n(\infty, x) = xH_{n-1}(\infty, x) + H_{n-2}(\infty, x) \quad (n \ge 2) \tag{6.10}$$

with initial conditions

$$H_0(\infty, x) = -1 \text{ and } H_1(\infty, x) = (\Delta - x)/2. \tag{6.10'}$$

Proof: The proof can be obtained readily by (6.7), [4, Proposition 10], and Proposition 8. □

Let us conclude Observation 2 and the paper by showing the set of all rational values r of x for which $H_n(\infty, r)$ is a rational number. On the basis of the results established in [4, §5.1], we see that this set can be generated by the formula

$$r = \frac{U^2 - V^2}{UV}, \tag{6.11}$$

where U and V range over the set of all positive integers and are subject to the condition

$$U > (1+\sqrt{2})V. \tag{6.12}$$

The fulfillment of inequality (6.12) is necessary to satisfy the inequality $r > 2$ which, in turn, is required for the convergence of the series (6.5). It can be proved readily that the condition $\text{g.c.d.}(U, V) = 1$ must be imposed to obtain all *distinct* values of r.

ACKNOWLEDGMENT

The contribution of the first two authors has been given within the framework of an agreement between the Italian PT Administration and the Fondazione Ugo Bordoni.

REFERENCES

1. D. F. Bailey. "More Binomial Coefficient Congruences." *The Fibonacci Quarterly* **30.2** (1992):121-25.
2. L. Dickson. "The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of Linear Group I." *Ann. Math.* **11** (1896):65-120.
3. P. Filipponi & A. F. Horadam. "Derivative Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers* **4:**99-108. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1991.
4. P. Filipponi, O. Brugia, & A. F. Horadam. "A Note on the Improper Use of a Formula for Fibonacci Numbers." *Int. J. Educ. Sci. Technol.* **24.1** (1993):9-21.
5. A. F. Horadam & P. Filipponi. "Integration Sequences of Fibonacci and Lucas Polynomials." In *Applications of Fibonacci Numbers* **5:**317-30. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1993.
6. H. Lausch & W. Nöbauer. *Algebra of Polyomials.* Amsterdam: North Holland, 1973.
7. Da-Xing Li. "Cryptanalysis of Public-Key Distribution Systems Based on Dickson Polynomials." *Electronic Letters* **27.3** (1991):228-29.
8. R. Lidl & W. B. Müller. "Permutation Polynomials in RSA-Cryptosystems." In *Advances in Cryptology, Proc. of CRYPTO '83,* pp. 293-301. Ed. D. Chaum. New York: Plenum, 1984.
9. R. Lidl, W. B. Müller, & A. Oswald. "Some Remarks on Strong Fibonacci Pseudoprimes." *Applicable Algebra in Eng. Comm. and Comp.* **1.1** (1990):59-65.
10. R. Lidl & W. B. Müller. "Generalization of the Fibonacci Pseudoprimes Test." *Discrete Mathematics* **92** (1991):211-20.
11. W. B. Müller & W. Nöbauer. "Some Remarks on Public-Key Cryptosystems." *Studia Sci. Math. Hungar.* **16** (1981):71-76.
12. W. B. Müller & W. Nöbauer. "Crypanalysis of the Dickson-Scheme." In *Lecture Notes in Computer Science* **219:**71-76. Berlin: Springer-Verlag, 1985.
13. W. B. Müller & A. Oswald. "Generalized Fibonacci Pseudoprimes and Probable Primes." In *Applications of Fibonacci Numbers* **5:**459-64. Ed. G. E. Bergum, A. N. Philippou, & A. F. Horadam. Dordrecht: Kluwer, 1993.
14. L. Rédei. *Algebra.* Vol. I. New York: Pergamon Press, 1967.
15. J. Riordan. *Combinatorial Identities.* New York: Wiley, 1968.
16. P. Smith. "LUC Public-Key Encryption." *Dr. Dobb's Journal* (January 1993):44-49, 90-92.

AMS Classification Numbers: 11B39, 11B65, 11B83

❖❖❖