Functiones et Approximatio
XXVIII (2000), 97–104

To Professor Włodzimierz Staś on the occasion of his 75-th birthday

LUCAS PSEUDOPRIMES

ANDRZEJ ROTKIEWICZ

Abstract: Theorem on four types of pseudoprimes with respect to Lucas sequences are proved. If n is an Euler-Lucas pseudoprime with parameters P and Q and n is an Euler pseudoprime to base Q, $(n, P) = 1$, then n is Lucas pseudoprime of four kinds.

Let U_n be a nondegenerate Lucas sequence with parameters P and $Q = \pm 1$, $\varepsilon = \pm 1$. Then, every arithmetic progression $ax + b$, where $(a, b) = 1$ which contains an odd integer n_0 with the Jacobi symbol $\left(\frac{D}{n_0}\right)$ equal to ε, contains infinitely many strong Lucas pseudoprimes n with parameters P and $Q = \pm 1$ such that $\left(\frac{D}{n}\right) = \varepsilon$ which are at the same time Lucas pseudoprimes of each of the four types.

Keywords: Pseudoprime, Dickson pseudoprime, Lucas pseudoprime, Euler pseudoprime, Lucas sequence

A *pseudoprime* to base a is a composite n such that $a^{n-1} \equiv 1 \bmod n$.

An odd composite number n is an *Euler pseudoprime* to base c if $(c, n) = 1$ and $c^{(n-1)/2} \equiv \left(\frac{c}{n}\right) \bmod n$, where $\left(\frac{c}{n}\right)$ is the Jacobi symbol.

Let D, P and Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$. The Lucas sequences U_k and V_k are defined recursively for $k \geq 2$ by

$$U_k = PU_{k-1} - QU_{k-2}, \qquad V_k = PV_{k-1} - QV_{k-2}.$$

For $k \geq 0$, we also have

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad V_k = \alpha^k + \beta^k,$$

where α and β are distinct roots of $x^2 - Px + Q = 0$.

We shall consider non-degenerate Lucas sequences, i.e. $U_k \neq 0$ if $k \geq 1$ (i.e. α/β is not a root of unity which is equivalent with $D = P^2 - 4Q \neq 0, -2Q, -3Q$).

For an odd prime n with $(n, QD) = 1$ we have (cf. [2], [7]):

$$U_{n-\left(\frac{D}{n}\right)}(P, Q) \equiv 0 \bmod n, \tag{1}$$

2000 Mathematics Subject Classification: primary 11A07; secondary 11B39.

$$U_n(P,Q) \equiv \left(\frac{D}{n}\right) \bmod n, \tag{2}$$

$$V_n(P,Q) \equiv P \bmod n, \tag{3}$$

$$V_{n-(\frac{D}{n})} \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n. \tag{4}$$

For every positive integer n the congruences (1), (2) and (3) are linearly dependent mod$n$:

We have

$$AU_{n-(\frac{D}{n})} + B\left(U_n - \left(\frac{D}{n}\right)\right) + C(V_n - V_1) = 0 \tag{5}$$

in which

$$A = 2\alpha\beta, \quad B = -(\alpha+\beta), \quad C = 1 \qquad \text{for } \left(\frac{D}{n}\right) = 1$$

and

$$A = -2, \quad B = \alpha+\beta, \quad C = 1 \qquad \text{for } \left(\frac{D}{n}\right) = -1.$$

Thus if $(n, 2PQD) = 1$ any two of the congruences (1), (2), (3) imply the other one.

Now we shall prove the following

Proposition P. *The natural number n, where $(n, 2QD) = 1$ satisfies (1), (2), (3) and (4) if and only if either*

$$\left(\frac{D}{n}\right) = 1, \quad \alpha^n \equiv \alpha \bmod n \quad \textit{and} \quad \beta^n \equiv \beta \bmod n$$

or

$$\left(\frac{D}{n}\right) = -1, \quad \alpha^n \equiv \beta \bmod n \quad \textit{and} \quad \beta^n \equiv \alpha \bmod n.$$

Proof. Let $(\frac{D}{n}) = 1$, $(n, 2QD) = 1$, $\alpha^n \equiv \alpha \bmod n$, $\beta^n \equiv \beta \bmod n$, then $\alpha^{n-1} - \beta^{n-1} \equiv 0 \bmod n$ and $U_{n-1} \equiv 0 \bmod n$, $\alpha^n - \beta^n \equiv \alpha - \beta \bmod n$, hence $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv 1 \bmod n$, $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv (\frac{D}{n}) \bmod n$; $\alpha^n + \beta^n \equiv \alpha + \beta \bmod n$, $V_n \equiv P \bmod n$; $\alpha^{n-1} + \beta^{n-1} \equiv 1 + 1 \equiv 2 \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$, $V_{n-(\frac{D}{n})} \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$.

If $(\frac{D}{n}) = -1$, $(n, QD) = 1$, $\alpha^n \equiv \beta \bmod n$ and $\beta^n \equiv \alpha \bmod n$, then $\alpha^{n+1} \equiv \alpha\beta \bmod n$, $\beta^{n+1} \equiv \alpha\beta \bmod n$, hence $(\alpha^{n+1} - \beta^{n+1})/(\alpha - \beta) \equiv 0 \bmod n$, $U_{n-(\frac{D}{n})} \equiv 0 \bmod n$; $\alpha^n - \beta^n \equiv \beta - \alpha \bmod n$, hence $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv -1 \equiv (\frac{D}{n}) \bmod n$, $U_n \equiv (\frac{D}{n}) \bmod n$; $\alpha^n + \beta^n \equiv \beta + \alpha \bmod n$, $V_n \equiv P \bmod n$; $\alpha^{n+1} + \beta^{n+1} \equiv \beta\alpha + \alpha\beta \equiv 2\alpha\beta \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$, $V_{n-(\frac{D}{n})} \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$.

Conversely, if n, where $(n, 2QD) = 1$, satisfies the congruences (2) and (3) then for $\left(\frac{D}{n}\right) = 1$ we have $\alpha^n + \beta^n \equiv \alpha + \beta \bmod n$, $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv 1 \bmod n$, hence $\alpha^n + \beta^n \equiv \alpha + \beta \bmod n$, $\alpha^n - \beta^n \equiv \alpha - \beta \bmod n$, $2\alpha^n \equiv 2\alpha \bmod n$, $2\beta^n \equiv 2\beta \bmod n$ and since $(n, 2QD) = 1$ we have $\alpha^n \equiv \alpha \bmod n$, $\beta^n \equiv \beta \bmod n$.

If n, where $(n, 2QD) = 1$, satisfies the congruences (2) and (3) then for $\left(\frac{D}{n}\right) = -1$ we have $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv -1 \bmod n$, $\alpha^n + \beta^n \equiv \alpha + \beta \bmod n$, hence $\alpha^n - \beta^n \equiv \beta - \alpha \bmod n$, $\alpha^n + \beta^n \equiv \beta + \alpha \bmod n$, $2\alpha^n \equiv 2\beta \bmod n$, $2\beta^n \equiv 2\alpha \bmod n$ and since $(n, 2QD) = 1$ we have $\alpha^n \equiv \beta \bmod n$, $\beta^n \equiv \alpha \bmod n$. ∎

A composite n is called a *Lucas pseudoprime with parameters P and Q* if $(n, 2QD) = 1$ and (1) holds.

Many results have been published about these numbers (see [1], [2], [3], [4], [6], [7], [8], [9], [10], [11], [12], [13]).

Simple examples show that a composite n satisfying one of the congruences (1), (2), (3), (4) does not necessarily satisfy the others. It is easy to check that the number $323 = 17 \cdot 19$ is a Lucas pseudoprime with parameters $P = 1$, $Q = -1$ but does not satisfy the congruences (2), (3) and (4). Hence three other kinds of pseudoprimes can be distinguished (see [2]).

A composite n such that the congruence (3) holds are called *Dickson pseudoprime* with parameters *P and Q* (see [5], [6]).

A composite number n such that the congruence (2) holds are called *Lucas pseudoprime of the second kind with parameters P* and Q.

Yorinaga (see [14]) proved that there exist infinitely many *Lucas pseudoprimes of the second kind with parameters $P = 1$, $Q = -1$*. He also published (see [14]) a table of all 109 such numbers n up to 707000. The least such number is $n = 4181 = 37 \cdot 113$. The number 4181 is also the least composite number n which satisfies all congruences (1), (2), (3) and (4) for $P = 1$, $Q = -1$.

A composite number n which satisfies the congruence (4) is called *Dickson pseudoprime of the second kind with parameters P and Q*.

Remark. If D is a square and n is a Carmichael number with $(n, QD) = 1$ then all congruences (1), (2), (3) and (4) hold. Indeed, if D is a square $(n, QD) = 1$ and n is a Carmichael number then α and β are rational integers $\neq 0$, $\left(\frac{D}{n}\right) = 1$ and $(\alpha^{n-1} - \beta^{n-1})/(\alpha - \beta) \equiv 0 \bmod n$; $(\alpha^n - \beta^n)/(\alpha - \beta) \equiv (\alpha - \beta)/(\alpha - \beta) \equiv 1 \equiv \left(\frac{D}{n}\right) \bmod n$; $\alpha^n + \beta^n \equiv \alpha + \beta \bmod n$ and $\alpha^{n-1} + \beta^{n-1} \equiv 2 \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n$.

In 1994 Alford, Granville & Pomerance (see [1]) proved that there are infinitely many Carmichael numbers.

If D is a square, $\alpha > 1$ is a positive integer, $\beta = \pm 1$ that is $P = \alpha \pm 1$, $Q = \pm\alpha$, $(n, 2QD) = 1$ and n is a Lucas pseudoprime with parameters P and Q then $\alpha^n \equiv \alpha \bmod n$, $\beta^n = (\pm 1)^n \equiv \pm 1 \bmod n$ and by proposition P the number n satisfies all congruences (1), (2), (3) and (4).

The following problems arise

Problem 1. *Let D be a square, P and Q be given integers, $\langle P, Q\rangle \neq \langle \alpha \pm 1, \pm\alpha\rangle$ i.e. $\beta \neq \pm 1$.*

Do there exist in every arithmetic progression $ax + b$, where $(a, b) = 1$, *infinitely many*

a) *Lucas pseudoprimes of the second kind with parameters* P *and* Q*?*
b) *Dickson pseudoprimes with parameters* P *and* Q*?*
c) *Dickson pseudoprimes of the second kind with parameters* P *and* Q*?*

For example: do there exist infinitely many composite n *such that* $3^n+2^n \equiv 5 \bmod n$ *in every arithmetic progression* $ax+b$*, where* $(a,b)=1$*?*

Problem 2. *Given integers* $P, Q \neq \pm 1$ *with* $D = P^2 - 4Q$ *not a square, do there exist infinitely many*

a') *Lucas pseudoprimes of the second kind with parameters* P *and* Q*?*
b') *Dickson pseudoprimes with parameters* P *and* Q*?*
c') *Dickson pseudoprimes of the second kind with parameters* P *and* Q*?*
d') *Arithmetic progressions formed from three different Dickson pseudoprimes?*

Problem 3. *Find a composite* n *with* $(\frac{D}{n}) = -1$, $(n, 2PQD) = 1$, $Q \neq \pm 1$ *which satisfies all congruences* (1), (2), (3) *and* (4). *Do there exist infinitely many such composite* n*?*

An odd composite n is an *Euler-Lucas pseudoprime with parameters* P and Q (see [11]) and

$$U_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n \quad \text{if} \quad \left(\frac{Q}{n}\right) = 1$$

or

$$V_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n \quad \text{if} \quad \left(\frac{Q}{n}\right) = -1.$$

We shall prove the following

Theorem 1. *If* n *is an Euler-Lucas pseudoprime with parameters* P *and* Q *and* n *is an Euler pseudoprime to base* Q, $(n,P)=1$, *then* n *satisfies all congruences* (1), (2), (3) *and* (4).

Proof. We have (see [10])

$$V_n - Q^{(n-1)/2}P = DU_{(n-1)/2}U_{(n+1)/2} \tag{6}$$

$$V_n + Q^{(n-1)/2}P = V_{(n-1)/2}V_{(n+1)/2}. \tag{7}$$

Since n is an Euler-Lucas pseudoprime with parameters P and Q we have

$$U_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n \quad \text{if} \quad \left(\frac{Q}{n}\right) = 1 \tag{8}$$

$$V_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n \quad \text{if} \quad \left(\frac{Q}{n}\right) = -1. \tag{9}$$

Let $(\frac{Q}{n}) = 1$. Since n is an Euler pseudoprime to base Q we have $Q^{(n-1)/2} \equiv (\frac{Q}{n}) \equiv 1 \bmod n$.

By (8) we have $U_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n$, hence

$$DU_{(n-1)/2}U_{(n+1)/2} \equiv 0 \bmod n,$$

and from (6) we get

$$V_n - Q^{(n-1)/2}P \equiv 0 \bmod n \quad \text{and since} \quad Q^{(n-1)/2} \equiv 1 \bmod n$$

we have $V_n \equiv P \bmod n$ and n is a Dickson pseudoprime with parameters P and Q, and since n satisfies the congruence (1) and (3), $(n, 2PQD) = 1$, hence n satisfies all congruences (1), (2), (3) and (4).

If $(\frac{Q}{n}) = -1$, then since n is an Euler pseudoprime to base Q, we have $V_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n$, hence

$$V_{(n-1)/2} \cdot V_{(n+1)/2} \equiv 0 \bmod n.$$

Since $Q^{(n-1)/2} \equiv -1 \bmod n$, be (7) we have $V_n + (-1)P \equiv 0 \bmod n$ and $V_n \equiv P \bmod n$ and n is a Dickson pseudoprime with parameters P and Q, and since n satisfies the congruence (1) and (3), hence n satisfies all congruences (1), (2), (3) and (4). ■

Theorem 2. *If n is an Euler-Lucas pseudoprime with parameters P and Q, $(n, 2PQD) = 1$ and n is a Dickson pseudoprime with parameters P and Q, then n is an Euler pseudoprime to base Q.*

Proof. Suppose that n is an Euler-Lucas pseudoprime with parameters P and Q.

Let $(\frac{Q}{n}) = 1$ then by (8), $U_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n$, hence by (6), $V_n - Q^{(n-1)/2}P \equiv 0 \bmod n$ and $V_n \equiv Q^{(n-1)/2}P \bmod n$. Since n is a Dickson pseudoprime with parameters and Q we have $V_n \equiv P \bmod n$. Thus $Q^{(n-1)/2}P \equiv P \bmod n$ and since $(n, P) = 1$ we have $Q^{(n-1)/2} \equiv 1 \equiv (\frac{Q}{n}) \bmod n$.

Since n is a Dickson pseudoprime with parameters P and Q we have $V_n \equiv P \bmod n$. Thus $Q^{(n-1)/2}P \equiv P \bmod n$ and since $(n, P) = 1$ we have $Q^{(n-1)/2} \equiv 1 \equiv (\frac{Q}{n}) \bmod n$.

If $(\frac{Q}{n}) = -1$ then by (9) we have $V_{(n-(\frac{D}{n}))/2} \equiv 0 \bmod n$, hence $V_{(n-1)/2}V_{(n+1)/2} \equiv 0 \bmod n$ hence by (7), $V_n \equiv -Q^{(n-1)/2}P \bmod n$.

Since n is a Dickson pseudoprime with parameters P and Q we have $V_n \equiv P \bmod n$. Thus $-Q^{(n-1)/2}P \equiv P \bmod n$ and since $(n, P) = 1$ we have $Q^{(n-1)/2} \equiv -1 \equiv (\frac{Q}{n}) \bmod n$ and in the both cases we have $Q^{(n-1)/2} \equiv (\frac{Q}{n}) \bmod n$ and n is an Euler pseudoprime to base Q. ■

R. Baillie and S. S. Wagstaff (see [2], Theorem 5) proved the following theorem:

Suppose $(n, 2QD) = 1$, $U_n \equiv (\frac{D}{n}) \bmod n$, and n is an Lucas pseudoprime with parameters P and Q.

If n is an Euler pseudoprime to base Q, then n is an Euler-Lucas pseudoprime with parameters P and Q.

Now we shall prove the following theorem

Theorem 3. *If a square-free number n is a Dickson pseudoprime of the second kind with parameters P and Q, and n is an Euler pseudoprime to base Q, then n is an Euler-Lucas pseudoprime with parameters P and Q.*

Proof. If n is a Dickson pseudoprime of the second kind with parameters P and Q, then
$$\alpha^{n-(\frac{D}{n})} + \beta^{n-(\frac{D}{n})} \equiv 2Q^{(1-(\frac{D}{n}))/2} \bmod n.$$

We consider four cases.

a) If $(\frac{D}{n}) = 1$, $(\frac{Q}{n}) = 1$, then

$$\alpha^{n-1} + \beta^{n-1} \equiv 2 \bmod n,$$
$$D\left(\frac{\alpha^{(n-1)/2} - \beta^{(n-1)/2}}{\alpha - \beta}\right)^2 + 2(\alpha\beta)^{(n-1)/2} \equiv 2 \bmod n$$

and since n is an Euler pseudoprime to base Q, $Q^{(n-1)/2} \equiv (\frac{Q}{n}) \equiv 1 \bmod n$, $2(\alpha\beta)^{(n-1)/2} \equiv 2 \bmod n$.

Thus since n is squarefree and $(n, D) = 1$, from $n \mid D\left(\frac{\alpha^{(n-1)/2}-\beta^{(n-1)/2}}{\alpha-\beta}\right)^2$ we get $n \mid U_{(n-1)/2} = U_{(n-(\frac{D}{n}))/2}$, $(\frac{Q}{n}) = 1$ and n is an Euler-Lucas pseudoprime with parameters P and Q.

b) If $(\frac{D}{n}) = 1$, $(\frac{Q}{n}) = -1$, then

$$\alpha^{n-1} + \beta^{n-1} \equiv 2 \bmod n,$$
$$(\alpha\beta)^{(n-1)/2} \equiv \left(\frac{Q}{n}\right) \equiv -1 \bmod n,$$

$(\alpha^{(n-1)/2} + \beta^{(n-1)/2})^2 - 2(\alpha\beta)^{(n-1)/2} \equiv 2 \bmod n$ and since n is an Euler pseudoprime to base Q, $Q^{(n-1)/2} \equiv (\frac{Q}{n}) \equiv -1 \bmod n$, hence $-2(\alpha\beta)^{(n-1)/2} \equiv 2 \bmod n$.

Thus since n is squarefree from $n \mid \left(\alpha^{n-1)/2} + \beta^{(n-1)/2}\right)^2$ we get that $n \mid \alpha^{(n-1)/2} + \beta^{(n-1)/2}$, $(\frac{Q}{n}) = -1$ and n is an Euler-Lucas pseudoprime with parameters P and Q.

c) If $(\frac{D}{n}) = -1$, $(\frac{Q}{n}) = 1$, then

$$\alpha^{n+1} + \beta^{n+1} \equiv 2 \bmod n,$$
$$D\left(\frac{\alpha^{(n+1)/2} - \beta^{(n+1)/2}}{\alpha - \beta}\right)^2 + 2(\alpha\beta)^{(n+1)/2} \equiv 2\alpha\beta \bmod n$$

and since n is an Euler pseudoprime to base Q, $(\frac{Q}{n}) = 1$ we have $Q^{(n-1)/2} \equiv (\frac{Q}{n}) \equiv 1 \bmod n$, hence $2(\alpha\beta)^{(n+1)/2} \equiv 2\alpha\beta \bmod n$.

Thus since n is squarefree $(D, n) = 1$, $n \mid D\left(\frac{\alpha^{(n+1)/2}-\beta^{(n+1)/2}}{\alpha-\beta}\right)^2$ we get $n \mid U_{(n+1)/2} = U_{(n-(\frac{D}{n}))/2}$, $(\frac{Q}{n}) = 1$ and n is an Euler-Lucas pseudoprime with parameters P and Q.

d) If $\left(\frac{D}{n}\right) = -1$, $\left(\frac{Q}{n}\right) = -1$, then

$$\alpha^{n+1} + \beta^{n+1} \equiv 2\alpha\beta \bmod n,$$
$$\left(\alpha^{(n+1)/2} + \beta^{(n+1)/2}\right)^2 - 2(\alpha\beta)^{(n+1)/2} \equiv 2\alpha\beta \bmod n.$$

Since n is an Euler pseudoprime to base Q with $\left(\frac{Q}{n}\right) = -1$ we have $(\alpha\beta)^{(n-1)/2} \equiv -1 \bmod n$, hence $-2(\alpha\beta)^{(n+1)/2} \equiv 2\alpha\beta \bmod n$.

Thus since n is squarefree from $n \mid \left(\alpha^{(n+1)/2} + \beta^{(n+1)/2}\right)^2$ we get $n \mid \alpha^{(n+1)/2} + \beta^{(n-(\frac{D}{n}))/2} = V_{(n-(\frac{D}{n}))/2}$, $\left(\frac{Q}{n}\right) = -1$ and n is an Euler-Lucas pseudoprime with parameters P and Q. ∎

A composite n is called *a strong Lucas pseudoprime with parameters P and Q* (see [11]) if $(n, 2QD) = 1$, $n - \left(\frac{D}{n}\right) = 2^s \cdot r$, r odd and either

$$U_r \equiv 0 \bmod n \quad \text{or} \quad V_{2^t r} \equiv 0 \bmod n \quad \text{for some } t,\ 0 \le t < s. \tag{10}$$

In the joint paper [13] with A. Schinzel we proved the following theorem T.

Theorem T. *Given integers P, Q with $D = P^2 - 4Q \neq 0, -Q, -2Q, -3Q$ and $\varepsilon = \pm 1$, every arithmetic progression $ax + b$, where $(a, b) = 1$ which contains an odd integer n_0 with $\left(\frac{D}{n_0}\right) = \varepsilon$ contains infinitely many strong Lucas pseudoprimes n with parameters P and Q such that $\left(\frac{D}{n}\right) = \varepsilon$. The number $N(X)$ of such strong pseudoprimes not exceeding X satisfies*

$$N(X) > c(P, Q, a, b, \varepsilon)\frac{\log X}{\log\log X},$$

where $c(P, Q, a, b, \varepsilon)$ is a positive constant depending on P, Q, a, b, ε.

Every strong Lucas pseudoprime with parameters P and Q is an Euler-Lucas pseudoprime with parameters P and Q (see [2]) and $Q^{(n-1)/2} \equiv \left(\frac{Q}{n}\right) \bmod n$ for n odd and $Q = 1$, or $Q = -1$, thus from theorem 1 and theorem T it follows the following

Theorem 4. *Let U_n be a nondegenerate Lucas sequence with parameters P and $Q = \pm 1$. Then, every arithmetic progression $ax + b$, where $(a, b) = 1$ which contains an odd integer n_0 with $\left(\frac{D}{n_0}\right) = \varepsilon$ contains infinitely many strong Lucas pseudoprimes n with parameters P and $Q = \pm 1$ such that $\left(\frac{D}{n}\right) = \varepsilon$, which satisfy congruences (1), (2), (3) and (4) simultaneously and the number $N(X)$ of strong pseudoprimes not exceeding X satisfies*

$$N(X) > c(P, a, b)\frac{\log X}{\log\log X},$$

where $c(P, a, b)$ is a positive constant depending on P, a, b.

The above theorem extends the theorem 2 of my paper [10] that if a and b are fixed coprime positive integers, $Q = \pm 1$, $(P, Q) \neq (1, 1)$, $D = P^2 - 4Q$

then in every arithmetic progression $ax + b$ there exist infinitely many composite n such that we have simultaneously

$$U_{n-\left(\frac{D}{n}\right)} \equiv 0 \bmod n, \quad U_n \equiv \left(\frac{D}{n}\right) \bmod n, \quad V_n \equiv V_1 \bmod n.$$

References

[1] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **140** (1994), 703–722.

[2] R. Baillie & S. Wagstaff Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417.

[3] H. J. A. Duparc, *On almost primes of the second order*, Math. Centrum Amsterdam. Rap. ZW 1955-013, (1955), 1-13 .

[4] E. Lieuwens, *Fermat Pseudo-Primes*, Ph.D. Thesis, Delft 1971.

[5] Siguna M. S. Müller, *Pseudoprimes & Primality Testing Based on Lucas Functions*, Ph.D. Thesis, Klagenfurt, 1996.

[6] W. B. Müller and A. Oswald, *Generalized Fibonacci pseudoprimes and probable primes*, Application of Fibonacci Numbers **5** (1993), 459–464.

[7] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York – Heidelberg – Berlin, 1996.

[8] A. Rotkiewicz, *Sur les nombres composés tels que* $n \mid 2^n - 2$ *et* $n \nmid 3^n - 3$, Bull. Soc. Math. Phys. Serbie **15** (1963), 7-11.

[9] A. Rotkiewicz, *Pseudoprime numbers and their generalizations*, Student Association of the Faculty of Sciences, University of Novi Sad, Novi Sad 1972, pp. i+169.

[10] A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequences*, Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys. **21** (1978), 793–797.

[11] A. Rotkiewicz, *On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters* L, Q *in arithmetic progression*, Math. Comp. **39** (1982), 239–247.

[12] A. Rotkiewicz, *On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. **68** (1994), 145–151.

[13] A. Rotkiewicz and A. Schinzel, *On Lucas pseudoprimes with a prescribed value of the Jacobi symbol*, Bull. Polish Acad. Sci. Math. **48** (2000), 77–80.

[14] M. Yorinaga, *On a congruential property of Fibonacci numbers. Numerical experiments. Considerations and Remarks*, Math. J. Okayama Univ., **19** (1976), 5–10, 11–17.

Address: Institute of Mathematics, Polish Academy of Sciences, ul. Śniadeckich 8, skr. poczt. 137, 00-950 Warszawa, Poland
E-mail: rotkiewi@impan.gov.pl
Received: 21 December 1999