BUI MINH PHONG
Eötvös Loránd University, Computer Center

RECURRENCE SEQUENCES AND PSEUDOPRIMES

ABSTRACT: In this paper we will present a summary of the most improtant results on recurrence sequences and pseudoprimes which we have discovered between 1974—1988.

I. RECURRENCE SEQUENCES

Let $G = G(G_0, G_1, A, B) = \{G_n\}_{n=0}^{\infty}$ be a second order linear recurrence defined by integer constans G_0, G_1, A, B and the recurrence

(1.1) $$G_n = AG_{n-1} - BG_{n-2} \qquad (n > 1),$$

where $AB \neq 0, D = A^2 - 4B \neq 0$ and $|G_0| + |G_1| \neq 0$. Let γ and δ be the roots of the characteristic polynomial $x^2 - Ax + B = 0$. The sequence $G(G_0, G_1, A, B)$ is called non-degenerate if γ / δ is not a root of unity. If $G_0 = 0$ and $G_1 = 1$, then we denote the sequence $G(0, 1, A, B)$ by $R = R(A, B)$. The sequence R is called Lucas sequence and R_n is called a Lucas number. In

the case where $A=-B=1$, the sequence $R(1,-1)$ is the Fibonacci sequence and we denote its terms by $F_0, F_1, F_2 \ldots$.

D. H. Lehmer *(Ann. Math. 31,1930,419—448)* generalized some results of Lucas on the divisibility properties of Lucas numbers to the terms of the sequence $U=U(L,M)=\{U_n\}_{n=0}^{\infty}$ which is defined by integer constants $L, M, U_0=0, U_1=1$ and the recurrence

$$U_n=\begin{cases} LU_{n-1}-MU_{n-2} & \text{for } n\not\equiv 0 \pmod 2 \\ U_{n-1}-MU_{n-2} & \text{for } n\equiv 0 \pmod 2, \end{cases} \tag{1.2}$$

where $LM\neq 0$ and $K=L-4M\neq 0$. The sequence U is called a Lehmer sequence and U_n is called a Lehmer number. We also say that the sequence $U(L,M)$ is non-degenerate if α/β is not root of unity, where α and β denote the roots of $z^2-L^{1/2}z+M=0$. It should be observed that Lucas numbers are also Lehmer numbers up to a possible multiplication by an integer factor.

I.1. *Generalized Lehmer sequences*

In [18] we define a generalized Lehmer sequence as follows:

Let H_0, H_1, L and M be integers with conditions $LM\neq 0$, $K=L-4M\neq 0$ and $|H_0|+|H_1|\neq 0$. A generalized Lehmer sequence is a sequence $H_0, H_1, \ldots H_n, \ldots$ of integer numbers satisfying a relation

(1.3) $$H_n = \begin{cases} LH_{n-1} - MH_{n-2} \text{ for } n \not\equiv 0 \pmod 2 \\ H_{n-1} - MH_{n-2} \text{ for } n \equiv 0 \pmod 2 \end{cases}.$$

We shall denote it by $H = H(H_0, H_1, L, M) = \{H_n\}_{n=0}^{\infty}$, and so $H(0,1,L,M)$ is the Lehmer sequence $U(L,M)$.

It was shown in [18] that in the case when $L = A^2$ and $M = B$ terms of sequence G defined in (1.1) are also terms of sequence H giving in (1.3) up to possible multiplication by an integer factor. Thus the sequences H are much more general sequences than the sequences G. Some authors have studied the lower and upper bound for the terms of the sequence G which is given in (1.1) with integer constants G_0, G_1, A and B. Let γ and δ be the roots of the equation $x^2 - Ax + B = 0$ with condition $|\gamma| \geqq |\delta|$. For example, K. Mahler *(J. Math. Sci. 1,1966, 12—17)* proved that if $D = A^2 - 4B < 0$ and ε is a positive constant, then there is an effectively computable constant n_0 depending only on ε such that

$$|G_n| \geqq |\gamma|^{(1-\varepsilon)n} \qquad \text{for} \qquad n > n_0.$$

From a result of T. N. Shorey and C. L. Stewart *(Math. Scand. 52,1983,24—36)* it follows that

$$|G_n| \geqq |\gamma|^{1-C_1 \log n}$$

for $n > C_2$, where C_1, C_2 are positive numbers which are effectively computable in terms of G_0, G_1, A and B. For the above constants P. Kiss *(Math. Sem. Notes (Kobe Univ.)*

7,1979,145—152) gave the explicit values, proving that $G_n \neq 0$ for $n > n_1$, where

$$n_1 = \max\left[2^{510}(\log|8B|)^{25}, 4\left(\log|G_0| + \log 4|D|^{1/2}\right)/\log 2\right],$$

furthermore if $D < 0$ and $n > n_1$, then

$$\frac{|c|}{2|D|^{1/2}}|\gamma|^n \cdot n^{-C_3} < |G_n| \leqq \frac{2|c|}{|D|^{1/2}}|\gamma|^n$$

where $c = G_1 - G_0\gamma$ and

$$C_3 = 2e200^{40}\log|8B|(1+\log\log|8B|)\log|16B|\left(G_0^2 + G_1^2\right).$$

In [18] we extended the results mentioned above to sequences $H(H_0, H_1, L, M)$, giving necessary and sufficient conditions for sequences H which have zero terms, furthermore giving lower and upper bounds for the terms. By using some results of M. Waldschmidt *(Acta Arith. 37, 1979, 257—283)* and C. L. Stewart *(Transcendence Theory, New York, 1977)* on linear forms in logarithms of algebraic numbers, we proved

Theorem 1.1. ([18], Theorem 2) *Let* $H = H(H_0, H_1, L, M)$ *be a generalized Lehmer sequence which is defined in (1.3). Let d=(L,M) and* $K = L - 4M$.

If $LK > 0$, *then* $H_n \neq 0$ *for* $n > max\ [13, min\ (|H_0|+1, |H_1|+2)]$.

If $LK < 0$, *then* $H_n \neq 0$ *for* $n > max\ (N_1, N_2)$, *where*

$$N_1 = min\left[2^{67}\log|4M|, e^{398}\right]$$

and

$$N_2 = min\left[\frac{4}{\log 2}\log|dH_0|, \frac{4}{\log 2}\log|H_1|\right].$$

Theorem 1.2. ([18], Theorem 3) *Let* $H = H(H_0, H_1, L, M)$ *be a generalized Lehmer sequence which is defined in (1.3) with the condition* $LK < 0$.

Then for $n > 2^{57}\log\left\{|4M|\left(H_o^{\,2} + H_1^{\,2}\right)\right\}$, *we have*

$$\frac{|a|}{2|LK|^{1/2}}|\alpha|^n \cdot n^{-C_0} < |H_n| < \frac{2|a|}{|K|^{1/2}}|\alpha|^n,$$

where

$$C_0 = 2^{80}\log|4M|\log\log|4M|\log\left\{|4M|\left(H_0^{\,2} + H_1^{\,2}\right)\right\},$$

$$a = H_1 - L^{1/2}H_0\beta,$$

and α, β *are roots of* $z^2 - L^{1/2}\cdot z + M = 0$.

We note that in the case $LK > 0$ Theorem 1.2 also holds.

I.2. *Prime divisors of Lehmer sequences*

Let $R = R(A, B)$ be a Lucas sequence. Assume that $(A, B) = 1$ and the sequence is non-degenerate, that is if γ and δ denote the roots of the characteristic polynomial $x^2 - Ax + B = 0$, then γ/δ is not a root of unity. It is known that in this case

$$R_n = \frac{\gamma^n - \delta^n}{\gamma - \delta} \tag{1.4}$$

for any $n \geq 0$. In the special case $(A; B = (3; 2)$ the terms of sequence R are $R_n = 2^n - 1$. For this sequence P. Erdős

(Istrael J. Math. 9, 1971, 43—48) proved that there are positive constants c and c' such that

$$\sum_{p|(2^n-1)} \frac{1}{p} < \log\log\log n + c$$

for distinct prime divisors and

$$\sum_{d|(2^n-1)} \frac{1}{d} < c' \cdot \log\log n$$

for the distinct positive divisors of the terms. Erdős note that similar results hold for the divisors of the numbers $Q^n - 1$ (Q is a positive integer), but he asked that the constants c and c' in this case depend on Q or not. In [14] with P. Kiss we extended these results for Lucas numbers, futhermore we give their improvments by showing that the constants in the inequalities do not depend on the sequence. For Lehmer sequences we proved in [10] (Chapter 4, Theorem 4.1.) the following

Theorem 1.3. ([10]) Let $U = U(L,M)$ *be the non-degenerate Lehmer sequence defined in (1.2) . Then there are positive absolute constants* c *and* c^**, which do not depend on the sequence* U*, such that*

$$\sum_{p|U_n} \frac{1}{p} < \log\log\log n + c$$

and

$$\sum_{d|U_n} \frac{1}{d} < c^* \cdot \log\log n$$

for any $n > N_0$*, where* N_0 *depends only on the sequence* $U(L,M)$.

A natural number m is called weakly composite if the reciprocal sum of its distinct prime divisors is not greater than 2, i.e.

$$\sum_{p|m} \frac{1}{p} \leq 2.$$

Proving conjecture of I. Kátai, J. Galambos *(Proc. Amer. Math. Soc. 29, 1986, 215—216)* showed that for any sufficiently large n there is a weakly composite number between n and $n+\log\log\log n$. In [10] (Chapter 4, Theorem 4.2) we proved

Theorem 1.4. ([10]) Let $U = U(L,M)$ *be a non-degenerate Lehmer sequence. For any* $n > 3$ *there is a Lehmer number* U_m *such that*

$$\sum_{p|U_m} \frac{1}{p} < C$$

and $n < m \leq n + \log\log n$, *where C is a constant depending only on* L *and* M.

We note that this result is an extension of result of P. Kiss and B. M. Phong [13] who proved a similar estimation for a non-degenerate Lucas sequence.

I.3. *Some Diophantine equations concerning recurrence sequences*

A linear recurrence $W = \{W_n\}_{n=0}^{\infty}$ of order $k(>1)$ is defined by integers $A_0, A_1, \ldots, A_{k-1}$ and by recursion

$$W_n = A_o W_{n-1} + A_1 W_{n-2} + \ldots + A_{k-1} W_{n-k} \quad (n \geq k),$$

where the initial values $W_0, W_1, \ldots, W_{k-1}$ are fixed not all zero integers and $A_{k-1} \neq 0$. Denote the distinct roots of characteristic polynomial

$$f(x) = x^k - A_0 x^{k-1} - \ldots - A_{k-1}$$

by $\alpha_0, \alpha_1, \ldots, \alpha_t$, where α_i has multiplity m_i. It is known that for $n \geq 0$

$$W_n = f_1(n)\alpha_1^n + f_2(n)\alpha_2^n + \ldots + f_t(n)\alpha_t^n,$$

where $f_i(n)$ is a polynomial of degree at most $m_i - 1$, furthermore the coefficients of $f_i(n)$ are algebraic numbers from the field $Q(\alpha_1, \ldots, \alpha_t)$. We say that the sequence W is non-degenerate if $t > 1$ *and* α_i / α_j is not a root of unity for $t \geq j > i \geq 1$.

Let $p_1, p_2, \ldots, p_r$ be primes and we denote by S the set of integers which have only these primes as prime factors.

K. Győry, P. Kiss and A. Schinzel *(Colloq. Math. 45, 1981, 75—80)* showed that if W is a non-degenerate Lucas sequence R, then

(1.5) $$W_x \in S$$

holds only for finitely many sequences W and for finitely many integers x. K. Győry *(Acta Arith. 40, 1982, 369—373)* improved this result giving explicit upper bound for x and for the constants of Lucas sequences which satisfy (1.5).

The Diophantine equation

$$W_x = sy^q \tag{1.6}$$

was also studied by several authors. T. N. Shorey and C. L. Stewart *(Math. Scand. 52, 1983, 24—36)* proved that if $y > 1$, $q > 1$ are integers and W is a non-degenerate recurrence of order k for which $m_1 = 1$ and $|\alpha_1| > |\alpha_j|$ $(j = 2,\ldots,t)$, then (1.6) implies the inequality $q < C_4$, where C_4 is an effectively computable constant in the terms of s and the parameters of sequence W. They showed that x and y are also bounded for second order recurrences. A. Pethő *(J. of Number Theory 15, 1982, 5—13)* proved similar results for second order recurrences supposing $(A_0, A_1) = 1$ and $s \in S$. For recent general results we refer to the monograph by T. N. Shorey and R. Tijdeman *(Exponential Diophantine Equations, Cambridge University Press, 1986)*, further to the references there.

The following problem remained open : if $|\alpha_1| = \ldots = |\alpha_t|$, then the equation (1.6) has finite or infinite solutions?

Let $R = R(A,B)$ be a Lucas sequence defined by integers A,B. For fixed integer $k > 0$ we put

$$T_0(k) \quad := k, \quad T_n(k) := R_{kn} / R_n \quad (\text{n=1,2,...}).$$

As it is known, $T_n(k) - s$ are integers. Let $T(k) = \{T_n(k)\}_{n=0}^{\infty}$. L. Somer *(Fibonacci Quart. 22, 1984, 98—100)* proved that the sequence $T(k)$ is a linear integeral recurrence of order k, furthermore the order k is minimal. Indeed, by using (1.4) we get

$$T_n(k) = \left(\gamma^{k-1}\right)^n + \left(\gamma^{k-2}\delta\right)^n + \ldots + \left(\delta^{k-1}\right)^n = (\alpha_1)^n + \ldots + (\alpha_k)^n,$$

where $\alpha_i = \gamma^{k-i}\delta^{i-1}$. If $D = A^2 - 4B < 0$, then $|\alpha_1| = \ldots = |\alpha_t| = |\gamma|^{k-1}$. Consequently, the investigation of the Diophantine equation $T_x = sy^q$ has meaning. In [12] we proved with I. Joó that the Diophantine equation

$$T_x(k) = sy^q$$

in integers $s \in S$, $q>2$, x, $|y|>1$ implies $\max(|s|,|y|,x,q) < C_5$, where C_5 is an effectively computable constant depending only on A, B, k and S. By using the theorem of T. N. Shorey, A. van der Poorten, R. Tijdeman and A. Schinzel *(Transcendence Theory, New York, 1977)* concerning the Thue-Mahler equation and the theorem of C. L. Stewart *(Transcendence Theory, New York, 1977)* on linear forms in logarithms of algebraic numbers, in [10] (Theorem 3.1) we improved the above result, namely we showed the following

Theorem 1.5. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence with the condition $(L,M) = 1$. Let $k > 1$ be an integer.*

Then all solutions of the Diophantine equation

$$U_{kx} / U_x = sy^q$$

in integers $s \in S$, $y \neq 0$, $q > 2$ satisfy

$$\max(x, |y|, q, |s|) < C_6$$

for $|y| > 1$ and

$$\max(x, |s|, |L|, |M|, k) < C_7$$

for the case when $|y| = 1$, $kx > 6$, $(k;x) \neq (2;4),(2;5)$, where C_6 and C_7 are effectively computable constants, C_6 depends only L, M, k and S, C_7 depends only on S.

Theorem 1.6. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence. Then the equation*

$$|U_x| = |U_y|$$

has non solutions in non-negative integers x, y with $x \neq y$ and $\max(x,y) > \min\left(e^{398}, 2^{67} \log|4M|\right)$.

I.4. *Lucas primitive roots*

Let $R = R(A,B)$ be a Lucas sequence defined by integers $R_0 = 0$, $R_1 = 1$, A, B and the recursion

$$R_{n+1} = AR_n - BR_{n-1} \quad \text{for } n > 0.$$

The sequence $R(1,-1)$ is the Fibonacci sequence F.

Let p be an odd prime with $B \not\equiv 0 \pmod{p}$ and let $e > 0$ be an integer. The positive integer $r = r(p^e)$ is called the rank of apparition of p^e in the sequence R if $R_r \equiv 0 \pmod{p^e}$ and $R_m \not\equiv 0 \pmod{p^e}$ for $0 < m < r$; furthermore $\nu = \nu(p^e)$ is called the period of the sequence R modulo p^e if it is the smallest positive integer for which $R_n \equiv 0 \pmod{p^e}$ and $R_{n+1} \equiv 1 \pmod{p^e}$. In the Fibonacci sequence, we denote the rank of apparition of p^e and period of F modulo p^e by $f(p^e)$ and $\pi(p^e)$, respectively.

Let the number R be a primitive root $\pmod{p^e}$. If $x = g$ satisfies the congruence

$$f(x) = x^2 - Ax + B \equiv 0 \pmod{p^e}, \tag{1.7}$$

then we say that R is a Lucas primitive root $\pmod{p^e}$ with parameters A and B. This is the generalization of the definition of Fibonacci primitive roots (FPR) modulo p that was given by D. Shanks for the case $A = -B = 1$ *(Fibonacci Quart., 10. 1973, 163—168, 181).*

The conditions for the existence of FPR $\pmod{p}$ and their properties were studied by several authors. For example, D. Shanks proved that if there exists a FPR $\pmod{p^e}$ then $p = 5$

or $p \equiv \pm 1 \pmod{10}$; furthermore, if $p \neq 5$ and there are FPR's $(\mathrm{mod}\ p)$ then the number of FPR's is two or one, according to whether $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$. D. Shanks and L. Taylor *(Fibonacci Quart. 11. 1973, 159—160)* have shown that if g is a FPR $(\mathrm{mod}\ p)$ then $g-1$ is a FPR $(\mathrm{mod}\ p)$. M. J. DeLeon *(Fibonacci Quart. 15, 1977, 353—355)* proved that there is a FPR $(\mathrm{mod}\ p)$ if and only if $\ell(p) = p-1$. In [1] with P. Kiss we studied the connection between the rank of apparition of a prime p and the existence of FPR's $(\mathrm{mod}\ p)$. We proved that there is exactly one FPR $(\mathrm{mod}\ p)$ if and only if $f(p) = p-1$ or $p = 5$; moreover, if $p \equiv 1 \pmod{10}$ and there exitst two FPR's $(\mathrm{mod}\ p)$ or non FPR exists, then $f(p) < p-1$. M. E. Mays *(Fibonacci Quart, 20. 1982, 111)* showed that if booth $p = 60k-1$ and $q = 30k-1$ are primes then there is a FPR $(\mathrm{mod}\ p)$.

In [16] we given some connections among the rank of apparition of p^e in the Lucas sequence R, the period of R modulo p^e, and Lucas primitive roots $(\mathrm{mod}\ p^e)$; furthermore we shown necessary and sufficient conditions for the existence of Lucas primitive roots $(\mathrm{mod}\ p^e)$.

Theorem 1.7. ([16]) *Let R be Lucas sequence defined by integers $A \neq 0$ and $B = -1$, let p be an odd prime with $D = A^2 + 4 \not\equiv 0 \pmod p$, and let $e > 0$ be an integer. Then there is a Lucas primitive root* $(\mathrm{mod}\ p^e)$ *if and only if*

$$\ell(p^e) = \Phi(p^e)$$

where Φ *denotes the Euler function. There is exactly one Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if* $\psi(p^e) = \Phi(p^e)$ *and* $p \equiv -1 \,(\mathrm{mod}\, 4)$, *and there are exactly two Lucas primitive roots* $(\mathrm{mod}\, p^e)$ *if* $\psi(p^e) = \Phi(p^e)$ *and* $p \equiv 1 \,(\mathrm{mod}\, 4)$.

Theorem 1.8. ([16]) *Let* R *be Lucas sequence defined by integers* $A \neq 0$ *and* $B = -1$, *let* p *be an odd prime with* $D = A^2 + 4 \not\equiv 0 \,(\mathrm{mod}\, p)$, *and let* $e > 0$ *be an integer. Then there is exactly one Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if and only if* $r(p^e) = \Phi(p^e)$ *and* $p \equiv 1 \,(\mathrm{mod}\, 4)$, *and exactly two Lucas primitive roots* $(\mathrm{mod}\, p^e)$ *exist if and only if*

$$r(p^e) = \Phi(p^e)/2 \qquad \text{and} \qquad p \equiv 1 \,(\mathrm{mod}\, 8)$$

or

$$r(p^e) = \Phi(p^e)/4 \qquad \text{and} \qquad p \equiv 5 \,(\mathrm{mod}\, 8).$$

From these theorems, some other results follow.

Collary 1.9. *If* R, p *and* e *satisfy the conditions of Theorem 1.8 and* $r(p^e) = \Phi(p^e)$, *then* g *is a Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if and only if* $x = g$ *satisfies the congruence*

$$R_n x + R_{n-1} \equiv -1 \,(\mathrm{mod}\, p^e),$$

where $n = \Phi(p^e)/2$.

Corollary 1.10. *If* R, p *and* e *satisfy the conditions of Theorem 1.8 and* g *is a Lucas primitive root* $(\mathrm{mod}\, p^e)$, *then* g-A *is a primitive root* $(\mathrm{mod}\, p^e)$.

We note that these results remain valid for Fibonacci primitive roots. In this case the following problem also remained open: Do there exist infinitely many primes p such that

$$\ell(p) = p - 1 \ ?$$

II. PSEUDOPRIMES

A problem, commonly attributed to the ancient Chinese, was to ascertain whether a natural number n must be a prime if it satisfies the congruence

$$2^n \equiv 2 \pmod{n}. \tag{2.1}$$

The question remained open until 1819, when Sarrus showed that $2^{341} \equiv 2 \pmod{341}$, yet $341=11.31$ is a composite number. In particular, a crude converse of Fermat's little theorem is false. In 1904, M. Cipolla *(Annali di Matematica 9, 1904, 139—160)* proved that there are infinitely many composite natural numbers n which satisfy the congruence (2.1).

Let $c>1$ be an integer. A composite natural n is called pseudoprime to base $c>1$ if

$$c^n \equiv c \pmod{n}. \tag{2.2}$$

If a composite natural n with $(n,c)=1$ and satisfies the congruence

$$c^{(n-1)/2} \equiv (c/n) \pmod{n}, \tag{2.3}$$

then n is called an Euler-pseudoprime to base c, where (c/n) denotes the Jacobi symbol. We simply say n is a pseudoprime (or an Euler-pseudoprime) if it is one to base 2.

The properties of pseudoprimes and their generalizations have been studied intensively, since they can be used for primality tests. For results and problems concerning pseudoprimes and their generalizations we refer to the works by A. Rotkiewicz *(Pseudoprime numbers and their generalizations, Univ. of Novi Sad, 1972),* E. Lieuwens *(Fermat pseudoprimes, Doctor thesis, Delft, 1971),* C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. *(The pseudoprimes to 25.10^9, Math. Comp. 35, 1980, 1003—1026),* further to the references there.

II. 1. *Lucas and Lehmer pseudoprimes*

Let $R = R(A,B)$ be a Lucas sequence defined by integers $R_0 = 0$, $R_1 = 1$, A and B. Let $D = A^2 - 4B \neq 0$, and we assume that the sequence R is non-degenerate. Let $S = S(A,B)$ be the sequence $G(2,A,A,B)$, that is $S_0 = 2$, $S_1 = A$ and $S_{n+1} = AS_n - BS_{n-1}$ $(n > 0)$. For odd primes n with $(n,D) = 1$, as it is well-known, we have

$$R_{n-(D/n)} \equiv 0 \pmod{n}, \tag{2.4}$$

$$R_n \equiv (D/n) \pmod{n}, \tag{2.5}$$

$$S_n \equiv S_1 \pmod{n} \tag{2.6}$$

and for odd prime n with $(n,BD) = 1$

$$(2.7)\quad \begin{cases} R_{(n-(D/n))/2} \equiv 0 & (\mathrm{mod}\, n) \text{ when } (B/n)=1 \\ S_{(n-(D/n))/2} \equiv 0 & (\mathrm{mod}\, n) \text{ when } (B/n)=-1, \end{cases}$$

where $(\ /n)$ is the Jacobi symbol. If n is composite, $(n,2D)=1$, but (2.4) still holds, then n is called a Lucas pseudoprime with parameteres A,B. Furthermore, if n is composite, $(n,2D)=1$ and satisfies the congruence (2.7), then n is called Euler-Lucas pseudoprime. It can be easily seen that in the case when $A=c+1$ and $B=c$, by using (1.4), we have $R_n=(c^n-1)/(c-1)$, and so the definitions of Lucas and Euler-Lucas pseudoprimes are generalizations of pseudoprimes and Euler pseudoprimes to base $c>1$.

We list some results which are in connection with ours. C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. *(Math. Comp. 35, 1980, 1003—1026)* proved that for given positive integer s there is an Euler-pseudoprime which is a product of exactly s distinct primes. From results of A. J. van der Poorten and A. Rotkiewicz *(J. Austra. Math. Soc. Ser. A 29, 1980, 316—321)* it follows that there are infinitely many Euler pseudoprimes to base an integer $c>1$, which are of the form $ax+b$, where $(a,b)=1$. On the other hand, P. Erdős *(Amer. Math. Monthly 56, 1949, 623—624)* and E. Lieuwens *(Doctor thesis, Delft, 1971)* proved that for any integers c, $s>1$ there are infinitely many pseudoprimes to base c which are products of exactly s primes. This result was extended by P. Kiss, B. M. Phong and E. Lieuwens in [5] for Euler-Lucas pseudoprimes, among others, we proved that if $R=R(A,B)$ is a non-degenerate Lucas sequence with $D=A^2-4B>0$ and a,

s are positive integers, then there exist infinitely many Euler-Lucas pseudoprimes with parameters A, B which are products of exactly s primes of the form $ax+1$.

A. Rotkiewicz *(Bull. Acad. Polon. Sci. Ser. Sci. Math. Astr. Phys. 20, 1972, 349—354)* gave a proper generalization of ordinary pseudoprimes for Lehmer sequences. Let $U=U(L,M)$ be the non-degenerate Lehmer sequence defined by integers L, M and by (1.2). Let $V=V(L,M)=\{V_n\}_{n=0}^{\infty}$ be the sequence defined $V_0=2$ and by the relation

$$V_n = U_{2n}/U_n \qquad (n=1,2,\dots).$$

Similarly to the congruences (2.4)-(2.7), it is also known that for odd prime n with $(n,LK)=1$, we have

(2.8) $\quad U_{n-(LK/n)} \equiv 0 \pmod{n}$,

(2.9) $\quad U_n \equiv (K/n) \pmod{n}$

(2.10) $\quad V_n \equiv (L/n) \pmod{n}$,

and for odd prime n with $(n,LK)=1$

$$(2.11)\quad \begin{cases} U_{(n-(LK/n))/2} \equiv 0 \pmod{n} & \text{when } (LM/n)=1 \\ V_{(n-(LK/n))/2} \equiv 0 \pmod{n} & \text{when } (LM/n)=-1. \end{cases}$$

An odd composite n is called a Lehmer pseudoprime with parameters L, M if $(n,LMK)=1$ and (2.8) holds, and it is an Euler-Lehmer pseudoprime if (2.11) is true. Some results of

A. Rotkiewicz *(Math. Comp. 39, 1982, 239—247)* imply that for the non-degenerate Lehmer sequence $U(L,M)$ with $L>0$ and $K=L-4M>0$ every arithmetic progression $ax+b$, where $(a,b)=1$, contains an infinite number of Euler-Lehmer pseudoprimes with parameters L and M.

Using some theorems of A. Schinzel *(Acta Arith. 8, 1963, 213—223)* and J. Wójcik *(Acta Arith. 40, 1982, 155—174; Acta Arith. 40, 117—131)* we proved the following

Theorem 2.1. ([7]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence and let $s>1$ be an integer. Then there exists a positive integer w_0 such that for any integers a,b with condition $(a,bw_o)=1$ and for infinitely many primes p of the form $ax+b$ there exist an Euler-Lehmer pseudoprime which is the product of exactly s distinct primes and p is the least prime divisor of it.*

Theorem 2.2. ([17]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence with $LK=L(L-4M)>0$ and let a,s be positive integers. Then there are infinitely many Euler-Lehmer pseudoprimes which are products of exactly s primes of the form $ax+1$.*

A. Rotkiewicz *(Bull. Acad. Polon. Sci. Ser. Sci. Math. Astr. Phys. 21, 1972, 793—797)* showed that if $R(A,B)$ is non-degenerate Lucas sequence for which $B=1$ or $B=-1$, and a,b are relatively prime integers, then there exist infinitely many composite numbers n of the form $ax+b$ which satisfy

the congruences (2.4), (2.5) and (2.6) simultaneously. A similar result also holds for Lehmer sequences.

Theorem 2.3. ([7]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence for which $M = \pm 1$ and $LK = L(L \pm 4) > 0$. Then for any fixed positive integer s there are infinitely many Euler-Lehmer pseudoprimes n which are products of exactly s distinct primes of the form $ax+1$ and satisfy the congruences (2.8), (2.9) and (2.10) simultaneously.*

In the following we say that n is a perfect Lehmer pseudoprime with parameteres L,M if $(n, 2LMK) = 1$ and the congruences (2.8), (2.9), (2.10) hold. Improving a result of [8] concerning Lucas sequences, in [10] we showed

Theorem 2.4. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence. Then the following three conditions are dependent:*

(i) n is a perfect Lehmer pseudoprime with parameters L,M

(ii) n is an Euler-Lehmer pseudoprime with parameters L,M

(iii) n is an Euler pseudoprime to base M.

That is, from any two ones of them, the third one follows.

II.2. *A generalized solution of A. Rotkiewicz's problem*

A. Rotkiewicz asked in his book the following question. "Let $c,k > 1$ be fixed positive integers. Do there exist infinitely

many composite integers n such that $n|(c^{n-k}-1)$?" *(Pseudoprime Numbers and Their Generalizations, Univ. of Novi Sad, 1972, problem 18)*. It is known as above that the answer is affirmative in the case $k=1$; the numbers satisfying the condition are pseudoprimes to base c. A general result was obtained by A. Makowski *(Simon Stevin 36, 1972, 71)*: For any natural number $k \geq 2$ there are infinitely many composite n such that

$$c^{n-k} \equiv 1 \pmod{n} \tag{2.12}$$

for any positive integer c with $(c,n)=1$. This result was proved earlier by D. C. Morrow *(Amer. Math. Monthly 58, 1951, 329—330)* in the case $k=3$. In this proof, Makowski showed that there are infinitely many integers n of the form $n=p.k$ (where p is a prime) such that congruence (2.12) holds for any positive integer c if $(c,n)=1$. Naturally, $(k,c)=1$ for these numbers, and so the question remained unanswered if c and k are fixed and $(k,c)>1$. In the case $(k,c)>1$, A. Rotkiewicz obtained two results: He proved that (2.12) has infinitely many solutions if $k=3$ and c is an arbitrarily fixed positive integer, or if $k=2$ and $c=2$ (see Theorem 32 in his book and *Math. Comp. 43, 1984, 271—272,* respectively).

In [9] with P. Kiss we gave a general solution of the problem, namely we proved

Theorem 2.5 ([9]) *Let* $c(<1)$ *and* k *be fixed positive integers. Then there are infinitely many composite integers* n *satisfying the congruence (2.12).*

In [17] we considered the following congruence

$$a^{n-k} \equiv b^{n-k} \pmod{n}, \tag{2.13}$$

where a,b and k are given positive integers with conditon $(a,b)=1$. Improving Theorem 2.5 we proved the following

Theorem 2.6. ([17]) *The congruence (2.13) has infinitely many composite solutions* n *if neither* (a,b,k) *is one of the following triples:*

$$\begin{aligned} &(2^u+1, 2^u-1, 3) && \text{for } u>1, \\ &(5.2^v+1, 5.2^v-1, 3) && \text{for } v>0, \\ &(c+1, c, 2); (c+3, c, 2) && \text{for } c>1. \end{aligned}$$

We note that W. L. McDaniel *(Colloq. Math. 59, 1990, 177—190)* independently proven this theorem and some generalizations of it. We obtained a similar result of Theorem 2.6 for Lehmer pseudoprimes.

Theorem 2.7. ([17]) *Let* $U=U(L,M)$ *be a non-degenerate Lehmer sequence. Then there is a positive integer* k_0 *such that for any fixed* $k>k_0$ *the congruence*

$$U_{n-k(LK/n)} \equiv 0 \qquad (\mathrm{mod}\, n)$$

has infinitely many composite solutions n. *Moreover, if* $k > 1$ *and* $(k, M) = 1$, *then there exist infinitely many composite integers* n *satisfying a congruence*

$$U_{n-k} \equiv 0 \qquad (\mathrm{mod}\, n).$$

II. 3. *Super Lucas and super Lehmer pseudoprimes*

We say that n is a super pseudoprime to base integer $c > 1$ if each divisor of it is a prime or a pseudoprime to base c. Similarly to super pseudoprimes to base c, we say that n is a super Lucas (super Lehmer) pseudoprime if each divisor of it is a prime or a Lucas (Lehmer) pseudoprime.

K. Szymiczek *(Elem. Math. 21. 1966, 59)* showed that $F_n F_{n+1}$ is a super pseudoprime to base 2 for any $n > 1$, where

$$F_n = 2^{2^n} + 1$$

is the n-th Fermat number. From the result of K. Szymiczek *(Colloq. Math. 13, 1964/65. 259—263)* it follows that there are infinitely many super pseudoprimes to base 2 which are products of exactly three primes. This result was extended by J. Fehér and P. Kiss *(Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 26, 1983. 157—159)* for super pseudoprimes to base c, where $c > 1$ is an integer with $c \not\equiv 0 (\mathrm{mod}\, 4)$. A. Rotkiewicz *(Glasgow Math. J. 9, 1968, 83—86)* has obtained another generalization of Szymiczek's result, he proved that for infinitely many primes p of the form $ax + b$, where $(a, b) = 1$,

there exist primes q and r such that pqr is a super pseudoprime to base 2. In [6] we extended the result of Rotkiewicz and the result of Fehér and Kiss mentioned above proving that form every integers $a>1$ and $c>1$ there are infinitely many triplets of distinct primes p,q and r of the for $ax+1$ such that pqr is a super pseudoprime to base c. We also showed that if the square-free kernel of the base c is congruent to ± 1 modulo *4,* then the series $\sum 1/\log n$ is divergent, where n runs through all super pseudoprimes to base c which are products of exactly three distinct primes.

P. Kiss *(Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 28, 1986, 153—159)* studied the super Lucas pseudoprimes for non-degenerate Lucas sequences $R(A,B)$ and proved that R_{2p}/A is a super pseudoprime with parameters A,B for every large prime p, furthermore he showed that the series $\sum 1/\log n$, where n runs through all super Lucas pseudoprimes with parameters A and B, is divergent.

In [11], by using some result of J. Wójcik *(Acta Arith. 40, 1981/82, 155—174; 41, 1982, 117—131)* we improved above result as follows:

Theorem 2.8. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence. Then there exists a positive integer w_1 such that for infinitely many primes p of the form $ax+b$, where $(a,b)=1$ and $b\equiv 1 \pmod{(a,w_1)}$, there are primes q and r such that pqr is a super Lehmer pseudoprime with*

parameteres L,M. The constant w_1 is effectively computable in the terms of L and M.

Theorem 2.9. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence with condition $LK=L(L-4M)>0$ and let $a>1$ be an integer. Then there are infinitely many triplets of distinct primes p,q and r of the form $ax+1$ such that pqr is a super Lehmer pseudoprime with parameteres L,M.*

Theorem 2.10. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence. Let S_1 and S_2 denote the set of all super Lehmer pseudoprimes with parameters L,M which are determined in Theorem 2.8 and Theorem 2.9, respectively. Then the series*

$$\sum_{n\in S_1}\frac{1}{\log n} \text{ and } \sum_{n\in S_2}\frac{1}{\log n}$$

are divergent.

We note that the conditions of Theorem 2.8 are satisfied for any integer $a>1$ if $b=1$ and for every pairs a,b with $(a,b,w_1)=1$. It is obvious that these results remain valid if we replace the super Lehmer pseudoprimes with super Lucas pseudoprimes. For example, from Theorem 2.10 we get.

Corollary 2.11. *For every integers $a,c>1$ the series $\sum 1/\log n$, where n runs through all super pseudoprimes to base c which are products of exactly three distrinct primes of the form $ax+1$, is divergent.*

II. 4. *The distribution of Lehmer pseudoprimes*

Let $\mathscr{A}(c,x)$ be denote the number of pseudoprimes to base c not exceeding x. In the case $c=2$ we denote $\mathscr{A}(2,x)$ by $\mathscr{A}(x)$. It is known that there exist positive constants C_1 and C_2 such that for all large x

$$C_1 \cdot \log x \leq \mathscr{A}(x) \leq x \cdot \exp\{-C_2(\log x \log\log x)^{1/2}\},$$

where the lower and the upper bound is due to D. H. Lehmer *(Amer. Math. Monthly 43, 1936, 347—354)* and P. Erdős *(Publ.Math. Debrecen. 4, 1956, 201—206)*, respectively. C. Pomerance improved these results showing that for all large x

$$\mathscr{P}(x) \geq \exp\{(\log x)^{5/14}\}$$

and

$$\mathscr{P}(x) \leq x \cdot \exp\{-\log x \log\log\log x / 2 \cdot \log x\}$$

(see Illinois J. Math. 26, 1982, 4—9 and *Math. Comp. 37, 1981, 587—593).*

Let $R = R(A,B)$ be non-degenerate Lucas sequence. Let $\mathscr{A}(R,x)$ be denote the number of all Lucas pseudoprimes with parameteres A,B not exceeding x. R. Baillie and S. S. Wagstaff, Jr. *(Math. Comp. 35. 1980, 1391—1417)* proved that there are positive constants C_3 and C_4 such that for all large x

$$\mathscr{P}(R,x) < x \cdot \exp\{-C_3(\log x \log\log x)^{1/2}\}$$

for any sequence R and

$$\mathscr{P}(R,x) > C_4 \cdot \log x$$

for sequences R for which $D = A^2 - 4B > 0$ but D is not a perfect square. This lower bound was extended by P. Kiss *(Ann. Univ. Sci. Budapest, Sect. Math. 28, 1986, 153—159)* to all non-degenerate Lucas sequences R. Very recently P. Erdős, P. Kiss and A. Sárközy *(Math. Comp. 51, 1988, 315—323)* improved the lower bound for $\mathcal{P}(R,x)$ extending Pomerance's result for Lucas pseudoprimes. They showed that there is a positive constant C_5 such that for all large x

$$\mathcal{P}(R,x) > \exp\left\{(\log x)^{C_5}\right\}$$

for any non-degenerate Lucas sequence R. In the proof of this result they showed only the existence of the constant C_5 and they noted that it would be interesting to get a reasonable numerical estimate for this constant.

By using some results of Selberg's sieve and a new idea concerning some congruences of Lehmer sequences, in [10] we extended the above result of Pomerance, Erdős, Kiss and Sárközy for Lehmer pseudoprimes, furthermore we gave a numerical value for C_5.

Theorem 2.12. ([10]) *Let $U = U(L,M)$ be a non degenerate Lehmer sequence and let $\mathcal{P}(U,x)$ denote the number of all Lehmer pseudoprimes with parameters L and M not exceeding x. Then for all large x we have*

$$\mathcal{P}(U,x) > \exp\left\{(\log x)^{1/35}\right\}$$

and

$$\mathcal{P}(U,x) < x \cdot \exp\{-\log x \cdot \log\log\log x / 2\log x\}.$$

A. Rotkiewicz *(Acta Arith. 21, 1972, 251—259)* proved the following result: If $a > 6$ is a given integer, then for all large x $\neq \{n \leq x | n$ is pseudoprime and $n \equiv 1 (\mathrm{mod}\, a)\} \geq \log x / (2 \log 2) a$.

We improved this result showing the following

Theorem 2.13. ([10]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence and let $a > 1$ be an integer with condition $(a, M) = 1$. Then there is a positive constant C_6 such that for all large x, the number of all Lehmer pseudoprimes with parameters L, M which are congruent to 1 modulo a and not exceed x is greater than*

$$\exp\{(\log x)^{C_6}\}.$$

For super Lehmer pseudoprimes we obtained the following

Theorem 2.14. ([15]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence and let Δ denote the square-free kernel of M. $\max(L, K)$, where $K = L - 4M$. If $\Delta \equiv \pm 1 (\mathrm{mod}\, 4)$, then for all large x the number of all super Lehmer pseudoprimes with parameters L, M not exceeding x is greater than*

$$(4\Delta \log |\alpha|)^{-1} \cdot \log x,$$

where α, β denote the roots of $z^2 - L^{1/2} z + M = 0$ and $|\alpha| \geq |\beta|$.

Showing a conjecture of A. Rotkiewicz, A. Makowski *(Elem. Math. 29, 1974, 13)* proved that the series $\sum 1/\log n$, where n runs through all pseudoprimes to bace c, is

divergent. In [4] we extended this result showing that the series

$$\sum \frac{1}{\log_{s-1} n}$$

is divergent, where n runs through all pseudoprimes to base c which are products of exactly s primes. Here $\log_k$ denotes the k times iterated logarithm. It was proved in [7] that

Theorem 2.15. ([7]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence. The series*

$$\sum \frac{1}{\log_{s-2} n},$$

where n runs through all Lehmer pseudoprimes which are products of exactly $s(\geq 3)$ distinct primes, is divergent.

REFERENCES

[1] P. Kiss & B. M. Phong, On the connection between the rank of apparition of a prime p in Fibonacci sequence and the Fibonacci primitive roots, Fibonacci Quart. 15 (1977), 347—349.

[2] P. Kiss & B. M. Phong, On a function concerning second order recurrences, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 21. (1978), 119—122.

[3] P. Kiss & B. M. Phong, Divisibility properties in second order recurrences, Publ. Math. Debrecen 26 (1979), 187—197.

[4] B. M. Phong, A generalization of A. Makowski's theorem on pseudoprime numbers, Tap chi Toan hoc 7 (1979), 16—19, (in Vietnamese).
[5] P. Kiss, B. M. Phong & E. Lieuwens, On Lucas pseudoprimes which are products of s primes, Fibonacci Number and Their Applications, 1986, 133—139.
[6] B. M. Phong, On super pseudoprimes which are products of three primes, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 30 (1987), 125—129.
[7] B. M. Phong, On Lucas and Lehmer pseudoprime numbers, Matematikai Lapok (1982—1986), 79—92 (in Hungarian).
[8] B. M. Phong, Connections between Lucas pseudoprimes of different types, Tudományos Közl., Eger (1987), 55—67 (in Hungarian).
[9] P. Kiss & B. M. Phong, On a problem of A. Rotkiewicz, Math. Comp. 48 (1987), 751—755.
[10] B. M. Phong, Lehmer sequences and Lehmer pseudoprimes, Ph. D. Thesis, Budapest, 1987.
[11] B. M. Phong, On super Lucas and super Lehmer pseudoprimes, Studia Math. Hungar. 23. (1988), 435—442.
[12] I. Joó & B. M. Phong, On two Diophantine equations concerning Lucas sequences, Publ. Math. Debrecen 35 (1988), 301—307.
[13] P. Kiss & B. M. Phong, Weakly composite Lucas numbers, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 31 (1988), 179—182.

[14] P. Kiss & B. M. Phong, The reciprocal sum of prime divisors of Lucas numbers, Tudományos Közl., Eger (1988), 47—54.
[15] I. Joó & B. M. Phong, On super Lehmer pseudoprimes, Studia Math. Hungar. 25 (1990), 121—124.
[16] B. M. Phong, Lucas primitive roots, Fibonacci Quart. 29 (1991), 66—71.
[17] B. M. Phong, A generalized solution of A. Rotkiewicz's problem, Matematikai Lapok, 34 (1987), 109—119.
[18] B. M. Phong, On generalized Lehmer sequences, Acta Math. Hungar., 57 /3—4 (1991), 201—211.