LUCAS AND FROBENIUS PSEUDOPRIMES

ANDRZEJ ROTKIEWICZ

Abstract. We define several types of Lucas and Frobenius pseudoprimes and prove some theorems on these pseudoprimes. In particular: There exist infinitely many arithmetic progressions formed by three different Frobenius–Fibonacci pseudoprimes.

There are composite numbers, which behave in certain situation as they would be primes. The classical examples are pseudoprimes, which satisfy Fermat's congruence $a^{n-1} \equiv 1 \mod n$, where $(a, n) = 1$. Such numbers n are called pseudoprimes to base a.

The pseudoprimes are not just a curiosity, they are of considerable importance in factoring large integers and in deciding primality of large integers.

Applications of pseudoprimes to cryptography and computing have given pseudoprimes a more practical turn.

Several tests for primality involve recurrence sequences. For example, if we define the Fibonacci numbers by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$, then $F_{p-(5/p)} \equiv 0 \mod p$ if p is a prime and $(5/p)$ is the Legendre symbol.

A composite n is called a Fibonacci pseudoprime if $F_{n-(5/n)} \equiv 0 \mod n$, where n is composite and $(5/n)$ is the Jacobi symbol.

One reason that pseudoprimes based on recurrence sequences have attracted interest is that the pseudoprime for these sequences are often different from ordinary pseudoprimes.

In fact, nobody has applied for the \$620 offered for a Fibonacci pseudoprime n with $(5/n) = -1$, that is also a pseudoprime to the base 2 (Pomerance, Selfridge, Wagstaff [14], Guy [11]).

In 1909 Banachiewicz noted that all Fermat numbers $2^{2^n} + 1$ are primes or pseudoprimes to base 2 (see also Křižek, Luca and Somer [12]) and perhaps

Received: 18.06.2002. Revised: 17.02.2003.

this fact led Fermat to his false conjecture that all Fermat numbers are primes (Banachiewicz [2]).

Banachiewicz has tabulated all pseudoprimes below 2000 : $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $1387 = 19 \cdot 73$, $1729 = 7 \cdot 13 \cdot 19$, $1905 = 3 \cdot 5 \cdot 127$ (see Dickson [5, p. 94]).

P. Poulet [15] has tabulated all the odd pseudoprimes below 10^8 and C. Pomerance, J. L. Selfridge and S. S. Wagstaff Jr [14] have found them below $25 \cdot 10^9$.

In 2000 R. Pinch tabulated pseudoprimes to base 2 up to 10^{13}. There are 38975 such pseudoprimes up to 10^{11}, 101629 up to 10^{12} and 264239 up to 10^{13}.

The condition $2^{n-1} \equiv 1 \bmod n$ implies that n is odd.

If we replace this condition by the closely related $2^n \equiv 2 \bmod n$ then it is possible for n to be even. Let us call such a number an even pseudoprime. The first even pseudoprime is $161038 = 2 \cdot 73 \cdot 1103$ and it was found by D. H. Lehmer in 1950 (see Erdős [7]).

In 1951 N. G. Beeger proved that there exist infinitely many even pseudoprimes (see [3]).

In 1995 Rotkiewicz and Ziemak found 24 even pseudoprimes with $3, 4, 5, 6, 7$ and 8 prime factors (see [25]).

There are only 155 even pseudoprimes up to 10^{12} and 40 less than 10^{10}. These are listed in Pinch's paper in Table 9 of [13].

Recently Z. Zhang has tabulated all strong pseudoprimes $n < 10^{24}$ to the first ten primes bases $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$, which have the form $n = pq$ with p, q odd primes and $q - 1 = k(p - 1)$, $k = 2, 3, 4$. There are in total 44 such numbers (Zhang [27]).

Grantham introduced the definition of Frobenius pseudoprime to arbitrary monic polynomial in $\mathbb{Z}[x]$ (Grantham [9, 10], Crandall and Pomerance [4]).

We shall prove several theorems on Frobenius pseudoprimes for quadratic polynomials.

Let $P > 0$, Q be non-zero integers such that $D = P^2 - 4Q \neq 0$, $z^2 - Pz + Q = (z - \alpha)(z - \beta)$, $\alpha = \frac{P+\sqrt{D}}{2}$, $\beta = \frac{P-\sqrt{D}}{2}$.

DEFINITION 1. The sequences $u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ and $v_n(\alpha, \beta) = \alpha^n + \beta^n$ are called Lucas sequences with parameters P and Q.

The sequences u_n and v_n are defined recursively by $u_0 = 0$, $u_1 = 1$, $v_0 = 2$, $v_1 = P$ and $u_k = Pu_{k-1} - Qu_{k-2}$, $v_k = Pv_{k-1} - Qv_{k-2}$ for $k \geqslant 2$.

The sequences u_n and v_n are called non-degenerate if $\frac{\alpha}{\beta}$ is not a root of unity i.e. $P^2 \neq Q, 2Q, 3Q$. Then $|u_n|$, $|v_n|$ tend to infinity (as n tends to ∞).

DEFINITION 2 (Rotkiewicz [18, 19]). A composite number n is a Lucas pseudoprime with parameters P and Q if $(n, QD) = 1$ and

$$u_{n-(D/n)} \equiv 0 \bmod n, \text{ where } (D/n) \text{ is the Jacobi symbol.} \tag{1}$$

DEFINITION 3 (Rotkiewicz [23], see also Ribenboim [16]). A composite number n is a Lucas pseudoprime of the second kind with parameters P and Q if $(n, QD) = 1$ and

$$u_n \equiv (D/n) \bmod n. \tag{2}$$

DEFINITION 4 (Rotkiewicz [23]). A composite number n is a Dickson pseudoprime with parameters P and Q if

$$v_n \equiv P \bmod n. \tag{3}$$

DEFINITION 5 (Rotkiewicz [23]). A composite n is a Dickson pseudoprime of the second kind with parameters P and Q if $(n, QD) = 1$ and

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

In the special case $P = 1$, $Q = -1$ we call these numbers Fibonacci or Dickson–Fibonacci pseudoprimes.

It is easy to prove (Rotkiewicz [23]) the following

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

$$(D/n) = 1, \ \alpha^n \equiv \alpha \bmod n \text{ and } \beta^n \equiv \beta \bmod n$$

or

$$(D/n) = -1, \ \alpha^n \equiv \beta \bmod n \text{ and } \beta^n \equiv \alpha \bmod n.$$

Congruences (1), (2), (3) and (4) hold rarely when n is an odd composite number. Assuming $(n, 2PQD) = 1$, any two of the congruences imply the other two (Baillie and Wagstaff [1]).

By Fermat's theorem in $\mathbb{Q}(\sqrt{D})$: If p is an odd prime, $(p, 2QD) = 1$ then

$$\alpha^p \equiv \alpha \bmod p, \ \beta^p \equiv \beta \bmod p \quad \text{if } (D/p) = 1,$$

$$\alpha^p \equiv \beta \bmod p, \ \beta^p \equiv \alpha \bmod p \quad \text{if } (D/p) = -1,$$

where (D/p) is the Legendre symbol.

If $(p, 2QD) = 1$, $(D/p) = 1$ then $\alpha^p + \beta^p \equiv \alpha + \beta \bmod p$, $v_p \equiv P \bmod p$ and $\alpha^p - \beta^p \equiv \alpha - \beta \bmod p$, $\frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv 1 \equiv (D/p) \bmod p$, $u_p \equiv (D/p) \bmod p$.

For $(D/p) = -1$, $(p, 2QD) = 1$ we have $\alpha^p + \beta^p \equiv \beta + \alpha \bmod p$, $v_p \equiv P \bmod p$ and $\alpha^p - \beta^p \equiv \beta - \alpha \bmod p$, hence $\frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv -1 \equiv (D/p) \bmod p$, $u_p \equiv (D/p) \bmod p$.

It is easy to see that

$$2Q^{(1+(D/p))/2} v_{p-(D/p)} = Pv_p - (D/p)Du_p, \tag{5}$$

where p is a prime and $(p, 2QD) = 1$.

From the identity (5) and $v_p \equiv P \bmod p$, $u_p \equiv (D/p) \bmod p$ we get

$$2Q^{(1+(D/p))/2} v_{p-(D/p)} \equiv P^2 - (D/p)^2 (P^2 - 4Q) \equiv 4Q \bmod p,$$

hence

$$v_{p-(D/p)} \equiv 2Q^{(1-(D/p))/2} \bmod p.$$

Similarly, from the identity

$$2Q^{(1+(D/p))/2} u_{p-(D/p)} = Pu_p - (D/p)v_p, \tag{6}$$

where p is an odd prime and $(p, 2QD) = 1$ and from $u_p \equiv (D/p) \bmod p$, $v_p \equiv P \bmod p$ we get

$$2Q^{(1+(D/p))/2} u_{p-(D/p)} \equiv P(D/p) - P(D/p) \equiv 0 \bmod p,$$

hence $u_{p-(D/p)} \equiv 0 \bmod p$.

Thus if p is a prime and $(p, 2QD) = 1$ then all congruences (1), (2), (3) and (4) hold. Grantham [9, 10] gives the following proof of the congruence $u_{p-(D/p)} \equiv 0 \bmod p$ using the Frobenius automorphism which takes an element to its p-th power.

If $(D/p) = 1$ then $f(x) = x^2 - Px + Q$ factors mod p, and α and β are in a finite field $\mathbb{F}_p$ with p elements. Thus $\alpha^{p-1} \equiv \beta^{p-1} \equiv 1 \bmod p$. So $u_{p-1} \equiv (1-1)/(\alpha - \beta) = 0 \bmod p$. If $(D/p) = -1$, then $f(x)$ does not factor, and the roots of $f(x)$ lie in $\mathbb{F}_{p^2}$ with p^2 elements. The Frobenius automorphism permutes the roots of $f(x)$, so $\alpha^p \equiv \beta \bmod p$ and $\beta^p \equiv \alpha \bmod p$. Thus $u_{p+1} \equiv (\alpha\beta - \beta\alpha)/(\alpha - \beta) = 0 \bmod p$. □

DEFINITION 6 (Crandall and Pomerance [4, p. 133]). Let P, Q be integers with $D = P^2 - 4Q$ not a square. We say that a composite number n with $(n, 2QD) = 1$ is a Frobenius pseudoprime with respect to $f(x) = x^2 - Px + Q$ if

$$x^n \equiv \begin{cases} P - x \bmod (f(x), n) & \text{if } (D/n) = -1 \\ x \bmod (f(x), n) & \text{if } (D/n) = 1. \end{cases}$$

It is easy to give a criterion for a Frobenius pseudoprime with respect to a quadratic polynomial, in terms of the Lucas pseudoprimes and the Dickson pseudoprimes of the second kind.

THEOREM 0 (Crandall and Pomerance [4, p. 134]). *Let P, Q be integers with $D = P^2 - 4Q$ not a square and let n be a composite number with $(n, 2QD) = 1$. Then n is a Frobenius pseudoprime with respect to $x^2 - Px + Q$ (or Frobenius pseudoprime with parameters P and Q) if and only if*

$$u_{n-(D/n)} \equiv 0 \bmod n \quad \text{and} \quad v_{n-(D/n)} \equiv \begin{cases} 2Q \bmod n, & \text{when } (D/n) = -1 \\ 2 \bmod n, & \text{when } (D/n) = 1. \end{cases}$$

In other words:

A composite n is a Frobenius pseudoprime with respect to $x^2 - Px + Q$ if and only if n is a Lucas pseudoprime with parameters P and Q and a Dickson pseudoprime of the second kind with parameters P and Q.

DEFINITION 7 (Rotkiewicz [19]). An odd composite n is an Euler-Lucas pseudoprime with parameters P and Q if and only if $(n, QD) = 1$ and

$$u_{(n-(D/n))/2} \equiv 0 \bmod n \quad \text{if} \quad (Q/n) = 1,$$

or

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

DEFINITION 8. A Frobenius pseudoprime with parameters $P = 1$, $Q = -1$ is called a Frobenius–Fibonacci pseudoprime.

In [4, p. 134], [10, p. 22] and [11, p. 885] it is written that the first Frobenius–Fibonacci pseudoprime is $5777 = 53 \cdot 109$. It is not true, because the first Frobenius–Fibonacci pseudoprime is $n = 4181 = 37 \cdot 113$.

Let u_n be a non-degenarate Lucas sequence with parameters P and Q. The following theorems are known.

THEOREM 1 (Rotkiewicz [18, Theorem 1]). *Let $Q = \pm 1$. There exist infinitely many composite numbers $n = pq$, where p and q are different primes, which are Frobenius pseudoprimes with parameters P and $Q = \pm 1$.*

THEOREM 2 (Rotkiewicz [18, Theorem 2]). *Every arithmetical progression $ax + b$, where $(a, b) = 1$ contains infinitely many Frobenius pseudoprimes with parameters P and $Q = \pm 1$.*

THEOREM 3 (Rotkiewicz [17, Theorem 3]). *For every prime $p > n_0$, there exist infinitely many Lucas pseudoprimes with parameters P and Q which are divisible by p.*

Let u_n denote the n-th term of Fibonacci sequence, Yorinaga published in [26] a table of all 109 composite numbers n up to 707000 such that $u_n \equiv (n/5) \bmod n$. He called such numbers "converse numbers". From the table of Yorinaga we get 80 Fibonacci pseudoprimes of the second kind and 29 even converse numbers.

The table of Fibonacci pseudoprimes suggest the following questions:

1. Is it true that every square of a prime $\neq 2, 5$ is a Dickson–Fibonacci pseudoprime of the second kind? (Jerzy Browkin)
2. Is it true that every composite squarefree Dickson–Fibonacci pseudoprime of the second kind is a Frobenius pseudoprime? (Jerzy Browkin)
3. Do there exist infinitely many arithmetic progressions formed by three Frobenius–Fibonacci pseudoprimes?
4. Do there exist infinitely many Fibonacci pseudoprimes which are not Frobenius–Fibonacci pseudoprimes?
   The least such pseudoprime is $323 = 17 \cdot 19$.
5. Do there exist infinitely many Dickson–Fibonacci pseudoprimes of the second kind which are not Frobenius–Fibonacci pseudoprimes?
   The first such number is $n = 9$.
6. Do there exist infinitely many Dickson–Fibonacci pseudoprimes not divisible by 5 which are not Frobenius–Fibonacci pseudoprimes?
   The least such pseudoprime is $2737 = 7 \cdot 13 \cdot 23$.
7. Do there exist infinitely many Fibonacci pseudoprimes of the second kind which are not Frobenius–Fibonacci pseudoprimes?
   The least such pseudoprime is $6479 = 11 \cdot 19 \cdot 31$.

Now we shall prove that the answer for the first five questions is affirmative.

THEOREM 4. *The square of every prime $p \neq 2, 5$ and the square of every Fibonacci pseudoprime are Dickson–Fibonacci pseudoprimes of the second kind.*

PROOF. Let $n = p^2$, where p is a prime $\neq 2, 5$. From the formula

$$v_{4n} - 2 = 5\,(u_{2n})^2 \tag{7}$$

we get

$$v_{p^2-1} - 2 = v_{2\cdot\frac{(p-1)(p+1)}{2}} - 2 = 5\left(u_{\frac{(p-1)(p+1)}{2}}\right)^2. \tag{8}$$

From $p-(5/p) \mid \frac{(p-1)(p+1)}{2}$ we get $p^2 \mid \left(u_{\frac{(p-1)(p+1)}{2}}\right)^2$ and from (8) it follows that $v_{p^2-1} \equiv 2 \equiv 2(5/p^2) \bmod p^2$ and p^2 is a Dickson–Fibonacci pseudoprime of the second kind.

Also it is easy to see that $n = f^2$, where f denotes a Fibonacci pseudoprime is a Dickson–Fibonacci pseudoprime of the second kind. We have

$$v_{f^2-(5/f^2)} - 2 = v_{2\cdot\frac{(f-1)(f+1)}{2}} - 2 = 5\left(u_{\frac{(f-1)(f+1)}{2}}\right)^2$$

and

$$f \left| u_{f-(5/f)} \right| u_{\frac{(f-1)(f+1)}{2}}, \quad v_{f^2-1} - 2 \equiv 2(5/f^2) \bmod f^2,$$

and f^2 is a Dickson–Fibonacci pseudoprime of the second kind. □

REMARK. Since there is no prime number $p < 10^{13}$ such that $u_{p-(5/p)} \equiv 0 \bmod p^2$ (Dilcher [6]), there does not exist a Frobenius–Fibonacci pseudoprime of the form p^2 for $p < 10^{13}$.

THEOREM 5. *If n is a square-free Fibonacci–Dickson pseudoprime of the second kind then n is a Frobenius–Fibonacci pseudoprime.*

PROOF. By Theorem 3 from [23] 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 (that is $Q^{(n-1)/2} \equiv (Q/n) \bmod n$) then n is an Euler–Lucas pseudoprime with parameters P and Q.

In our case n is an Euler–Fibonacci pseudoprime and by Theorem 1 from [23] n is a Frobenius–Fibonacci pseudoprime. (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 a Frobenius–Lucas pseudoprime with parameters P and Q). □

THEOREM 6. *If p and $2p-1$ are primes of the form $30l+1$, $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$, then the numbers*

$$(9) \qquad \begin{aligned} a_1 &= \frac{\alpha^{(2p-1)p^m} - \beta^{(2p-1)p^m}}{\alpha^{p^m} - \beta^{p^m}}, \\ a_2 &= \frac{\alpha^{2p^{m+1}} - \beta^{2p^{m+1}}}{\alpha^{2p^m} - \beta^{2p^m}}, \\ a_3 &= \frac{\alpha^{(2p-1)p^m} + \beta^{(2p-1)p^m}}{\alpha^{p^m} + \beta^{p^m}} \end{aligned}$$

for $m = 1, 2, \ldots$ *form an arithmetic progression consisting of three Frobenius–Fibonacci pseudoprimes with Jacobi symbol* $(5/a_i) = 1$ *for* $i = 1, 2, 3$.

Since for example 31 and 61 are primes of the form $30l + 1$, from Theorem 6 it follows that:

There exist infinitely many arithmetic progressions formed by three different Frobenius–Fibonacci pseudoprimes: a_1, a_2, a_3 *with Jacobi symbol* $(5/a_i) = 1$ *for* $i = 1, 2, 3$.

PROOF OF THEOREM 6. First we shall prove that if $p = 6k + 1$ then $a_i \equiv 1 \bmod 4$ for $i = 1, 2, 3$.

We have $u_n \equiv 0, 1, 1, 2, 3, 1 \bmod 4$ for $n = 0, 1, 2, 3, 4, 5$ and the sequence $u_n \bmod 4$ has the period $(0, 1, 1, 2, 3, 1)$.

Also, we have $v_n \equiv 2, 1, 3, 0, 3, 3 \bmod 4$ for $n = 0, 1, 2, 3, 4, 5$ and the sequence $v_n \bmod 4$ has the period $(2, 1, 3, 0, 3, 3)$, hence $u_n, v_n \equiv 1 \bmod 4$ for $p = 6k + 1$ and

$$a_1 = \frac{u_{(2p-1)p^m}}{u_{p^m}} \equiv 1 \bmod 4, \quad a_2 = \frac{u_{p^{m+1}}}{u_{p^m}} \cdot \frac{v_{p^{m+1}}}{v_{p^m}} \equiv 1 \bmod 4,$$

$$a_3 = \frac{v_{(2p-1)p^m}}{v_{p^m}} \equiv 1 \bmod 4.$$

By formula (7) from [21] we have

$$2(2p-1)p^m \mid a_i - (5/a_i), \text{ where } (5/a_i) = 1, \ i = 1, 2, 3.$$

Thus

$$4(2p-1)p^{m+1} \mid a_i - 1 \text{ for } i = 1, 2, 3 \tag{11}$$

and

$$2(2p-1)p^m \left| \frac{a_1 - (5/a_1)}{2}, \ 2p^{m+1} \right| \frac{a_2 - (5/a_2)}{2}, \ 2(2p-1)p^m \left| \frac{a_3 - (5/a_3)}{2}, \right.$$

hence by Theorem 1 from [23], a_1, a_2, a_3 for $m = 1, 2, 3, \ldots$ form an arithmetic progression consisting of three Frobenius–Fibonacci pseudoprimes.

Let $\overline{k}$ denotes the square-free kernel of k, that is k divided by its greatest square.

THEOREM 7. *If* $P \equiv 1 \bmod 4$, $\alpha = \frac{P+\sqrt{D}}{2}$, $\beta = \frac{P-\sqrt{D}}{2}$, $D = P^2 - 4Q$, $Q = \pm 1$, $\overline{D}$ *denotes the square-free kernel of* D, $(P, Q) = 1$, $p > 3$ *and* $2p - 1$

are primes of the form $6\overline{D}p(\overline{D})x+1$, $(p(2p-1),PD)=1$, *then the numbers*

$$a_1=\frac{\alpha^{(2p-1)p^m}-\beta^{(2p-1)p^m}}{\alpha^{p^m}-\beta^{p^m}},$$

$$a_2=\frac{\alpha^{2p^{m+1}}-\beta^{2p^{m+1}}}{\alpha^{2p^m}-\beta^{2p^m}},$$

$$a_3=\frac{\alpha^{(2p-1)p^m}+\beta^{(2p-1)p^m}}{\alpha^{p^m}+\beta^{p^m}}$$

for $m=1,2,\ldots$ *form an arithmetical progression consisting of three Frobenius pseudoprimes with the Jacobi symbol* $(D/a_i)=1$, *and the numbers* a_1 *and* a_3 *have at least* $(m+1)$ *distinct prime factors, and the number* a_2 *has at least two distinct prime factors.*

PROOF. In the same way as in the proof of Theorem 6 we check that $a_i\equiv 1 \bmod 4$ and by the formula (8) from [22] we have

$$4p^{m+1}(2p-1)|a_i-(D/a_i)=a_i-1 \text{ for } i=1,2,3,$$

hence $2p^m(2p-1)\left|\frac{a_i-(D/a_i)}{2}\right.$, hence by Theorem 1 from [23] a_1, a_2, a_3 for $m=1,2,3,\ldots$ form an arithmetic progression consisting of three Frobenius pseudoprimes with parameters P and $Q=\pm 1$, such that a_1 and a_3 have at least $m+1$ distinct prime factors a_1 and a_2 has at least two distinct prime factors. □

THEOREM 8. *There exist infinitely many Fibonacci pseudoprimes which are Frobenius–Fibonacci pseudoprimes.*

1. *If* $p\equiv 1 \bmod 6$ *and* $p\equiv\pm 1 \bmod 5$ *then* u_{2p} *is a Fibonacci pseudoprime which is a Frobenius–Fibonacci pseudoprime.*
2. *If* $p\equiv 5 \bmod 6$ *and* $p>5$ *then* u_{2p} *is a Fibonacci pseudoprime which is not a Frobenius–Fibonacci pseudoprime.*

PROOF. Let $p\equiv 1 \bmod 6$, $p\equiv\pm 1 \bmod 5$. We have $u_{2p}=u_p\cdot v_p\geqslant u_7\cdot v_7=13\cdot 29=377$.

If $n=u_{2p}$, $p>5$ then $u_{2p}\equiv 1 \bmod 2$, $n=u_{2p}=u_p\cdot v_p\equiv(5/p) \bmod p$, $(5/u_{2p})=(5/p)$, $n-(5/n)\equiv 0 \bmod 2p$, hence $n=u_{2p}|u_{n-(5/n)}$ and n is a Fibonacci pseudoprime.

1. If $p\equiv 1 \bmod 6$ then $2p\equiv 2 \bmod 6$, hence $n=u_{2p}$, $u_{2p}\equiv 1 \bmod 4$. For $p\equiv\pm 1 \bmod 5$, $(5/n)=1$, $n|u_{(n-(5/n))/2}$, $(-1/n)=1$ and n is an Euler–Fibonacci pseudoprime, hence u_{2p} is a Frobenius–Fibonacci pseudoprime. For $p=19$ we have $u_{2p}=u_{38}=39088169=37\cdot 113\cdot 9349$ which is a Frobenius–Fibonacci pseudoprime.

2. If $p \equiv 5 \bmod 6$ and $p > 5$ then $2p \equiv 4 \bmod 6$, hence $u_{2p} \equiv 3 \bmod 4$. If $n = u_{2p}$ is a Dickson–Fibonacci pseudoprime then by the formula $v_n + (-1)^{\frac{n-1}{2}} = v_{\frac{n-1}{2}} \cdot v_{\frac{n+1}{2}}$ we have $u_p | u_{2p} = n | v_n - 1 = v_{\frac{n-1}{2}} \cdot v_{\frac{n+1}{2}}$, which is impossible since $(u_p, v_k) = 1$ for $p \geqslant 5$. Thus u_{2p} is not a Frobenius–Fibonacci pseudoprime. For $p = 17$ we get $u_{34} = 5702887 = 1597 \cdot 3571$ which is not a Frobenius–Fibonacci pseudoprime. □

THEOREM 9. *There exist infinitely many Dickson–Fibonacci pseudoprimes of the second kind which are not Frobenius–Fibonacci pseudoprimes.*

PROOF. Let $p = 5k \pm 1$ then $p | u_{p-(5/p)} = u_{p-1}$. Let $p^\alpha \| u_{p-1}$, $\alpha \geqslant 1$. We have $v_{4n} - 2 = 5(u_{2n})^2$, hence $v_{p^{2\alpha}-(5/p^{2\alpha})} - 2 = v_{p^{2\alpha}-1} - 2 = 5\left(\frac{u_{(p^\alpha-1)(p^\alpha+1)}}{2}\right)^2$. From $p^{2\alpha} \left| 5\left(\frac{u_{(p^\alpha-1)(p^\alpha+1)}}{2}\right)^2 \right.$ we get $v_{p^{2\alpha}-(5/p^{2\alpha})} \equiv 2 \equiv 2(5/p^{2\alpha}) \bmod p^{2\alpha}$ and $p^{2\alpha}$ is a Dickson–Fibonacci pseudoprime of the second kind. But from $p^\alpha \| u_{p-1}$ we get $p^\alpha \| u_{p^{2\alpha}-1}$, hence $p^{2\alpha} \not| u_{p^{2\alpha}-1}$ and $p^{2\alpha}$ is not a Fibonacci pseudoprime, hence $p^{2\alpha}$ is not a Frobenius–Fibonacci pseudoprime. □

By Theorem 4 from [23] the following theorem holds

Let u_n be a non-degenerate 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 $(D/n_0) = \varepsilon$, contains infinitely Frobenius-Lucas pseudoprimes such that $(D/n) = \varepsilon$.

DEFINITION 9. A composite number n is called a strong Lucas pseudoprime with parameters P and Q if $(n, 2QD) = 1$, $n - (D/n) = 2^s r$, r odd and

(12) either $u_r \equiv 0 \bmod n$ or $v_{2^t r} \equiv 0 \bmod n$ for some t, $0 \leqslant t < s$.

Erdős, Kiss and Sárközy [8] have shown that there are more than $e^{(\log x)^c}$ Lucas pseudoprimes up to x with coprime parameters P, Q, where $c > 0$ does not depend on P, Q and $x > x_0(P, Q)$.

In his recent dissertation on Frobenius pseudoprimes (Grantham [9]) has replaced $e^{(\log x)^c}$ by x^c and lifted the restriction $(P, Q) = 1$, however in both papers the Jacobi symbol is 1, not -1.

In this connection C. Pomerance put forward the following problem:

Given integers P, Q with $D = P^2 - 4Q$ not a square, do there exist infinitely many, or at least one, Lucas pseudoprimes n with parameters P and Q satisfying $(D/n) = -1$?

An affirmative answer to this problem in the strong sense (infinitely many) is given by the following theorem (Rotkiewicz and Schinzel [24]) which follows from the result by Rotkiewicz [20].

THEOREM. *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 $(D/n_0) = \varepsilon$, contains infinitely many strong Lucas pseudoprimes n with parameters P and Q such that $(D/n) = \varepsilon$. The number $\mathcal{N}(X)$ of such strong pseudoprimes n not exceeding X is at least equal to*

$$\frac{1 + o(1)}{3\varphi(a_1)\log(|\alpha| + |\beta|)} \frac{\log X}{\log\log X},$$

where a_1 is determined by a, b, P, Q.

TABLES prepared by Jerzy Browkin

The following tables contain pseudoprimes of different kinds below 10^6. More precisely,

Table 1 contains Fibonacci pseudoprimes.

Table 2 contains Fibonacci pseudoprimes of the second kind.

Table 3 contains Dickson–Fibonacci pseudoprimes not divisible by 5.

Table 4 contains Dickson–Fibonacci pseudoprimes of the second kind not divisible by 5, with squares of primes $\neq 2, 5$ omitted.

Table 5 contains Frobenius pseudoprimes (i.e. numbers appearing simultaneously in any two of the preceding tables).

Table 6 contains arithmetic progressions with terms belonging to Tables 1–5, respectively.

To present the contents of Table 1 we use the notation of J. Grantham [10].

Let n be a Fibonacci pseudoprime, denote $f(X) = X^2 - X - 1$, and let $X^n \equiv aX + b \bmod (f(X), n)$, where $a, b \in (-n/2, n/2)$.

It turns out that for $n < 10^6$ always $b = 0$ or $b = -a$, moreover $d := \gcd(n, a - 1) > 1$, provided $a \neq \pm 1$.

Thus if $d > 1$ then gcmd$(X^n - X, f(X))$ does not exist, and the Factorization Step fails.

All congruences below are modulo $(f(X), n)$.

If $b = 0$, then $f(X^n) \equiv f(aX) \equiv (a^2 - a)X + (a^2 - 1)$. Hence $f(X^n) \equiv 0$ iff $a = 1$.

If $b = -a$, then $f(X^n) \equiv f(a(X - 1)) \equiv -(a^2 + a)X + (2a^2 + a - 1)$. Hence $f(X^n) \equiv 0$ iff $a = -1$.

Thus the Frobenius Step fails iff $aX + b \neq X, 1 - X$.

Now, if $aX + b = X$, then $X^n - X \equiv 0$. Hence

$$F_1(X) = f(X), \qquad \text{and} \quad S = 0.$$

If $aX + b = 1 - X$, then $X^n - X \equiv -2X + 1$. Hence

$$F_1(X) = \operatorname{gcmd}(X^n - X, f(X)) = 1.$$

Since $X^n - X \equiv 1 - X$, and $f(1-X) = f(X)$, then $(1-X)^n \equiv 1-(1-X) = X$. Hence

$$X^{n^2} \equiv (1 - X)^n \equiv X, \qquad \text{thus} \quad F_2(X) = f(X), \quad \text{and} \quad S = 1.$$

In Table 1, for every Fibonacci pseudoprime $n < 10^6$ we give $aX + b$ and d, provided $|a| > 1$.

It is easy to verify (in Table 1) that for a Fibonacci pseudoprime $n < 10^6$ with $aX + b = X$ or $1 - X$, we have $(-1)^S = (5/n)$, i.e. the Jacobi Step always holds.

Therefore a Fibonacci pseudoprime $n < 10^6$ is a Frobenius pseudoprime iff $X^n \equiv X$ or $1 - X \mod (f(X), n)$.

Computations have been performed using the package GP/PARI, version 1.39.

Table 1

n	$ax + b$	d
$323 = 17 \cdot 19$	$x - 1$	
$377 = 13 \cdot 29$	$-144(x - 1)$	29
$1891 = 31 \cdot 61$	$-123x$	31
$3827 = 43 \cdot 89$	$-1334(x - 1)$	89
$4181 = 37 \cdot 113$	x	
$5777 = 53 \cdot 109$	$-x + 1$	
$6601 = 7 \cdot 23 \cdot 41$	$2092x$	41
$6721 = 11 \cdot 13 \cdot 47$	x	
$8149 = 29 \cdot 281$	$842x$	29
$10877 = 73 \cdot 149$	$-x + 1$	
$11663 = 107 \cdot 109$	$x - 1$	
$13201 = 43 \cdot 307$	x	
$13981 = 11 \cdot 31 \cdot 41$	$1024x$	$11 \cdot 31$
$15251 = 101 \cdot 151$	x	
$17119 = 17 \cdot 19 \cdot 53$	$4504x$	19
$17711 = 89 \cdot 199$	$-6765x$	199
$18407 = 79 \cdot 233$	$x - 1$	
$19043 = 137 \cdot 139$	$x - 1$	
$23407 = 89 \cdot 263$	$x - 1$	
$25877 = 113 \cdot 229$	$8474(x - 1)$	229
$27323 = 89 \cdot 307$	$-12281(x - 1)$	89

Table 1 (cont.)

n	$ax+b$	d
$30889 = 17 \cdot 23 \cdot 79$	$13431x$	$17 \cdot 79$
$34561 = 17 \cdot 19 \cdot 107$	x	
$34943 = 83 \cdot 421$	$x-1$	
$35207 = 17 \cdot 19 \cdot 109$	$x-1$	
$39203 = 197 \cdot 199$	$x-1$	
$40501 = 101 \cdot 401$	$13232x$	101
$50183 = 7 \cdot 67 \cdot 107$	$-14337(x-1)$	$67 \cdot 107$
$51841 = 47 \cdot 1103$	x	
$51983 = 227 \cdot 229$	$x-1$	
$52701 = 3 \cdot 11 \cdot 1597$	$-17566x$	$11 \cdot 1597$
$53663 = 103 \cdot 521$	$x-1$	
$60377 = 173 \cdot 349$	$19894(x-1)$	349
$64079 = 139 \cdot 461$	x	
$64681 = 71 \cdot 911$	x	
$67861 = 79 \cdot 859$	x	
$68101 = 11 \cdot 41 \cdot 151$	$-6643x$	$11 \cdot 151$
$68251 = 131 \cdot 521$	x	
$75077 = 193 \cdot 389$	$-x+1$	
$78409 = 89 \cdot 881$	$-17621x$	89
$79547 = 13 \cdot 29 \cdot 211$	$x-1$	
$82983 = 3 \cdot 139 \cdot 199$	$x-1$	
$86063 = 89 \cdot 967$	$x-1$	
$88601 = 41 \cdot 2161$	$-15128x$	41
$88831 = 211 \cdot 421$	$-843x$	211
$90061 = 113 \cdot 797$	x	
$90287 = 17 \cdot 47 \cdot 113$	$30737(x-1)$	$17 \cdot 113$
$94667 = 137 \cdot 691$	$x-1$	
$96049 = 139 \cdot 691$	x	
$97921 = 181 \cdot 541$	x	
$100127 = 223 \cdot 449$	$-x+1$	
$104663 = 13 \cdot 83 \cdot 97$	$x-1$	
$13573 = 137 \cdot 829$	$-x+1$	
$115231 = 139 \cdot 829$	$-46425x$	139
$118441 = 83 \cdot 1427$	x	
$121103 = 347 \cdot 349$	$x-1$	
$121393 = 233 \cdot 521$	$-46368(x-1)$	521
$138601 = 17 \cdot 31 \cdot 263$	$-1053x$	$17 \cdot 31$
$142883 = 13 \cdot 29 \cdot 379$	$x-1$	
$145351 = 191 \cdot 761$	$47942x$	191
$146611 = 271 \cdot 541$	x	
$150121 = 23 \cdot 61 \cdot 107$	$32636x$	$61 \cdot 107$

Table 1 (cont.)

n	$ax+b$	d
$153781 = 61 \cdot 2521$	$-15127x$	61
$158717 = 13 \cdot 29 \cdot 421$	$38310(x-1)$	29
$161027 = 283 \cdot 569$	$-x+1$	
$162133 = 73 \cdot 2221$	$-x+1$	
$163081 = 17 \cdot 53 \cdot 181$	x	
$182513 = 229 \cdot 797$	$19924(x-1)$	229
$186961 = 31 \cdot 37 \cdot 163$	x	
$191351 = 179 \cdot 1069$	$-76969x$	179
$195227 = 197 \cdot 991$	$x-1$	
$197209 = 199 \cdot 991$	x	
$199801 = 7 \cdot 17 \cdot 23 \cdot 73$	$59569x$	$17 \cdot 73$
$200147 = 233 \cdot 859$	$x-1$	
$218791 = 331 \cdot 661$	$-1323x$	331
$219781 = 271 \cdot 811$	x	
$231703 = 263 \cdot 881$	$-x+1$	
$250277 = 353 \cdot 709$	$82954(x-1)$	709
$252601 = 41 \cdot 61 \cdot 101$	x	
$254321 = 263 \cdot 967$	x	
$257761 = 7 \cdot 23 \cdot 1601$	x	
$265881 = 3 \cdot 7 \cdot 11 \cdot 1151$	$-75965x$	$3 \cdot 11 \cdot 1151$
$266071 = 13 \cdot 97 \cdot 211$	$105923x$	211
$268801 = 13 \cdot 23 \cdot 29 \cdot 31$	x	
$272611 = 131 \cdot 2081$	x	
$283361 = 13 \cdot 71 \cdot 307$	x	
$283373 = 17 \cdot 79 \cdot 211$	$-66675(x-1)$	$79 \cdot 211$
$294527 = 383 \cdot 769$	$97664(x-1)$	769
$302101 = 317 \cdot 953$	x	
$303101 = 101 \cdot 3001$	x	
$306287 = 53 \cdot 5779$	$x-1$	
$316561 = 7 \cdot 41 \cdot 1103$	$112505x$	$7 \cdot 41$
$330929 = 149 \cdot 2221$	x	
$332949 = 3 \cdot 29 \cdot 43 \cdot 89$	$-5161x$	$29 \cdot 89$
$342271 = 31 \cdot 61 \cdot 181$	$11223x$	$31 \cdot 181$
$345913 = 37 \cdot 9349$	$-56093(x-1)$	9349
$380393 = 13 \cdot 29 \cdot 1009$	$29262(x-1)$	$29 \cdot 1009$
$381923 = 617 \cdot 619$	$4-1$	
$385307 = 13 \cdot 107 \cdot 277$	$-187251(x-1)$	$13 \cdot 277$
$399001 = 31 \cdot 61 \cdot 211$	x	
$429263 = 197 \cdot 2179$	$x-1$	
$430127 = 463 \cdot 929$	$-x+1$	

Table 1 (cont.)

n	$ax+b$	d
$433621 = 199 \cdot 2179$	x	
$438751 = 541 \cdot 811$	x	
$453151 = 151 \cdot 3001$	$-48017x$	151
$454607 = 163 \cdot 2789$	$x-1$	
$456301 = 181 \cdot 2521$	$-70589x$	181
$464101 = 11 \cdot 31 \cdot 1361$	$153792x$	$11 \cdot 31$
$489601 = 7 \cdot 23 \cdot 3041$	x	
$500207 = 409 \cdot 1223$	$x-1$	
$506521 = 19 \cdot 53 \cdot 503$	$-2013x$	$19 \cdot 53$
$507527 = 503 \cdot 1009$	$168504(x-1)$	1009
$512461 = 31 \cdot 61 \cdot 271$	x	
$520801 = 241 \cdot 2161$	x	
$530611 = 461 \cdot 1151$	x	
$548627 = 523 \cdot 1049$	$-183574(x-1)$	1049
$556421 = 431 \cdot 1291$	x	
$569087 = 127 \cdot 4481$	$x-1$	
$572839 = 691 \cdot 829$	$-8291x$	691
$600767 = 421 \cdot 1427$	$x-1$	
$607561 = 241 \cdot 2521$	$224370x$	2521
$629911 = 109 \cdot 5779$	$-5778x$	5779
$635627 = 563 \cdot 1129$	$-x+1$	
$636641 = 461 \cdot 1381$	x	
$636707 = 193 \cdot 3299$	$x-1$	
$638189 = 619 \cdot 1031$	x	
$642001 = 401 \cdot 1601$	$212932x$	401
$655201 = 23 \cdot 61 \cdot 467$	x	
$676367 = 29 \cdot 83 \cdot 281$	$x-1$	
$685583 = 827 \cdot 829$	$x-1$	
$697883 = 373 \cdot 1871$	$x-1$	
$721801 = 601 \cdot 1201$	$-2403x$	601
$722261 = 491 \cdot 1471$	x	
$732887 = 17 \cdot 19 \cdot 2269$	$x-1$	
$736163 = 857 \cdot 859$	$x-1$	
$741751 = 431 \cdot 1721$	x	
$753251 = 251 \cdot 3001$	$-69024x$	251
$753377 = 613 \cdot 1229$	$-251944(x-1)$	1229
$762841 = 17 \cdot 23 \cdot 1951$	$-66333x$	$17 \cdot 1951$
$765687 = 3 \cdot 13 \cdot 29 \cdot 677$	$x-1$	
$770783 = 13 \cdot 211 \cdot 281$	$x-1$	
$775207 = 509 \cdot 1523$	$x-1$	

Table 1 (cont.)

n	$ax+b$	d
$796111 = 31 \cdot 61 \cdot 421$	$-179768x$	31
$798571 = 37 \cdot 113 \cdot 191$	$37628x$	191
$828827 = 643 \cdot 1289$	$-277134(x-1)$	1289
$851927 = 881 \cdot 967$	$-x+1$	
$852841 = 11 \cdot 31 \cdot 41 \cdot 61$	x	
$853469 = 239 \cdot 3571$	x	
$873181 = 661 \cdot 1321$	$-2643x$	661
$925681 = 23 \cdot 167 \cdot 241$	x	
$948433 = 397 \cdot 2389$	$-136172(x-1)$	2389
$954271 = 691 \cdot 1381$	$-2763x$	691
$983903 = 443 \cdot 2221$	$x-1$	
$994517 = 17 \cdot 19 \cdot 3079$	$468009(x-1)$	$19 \cdot 3079$
$999941 = 577 \cdot 1733$	x	

Table 2

$4181 = 37 \cdot 113$	$161027 = 283 \cdot 569$	$520801 = 241 \cdot 2161$
$5777 = 53 \cdot 109$	$162133 = 73 \cdot 2221$	$530611 = 461 \cdot 1151$
$6479 = 11 \cdot 19 \cdot 31$	$163081 = 17 \cdot 53 \cdot 181$	$544159 = 7 \cdot 11 \cdot 37 \cdot 191$
$6721 = 11 \cdot 13 \cdot 47$	$168299 = 31 \cdot 61 \cdot 89$	$545279 = 7 \cdot 61 \cdot 1277$
$10877 = 73 \cdot 149$	$186961 = 31 \cdot 37 \cdot 163$	$553679 = 7 \cdot 19 \cdot 23 \cdot 181$
$13201 = 43 \cdot 307$	$196559 = 11 \cdot 107 \cdot 167$	$553839 = 3 \cdot 11 \cdot 13 \cdot 1291$
$15251 = 101 \cdot 151$	$197209 = 199 \cdot 991$	$556421 = 431 \cdot 1291$
$27071 = 11 \cdot 23 \cdot 107$	$219781 = 271 \cdot 811$	$575599 = 41 \cdot 101 \cdot 139$
$34561 = 17 \cdot 19 \cdot 107$	$231703 = 263 \cdot 881$	$618639 = 3 \cdot 7 \cdot 89 \cdot 331$
$44099 = 11 \cdot 19 \cdot 211$	$233519 = 11 \cdot 13 \cdot 23 \cdot 71$	$620279 = 11 \cdot 17 \cdot 31 \cdot 107$
$47519 = 19 \cdot 41 \cdot 61$	$252601 = 41 \cdot 61 \cdot 101$	$635627 = 563 \cdot 1129$
$51841 = 47 \cdot 1103$	$254321 = 263 \cdot 967$	$636641 = 461 \cdot 1381$
$54839 = 29 \cdot 31 \cdot 61$	$257761 = 7 \cdot 23 \cdot 1601$	$638189 = 619 \cdot 1031$
$64079 = 139 \cdot 461$	$268801 = 13 \cdot 23 \cdot 29 \cdot 31$	$641199 = 3 \cdot 13 \cdot 41 \cdot 401$
$64681 = 71 \cdot 911$	$272611 = 131 \cdot 2081$	$655201 = 23 \cdot 61 \cdot 467$
$65471 = 7 \cdot 47 \cdot 199$	$283361 = 13 \cdot 71 \cdot 307$	$670879 = 11 \cdot 71 \cdot 859$
$67861 = 79 \cdot 859$	$300847 = 37 \cdot 47 \cdot 173$	$689359 = 11 \cdot 29 \cdot 2161$
$68251 = 131 \cdot 521$	$302101 = 317 \cdot 953$	$701569 = 11 \cdot 23 \cdot 47 \cdot 59$
$72831 = 3 \cdot 11 \cdot 2207$	$303101 = 101 \cdot 3001$	$722261 = 491 \cdot 1471$
$75077 = 193 \cdot 389$	$327359 = 23 \cdot 43 \cdot 331$	$737471 = 7 \cdot 137 \cdot 769$
$78089 = 11 \cdot 31 \cdot 229$	$330929 = 149 \cdot 2221$	$741751 = 431 \cdot 1721$
$90061 = 113 \cdot 797$	$399001 = 31 \cdot 61 \cdot 211$	$809999 = 17 \cdot 29 \cdot 31 \cdot 53$
$96049 = 139 \cdot 691$	$417601 = 19 \cdot 31 \cdot 709$	$850541 = 29 \cdot 139 \cdot 211$
$97921 = 181 \cdot 541$	$430127 = 463 \cdot 929$	$851927 = 881 \cdot 967$
$100127 = 223 \cdot 449$	$433621 = 199 \cdot 2179$	$852841 = 11 \cdot 31 \cdot 41 \cdot 61$
$109871 = 17 \cdot 23 \cdot 281$	$438751 = 541 \cdot 811$	$853469 = 239 \cdot 3571$

Table 2 (cont.)

$113573 = 137 \cdot 829$	$451979 = 11 \cdot 17 \cdot 2417$	$881011 = 19 \cdot 89 \cdot 521$
$118441 = 83 \cdot 1427$	$486359 = 29 \cdot 31 \cdot 541$	$925681 = 23 \cdot 167 \cdot 241$
$139359 = 3 \cdot 11 \cdot 41 \cdot 103$	$489601 = 7 \cdot 23 \cdot 3041$	$954239 = 11 \cdot 13 \cdot 6673$
$146611 = 271 \cdot 541$	$510719 = 11 \cdot 29 \cdot 1601$	$993509 = 11 \cdot 181 \cdot 499$
$157079 = 13 \cdot 43 \cdot 281$	$512461 = 31 \cdot 61 \cdot 271$	$999941 = 577 \cdot 1733$

Table 3

$2737 = 7 \cdot 17 \cdot 23$	$162133 = 73 \cdot 2221$	$490841 = 13 \cdot 17 \cdot 2221$
$4181 = 37 \cdot 113$	$163081 = 17 \cdot 53 \cdot 181$	$497761 = 11 \cdot 37 \cdot 1223$
$5777 = 53 \cdot 109$	$179697 = 3 \cdot 7 \cdot 43 \cdot 199$	$512461 = 31 \cdot 61 \cdot 271$
$6721 = 11 \cdot 13 \cdot 47$	$186961 = 31 \cdot 37 \cdot 163$	$520801 = 241 \cdot 2161$
$10877 = 73 \cdot 149$	$194833 = 23 \cdot 43 \cdot 197$	$530611 = 461 \cdot 1151$
$13201 = 43 \cdot 307$	$197209 = 199 \cdot 991$	$556421 = 431 \cdot 1291$
$15251 = 101 \cdot 151$	$219781 = 271 \cdot 811$	$597793 = 7 \cdot 23 \cdot 47 \cdot 79$
$29281 = 7 \cdot 47 \cdot 89$	$228241 = 13 \cdot 97 \cdot 181$	$618449 = 13 \cdot 113 \cdot 421$
$34561 = 17 \cdot 19 \cdot 107$	$231703 = 263 \cdot 881$	$635627 = 563 \cdot 1129$
$51841 = 47 \cdot 1103$	$252601 = 41 \cdot 61 \cdot 101$	$636641 = 461 \cdot 1381$
$64079 = 139 \cdot 461$	$254321 = 263 \cdot 967$	$638189 = 619 \cdot 1031$
$64681 = 71 \cdot 911$	$257761 = 7 \cdot 23 \cdot 1601$	$639539 = 43 \cdot 107 \cdot 139$
$67861 = 79 \cdot 859$	$268801 = 13 \cdot 23 \cdot 29 \cdot 31$	$655201 = 23 \cdot 61 \cdot 467$
$68251 = 131 \cdot 521$	$272611 = 131 \cdot 2081$	$667589 = 13 \cdot 89 \cdot 577$
$75077 = 193 \cdot 389$	$283361 = 13 \cdot 71 \cdot 307$	$687169 = 7 \cdot 89 \cdot 1103$
$80189 = 17 \cdot 53 \cdot 89$	$302101 = 317 \cdot 953$	$697137 = 3 \cdot 7 \cdot 89 \cdot 373$
$90061 = 113 \cdot 797$	$303101 = 101 \cdot 3001$	$722261 = 491 \cdot 1471$
$96049 = 139 \cdot 691$	$327313 = 7 \cdot 19 \cdot 23 \cdot 107$	$741751 = 431 \cdot 1721$
$97921 = 181 \cdot 541$	$330929 = 149 \cdot 2221$	$851927 = 881 \cdot 967$
$100127 = 223 \cdot 449$	$399001 = 31 \cdot 61 \cdot 211$	$852841 = 11 \cdot 31 \cdot 41 \cdot 61$
$105281 = 11 \cdot 17 \cdot 563$	$430127 = 463 \cdot 929$	$853469 = 239 \cdot 3571$
$113573 = 137 \cdot 829$	$433621 = 199 \cdot 2179$	$920577 = 3 \cdot 7 \cdot 59 \cdot 743$
$118441 = 83 \cdot 1427$	$438751 = 541 \cdot 811$	$925681 = 23 \cdot 167 \cdot 241$
$146611 = 271 \cdot 541$	$455961 = 3 \cdot 11 \cdot 41 \cdot 337$	$930097 = 7 \cdot 23 \cdot 53 \cdot 109$
$161027 = 283 \cdot 569$	$489601 = 7 \cdot 23 \cdot 3041$	$999941 = 577 \cdot 1733$

Table 4

$1127 = 7^2 \cdot 23$	$116281 = 11^2 \cdot 31^2$	$399001 = 31 \cdot 61 \cdot 211$
$3751 = 11^2 \cdot 31$	$118441 = 83 \cdot 1427$	$405121 = 41^2 \cdot 241$
$4181 = 37 \cdot 113$	$139127 = 23^2 \cdot 263$	$430127 = 463 \cdot 929$
$4901 = 13^2 \cdot 29$	$142129 = 13^2 \cdot 29^2$	$433621 = 199 \cdot 2179$
$4961 = 11^2 \cdot 41$	$146611 = 271 \cdot 541$	$438751 = 541 \cdot 811$
$5777 = 53 \cdot 109$	$154697 = 37^2 \cdot 113$	$450241 = 11^2 \cdot 61^2$
$6721 = 11 \cdot 13 \cdot 47$	$161027 = 283 \cdot 569$	$472361 = 41^2 \cdot 281$
$7381 = 11^2 \cdot 61$	$162133 = 73 \cdot 2221$	$472453 = 37 \cdot 113^2$

Table 4 (cont.)

$10877 = 73 \cdot 149$	$163081 = 17 \cdot 53 \cdot 181$	$489601 = 7 \cdot 23 \cdot 3041$
$13201 = 43 \cdot 307$	$164561 = 43^2 \cdot 89$	$512461 = 31 \cdot 61 \cdot 271$
$15251 = 101 \cdot 151$	$177451 = 29^2 \cdot 211$	$520801 = 241 \cdot 2161$
$18081 = 3^2 \cdot 7^2 \cdot 41$	$186961 = 31 \cdot 37 \cdot 163$	$530611 = 461 \cdot 1151$
$25921 = 7^2 \cdot 23^2$	$195301 = 19^2 \cdot 541$	$556421 = 431 \cdot 1291$
$34561 = 17 \cdot 19 \cdot 107$	$197209 = 199 \cdot 991$	$566401 = 11^2 \cdot 31 \cdot 151$
$39249 = 3^2 \cdot 7^2 \cdot 89$	$203401 = 11^2 \cdot 41^2$	$567643 = 43^2 \cdot 307$
$47489 = 13^2 \cdot 281$	$203841 = 3^2 \cdot 11 \cdot 29 \cdot 71$	$629693 = 53 \cdot 109^2$
$51841 = 47 \cdot 1103$	$219781 = 271 \cdot 811$	$635627 = 563 \cdot 1129$
$53361 = 3^2 \cdot 7^2 \cdot 11^2$	$231601 = 31^2 \cdot 241$	$636641 = 461 \cdot 1381$
$58621 = 31^2 \cdot 61$	$231703 = 263 \cdot 881$	$638189 = 619 \cdot 1031$
$59711 = 29^2 \cdot 71$	$236321 = 29^2 \cdot 281$	$655201 = 23 \cdot 61 \cdot 467$
$64079 = 139 \cdot 461$	$252601 = 41 \cdot 61 \cdot 101$	$691041 = 3 \cdot 13^2 \cdot 29 \cdot 47$
$64681 = 71 \cdot 911$	$254321 = 263 \cdot 967$	$722261 = 491 \cdot 1471$
$65341 = 19^2 \cdot 181$	$257761 = 7 \cdot 23 \cdot 1601$	$741751 = 431 \cdot 1721$
$67861 = 79 \cdot 859$	$268801 = 13 \cdot 23 \cdot 29 \cdot 31$	$750541 = 11 \cdot 31^2 \cdot 71$
$68251 = 131 \cdot 521$	$272611 = 131 \cdot 2081$	$766151 = 29^2 \cdot 911$
$68481 = 3^2 \cdot 7 \cdot 1087$	$283361 = 13 \cdot 71 \cdot 307$	$794021 = 73^2 \cdot 149$
$71149 = 13^2 \cdot 421$	$302101 = 317 \cdot 953$	$798721 = 7 \cdot 11^2 \cdot 23 \cdot 41$
$75077 = 193 \cdot 389$	$303101 = 101 \cdot 3001$	$810703 = 47^2 \cdot 367$
$90061 = 113 \cdot 797$	$305041 = 11^2 \cdot 2521$	$815409 = 3^2 \cdot 7^2 \cdot 43^2$
$96049 = 139 \cdot 691$	$306181 = 53^2 \cdot 109$	$851927 = 881 \cdot 967$
$97921 = 181 \cdot 541$	$313501 = 37^2 \cdot 229$	$852841 = 11 \cdot 31 \cdot 41 \cdot 61$
$99541 = 13^2 \cdot 19 \cdot 31$	$321201 = 3^2 \cdot 89 \cdot 401$	$853469 = 239 \cdot 3571$
$100127 = 223 \cdot 449$	$330929 = 149 \cdot 2221$	$910081 = 19^2 \cdot 2521$
$104329 = 17^2 \cdot 19^2$	$354061 = 29^2 \cdot 421$	$925681 = 23 \cdot 167 \cdot 241$
$113573 = 137 \cdot 829$	$390241 = 19^2 \cdot 23 \cdot 47$	$999941 = 577 \cdot 1733$

Table 5

4181	64079	100127	197209	283361	489601	655201
5777	64681	113573	219781	302101	512461	722261
6721	67861	118441	231703	303101	520801	741751
10877	68251	146611	252601	330929	530611	851927
13201	75077	161027	254321	399001	556421	852841
15251	90061	162133	257761	430127	635627	853469
34561	96049	163081	268801	433621	636641	925681
51841	97921	186961	272611	438751	638189	999941

Table 6

Table no.	Arithmetic progression		
1	377,	79547,	158717
	1891,	399001,	796111
	138601,	268801,	399001
	186961,	219781,	252601
2	97921,	257761,	417601
	186961,	219781,	252601
3	6721,	29281,	51841
	97921,	163081,	228241
	186961,	219781,	252601
4	4961,	163081,	321201
	25921,	257761,	489601
	97921,	146611,	195301
	186961,	219781,	252601
	203841,	236321,	268801
	231601,	399001,	566401
5	186961,	219781,	252601

Tables 1 – 6 suggest the following conjectures (Jerzy Browkin).

CONJECTURE 1. *Let p and $q = p+2$ be primes, then pq is a Fibonacci pseudoprime iff $p \equiv 7 \bmod 10$.*

CONJECTURE 2. *Let p and $q = 2p+3$ be primes, then pq is a Fibonacci pseudoprime iff $p \equiv 3 \bmod 10$.*

CONJECTURE 3. *Let p and $q = 2p-1$ be primes, then pq is a Fibonacci pseudoprime iff $p \equiv 1 \bmod 10$.*

PROOF OF CONJECTURE 1. If $p \equiv 7 \bmod 10$ then $q = p+2 \equiv 9 \bmod 10$, hence $(5/p) = -1$, $(5/q) = 1$, $(5/pq) = -1$. We have $p | u_{p-(5/p)} = u_{p+1}$, $q | u_{q-(5/q)} = u_{p+2-1} = u_{p+1}$, $pq - (5/p) = p(p+2)+1 = (p+1)^2$, hence $pq | u_{p+1} | u_{(p+1)^2} = u_{pq-(5/pq)}$ and pq is a Fibonacci pseudoprime.

Conversely, if $p \not\equiv 7 \bmod 10$ then $p \equiv 3 \bmod 10$ or $p \equiv \pm 1 \bmod 10$.

If $p \equiv 3 \bmod 10$ then $p+2 \equiv 5 \bmod 10$ and pq is not a Fibonacci pseudoprime.

If $p \equiv 1 \bmod 10$ then $p+2 \equiv 3 \bmod 10$ and from $pq - (5/pq) = p(p+2)+1 = (p+1)^2$, $pq | u_{(p+1)^2}$, $p | u_{p-(5/p)}$, $(u_{p+1}, u_{p-1}) = u_2 = 1$, we get $p = 1$ and pq is not a Fibonacci pseudoprime.

If $p \equiv -1 \bmod 10$ and from $pq - (5/pq) = p(p+2) - 1 = p^2 + 2p - 1 = (p-1)(p+3) + 2$, and from $p | u_{(p-1)(p+3)+2}$, $p | u_{p-1}$ we get $p | u_2 = 1$, $p = 1$ and pq is not a Fibonacci pseudoprime. □

Below 10^6 we get the following Fibonacci pseudoprimes of the form $p(p+2)$: $17\cdot 19, 107\cdot 109, 137\cdot 139, 197\cdot 199, 227\cdot 229, 347\cdot 349, 617\cdot 619, 827\cdot 829, 857\cdot 859$.

PROOF OF CONJECTURE 2. Let p and $q = 2p+3$ be primes.

If $p \equiv 3 \bmod 10$ then $2p+3 \equiv -1 \bmod 5$, $2p+3 = 2(10k+3)+3 = 20k+9 \equiv 1 \bmod 4$, $(5/q) = 1$, $(5/pq) = -1$. By Euler's theorem for Fibonacci sequence (Ribenboim [16, p. 130], Rotkiewicz [19], p. 240) we have $u_{\frac{q-(5/pq)}{2}} = u_{\frac{(2p+3)-1}{2}} = u_{p+1} \equiv 0 \bmod q$, $pq-(5/pq) = p(2p+3)+1 = (p+1)(2p+1)$, $p|u_{p+1}$, hence $pq|u_{p+1}|u_{pq-(5/pq)}$ and pq is a Fibonacci pseudoprime.

Conversely, if $p \not\equiv 3 \bmod 10$ then $p \equiv 7 \bmod 10$ or $p \equiv \pm 1 \bmod 10$.

If $p \equiv 7 \bmod 10$ then $q = 2p+3 \equiv 7 \bmod 10$, hence $(5/p) = -1$, $(5/q) = -1$ and $(5/pq) = 1$ and from $pq-(5/pq) = p(2p+3)-1 = 2p^2+3p-1 = (p+1)(2p+1)-2$, we get $p|u_{pq-(5/pq)} = u_{(p+1)(2p+1)-2}$, $p|u_{p+1}$, hence $p|u_2 = 1$ and pq is not a Fibonacci pseudoprime.

If $p \equiv -1 \bmod 10$ $2p+3 \equiv 1 \bmod 10$ and from $pq-(5/pq) = p(2p+3)-1 = 2p^2+3p-1 = (p-1)(2p+5)+4$, and from $p|u_{p-1}$, $p|u_{p(2p+3)-1} = u_{(p-1)(2p+5)+4}$ we get $p|u_4 = 3$, hence $p = 3$, $q = 9$ and $p(2p+3)$ is not a Fibonacci pseudoprime.

If $p \equiv 1 \bmod 10$, then $2p+3 \equiv 5 \bmod 10$ and pq is not a Fibonacci pseudoprime. □

Below 10^6 we get the following Fibonacci pseudoprimes of the form $p(2p+3)$: $53\cdot 109, 73\cdot 149, 113\cdot 229, 173\cdot 349, 193\cdot 389, 223\cdot 449, 283\cdot 569, 353\cdot 709, 383\cdot 769, 463\cdot 929, 503\cdot 1009, 523\cdot 1049, 463\cdot 1129, 613\cdot 1229$ and $643\cdot 1289$.

PROOF OF CONJECTURE 3. If $p \equiv 1 \bmod 10$ then $2p-1 \equiv 1 \bmod 10$, then $(5/p) = (5/q) = (5/pq) = 1$, $q = 2p-1 = 2(10k+1)-1 = 20k+1 \equiv 1 \bmod 4$ and by Euler's theorem for the Fibonacci sequence we have $u_{\frac{q-(5/q)}{2}} = u_{\frac{(2p-1)-1}{2}} = u_{p-1} \equiv 0 \bmod q$, $p|u_{p-1}$, $pq-(5/pq) = p(2p-1)-1 = 2p^2-p-1 = (p-1)(2p+1)$ and $pq|u_{(p-1)(2p+1)} = u_{pq-(5/pq)}$ and pq is a Fibonacci pseudoprime.

Conversely, if $p \not\equiv 1 \bmod 10$ then $p \equiv -1 \bmod 10$ or $p \equiv \pm 3 \bmod 10$.

If $p \equiv -1 \bmod 10$ then $p|u_{p-1}$, $2p-1 \equiv -3 \equiv 7 \bmod 10$ and $(5/p) = 1$, $(5/q) = -1$, $(5/pq) = -1$, $pq-(5/pq) = p(2p-1)+1 = 2p^2-p+1 = (p-1)(2p+1)+2$, $pq|u_{pq-(5/pq)} = u_{p(2p-1)+1} = u_{(p-1)(2p+1)+2}$ and $p|u_{p-1}$, $p|u_{(p-1)(2p+1)+2}$, hence $p|u_2 = 1$ and pq is not a Fibonacci pseudoprime.

If $p \equiv 3 \bmod 10$ then $2p-1 \equiv 5 \bmod 10$ and pq is not a Fibonacci pseudoprime.

If $p \equiv -3 \bmod 10$, then $2p-1 \equiv -7 \bmod 10$, $(5/p) = -1$, $(5/q) = -1$, $(5/p) = -1$, $(5/pq) = 1$, $p|u_{p+1}$, $p|u_{pq-(5/pq)} = u_{p(2p-1)-1} = u_{2p^2-p-1} =$

$u_{(p+1)(2p-1)+2}$, hence $p|u_2 = 1$ and pq is not a Fibonacci pseudoprime. □

Below 10^6 we get the following Fibonacci pseudoprimes of the form $p(2p-1)$: $31 \cdot 61, 211 \cdot 421, 271 \cdot 541, 331 \cdot 661, 601 \cdot 1201, 661 \cdot 1321$ and $691 \cdot 1381$.

In Table 7 there are given all arithmetic progressions with terms below 10^6 which are Dickson-Fibonacci pseudoprimes of the second kind, including squares of primes $\neq 2, 5$. There are no progressions with four terms. Squares of primes are printed in bold.

Table 7

49,	**169,**	**289**	**18769,**	**76729,**	**134689**	**72361,**	405121,	**737881**
49,	**289,**	**529**	**19321,**	58621,	97921	**73441,**	146611,	219781
49,	**5329,**	**10609**	**19321,**	90061,	160801	**96721,**	163081,	**229441**
49,	**9409,**	18769	25921,	**32761,**	**39601,**	**96721,**	**177241,**	257761
121,	3751,	7381	25921,	52441,	78961	97921,	146611,	195301
121,	163081,	**326041**	25921,	257761,	489601	97921,	195301,	**292681**
169,	71149,	142129	25921,	**271441,**	**516961**	**121801,**	195301,	268801
289,	**2809,**	**5329**	**27889,**	**38809,**	**49729**	**128881,**	**160801,**	**192721**
289,	**18769,**	**37249**	**27889,**	**452929,**	**877969**	146611,	**292681,**	438751
361,	195301,	390241	**29929,**	**113569,**	197209	**160801,**	**502681,**	**844561**
529,	**1369,**	**2209**	**32761,**	65341,	97921	**167281,**	**212521,**	257761
841,	**32761,**	64681	**32761,**	97921,	163081	**167281,**	302101,	**436921**
841,	177451,	354061	**32761,**	272611,	512461	**167281,**	**410881,**	**654481**
961,	**11881,**	**22801**	**36481,**	90061,	**143641**	186961,	219781,	252601
961,	58621,	116281	**44521,**	97921,	**151321**	**192721,**	313501,	**434281**
961,	116281,	231601	51841,	**109561,**	**167281**	**201601,**	**361201,**	520801
1681,	203401,	405121	51841,	**516961,**	**982081**	203841,	236321,	268801
4961,	163081,	321201	**54289,**	**100489,**	**146689**	**212521,**	252601,	**292681**
5041,	**201601,**	**398161**	57121,	**491401,**	925681	219781,	438751,	**657721**
5329,	**37249,**	**69169**	**58081,**	231601,	405121	231601,	399001,	566401
6241,	**292681,**	**579121**	**58081,**	302101,	**546121**	257761,	**410881,**	**564001**
7921,	**22201,**	**36481**	**63001,**	313501,	**564001**	257761,	**516961,**	**776161**
7921,	164561,	32121	64681,	**361201,**	**657721**	313501,	438751,	**564001**
9409,	**12769,**	**16129**	65341,	**185761,**	306181	**332929,**	**375769,**	**418609**
10609,	**54289,**	**97969**	**66049,**	**208849,**	**351649**	**361201,**	**383161,**	405121
11449,	104329,	197209	**66049,**	**426409,**	**786769**	**410881,**	450241,	489601
12769,	**113569,**	**214369**	67861,	**78961,**	90061	450241,	520801,	**591361**

Acknowledgements. I thank very much Professor Jerzy Browkin for the above tables of five types of Fibonacci pseudoprimes and the arithmetic progressions consisting of these pseudoprimes.

References

[1] R. Baillie, S. Wagstaff Jr., *Lucas pseudoprimes*, Math. of Comput. **35** (1980), 1391–1417.

[2] T. Banachiewicz, *O związku pomiędzy pewnym twierdzeniem matematyków chińskich a formą Fermata na liczby pierwsze*, Spraw. Tow. Nauk., Warszawa, 2 (1909), 7–11.

[3] N. G. W. H. Beeger, *On even numbers m dividing $2^m - 2$*, Amer. Math. Monthly **58** (1951), 553–555.

[4] R. E. Crandall, C. Pomerance, *Prime Numbers. A Computational Perspective*, Springer, New York 2001.

[5] L. E. Dickson, *History of the Theory of Numbers.* vol. I: *Divisibility and Primality*, Carnegie Inst., Washington 1919.

[6] K. Dilcher, *Fermat numbers, Wieferich and Wilson primes: Computations and generations*, Proc. Conf. on Computational Number Theory and Public Key Cryptography, Warsaw. Sept. 2000, 1–22.

[7] P. Erdős, *On almost primes*, Amer. Math. Monthly **57** (1950), 404–407.

[8] P. Erdős, P. Kiss, A. Sárközy, *Lower bound for the counting function of Lucas pseudoprimes*, Math. of Comput. **51** (1988), 315–323.

[9] J. F. Grantham, *Frobenius pseudoprimes*, University of Georgia, Athens GA. 1997 (dissertation).

[10] J. F. Grantham, *Frobenius pseudoprimes*, Math. of Comput. **70** (2001), 871–891.

[11] R. K. Guy, *Unsolved Problems in Number Theory*, Springer–Verlag, New York 1994.

[12] M. Křižek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers, From Number Theory to Geometry*, Springer-Verlag, New York 2001.

[13] R.G.E. Pinch, *The pseudoprimes up to* 10^{13}, Algorithmic Number Theory, 4th International Symposium, ANTS-IV Leiden, The Netherlands, 2–7 July 2000, Proceedings (2000), 459–473.

[14] C. Pomerance, J. L. Selfridge, S. S. Wagstaff, *The pseudoprimes to* $25 \cdot 10^9$, Math. of Comput. **35** (1980), 1003–1026.

[15] P. Poulet, *Table des nombres composés vérifiant le théorème de Fermat pour le module 2 jusqu'à* 100.000.000, Sphinx **8** (1938), 42–52. Errata in Math. of Comput. **25** (1971), 944–945, Math. of Comput. **26** (1972), 814.

[16] P. Ribenboim, *The new Book of Prime Number Records*, Springer, New York 1996.

[17] A. Rotkiewicz, *On the pseudoprimes of the form $ax + b$ with respect to the sequence of Lehmer*, Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys. **20** (1972), 83–85.

[18] A. Rotkiewicz, *On the pseudoprimes with respect to the Lucas sequence*, Bull. Acad. Polon. Sci. Sér. Math. Astronom. Phys. **21** (1973), 793–797.

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

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

[21] A. Rotkiewicz, *There are infinitely many arithmetical progressions formed by three different Fibonacci pseudoprimes*, Applications of Fibonacci Numbers, Vol. 7, Ed. by G.E. Bergum, A.N. Philippou and A.F. Horadam. Kluwer Academic Publishers, Dordrecht, the Netherlands 1998, 327–332.

[22] A. Rotkiewicz, *Arithmetical progression formed by Lucas pseudoprimes*, Number Theory, Diophantine, Computational and Algebraic Aspects, Eds: György Kálmán, Attila Pethö and Vera T. Sós. Walter de Gruyter GmbH & Co., Berlin, New York 1998, 465–472.

[23] A. Rotkiewicz, *Lucas pseudoprimes*, Funct. Approximatio Comment. Math. **28** (2000), 97–104.

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

[25] A. Rotkiewicz, K. Ziemak, *On even pseudoprimes*, The Fibonacci Quarl. **33** (1995), 123–125.

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

[27] Z. Zhang, *Finding strong pseudoprimes to several bases*, Math. of Comput. **70** (2000), 863–872.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
00-956 WARSZAWA 10
POLAND
P.O. BOX 21
e-mail: rotkiewi@impan.gov.pl