Acta Math. Hung.
55 (3—4) (1990), 279—284.

ON GENERALIZED LUCAS PSEUDOPRIMES

I. JOÓ (Budapest)

To Professor L. Fejes Tóth on his 75th birthday

A composite solution of the congruence

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

is called a pseudoprime with respect to a if $k=1$. It is well-known that there exist infinitely many pseudoprimes with respect to any given non-zero a.

Let $a, k>1$ be fixed integers. In [11] A. Rotkiewicz asked the following question. "Do there exist infinitely many composite integers n satisfying (1)?"

Some investigations have shown that (1) has infinitely many composite solutions when (a, k) is subject to various restrictions (see [6], [10], [11], [12] and [13]). Finally, P. Kiss and B. M. Phong [4] proved that for any integers $a, k>1$ there exist infinitely many composite integers n for which (1) holds.

Recently, W. L. McDaniel [7, 8] and B. M. Phong [2] investigated the composite solutions n of the congruence

$$a^{n-k} \equiv b^{n-k} \pmod{n}, \tag{2}$$

where a, b and k are fixed positive integers. Their result shows that if $(a, b, k) \neq (2^s+1, 2^s-1, 3)$ for $s \geqq 2$ or either of $(c+1, c, 2)$ and $(c+3, c, 2)$ for $c \geqq 2$, then the congruence (2) also has infinitely many composite solutions n. In [9] W. L. McDaniel proved that there exist infinitely many triples (a, b, k) of each of the form $(2^s+1, 2^s-1, 3)$, $(c+1, c, 2)$ and $(c+3, c, 2)$ such that (2) has an infinitude of composite solutions.

In [2] B. M. Phong also studied a similar problem for Lucas and Lehmer sequences. Let A, B and D be integers such that $A^2-4B=D \neq 0$. A Lucas sequence $R=R(A, B)=\{R_n\}_{n=0}^{\infty}$ is defined by the initial terms $R_0=0$, $R_1=1$ and by the recursion $R_n=AR_{n-1}-BR_{n-2}$ for $n \geqq 2$. It is well-known that $R_n(A, B)=R_n=(\alpha^n-\beta^n)/(\alpha-\beta)$ for $n \geqq 0$, where α and β are distinct roots of the characteristic polynomial x^2-Ax+B of the sequence $R(A, B)$. In the following we say that $R(A, B)$ is a non-degenerate sequence if $(A, B)=1$ and α/β is not a root of unity.

Let $R=R(A, B)$ be a non-degenerate Lucas sequence. A composite solution n of the congruence

$$R_{n-k(D/n)}(A, B) \equiv 0 \pmod{n} \tag{3}$$

with $(n, 2BD)=1$ is called a Lucas pseudoprime with parameters A and B if $k=1$, where $D=A^2-4B$ and (D/n) denotes the Jacobi symbol.

It is well-known that infinitely many Lucas pseudoprimes with parameters A and B exist for all non-degenerate Lucas sequences $R(A, B)$. By Theorem 3 of

B. M. Phong [2] it follows that for any given non-degenerate Lucas sequence $R(A, B)$ there is a positive constant $k_0=k_0(A, B)$ such that for any integer $k>k_0$ the congruence (3) has infinitely many composite solutions n, furthermore if $k\geqq 2$ and $(k, B)=1$ then the congruence

$$R_{n-k} \equiv 0 \pmod{n} \tag{4}$$

also has an infinitude of composite solutions n. On the other hand, R. Baillie and S. S. Wagtaff, Jr. [1] proved that for any given integer D, any positive integer n with $(n, 2D)=1$ there exist exactly

$$\prod_{p|n} \{(n-(D/n), p-(D/p))-1\} \tag{5}$$

distinct values of A modulo n, for which there is an integer B such that $A^2-4B\equiv \equiv D \pmod{n}$ and

$$R_{n-(D/n)}(A, B) \equiv 0 \pmod{n}.$$

For any positive integer n we define n^* as follows:

$$1^* := 1 \quad \text{and} \quad n^* := n/\prod_{p|n} p \quad \text{if} \quad n>1,$$

where p runs through all primes divisors of n. Recently, I. Joó [3] proved that for any given positive integers n and k there exist

$$(n^*, k) \prod_{p|n} (n-k, p-1) \tag{6}$$

distinct values of a modulo n, for which the congruence (1) holds, furthermore the number of distinct pairs (a, b) is also given in [3], when $a-b=t$ is a given integer, satisfying (2).

The aim of the present paper is to extend some results mentioned above for the congruence (3). We shall use the following notation. If n is a positive integer we define n^* as above. For given integer $D\neq 0$ and for any positive integers n, k with $(n, 2D)=1$, we put

$$\delta_k(n) = n-k(D/n).$$

We shall prove the following two theorems.

THEOREM 1. *For any given non-zero integer D and positive integers n, k with $(n, 2D)=1$ and $n\geqq k$ there exist exactly*

$$(n^*, k) \prod_{p|n} \{(\delta_k(n), \delta_1(p))-1\} \tag{7}$$

distinct values of A modulo n, for which there is an integer B such that $A^2-4B\equiv \equiv D \pmod{n}$ and (3) holds.

THEOREM 2. *For any given non-zero integer D and positive integer $k\neq 2$, there exist infinitely many prime p and for each of them there are infinitely many non-degenerate Lucas sequences $R(A, B)$ such that the congruence (3) has an infinitude of composite solutions n and $A^2-4B\equiv D \pmod{p}$.*