ON PSEUDOPRIMES RELATED TO GENERALIZED LUCAS SEQUENCES

L. A. G. Dresel
3 Westcote Road, Reading, Berks, RG30 2DL, England

(*Submitted April 1995*)

1. INTRODUCTION

In this paper we consider the general sequences U_n and V_n satisfying the recurrences

$$U_{n+2} = mU_{n+1} + U_n, \quad V_{n+2} = mV_{n+1} + V_n, \tag{1.1}$$

where m is a given positive integer, and $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = m$.

We shall occasionally refer to these sequences as $U(m)$ and $V(m)$ to emphasize their dependence on the parameter m. They can be represented by the *Binet forms*

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \quad V_n = \alpha^n + \beta^n, \tag{1.2}$$

where $\alpha + \beta = m$ and $\alpha\beta = -1$, and we define $\Delta = \delta^2 = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = m^2 + 4$. When $m = 1$, these sequences reduce to F_n and L_n, with $\Delta = 5$.

Using (1.2), we can derive the identities (1.3) through (1.7), which correspond to well-known formulas that are proved, for instance, in [11]:

$$U_{2n} = U_n V_n, \tag{1.3}$$

$$V_{2n} = V_n^2 - 2(-1)^n, \tag{1.4}$$

$$\Delta U_n^2 = V_n^2 - 4(-1)^n, \tag{1.5}$$

$$2U_{n+s} = U_n V_s + V_n U_s, \tag{1.6}$$

$$2V_{n+s} = V_n V_s + \Delta U_n U_s. \tag{1.7}$$

When n is a prime p, we have

$$V_p = \alpha^p + \beta^p \equiv (\alpha + \beta)^p = m^p \pmod{p},$$

and using Fermat's "little theorem," this gives the well-known result

$$V_p \equiv m \pmod{p}, \text{ when } p \text{ is prime.} \tag{1.8}$$

Any composite numbers n satisfying the corresponding equation

$$V_n \equiv m \pmod{n} \tag{1.9}$$

are called pseudoprimes. Di Porto and Filipponi [7] have called such numbers *Fibonacci Pseudoprimes* of the m^{th} kind (m-F.Psps), whereas Bruckman [2] has called them *Lucas Pseudoprimes*. As a compromise, we shall call them V(m)-pseudoprimes or V(m)-psp. In the case of $m = 1$, when V_n becomes L_n, it has been proved that all V(1)-psp's are *odd*: see {14], [5], and [3]. In the more general case, since the interest in V(m)-psp's relates to tests for primality, only *odd* V(m)-psp's will be considered, as in [7], and we shall restrict the definition of pseudoprimes to *odd* composite n satisfying (1.9).

Suppose now that n satisfies (1.9). Then, for any prime factor p of n,

$$V_n \equiv m \pmod{p}, \tag{1.10}$$

or, if the factorization of n contains a prime power p^e, with $e \geq 1$,

$$V_n \equiv m \pmod{p^e}. \tag{1.11}$$

Now it is well-known that the sequence V modulo a prime power p^e is periodic. We shall denote the corresponding period of repetition by $R(p^e)$ or R, defined as the smallest positive integer R for which we have $V_R \equiv 2$ *and* $V_{R+1} \equiv m \pmod{p^e}$. Since $V_{2R} \equiv V_R \equiv V_0 = 2 \pmod{p^e}$, (1.4) shows that, if p is odd, the period R must be even. The sequence U modulo p^e is also periodic, and is known to have the same period R as the corresponding V-sequence, except when $\Delta \equiv 0 \pmod{p}$.

We also note that the entry point Z of p^e in the sequence U is defined as the smallest positive Z such that $U_Z \equiv 0 \pmod{p^e}$. It is well known that p^e divides U_n if and only if Z divides n. Also U_r divides U_n if and only if r divides n. Vinson [12] established the relationship between Z and the period R of the sequence U for the case $m = 1$, and we can easily prove that, for odd p, the same holds for any m, namely:

$$\text{if } Z \text{ is odd, then } R = 4Z; \tag{1.12}$$

$$\text{if } Z \equiv 2 \pmod{4}, \text{ then } R = Z; \tag{1.13}$$

$$\text{if } Z \equiv 0 \pmod{4}, \text{ then } R = 2Z. \tag{1.14}$$

In Sections 2 and 4, we shall derive relationships between n and R giving necessary and sufficient conditions for a number n to be a pseudoprime. In Section 3, we shall find conditions for the occurrence of square factors in such pseudoprimes, and present some numerical examples. Finally, in Section 5, we shall prove certain theorems concerning special forms of V(m)-pseudoprimes, Theorems 7-10 being generalizations of results proved by Di Porto and Filipponi for the case $m = 1$ in [7].

2. PSEUDOPRIMES AND THE PERIODICITY OF THE LUCAS SEQUENCE

Using (1.2), we can define U and V with negative subscripts, giving

$$U_{-n} = -(-1)^n U_n \quad \text{and} \quad V_{-n} = (-1)^n V_n. \tag{2.1}$$

Putting $s = 1$ and then $s = -1$, equation (1.7) gives the identities

$$2V_{n+1} = \Delta U_n + mV_n \quad \text{and} \quad 2V_{n-1} = \Delta U_n - mV_n, \tag{2.2}$$

and multiplying the two parts of (2.2) and using (1.5) gives the well-known identity

$$V_{n+1}V_{n-1} = V_n^2 - \Delta(-1)^n. \tag{2.3}$$

We shall now derive an important identity. Using (2.3) when n is *odd*, we have

$$\begin{aligned}(V_{n+1}+2)(V_{n-1}-2) &= V_{n+1}V_{n-1} - 2(V_{n+1} - V_{n-1}) - 4 \\ &= V_n^2 + \Delta - 2mV_n - 4,\end{aligned}$$

and since $\Delta = m^2 + 4$ this reduces to

$$(V_{n+1}+2)(V_{n-1}-2)=(V_n-m)^2 \quad (n \text{ odd}); \tag{2.4}$$

we shall call this the *key identity*, as it provides the basis for the proofs of several theorems in this paper. Our first theorem examines at what points of the periodic cycle we might find an *odd* n satisfying $V_n \equiv m \pmod{p^e}$, and is a generalization of the result proved for the case $e=1$ by Di Porto in [6].

Theorem 1: If n is odd and $V_n \equiv m \pmod{p^e}$, where $p>2$ is prime and $e \geq 1$, and if $R=R(p^e)$ is the period of the sequence $V(m)$ modulo p^e, then we have

$$\textit{either } n \equiv 1 \pmod{R} \quad \textit{or} \quad n \equiv \tfrac{1}{2}R-1 \pmod{R}; \tag{2.5}$$

since n is odd, the second alternative can occur only when $\frac{1}{2}R$ is even.

Proof: Putting $V_n \equiv m \pmod{p^e}$ in the key identity (2.4), we find that the right side of the identity is divisible by $(p^e)^2$, and it follows that at least one of the two factors on the left must be divisible by p^e. Thus, we have

$$\textit{either } V_{n-1} \equiv 2 \pmod{p^e} \quad \textit{or} \quad V_{n+1} \equiv -2 \pmod{p^e}. \tag{2.6}$$

Taking the first alternative, we have $V_{n-1} \equiv 2$ and $V_n \equiv m \pmod{p^e}$, showing that $n-1$ is a multiple of the period R in this case. Taking the second alternative, we have $V_n \equiv m$, together with $V_{n+1} \equiv -2$, so that the recurrence relation (1.1) gives $V_{n+2} \equiv -m \pmod{p^e}$. It follows from (1.1) that

$$V_{n+1+t} \equiv -V_t, \quad \text{for } t=0,1,2,\ldots,$$

showing that in this case $n+1$ is an odd multiple of half the period. Therefore, one or the other of the alternatives in (2.5) is true. Q.E.D.

Theorem 2: Let n be an odd V(m)-psp divisible by a prime power p^e, and let R be the period of the sequence $V(m)$ modulo p^e, $e \geq 1$. Then, for each such R, we have

$$\textit{either } n \equiv 1 \pmod{R} \quad \textit{or} \quad n = \tfrac{1}{2}R-1 \pmod{R}. \tag{2.7}$$

Note: If p is an odd prime and if R is the period of $V(m)$ modulo p, then using (1.8) and Theorem 1 with $n=p$ and $e=1$ gives

$$\textit{either } p \equiv 1 \pmod{R} \quad \textit{or} \quad p = \tfrac{1}{2}R-1 \pmod{R}; \tag{2.8}$$

this is equivalent to the well-known result that R divides either $p-1$ or $2(p+1)$ when $(\Delta, p)=1$; our derivation shows that (2.8) remains true also when $\Delta \equiv 0 \pmod{p}$.

3. ON THE OCCURRENCE OF SQUARE FACTORS IN A V(m)-PSEUDOPRIME

Theorem 3: If n is an odd V(m)-psp divisible by a prime power p^e, where $e>1$, then the periods of the sequence $V(m)$ modulo p^e and modulo p are the same.

Proof: Let $R(p^e)$ be the period modulo p^e, and $R(p)$ the period modulo p. Then $R(p^e)=p^f R(p)$, with $0 \leq f < e$, as was proved by E. Lucas [11], and for $m=1$ by Wall [13]. But

Theorem 2 shows that $R(p^e)$ and n have no common factor; therefore, p does not divide $R(p^e)$. Hence, $f=0$ and $R(p^e)=R(p)$.

Corollary: If a V(m)-psp is divisible by p^e, where $e>1$, and if p does not divide Δ, then p^e and p have the same entry point Z in the sequence $U(m)$.

Proof: This follows from Theorem 3 by Vinson's rules, as stated in (1.12)-(1.14). Note that when p^e divides Δ the period of $V(m)$ modulo p^e is 4, whereas that of $U(m)$ is $4p^e$.

Note: Bruckman [1] has proved a result equivalent to Theorem 3 for the case $m=1$. Furthermore, it has also been shown that, for $m=1$, $R(p^2)=pR(p)$ for all $p<10^4$ by Wall [13], for all $p<10^6$ by Dresel [10], and for all $p<10^9$ by H. C. Williams [15]. It then follows from Theorem 3 that any V(1)-psp less than 10^{18} must be square-free.

The situation for $m>1$ is rather different. Thus, for $m=2$, we obtain the *Pell* sequence with $U_7=P_7=169=13^2$, while P_{30} is divisible by 31^2. Correspondingly, we find that among the first seven V(2)-psp's there are three containing square factors, namely, $13^2, 31^2$, and $13^2\times 29$.

Let us call a prime p *divalent* in $U(m)$ if the entry points of p and p^2 in the $U(m)$-sequence are the same. For most of the values of $m\le 25$, we can find examples of divalent primes with $p<300$, the exceptional cases being $m=1,8,10,11,16$, and 17. In the case of $m=24$, we have five such primes, namely, 7, 11, 17, 37, and 41, and among the first 21 V(24)-psp's there are ten containing square factors, namely, $7^2, 11^2, 17^2, 7^3, 7^2\times 17, 3\times 17^2, 7^2\times 23, 11^3, 37^2$, and 41^2.

4. SUFFICIENT CONDITIONS FOR A V(m)-PSEUDOPRIME

We shall use the key identity (2.4) to prove the following lemma.

Lemma 1: If R is the period of the sequence V modulo p^e, where $p>2$ is prime and $e\ge 1$, and if p^c is the highest power of p that divides Δ, where $0\le c\le e$, then

(i) $V_R\equiv 2 \pmod{p^{2e-c}}$, and

(ii) conversely, if $V_{2t}\equiv 2 \pmod{p^{2e-c}}$, then R divides $2t$.

(iii) If, further, $\frac{1}{2}R$ is even, then we also have $V_{\frac{1}{2}R}\equiv -2 \pmod{p^{2e-c}}$ and $V_{\frac{1}{2}R-1}\equiv m \pmod{p^e}$.

Proof: By the definition of R, we have $V_R\equiv 2$ and $V_{R+1}\equiv m \pmod{p^e}$. Since R is even, putting $n=R+1$ in the key identity (2.4), we obtain

$$(V_R-2)(V_{R+2}+2)\equiv 0 \pmod{p^{2e}} \tag{4.1}$$

while

$$(V_{R+2}+2)-(V_R-2)=mV_{R+1}+4\equiv m^2+4=\Delta \pmod{p^e}. \tag{4.2}$$

(i) Since p^e divides (V_R-2) and p^c divides Δ, (4.2) shows that p^c is the highest power of p dividing $(V_{R+2}+2)$; hence, (4.1) gives $V_R\equiv 2 \pmod{p^{2e-c}}$.

(ii) Given $V_{2t}\equiv 2 \pmod{p^{2e-c}}$ and putting $n=2t$ in (1.5), we obtain $\Delta(U_{2t})^2\equiv 0 \pmod{p^{2e-c}}$ and, therefore, $(\Delta U_{2t})^2\equiv 0 \pmod{p^{2e}}$, giving $\Delta U_{2t}\equiv 0 \pmod{p^e}$. Finally, substituting in (2.2), we obtain $2V_{2t+1}\equiv 2m=2V_1 \pmod{p^e}$, so that $2t$ is a multiple of the period R modulo p^e.

(iii) If $\frac{1}{2}R$ is even, then (1.4) together with (i) above gives

$$(V_{\frac{1}{2}R})^2 = V_R + 2 \equiv 4 \pmod{p^{2e-c}};$$

hence, $V_{\frac{1}{2}R} \equiv -2 \pmod{p^{2e-c}}$, since $V_{\frac{1}{2}R} \equiv 2$ would contradict (ii). Then (1.5) gives $\Delta(U_{\frac{1}{2}R})^2 \equiv 0$ $(\bmod\, p^{2e-c})$ and, therefore, $(\Delta U_{\frac{1}{2}R})^2 \equiv 0 \pmod{p^{2e}}$, giving $\Delta U_{\frac{1}{2}R} \equiv 0 \pmod{p^e}$; finally, (2.2) gives $V_{\frac{1}{2}R-1} \equiv m \pmod{p^e}$.

Note: If $c = e$, so that p^e divides Δ, we have $V_2 = m^2 + 2 \equiv -2 \pmod{p^e}$ and $V_3 \equiv -m$, giving $R = 4$, and we have both $V_R \equiv 2$ and $V_{R+2} \equiv -2 \pmod{p^e}$.

We shall now prove the converse of Theorem 2, namely,

Theorem 4: Let n be odd and composite, and let R be the period of the sequence $V(m)$ modulo a prime power p^e, $e \geq 1$. If, for each p^e dividing n, we have

$$\textit{either } n \equiv 1 \pmod{R} \quad \textit{or} \quad n \equiv \tfrac{1}{2}R - 1 \pmod{R}, \tag{4.3}$$

then n is a V(m)-psp.

Proof: If the first alternative in (4.3) is true, then by definition of R we have $V_n = V_{kR+1} \equiv V_1 \equiv m \pmod{p^e}$; if the second alternative in (4.3) applies, then by Lemma 1(iii) we again have $V_n \equiv V_{\frac{1}{2}R-1} \equiv m \pmod{p^e}$. Thus, (1.11) is satisfied for each prime power p^e which divides n. Hence, (1.9) is true, showing that n is a V(m)-psp.

Note: Theorems 2 and 4 together give necessary and sufficient conditions for n to be a V(m)-psp and provide the basis for the proofs given in the next section. A different approach by Di Porto, Filipponi, and Montolivo [9] gives a sufficient (but not a necessary) condition expressed in terms of the prime factors of n.

We shall now prove a converse of Theorem 3, namely,

Theorem 5: If there is an odd prime p for which the sequence $V(m)$ has the same period R modulo p and p^e, $e > 1$, then p^e is a V(m)-psp.

Proof: By (2.8), we have *either* $p \equiv 1 \pmod{R}$ *or* $p \equiv \frac{1}{2}R - 1 \pmod{R}$. If the first alternative applies, we have $p^e \equiv 1 \pmod{R}$, and Theorem 4 shows that p^e is a V(m)-psp. If the second alternative applies, we have $\frac{1}{2}R$ even (as p is odd) and $p^e \equiv (\frac{1}{2}R - 1)^e \pmod{R}$, so that $p^e \equiv 1$ $(\bmod\, R)$ if e is even, and $p^e \equiv (\frac{1}{2}R - 1) \pmod{R}$ if e is odd. Since $R = R(p^e)$, Theorem 4 completes the proof.

Examples: For $m = 2$, we have 13^2 and 31^2 as V(2)-psp's.

Corollary: If $e > 1$ and p^e divides Δ, then p^e is a V(m)-psp.

Proof: If p^e divides Δ, $V(m)$ has the period 4 both modulo p and modulo p^e, so that the conditions of Theorem 5 are satisfied.

Examples: For $m = 11$, we have $\Delta = m^2 + 4 = 125 = 5^3$, and both 25 and 125 are V(11)-psp's. Similarly, for $m = 14$, $\Delta = 200$, so that 25 is a V(14)-psp.

Note: Theorem 5 may be regarded as a special case of Theorem 6 below.

5. SOME SPECIAL FORMS OF V(m)-PSEUDOPRIMES

Theorem 6: If n is odd, composite, and such that all its prime or prime power factors have the same period R in the sequence $V(m)$, then n is a V(m)-psp.

Proof: If $\frac{1}{2}R$ is odd, then by (2.8) n is the product of primes p_j satisfying $p_j = Rk_j + 1$. It is easily seen that the product of two or more such primes satisfies $n = kR + 1$, and the result then follows from Theorem 4. In the same way, if $\frac{1}{2}R$ is even, n is the product of primes of the form $p_j = Rk_j + 1$ *or* of the form $q_i = \frac{1}{2}Rh_i - 1$, where h_i is odd. The product of such primes is again of one or other of these forms, depending on whether the number of primes of the form q_i is even or odd. The result then follows from Theorem 4 as before.

Example: The sequence $V(2)$ has the same period 40 modulo the primes 19 and 59; therefore, their product 1121 is a V(2)-psp.

Corollary: If n is an odd composite number dividing Δ, then n is a V(m)-psp.

Proof: The period of $V(m)$ modulo any prime or p^e that divides Δ is 4. Q.E.D.

We shall use Theorems 4 and 6 to show that certain expressions are V(m)-psp, thus generalizing some results proved for the special case $m = 1$ by Di Porto and Filipponi in [7], and by Bruckman in [2], [4]. First, we shall state some basic facts.

Lemma 2: ***(i)*** U_n and V_n have no odd common factors.
(ii) If p is an odd prime dividing Δ, then $(p, V_n) = 1$ for all n.

These well-known results are easily proved by *reductio ad absurdum* from (2.2).

Lemma 3: For all m, we have

$$U_{2s} \equiv sm \pmod{m^3} \quad \text{and} \quad U_{2s+1} \equiv 1 \pmod{m^2}, \tag{5.1}$$

$$V_{2s} \equiv 2 \pmod{m^2} \quad \text{and} \quad V_{2s+1} \equiv (2s+1)m \pmod{m^3}. \tag{5.2}$$

This is easily proved by induction on s.

Lemma 4: ***(i)*** When m is odd, then U_n and V_n are odd if and only if 3 does not divide n.
(ii) When m is even, then U_n and V_n / m are odd if n is odd.

Theorem 7: If $q > 3$ (*or*, when m is even, $q \geq 3$) is prime and $(\Delta, q) = 1$, and if U_q is composite, then U_q is a V(m)-psp.

Proof: Since q is prime, all the factors of U_q have q as their entry point in the sequence $U(m)$ and, by (1.12), their period is $4q$. Since $(\Delta, q) = 1$, they have the same period in the $V(m)$-sequence. Also, by Lemma 4, U_q is odd. Hence, Theorem 6 applies.

Examples: For $m = 1$, see [8]; for $m = 2$, the following Pell numbers are V(2)-psp's: $U_7 = 169 = 13^2$, $U_{17} = 137 \times 8297$, $U_{19} = 37 \times 179057$, and $U_{23} = 229 \times 982789$.

Theorem 8: ***(i)*** If $T = 2^k, k \geq 1$, and m is odd, then V_T, if composite, is a V(m)-psp.
(ii) If m is even, and $T = 2^k, k \geq 1$, then $V_T / 2$, if composite, is a V(m)-psp.

Proof: If m is odd, then V_T is odd since $T = 2^k$ is not divisible by 3. But if m is even, (5.2) gives $V_T \equiv 2 \pmod{m^2}$, so that $V_T / 2$ is odd. Next, consider any odd prime p that divides V_T; then, by Lemma 2, neither U_T nor Δ are divisible by p. Also, $U_{2T} = U_T V_T$; therefore, any odd p or p^e that divides V_T has the entry point $2T$ in the U-sequence and, therefore, the period $4T$ by (1.14). Since $(p, \Delta) = 1$, the period is the same for the V-sequence, and the results then follow from Theorem 6.

Examples: For $m = 11, V_2 = 123 = 3 \times 41$ and $V_4 = 15127 = 7 \times 2161$ are V(11)-psp. For $m = 24$, $V_2 / 2 = 289 = 17^2$ and $V_4 / 2 = 167041 = 7^3 \times 487$ are V(24)-psp.

Theorem 9: If $q > 3$ (*or*, when m is even, $q \geq 3$) is prime and $(m, q) = 1$, and if V_q / m is composite, then V_q / m is a V(m)-psp.

Proof: We have $U_{2q} = U_q V_q$, and V_q and U_q have no odd common factor. Hence, any odd prime p which divides V_q has entry point 2 or $2q$ in the U-sequence. But $U_2 = m$, and (5.2) gives $V_q / m \equiv q \pmod{m^2}$, so that V_q / m is odd and prime to m. Therefore, any p or p^e dividing V_q / m has entry point $2q$. By (1.13), the corresponding period is $R = 2q$, and this is also the period in the $V(m)$-sequence, since $(p, \Delta) = 1$ by Lemma 2(ii). Hence, Theorem 6 applies.

Note: By (2.8), any factor of V_q / m would be of the form $2qk + 1$.

Example: When $m = 2$, $V_{11} / 2 = 8119 = 23 \times 353$ is a V(2)-psp.

Theorem 10: If n is a V(m)-psp which is odd (and not divisible by 3 when m is odd), and if $(n, m) = 1$, then the same is true for $N = V_n / m$.

Proof: We have $U_{2n} = U_n V_n$; therefore, any odd prime p or p^e which divides V_n also divides U_{2n} but not U_n, and by (1.13) the corresponding period R divides $2n$. Since n is V(m)-psp, $V_n \equiv m \pmod{n}$, and since $(n, m) = 1$, we have $V_n / m \equiv 1 \pmod{n}$. But V_n / m is odd by Lemma 4, hence $V_n / m \equiv 1 \pmod{2n}$. Since R divides $2n$, we have $V_n / m \equiv 1 \pmod{R}$; furthermore, since n is the product of odd numbers, say $n = pq$, V_n is divisible by V_p so that V_n / m is divisible by V_p / m and, therefore, V_n / m is composite. Hence, Theorem 4 shows that $N = V_n / m$ is a V(m)-psp. It remains to show that N satisfies $(N, m) = 1$ and that $(N, 3) = 1$ if $(n, 3) = 1$.

Since n is odd, (5.2) shows that $V_n / m \equiv n \pmod{m^2}$, and since $(n, m) = 1$, it follows that V_n / m also is prime to m. Furthermore, the entry point of 3 in $U(m)$ is 2 if 3 divides m and 4 otherwise. In the first case, since $V_n / m \equiv n \pmod{m^2}$, 3 does not divide V_n / m if it does not divide n. In the second case, since $2n$ is not divisible by 4, it follows that $U_n V_n$ is not divisible by 3; therefore, $(N, 3) = 1$. Q.E.D.

Corollary: Given one V(m)-psp satisfying the conditions of this theorem, we can find infinitely may such V(m)-psp.

Example: Since 169 is a V(2)-psp, there are infinitely many V(2)-psp's.

REFERENCES

1. P. S. Bruckman. "On Square-Free Lucas Pseudoprimes." *Pi Mu Epsilon Journal* **9.9** (1993): 590-95.
2. P. S. Bruckman. "On the Infinitude of Lucas Pseudoprimes." *The Fibonacci Quarterly* **32.2** (1994):153-54.
3. P. S. Bruckman. "Lucas Pseudoprimes Are Odd." *The Fibonacci Quarterly* **32.2** (1994): 155-57.
4. P. S. Bruckman. "On a Conjecture of Di Porto and Filipponi." *The Fibonacci Quarterly* **32.2** (1994):158-59.
5. A. Di Porto. "Nonexistence of Even Fibonacci Pseudoprimes of the 1st Kind." *The Fibonacci Quarterly* **31.2** (1993):173-77.
6. A. Di Porto. "A Note on the Dickson Public-Key Cryptosystem." *La Comunicazione* **43** (1994):59-62.
7. A. Di Porto & P. Filipponi. "A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers." *Lecture Notes in Computer Science* **330** (1988):211-23.
8. A. Di Porto & P. Filipponi. "More on the Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **27.3** (1989):232-42.
9. A. Di Porto, P. Filipponi, & E. Montolivo. "On the Generalized Fibonacci Pseudoprimes." *The Fibonacci Quarterly* **28.4** (1990):347-54.
10. L. A. G. Dresel. "Letter to the Editor." *The Fibonacci Quarterly* **15.4** (1977):346.
11. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1** (1878):184-240. Trans. S. Kravitz, ed. D. Lind, The Fibonacci Association, 1969.
12. J. Vinson. "The Relation of the Period Modulo m to the Rank of Apparition of m in the Fibonacci Sequence." *The Fibonacci Quarterly* **1** (April 1963):37-45.
13. D. D. Wall. "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960):525-32.
14. D. J. White, J. N. Hunt, & L. A. G. Dresel. "Uniform Huffman Sequences Do Not Exist." *Bull. London Math. Soc.* **9** (1977):193-98.
15. H. C. Williams. "A Note on the Fibonacci Quotient $F_{p-\varepsilon}/p$." *Canadian Math. Bulletin* **25** (1982):366-70.

AMS Classification Numbers: 11B39, 11A07, 11B50

❖❖❖