Journal of Mathematical Research with Applications
Nov., 2019, Vol. 39, No. 6, pp. 563–574
DOI:10.3770/j.issn:2095-2651.2019.06.003
Http://jmre.dlut.edu.cn

On the Applications of the Linear Recurrence Relationships to Pseudoprimes

Tianxiao HE[1,*], **Peter J.-S. SHIUE**[2]
1. *Department of Mathematics, Illinois Wesleyan University, Bloomington, IL* 61702-2900*, U. S. A;*
2. *Department of Mathematical Sciences, University of Nevada, Las Vegas,*
Las Vegas, Nevada, 89154-4020*, U. S. A*

Dedicated to the Memory of Professor L. C. HSU on the Occasion of His 100th Birthday

Abstract We present here some results on the applications of linear recursive sequences of order 2 to the Fermat pseudoprimes, Fibonacci pseudoprimes, and Dickson pseudoprimes.

Keywords Girard-Waring identities; Recursive sequences; Fermat's pseudoprimes; Fibonacci numbers; Lucas numbers; Fibonacci pseudoprimes; Dickson numbers; Dickson pseudoprimes

MR(2010) Subject Classification 05A15; 05A05; 15B36; 15A06; 05A19; 11B83

1. Introduction

In this paper, we are concerned with the applications of Binet formula of recursive sequences of order 2 and the following Girard-Waring identities to pseudoprimes:

$$x^n + y^n = \sum_{0\le k\le [n/2]} (-1)^k \frac{n}{n-k}\binom{n-k}{k}(x+y)^{n-2k}(xy)^k \tag{1.1}$$

and

$$\frac{x^{n+1} - y^{n+1}}{x-y} = \sum_{0\le k\le [n/2]} (-1)^k \binom{n-k}{k}(x+y)^{n-2k}(xy)^k. \tag{1.2}$$

Albert Girard published these identities in Amsterdam in 1629 and Edward Waring published similar material in Cambridge in 1762–1782. These may be derived from the earlier work of Sir Isaac Newton. It is worth noting that $(-1)^k \frac{n}{n-k}\binom{n-k}{k}$ is an integer because

$$\begin{aligned}\frac{n}{n-k}\binom{n-k}{k} &= \binom{n-k}{k} + \binom{n-k-1}{k-1}\\ &= 2\binom{n-k}{k} - \binom{n-k-1}{k}.\end{aligned}$$

The proofs of formulas (1.1) and (1.2) can be seen in Comtet [1, p. 198] and the survey paper by Gould [2]. Recently, Shapiro and one of the authors [3] gave a different proof of (1.2) by using Riordan arrays.

Received May 5, 2019; Accepted October 20, 2019
* Corresponding author
E-mail address: the@iwu.edu (Tianxiao HE)

The following result was shown in authors' paper [4]

Proposition 1.1 *Let $\{a_n\}$ be a sequence of order 2 satisfying linear recurrence relation*

$$a_n = pa_{n-1} + qa_{n-2}, \quad n \geq 2, \tag{1.3}$$

for some non-zero constants p and q and initial conditions a_0 and a_1, and let α and β be two roots of of quadratic equation $x^2 - px - q = 0$. Then

$$a_n = \begin{cases} (\frac{a_1-\beta a_0}{\alpha-\beta})\alpha^n - (\frac{a_1-\alpha a_0}{\alpha-\beta})\beta^n, & \text{if } \alpha \neq \beta; \\ na_1\alpha^{n-1} - (n-1)a_0\alpha^n, & \text{if } \alpha = \beta. \end{cases}$$

If $p = q = 1$, $a_0 = 0$, and $a_1 = 1$, then (1.3) yields the Fibonacci sequence (F_n). The roots of the characteristic polynomial $x^2 - x - 1 = 0$ are

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1-\sqrt{5}}{2}.$$

From Proposition 1.1 we have the expression of F_n as

$$F_{n+1} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} = \frac{1}{\sqrt{5}}\big((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}\big).$$

The Lucas numbers are defined by

$$L_n = \alpha^n + \beta^n = (\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n.$$

A composite number n is called a Fibonacci pseudoprime number (or simply Fpsp.) if it satisfies

$$L_n \equiv 1 \pmod n \tag{1.4}$$

(see, for example, André-Jeannin [5]). Noting $\alpha + \beta = 1$ and $\alpha\beta = -1$, from Girard-Waring identity,

$$L_n = \sum_{0 \leq k \leq [n/2]} \frac{n}{n-k}\binom{n-k}{k} = 1 + n \sum_{1 \leq k \leq [n/2]} \frac{1}{n-k}\binom{n-k}{k}. \tag{1.5}$$

Hence, n is a Lucas pseudoprime if and only if $\sum_{1 \leq k \leq [n/2]} \frac{1}{n-k}\binom{n-k}{k}$ is an integer.

In next section, we discuss the construction of Fermat pseudoprimes by using linear recursive sequences of order 2. The corresponding discussion for the Fibonacci pseudoprimes and Dickson pseudoprimes are given in Sections 3 and 4, respectively.

2. Fermat pseudoprimes and recursive sequences

For an integer $a > 1$, if a composite number n, $\gcd(a, n) = 1$, divides $a^{n-1} - 1$, then n is called a Fermat pseudoprime in base a.

Let the sequence (a_n) be defined by

$$a_n = (\alpha + 1)a_{n-1} - \alpha a_{n-2} \tag{2.1}$$

for $n \geq 2$ with $\alpha \neq 0, 1$ and initial conditions $a_0 = 0$ and $a_1 = 1$. Then Proposition 1.1 implies

$$a_n = \frac{\alpha^n - 1}{\alpha - 1}. \tag{2.2}$$

We may have the following result connecting the linear recurrence relations of order 2 and Fermat pseudoprimes.

Proposition 2.1 *If a composite number n is a Fermat pseudoprime in base α, where $(\alpha-1, n) = 1$. Then (a_n) defined by (2.1), or equivalently, (2.2), is also a Fermat pseudoprime in base α. Particularly, if n is a Fermat pseudoprime in base 2, then $2^n - 1$ is also a Fermat pseudoprime in base 2.*

Proof Let n be a Fermat psp. to the base of α, i.e., $n|(\alpha^{n-1} - 1)$. Hence $\alpha^{n-1} - 1 = kn$ for some positive integer k. Denote $N = (\alpha^n - 1)/(\alpha - 1)$. Then

$$N - 1 = \alpha \frac{\alpha^{n-1} - 1}{\alpha - 1}.$$

We write $N = x - 1$, where the integer

$$x = N + 1 = \frac{\alpha^n + \alpha - 2}{\alpha - 1},$$

which implies $\alpha^n = x(\alpha - 1) - \alpha + 2$. Using this equation, $(\alpha - 1, n) = 1$, $\alpha^{n-1} - 1 = kn$ and the above (1.3), we may write the integer

$$\begin{aligned} \alpha^{N-1} - 1 &= \alpha^{\alpha(\alpha^{n-1}-1)/(\alpha-1)} - 1 = \alpha^{\alpha kn/(\alpha-1)} - 1 \\ &= (x(\alpha - 1) - \alpha + 2)^{\alpha k/(\alpha-1)} - 1 =: f(x), \end{aligned}$$

a function of integer. Since $(x - 1)|f(x)$ due to $f(1) = 0$ (here $x = 1$ implies $N = 0$, or equivalently, $\alpha^n = 1$), we obtain $N|(\alpha^{N-1} - 1)$, i.e., $N = (\alpha^n - 1)/(\alpha - 1)$ is a Fermat psp. to the base α. □

Remark 2.2 Steuerwald [6] (see also in [7]) give a different approach to prove that $f(n) := (\alpha^n - 1)/(\alpha - 1)$ is a Fermat pseudoprime in base α when $(\alpha - 1, n) = 1$. His process and our Proposition 2.1 lead to an infinite increasing sequence of Fermat pseudoprimes in base α, $n < f(n) < f(f(n)) < f(f(f(n))) < \cdots$, which grows as n, α^n, α^{α^n}, $\alpha^{\alpha^{\alpha^n}}$, ... Janjić [8] gives a combinatorial explanation to the function $f(n) = (b^n - 1)/(b - 1)$ and its special case $2^n - 1$. An interesting question might be raised: What is a combinatorial explanation of the composition of $f(n)$ with itself?

Proposition 2.3 *If a composite number n is an odd Fermat pseudoprime in base α, where $\alpha \neq 0, 1$ and $(\alpha + 1, n) = 1$. Then (b_n) defined by $b_{n+2} = (\alpha - 1)b_{n+1} + \alpha b_n$ for $n \geq 2$ with the initial conditions $b_0 = 0$ and $b_1 = 1$, or equivalently,*

$$b_n = \frac{\alpha^n + 1}{\alpha + 1},$$

is also a Fermat pseudoprime in base α.

Proof Proposition 2.3 can be proved using a similar argument in the proof of Proposition 2.1 and is omitted. □

Remark 2.4 Dubner and Granlund [9] test the numbers $b_n = (\alpha^n + 1)/(\alpha + 1)$ for primality or probable primality for $2 \le \alpha \le 200$ and large n. Since b_n can be prime only if n is an old prime, Proposition 2.3 discusses the primality for the case that odd integer n is not a prime but a pseudoprime.

Remark 2.5 Propositions 2.1 and 2.3 can be proved by using another way. We demonstrate the proof by using the former one. This proof is an analogy to the proof of Problem 7 shown on Page 219 of Koblitz [10] and the proof of Example 2 shown on Page 124 of Yu and Shiue [11]. For the sake of readers convenience, we present a modified proof below.

Since n is a pseudoprime with respect to base α, n is an odd composite number satisfying $(\alpha, n) = 1$. In addition, $2 \not| n$. Hence,

$$2 \not| N := \frac{\alpha^n - 1}{\alpha - 1} = \alpha^{n-1} + \alpha^{n-2} + \cdots + 1.$$

If $n = kl$, $k, l > 1$, then $2 \not| k$ and $2 \not| l$. Therefore,

$$N = \frac{\alpha^{kl} - 1}{\alpha - 1} = (\alpha^{l-1} + \alpha^{l-2} + \cdots + 1)(\alpha^{l(k-1)} + \alpha^{l(k-1)-1} + \cdots + 1),$$

which implies N is an odd composite number. Noting

$$N - 1 = \frac{\alpha^n - 1}{\alpha - 1} - 1 = \alpha\frac{\alpha^{n-1} - 1}{\alpha - 1},$$

we have

$$(\alpha - 1)(N - 1) = \alpha(\alpha^{n-1} - 1).$$

Since $n|(\alpha^{n-1} - 1)$ and $(\alpha - 1, n) = 1$, we have $n|(N - 1)$. Hence, we have $N - 1 = nu$ for some integer u. Furthermore, from

$$\alpha^n - 1 = N(\alpha - 1) \equiv 0 \pmod N,$$

we have $\alpha^n \equiv 1 \pmod N$, which implies $\alpha^n = Nv + 1$ for some integer v. Combining $N - 1 = nu$ and $\alpha^n = Nv + 1$, we obtain

$$\alpha^{N-1} - 1 = \alpha^{nu} - 1 = (Nv + 1)^u - 1 = Nw$$

for some integer w, or equivalently,

$$\alpha^{N-1} \equiv 1 \pmod N,$$

i.e., $N = (\alpha^n - 1)/(\alpha - 1)$ is a pseudoprime with respect to base α.

3. Fibonacci pseudoprimes of the m^{th} kind and recursive sequences

If recursive relation (1.3) can be written as

$$a_{n+2} = ma_{n+1} + a_n, \tag{3.1}$$

where m is a natural number, then the generalized Fibonacci numbers $U_n(m)$ and the generalized Lucas numbers $a_n = V_n(m)$ (or simply V_n) are defined [12,13] by

$$U_{n+2} = mU_{n+1} + U_n; U_0 = 0, U_1 = 1 \tag{3.2}$$

and

$$V_{n+2} = mV_{n+1} + V_n; V_0 = 2, V_1 = m, \tag{3.3}$$

respectively. These numbers can also be expressed in [13] by means of the closed forms, called Binet forms,

$$U_n = \frac{\alpha^n - \beta^n}{\Delta}, \quad V_n = U_{n-1} + U_{n+1} = \alpha^n + \beta^n, \tag{3.4}$$

where

$$\Delta = \sqrt{m^2+4}, \quad \alpha = \frac{m+\Delta}{2}, \quad \beta = \frac{m-\Delta}{2}. \tag{3.5}$$

The notations α_m, β_m and Δ_m will be employed whenever the meaning of α, β and Δ can be misunderstood. By the above equations, it can be seen that $\alpha+\beta = m$ and $\alpha\beta = -1$. Moreover, it can be noted that, letting $m = 1$ in (3.2) and (3.3), the classical Fibonacci numbers F_n, and Lucas numbers L_n turn out, respectively. A further interesting expression for V_n is [14]

$$V_n = \sum_{i=0}^{[n/2]} C_{n,i} m^{n-2i}, \tag{3.6}$$

where $C_{n,0} = 2$ and $C_{n,i} = n\binom{n-i}{i}/(n-i)$. We may re-write V_n as

$$V_n = 2m^n + n \sum_{i=1}^{[n/2]} \frac{C_{n,i}}{n} m^{n-2i}, \quad n \geq 1 \tag{3.7}$$

and note that, if n is a prime, then $\frac{C_{n,i}}{n}$ is an integer, thus we may use Fermat's little theorem to establish the following fundamental property of V_n:

$$V_n(m) \equiv m \pmod{n} \tag{3.8}$$

for any natural number m and prime number n. However, the converse is not true, i.e., there exist odd composites that satisfy the above congruence. Thus, we may define Fibonacci Pseudoprimes of the mth kind as follows [15].

Definition 3.1 *Let Lucas numbers, $V_n(m)$, be defined by (3.3), where m is an integer, and let n be an odd composite integer. If n satisfies (3.8), then n is called a Fibonacci Pseudoprime of the mth kind, or m-Fpsp. in short.*

We denote all m-Fpsps. by $s_k(m)$ $(k = 1, 2, \ldots)$ (see [16,17]). The corresponding sets will be denoted by S_m, while the sets of all m-Fpsps. not exceeding a given n will be denoted by $S_{m,n}$. For example, $s_1(1) = 705 = 3 \cdot 5 \cdot 47$, $s_1(2) = 169 = 13^2$, $s_1(3) = 33 = 3 \cdot 11$, etc.

Let ℓ be any odd integer. We consider a recursive relation related to (3.1)

$$w_{n+2} = (\alpha^\ell + \beta^\ell)w_{n+1} - \alpha^\ell\beta^\ell w_n, \quad w_0 = 2, \; w_1 = \alpha^\ell + \beta^\ell, \tag{3.9}$$

where α and β are presented in (3.5). It is easy to see

$$w_n = \alpha^{\ell n} + \beta^{\ell n}. \tag{3.10}$$

We now establish the following result.

Proposition 3.2 *Let m and ℓ be a natural integer and an odd integer, respectively, and let*

$\alpha=\alpha_m$ and $\beta=\beta_m$ be defined as (3.5). If n is an m-Fpsp., then n is also $\alpha^\ell+\beta^\ell$-Fpsp. Furthermore, $\alpha^\ell+\beta^\ell$ can be evaluated by using

$$\alpha^\ell+\beta^\ell=\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}m^{\ell-2i}. \tag{3.11}$$

Proof Let w_n be given by (3.10). By using Girard-Waring identity, we have

$$\begin{aligned}w_n=(\alpha^n)^\ell+(\beta^n)^\ell&=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(\alpha^n\beta^n)^i(\alpha^n+\beta^n)^{\ell-2i}\\&=\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}V_n^{\ell-2i},\end{aligned}$$

where V_n is the nth Lucas number defined by (3.3). If n is an m-Fpsp., then $V_n\equiv m\ (\operatorname{mod} n)$, which implies that

$$w_n\equiv\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}m^{\ell-2i}\ (\operatorname{mod} n).$$

Using Girard-Waring identity yields

$$\alpha^\ell+\beta^\ell=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(\alpha\beta)^i(\alpha+\beta)^{\ell-2i}=\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}m^{\ell-2i},$$

we have proved (3.11) and obtain that

$$w_n\equiv\alpha^\ell+\beta^\ell\ (\operatorname{mod} n)$$

for an m-Fpsp. number n. In other words, (w_n) are Lucas number sequence defined by (3.9). From the definition of Fpsps., we immediately know that n is also an $\alpha^\ell+\beta^\ell$-Fpsp. if it is an m-Fpsp., which completes the proof. □

Remark 3.3 Our $\alpha^\ell+\beta^\ell$ test shown in Proposition 3.2 gives a different approach of Theorem 6 in [17]. Furthermore, our constructive result has an explicit form. By using the following example demonstration, we will see how efficient our constructive approach is in the computation of high order Fpsps.

Example 3.4 For $m=1$, we have

$$\begin{aligned}&\alpha_1^3+\beta_1^3=\sum_{i=0}^{1}\frac{3}{3-i}\binom{3-i}{i}=4,\ \ \alpha_1^5+\beta_1^5=\sum_{i=0}^{2}\frac{5}{5-i}\binom{5-i}{i}=11,\\&\alpha_1^7+\beta_1^7=\sum_{i=0}^{3}\frac{7}{7-i}\binom{7-i}{i}=29,\ \ \alpha_1^9+\beta_1^9=\sum_{i=0}^{4}\frac{9}{9-i}\binom{9-i}{i}=76,\\&\alpha_1^{11}+\beta_1^{11}=\sum_{i=0}^{5}\frac{11}{11-i}\binom{11-i}{i}=199,\\&\alpha_1^{13}+\beta_1^{13}=\sum_{i=0}^{6}\frac{13}{13-i}\binom{13-i}{i}=521,\end{aligned}$$

$$\alpha_1^{15} + \beta_1^{15} = \sum_{i=0}^{7} \frac{15}{15-i}\binom{15-i}{i} = 1364.$$

Thus, if n is a 1-Fpsp., it is also 4, 11, 29, 76, 199, 521, 1364-, etc. Fpsps.

Similarly, if n is a 2-Fpsp., it is also 14, 82, 478, 2786, 16238, 94642, 551614-, etc. Fpsps.

If n is a 3-Fpsp., it is also 36, 393, 4287, 46764, 510117, 5564523, 60699636-, etc. Fpsps.

If n is a 4-Fpsp., it is also 76, 1364, 24476, 439204, 788196, 141422324, 2537720636-, etc. Fpsps.

If n is a 5-Fpsp., it is also 140, 3775, 101785, 2744420, 73997555, 1995189565, 53796120700-, etc. Fpsps.

If n is a 6-Fpsp., it is also 234, 8886, 337434, 12813606, 486579594, 18477210966, 701647437114-, etc. Fpsps.

If n is a 7-Fpsp., it is also 364, 18557, 946043, 48229636, 2458765393, 125348805407, 6390330310364-, etc. Fpsps.

If n is a 8-Fpsp., it is also 536, 35368, 2333752, 153992264, 10161155672, 670482282088, 44241669462136-, etc. Fpsps.

If n is a 9-Fpsp., it is also 756, 62739, 5206581, 432083484, 35857722591, 2975758891569, 246952130277636-, etc. Fpsps.

If n is a 10-Fpsp., it is also 1030, 105050, 10714070, 1092730090, 111447755110, 11366578291130, 1159279537940150-, etc. Fpsps.

If n is a 11-Fpsp., it is also 1364, 167761, 20633239, 2537720636, 312119004989, 38388099893011, 4721424167835364-, etc. Fpsps.

If n is a 12-Fpsp., it is also 1764, 257532, 37597908, 5489037036, 801361809348, 116993335127772, 17080225566845364-, etc. Fpsps.

If n is a 13-Fpsp., it is also 2236, 382343, 65378417, 11179326964, 1911599532427, 326872340718053, 55893258663254636-, etc. Fpsps.

If n is a 14-Fpsp., it is also 2786, 551614, 109216786, 21624372014, 4281516441986, 847718631141214, 167844007449518386-, etc. Fpsps.

If n is a 15-Fpsp., it is also 3420, 776325, 176222355, 40001698260, 9080209282665, 2061167505466695, 467875943531657100-, etc. Fpsps.

By using the above table, one may focus on smaller number Fpsps in the primality test of Fpsps.

4. Dickson pseudoprimes and recursive sequences

We now extend the results about the number recursive sequences shown in Proposition 3.2 to the Dickson pseudoprimes (D-Psps). The sequence of Dickson polynomials of the first kind, $(D_n(x,a))$ with a in a commutative ring or a finite field, is defined by

$$D_{n+2}(x,a) = xD_{n+1}(x,a) - aD_n(x,a), \quad n \geq 0, \tag{4.1}$$

and $D_0(x,a) = 2$ and $D_1(x,a) = x$. Two roots of the characterized polynomial of the recursive relation (4.1) are

$$\alpha = \frac{x+\sqrt{x^2-4a}}{2}, \quad \beta = \frac{x-\sqrt{x^2-4a}}{2}. \tag{4.2}$$

From Proposition 1.1, we may present $D_n(x,a)$ as

$$D_n(x,a) = \alpha^n + \beta^n = \sum_{i=0}^{[n/2]} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}. \tag{4.3}$$

Noting that the coefficients of D_n are integers of $a \in \mathbb{Z}$.

For a survey of many properties of Dickson polynomials including applications to cryptography and number theory [18–20].

From Lidl and Müller [15], we have the following definition of Dickson pseudoprimes.

Definition 4.1 *An odd composite integer n satisfying*

$$D_n(b,a) \equiv b \pmod n \tag{4.4}$$

for $b \in \mathbb{N}$ and $a \in \mathbb{Z}$ is called a Dickson pseudoprime (Dpsp) of the kind (b,a), or Dpsp(b,a) in short.

Many pseudoprimes can be considered as special cases of Dpsps. For instance, if $a = 0$ and $(b,n) = 1$, then $D_n(b,0) = b^n$, and the Dpsps defined in (4.4) is reduced to

$$b^n \equiv b \pmod n,$$

i.e., n is a Fermat pseudoprime to the base b.

If $b = 1$ and $a = -1$, then (4.4) reduces to

$$L_n = D_n(1,-1) \equiv 1 \pmod n,$$

i.e., n is a Lucas psp.

If $b = m$ and $a = -1$, then (4.4) reduces to

$$F_n(m) = D_n(m,-1) \equiv m \pmod n,$$

i.e., n is m-Fpsp.

Proposition 4.2 *Let b and ℓ be a natural integer and an odd integer, respectively, and let $\alpha = \alpha(x)$ and $\beta = \beta(x)$ be defined as (4.2). If n is an Dpsp(b,a), where $a^n \equiv a \pmod n$, then*

$$D_{n\ell}(b,a) \equiv D_\ell(b,a) \pmod n, \tag{4.5}$$

where $D_n(x,a)$ is defined by (4.3). Particularly, for $a = 1$, we have

$$D_{n\ell}(b,1) \equiv D_\ell(b,1) \pmod n. \tag{4.6}$$

And when $a = -1$ and n is odd, we have

$$D_{n\ell}(b,-1) \equiv D_\ell(b,-1) \pmod n. \tag{4.7}$$

Furthermore, $D_\ell(b,a)=\alpha^\ell+\beta^\ell$ can be evaluated by using

$$D_\ell(b,-1)=\alpha(b)^\ell+\beta(b)^\ell=\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}b^{\ell-2i}. \tag{4.8}$$

Proof Let α and β be two roots of the characterized polynomial of the recursive relation (4.1), which are shown in (4.2), and let ℓ be any odd integer. By using Girard-Waring identity, we have

$$(\alpha^n)^\ell+(\beta^n)^\ell=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(\alpha^n\beta^n)^i(\alpha^n+\beta^n)^{\ell-2i},$$

which implies

$$D_{n\ell}(x,a)=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(a^n)^i(D_n(x,a))^{\ell-2i}. \tag{4.9}$$

Similarly,

$$D_\ell(x,a)=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}a^ix^{\ell-2i}. \tag{4.10}$$

From (4.9) and (4.10), for Fpsp. number n with respect to base b we have

$$\begin{aligned}D_{n\ell}(b,a)&=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(a^n)^i(D_n(b,a))^{\ell-2i}\\&\equiv\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}(a^n)^ib^{\ell-2i}\ (\mathrm{mod}\, n)\end{aligned} \tag{4.11}$$

and

$$D_\ell(b,a)=\sum_{i=0}^{[l/2]}(-1)^i\frac{\ell}{\ell-i}\binom{\ell-i}{i}a^ib^{\ell-2i}, \tag{4.12}$$

respectively. If $a^n\equiv a\ (\mathrm{mod}\, n)$, then

$$D_{n\ell}(b,a)\equiv D_\ell(b,a)\ (\mathrm{mod}\, n),$$

where $D_\ell(b,a)$ satisfies (4.5). When $a=1$, then $a^n\equiv a\ (\mathrm{mod}\, n)$, (4.6) holds. When $a=-1$, noticing n is odd, we know (4.11) and (4.12) are equivalent. Namely,

$$D_{n\ell}(b,-1)=\sum_{i=0}^{[l/2]}\frac{\ell}{\ell-i}\binom{\ell-i}{i}b^{\ell-2i}\equiv D_\ell(b,-1)\ (\mathrm{mod}\, n), \tag{4.13}$$

which completes the proof. □

Remark 4.3 The case of (4.11) is shown in Lidl and Müller [15].

In [15], Theorem 1.5 gives the following result: If an odd composite integer n passes the (b,r)-test for being an (b,r)-Dpsp and the $(r,0)$-test for being a base r pseudoprime, then it passes also the $(D_{2k+1}(b,r);r^{2k+1})$-tests, for $k=1,2,\ldots$. We will present here an alternative proof of this result by using our linear recurrence method shown above. More precisely, for any $b\in\mathbb{N}$ and $r\in\mathbb{Z}$, we define

$$\alpha=\frac{b+\sqrt{b^2-4r}}{2},\quad \beta=\frac{b-\sqrt{b^2-4r}}{2}, \tag{4.14}$$

and the recursive sequence (a_n) generated by

$$a_{n+2} = ba_{n+1} - a_n, \tag{4.15}$$

$a_0 = 2$ and $a_1 = b$. Thus, we have $\alpha + \beta = b$ and $\alpha\beta = r$, and $a_n = D_n(b, r)$. From Proposition 1.1, we have

$$a_n = D_n(b, r) = \alpha^n + \beta^n.$$

Now, we consider the sequence

$$w_{n+2} = (\alpha^\ell + \beta^\ell)w_{n+1} - r^\ell w_n, \tag{4.16}$$

$w_0 = 2$, and $w_1 = \alpha^\ell + \beta^\ell$, where α and β are given in (4.14) and $r = \alpha\beta$, and $\ell \in \mathbb{N}$. From (4.3) for $r = \alpha\beta$ we have

$$\begin{aligned} w_n &= D_n(\alpha^\ell + \beta^\ell, r^\ell) = (\alpha^\ell)^n + (\beta^\ell)^n = (\alpha^n)^\ell + (\beta^n)^\ell \\ &= \sum_{i=0}^{[\ell/2]} (-1)^i \frac{\ell}{\ell - i} \binom{\ell - i}{i} (\alpha^n\beta^n)^i (\alpha^n + \beta^n)^{\ell-2i} \\ &= \sum_{i=0}^{[\ell/2]} (-1)^i \frac{\ell}{\ell - i} \binom{\ell - i}{i} (r^n)^i (D_n(b, r))^{\ell-2i}. \end{aligned} \tag{4.17}$$

From the assumption of that n is a (b, r)-Dpsp we have

$$D_n(b, r) \equiv b \,(\mathrm{mod}\, n).$$

Hence, the last equation of (4.17) implies

$$w_n \equiv \sum_{i=0}^{[\ell/2]} (-1)^i \frac{\ell}{\ell - i} \binom{\ell - i}{i} (r^n)^i b^{\ell-2i} \ (\mathrm{mod}\, n), \tag{4.18}$$

where $b = \alpha + \beta$. Since n passes the $(r, 0)$-test for being a base r pseudoprime, there exists

$$r^n \equiv r \,(\mathrm{mod}\, n),$$

which devotes to the following change of (4.18):

$$w_n \equiv \sum_{i=0}^{[\ell/2]} (-1)^i \frac{\ell}{\ell - i} \binom{\ell - i}{i} r^i b^{\ell-2i} \ (\mathrm{mod}\, n). \tag{4.19}$$

On the other hand, from (4.3) we have

$$\alpha^\ell + \beta^\ell = \sum_{i=0}^{[\ell/2]} (-1)^i \frac{\ell}{\ell - i} \binom{\ell - i}{i} r^i b^{\ell-2i}, \ b = \alpha + \beta, \text{ and } r = \alpha\beta. \tag{4.20}$$

Combining (4.19) and (4.20) yields

$$\begin{aligned} w_n = D_n(\alpha^\ell + \beta^\ell, r^\ell) &= D_n(D_\ell(b, r), r^\ell) \equiv \alpha^\ell + \beta^\ell \ (\mathrm{mod}\, n) \\ &\equiv D_\ell(b, r) \ (\mathrm{mod}\, n) \end{aligned}$$

for all $\ell \in \mathbb{N}$. Hence, for odd integer $\ell = 2k + 1$ w_n passes the $(D_{2k+1}(b, r), r^{2k+1})$-test for $k = 1, 2, \ldots$. (Actually, w_n passes $(D_\ell(b, r), r^\ell)$-test for all $\ell \in \mathbb{N}$.)

The recursive sequence defined by (4.16) can be written as

$$w_n = D_n(\alpha^\ell + \beta^\ell, r^\ell) = D_n(D_\ell(b, r), r^\ell),$$

where $b = \alpha + \beta$ and $r = \alpha\beta$. Since

$$w_n = (\alpha^\ell)^n + (\beta^\ell)^n = (\alpha^n)^\ell + (\beta^n)^\ell,$$

the sequence (w_n) can be considered to be defined by

$$w_{\ell+2} = (\alpha^n + \beta^n)w_{\ell+1} - r^n w_\ell,$$

$w_0 = 2$, $w_1 = \alpha^n + \beta^n$, where $r = \alpha\beta$. Similarly, we may write

$$w_\ell = D_\ell(\alpha^n + \beta^n, r^n) = D_\ell(D_n(b, r), r^n),$$

where $b = \alpha + \beta$ and $r = \alpha\beta$. Thus we have the following result for the Dickson polynomial sequence.

Proposition 4.4 *Let $(D_n(x, a))$ be the Dickson polynomial sequence defined by (4.1). Then it has a kind of commutative law with respect to the composition in the sense of*

$$D_n(D_\ell(x, a), a^\ell) = D_\ell(D_n(x, a), a^n),$$

where $n, \ell \in \mathbb{N}$.

By using Proposition 4.4, we may construct an endless chain of Dickson pseudoprime sequences.

References

[1] L. COMTET. *Advanced Combinatorics*. Reidel, Dordrecht, 1974.

[2] H. W. GOULD. *The Girard-Waring power sum formulas for symmetric functions and Fibonacci sequences*. Fibonacci Quart., 1999, **37**(2): 135–140.

[3] Tianxiao HE, L. W. SHAPIRO. *Row sums and alternating sums of Riordan arrays*. Linear Algebra Appl., 2016, **507**: 77–95.

[4] Tianxiao HE, P. J.-S. SHIUE. *On sequences of numbers and polynomials defined by linear recurrence relations of order 2*. Int. J. Math. Math. Sci., 2009, Art. ID 709386, 21 pp.

[5] R. ANDRÉ-JEANNIN. *On the existence of even Fibonacci pseudoprimes with parameters P and Q*. Fib. Quart., 1996, **34**: 75–78.

[6] R. STEUERWALD. *Über die Kongruenz $a^{n-1} \equiv 1 \pmod n$*. Kl. Bayer. Akad. Wiss. München, 1948.

[7] P. RIBENBOIM. *The Little Book of Bigger Primes, Second Edition*. Springer-Verlag, New York, 2004.

[8] M. JANJIĆ. *Words and linear recurrences*. J. Integer Seq., 2017, **20**(9): Art. 18. 1. 4, 16 pp.

[9] H. DUBNER, T. GRANLUND. *Primes of the form $(b^n + 1)/(b + 1)$*. J. Integer Seq., 2000, **3**(2): Article 00.2.7, 8 pp.

[10] N. KOBLITZ. *A Course in Number Theory and Cryptography*. Second edition. Graduate Texts in Mathematics, 114, Springer-Verlag, New York, 1994.

[11] X. Y. YU, P. J.-S. SHIUE. *Introduction to Cryptography and Number Theory*. Shandong Scientific Press, 1993. (in Chinese)

[12] M. BICKNELL. *A primer for the Fibonacci numbers (VII)*. Fibonacci Quart., 1970, **8**(4): 407–420.

[13] M. BICKNELL. *A primer on the Pell sequence and related sequences*. Fibonacci Quart., 1975, **13**(4): 345–349.

[14] O. BRUGIA, P. FILIPPONI. *Waring formulae and certain combinational identities*. Fondaz. Ugo Bordoni Techn. Rep. 3B5986, Oct. 1986.

[15] R. LIDL, W. B. MÜLLER. *Generalizations of the Fibonacci pseudoprimes test.* Discrete Math., 1991, **92**(1-3): 211–220.

[16] A. DI PORTO, P. FILIPPONI. *A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers.* Springer, Berlin, 1988.

[17] A. DI PORTO, P. FILIPPONI. *More on the Fibonacci pseudoprimes.* Fibonacci Quart., 1989, **27**(3): 232–242.

[18] R. LIDL, G. L. MULLEN, G. TURNWALD. *Dickson Polynomials.* John Wiley & Sons, Inc., New York, 1993.

[19] L. C. HSU, G. L. MULLEN, P. J.-S. SHIUE. *Dickson-Stirling numbers.* Proc. Edinburgh Math. Soc., 1997, **40**(3): 409–423.

[20] L. C. HSU, P. J.-S. SHIUE. *A note on Dickson-Stirling numbers.* J. Combin. Math. Combin. Comput., 2000, **34**: 77–80.