J. Symbolic Computation (1995) **20**, 151–161

Constructing Carmichael Numbers which are Strong Pseudoprimes to Several Bases[†]

FRANÇOIS ARNAULT[‡]

Université de Limoges, Faculté des Sciences, URA 1586,
Laboratoire d'Arithmétique de Calcul formel et d'Optimisation,
123, av Albert Thomas, 87060 Limoges Cedex, France

(Received 26 September 1994)

We describe here a method of constructing Carmichael numbers which are strong pseudoprimes to some sets of prime bases. We apply it to find composite numbers which are found to be prime by the Rabin–Miller test of packages as Axiom or Maple. We also use a variation of this method to construct strong Lucas pseudoprimes with respect to several pairs of parameters.

1. Introduction

1.1. THE RABIN–MILLER TEST

The Rabin–Miller test is based on the following strengthened version of Fermat's little theorem:

THEOREM 1.1. *If n is a prime number such that $\gcd(n, 2b) = 1$, then one of the following conditions is satisfied, where $n - 1 = 2^k q$ with q odd,*

$$b^q \equiv 1 \quad \text{modulo } n, \text{ or}$$
$$\text{there exists an integer } i \text{ such that } 0 \le i < k \text{ and } b^{2^i q} \equiv -1 \text{ modulo } n.$$

If n is composite but satisfies this property, it is called a *strong pseudoprime to the base b* and, for short, we write "n is a spsp(b)". By the Rabin–Monier theorem (Monier, 1980), if n is odd and composite, the number of bases b such that $0 < b < n$ and n is spsp(b) is less than $n/4$. So, for odd composite n and random b, the probability that n is a spsp(b) is less than $1/4$. The Rabin–Miller test proceeds as follows: it checks if the number n satisfies the relations of Theorem 1.1 for several bases b. If, for some b these relations do not hold, then n is certainly composite. Conversely, if n is composite, then we are likely to find some b for which these relations do not hold and n is very unlikely to be declared prime.

[†] This work was done while the author was working at the University of Poitiers, France.

[‡] E-mail: `arnault@unilim.fr`

0747–7171/95/080151 + 11 $12.00/0

In Arnault (1995) we have constructed numbers which are the product of two primes but are strong pseudoprimes to some sets of several bases, chosen in advance. We construct here such numbers which are the product of three or more primes. We apply the method to the bases used by the software Axiom 1.1 and Maple V.2 and so, the numbers we find pass the Rabin–Miller test of these packages.

1.2. THE LUCAS TEST

Let P and Q be integers such that $D = P^2 - 4Q$ is not a perfect square. The Lucas sequences associated with the parameters P, Q are defined by

$$\begin{array}{lll} U_0 = 0 & U_1 = 1 & U_{k+2} = PU_{k+1} - QU_k \\ V_0 = 2 & V_1 = P & V_{k+2} = PV_{k+1} - QV_k. \end{array}$$

Consider the two roots α and β of the trinomial $X^2 - PX + Q$ in the ring of integers of $\mathbb{Q}(\sqrt{D})$. It is easy to see that, for all $k \in \mathbb{N}^*$,

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \qquad V_k = \alpha^k + \beta^k. \tag{1}$$

For n integer, we note $\varepsilon(n)$ the Jacobi symbol (D/n). The strong Lucas test is based on the following result.

THEOREM 1.2. *If n is a prime number such that* $\gcd(n, 2QD) = 1$. *Then one of the following conditions is satisfied, where we put $n - \varepsilon(n) = 2^k q$ with q odd,*

$$n \mid U_q, \text{ or}$$
$$\text{there exists } i \text{ such that } 0 \le i < k \text{ and } n \mid V_{2^i q}.$$

If n is composite but satisfies this property, it is called a *strong Lucas pseudoprime with respect to the parameters P and Q*. Shortly, we write "n is a slpsp(P, Q)". From a result in Arnault (submitted), for random P, Q such that $P^2 - 4Q$ is congruent modulo n to a given D relatively prime to n, the probability that n is a slpsp(P, Q) is less than $4/15$, provided n is a composite distinct from 9 and is not the product of twin primes.

The strong Lucas test is similar to the Rabin–Miller test but uses the Theorem 1.2 instead of Theorem 1.1. We will also construct, in Sections 6 and 7, strong Lucas pseudoprimes to some sets of pairs (P, Q).

2. Preliminaries

Throughout this paper, the number n is a product $p_1 p_2 \cdots p_h$ of odd primes with $h \ge 3$ odd (except in Section 5) and such that $p_1 < p_2 < \cdots < p_h$. Also, we put $\varepsilon = \pm 1$ and

$$k_i = \frac{p_i - \varepsilon}{p_1 - \varepsilon}, \qquad m_i = \frac{\prod_{j \ne i} p_j - 1}{p_i - \varepsilon}, \qquad \text{for } 1 \le i \le h.$$

We need two basic lemmas. For $s \in \mathbb{N}^*$, we note $v_2(s)$ the greatest integer t such that $2^t \mid s$:

LEMMA 2.1. *If the k_i are integers, they all are odd if and only if*

$$v_2(p_1 - \varepsilon) = v_2(p_2 - \varepsilon) = \cdots = v_2(p_h - \varepsilon) = v_2(n - \varepsilon).$$

PROOF. Put $v = v_2(p_1 - \varepsilon)$. We have $v_2(p_i - \varepsilon) = v$ if and only if k_i is odd. If all the k_i are odd, we have $p_i \equiv 2^v + \varepsilon$ modulo 2^{v+1}. So, as h is odd, $n \equiv (2^v + \varepsilon)^h \equiv 2^v + \varepsilon$ modulo 2^{v+1}. Hence $v_2(n - \varepsilon) = v$. □

LEMMA 2.2. *We have the following assertions:*

$$p_i - \varepsilon \textit{ divides } n - \varepsilon \Leftrightarrow m_i \textit{ is an integer},$$
$$k_i \textit{ is an integer for all } i \geq 2 \Rightarrow m_1 \textit{ is an integer.}$$

PROOF. The first claim can be reformulated in the following way

$$n \equiv \varepsilon \text{ modulo } (p_i - \varepsilon) \Leftrightarrow \prod_{j \neq i} p_j \equiv 1 \text{ modulo } (p_i - \varepsilon).$$

Hence, it follows from the trivial relations $p_i \equiv \varepsilon$ modulo $(p_i - \varepsilon)$. Also, the last implication is clear if we write its left-hand side $p_i \equiv \varepsilon$ modulo $(p_1 - \varepsilon)$ for all $i \geq 2$. □

REMARK 2.3. *The formulae $p_j = k_j(p_1 - \varepsilon) + \varepsilon$ show that the coefficients k_i and m_i satisfy the relation $k_i m_i = f_i(p_i)$ where f_i is the polynomial*

$$f_i(X) = \frac{\prod_{j \neq i}(k_i(X-1)+1) - 1}{X - 1}. \qquad (2)$$

(For example, with $h = 3$, we have $f_2(X) = k_3 X + \varepsilon$ and $f_3(X) = k_2 X + \varepsilon$.) The condition "$m_i$ is an integer" can be written like "p_1 is a root of f_i modulo k_i".

3. carmichael numbers which are strong pseudoprimes

3.1. CARMICHAEL NUMBERS

Recall that a positive composite interger m is a Carmichael number if it satisfies

$$b^{m-1} \equiv 1 \text{ modulo } m \qquad \text{for all } b \text{ relatively prime to } m.$$

We use the notations of Section 2 in the case $\varepsilon = 1$. It is well known that Carmichael numbers are the square free integers m such that $p - 1 \mid m - 1$ for all prime p dividing m. In particular, from Lemma 2.2, we have

LEMMA 3.1. *Let $n = p_1 p_2 \cdots p_h$ be a product of distinct odd primes and define*

$$k_i = \frac{p_i - 1}{p_1 - 1}, \qquad m_i = \frac{\prod_{j \neq i} p_j - 1}{p_i - 1}, \qquad \textit{for } 1 \leq i \leq h.$$

If the coefficients k_i and m_i are integers for all i such that $2 \leq i \leq h$, then n is a Carmichael number.

3.2. STRONG PSEUDOPRIMES

We describe here some additional sufficient conditions for n to be a strong pseudoprime to base b.

LEMMA 3.2. *Suppose that $n = p_1 p_2 \cdots p_n$ is a product of distinct odd primes and that the coefficients k_i and m_i defined in Lemma 3.1 are integers (hence n is a Carmichael* *number). Suppose moreover that the k_i are odd. If n is relatively prime to b and the relations*

$$\left(\frac{b}{p_i}\right) = -1 \qquad \textit{for all } i \textit{ such that } 1 \le i \le h \tag{3}$$

are satisfied, then n is a strong pseudoprime to the base b.

Proof. From Lemma 2.1, the ratio $(n-1)/(p_i-1)$ is odd for all i. So, as $b^{(p_i-1)/2} \equiv \pm 1$ modulo p_i, we have

$$b^{(n-1)/2} \equiv b^{(p_i-1)/2} \equiv \left(\frac{b}{p_i}\right) \qquad \text{modulo } p_i \qquad \text{for } 1 \le i \le h.$$

Hence, the assumptions imply that $b^{(n-1)/2} \equiv -1$ modulo n. This is sufficient for n to be a strong pseudoprime to the base b. □

If b is prime, the quadratic reciprocity law can be used to find a set $S_b \subseteq \mathbb{Z}/4b\mathbb{Z}$ such that, for p prime, we have

$$\left(\frac{b}{p}\right) = -1 \Leftrightarrow p \bmod 4b \in S_b.$$

As $p_i = k_i(p_1 - 1) + 1$ for all i such that $1 \le i \le h$, the condition (3) can be written

$$k_i(p_1 - 1) + 1 \bmod 4b \in S_b \qquad \text{for all } i \text{ such that } 1 \le i \le h.$$

If the coefficients k_i are relatively prime to b, this condition becomes

$$p_1 \bmod 4b \in \bigcap_{i=1}^{h} k_i^{-1}(S_b + k_i - 1), \tag{4}$$

where k_i^{-1} denotes an inverse of k_i modulo $4b$ and $k_i^{-1}(S_b + k_i - 1)$ is the set $\{k_i^{-1}(s + k_i - 1) \mid s \in S\}$.

4. Application to the Primality Tests of Maple and Axiom

The primality test of Maple V.2 consists of three stages. The first is a search for factors less than 1000. The second is an actual Rabin–Miller test. The bases used are 2, 3, 5, 7, 11 (however more bases can be used, on request). The last stage consists in checking if n is not of the form

$$(u+1)\left(k\frac{u}{2}+1\right) \quad \text{with } 3 \le k \le 9 \qquad \text{or} \qquad (u+1)(ku+1) \quad \text{with } 5 \le k \le 20.$$

This last stage is relevant to Pomerance *et al.* (1980), in which can be found three examples of such numbers which are strong pseudoprimes to four from these five bases. In the code of Maple, there is also the following comment: *Presently there are no composite numbers known to us that will make* `isprime()` *return true.*

4.1. Example with $h = 3$

Nevertheless, it is easy to check that, if $h = 3$, $k_2 = 13$ and $k_3 = 41$, the right hand side of (4) is not empty, for each of the five bases used by Maple. For example, the condition (4) is satisfied for each of these bases as soon as we have the following relations:

Table 1.

for $b = 2$:	$p_1 \equiv 3$	(mod 8)
for $b = 3$:	$p_1 \equiv 7$	(mod 12)
for $b = 5$:	$p_1 \equiv 3$	(mod 20)
for $b = 7$:	$p_1 \equiv 15$	(mod 28)
for $b = 11$:	$p_1 \equiv 23$	(mod 44)

Moreover, the equalities $p_1 p_i - 1 = p_1(p_i - 1) + (p_1 - 1)$ (for $i = 2, 3$) show that the coefficients m_i can be written (see Remark 2.3):

$$m_2 = \frac{k_3 p_1 + 1}{k_2} \qquad \text{and} \qquad m_3 = \frac{k_2 p_1 + 1}{k_3}.$$

These are integers as soon as

$$p_1 \equiv -k_3^{-1} = 6 \quad \text{modulo } 13 \qquad \text{and} \qquad p_1 \equiv -k_2^{-1} = 22 \quad \text{modulo } 41.$$

Using the extended Euclidean algorithm, we can compute that these two congruences and those from Table 1 are together equivalent to

$$p_1 \equiv 827\,443 \ \text{ modulo } \ 4\,924\,920. \tag{5}$$

So, we have:

Lemma 4.1. *Let p_1 be a prime satisfying the relation (5) and such that $p_2 = 13(p_1-1)+1$ and $p_3 = 41(p_1 - 1) + 1$ are prime. Then, the product $p_1p_2p_3$ is a Carmichael number and a strong pseudoprime to the bases 2, 3, 5, 7 and 11.*

Because the prime $p_1 = 286\,472\,803$ satisfies these conditions, the following number

$$12\,530\,759\,607\,784\,496\,010\,584\,573\,923 = 286\,472\,803 \cdot 3\,724\,146\,427 \cdot 11\,745\,384\,883 \tag{6}$$

passes the Maple test.

4.2. Example with $h = 5$

We give another example, this time with $h = 5$. We first choose coefficients k_i such that the right hand of (4) is not empty and such that the polynomials $f_i(X) \in \mathbb{Z}[X]$ defined by (2) have a root modulo k_i. The values $(k_2, k_3, k_4, k_5) = (13, 41, 53, 101)$ are suitable and the conditions of Table 1 will again imply the relations (4). Also, if

$$p_1 \equiv 4 \text{ modulo } 13,\ p_1 \equiv 21 \text{ modulo } 41,\ p_1 \equiv 41 \text{ modulo } 53 \text{ and } p_1 \equiv 54 \text{ modulo } 101,$$

then p_1 will be a root of each f_i modulo k_i.

These four relations and those of Table 1 can be mixed together

$$p_1 \equiv 14\,354\,973\,403 \ \text{ modulo } \ 26\,363\,096\,760. \tag{7}$$

So, we obtain

Lemma 4.2. *Let p_1 be a prime satisfying (7) and such that $p_2 - 13(p_1 - 1) + 1$, $p_3 = 41(p_1 - 1) + 1$, $p_4 = 53(p_1 - 1) + 1$ and $p_5 = 101(p_1 - 1) + 1$ are prime. The product $n = p_1p_2p_3p_4p_5$ is a Carmichael number and is a strong pseudoprime to the bases 2, 3, 5, 7 and 11.*

For example, take

$$p_1 = 343\,367\,327\,175\,643.$$

The product $p_1p_2p_3p_4p_5$ is

$$n = 13\,618\,186\,946\,913\,248\,902\,029\,336\,585\,225\,618\,237\,728\,639\,469\,119\,284\,611\,739\,065$$
$$110\,030\,838\,492\,720\,163$$

and passes the Maple test.

4.3. THE AXIOM TEST

The primality test of Axiom release 1.1 is a Rabin–Miller test where the set of bases used depends on the size of the number tested. For numbers less than 341 550 071 728 321, the Axiom test is always correct due to the results of Jaeschke (1993). For numbers greater than this bound, the Axiom test uses the first ten odd prime bases 3, 5, 7, 11, 13, 17, 19, 23, 29 and 31. Release 1.1 benefits from several improvements, outlined below and added by Davenport (1992), which catch the numbers produced in Jaeschke (1993) and Arnault (1995).

When $n = 2^kq$ is checked for strong pseudoprimality, one first compute b^q modulo n and then use repeating squaring to see if there exists an i such that $b^{2^iq} \equiv -1$ modulo n. Whenever we find such an $i > 0$, we get a square root of -1 modulo n, namely $b^{2^{i-1}q}$. One idea of Davenport is to collect and count the distinct square roots of -1 we get in this process. If more than two square roots are found, then n is surely composite, even if it is a strong pseudoprime to all used bases.

The Axiom test searches also for numbers of specific forms, as the numbers produced in Arnault (1995) which are of the form $n = (u+1)(2u+1)$. Indeed these numbers satisfy $8n + 1 = (4u + 3)^2$ and they are easily spotted by this release of Axiom, which checks if $8n + 1$ is a perfect square.

The Axiom test reserves a special treatment to numbers n which satisfy

$$b^{(n-1)/2} \equiv 1 \text{ modulo } n$$

for the 10 bases above. These numbers are considered as suspicious and are submitted to additional strong pseudoprimality tests with other bases until one base b is found such that $b^{(n-1)/2} \equiv -1$ modulo n or some strong pseudoprimality test fails. Fortunately for the success of the method described here, the numbers which satisfy

$$b^{(n-1)/2} \equiv -1 \text{ modulo } n$$

for the first 10 odd prime bases are not considered as suspicious.

In spite of these improvements, we are able to find composite numbers which pass the Axiom 1.1 test. For example, let $h = 3$, $k_2 = 37$, and $k_3 = 43$. The right hand of (4) is not empty, for each of the ten bases used by Axiom, in which we choose values from Table 2.

Also, the coefficients m_2 and m_3 will be integers as soon as

$$p_1 \equiv 9 \text{ modulo } 37 \qquad \text{and} \qquad p_1 \equiv 31 \text{ modulo } 41.$$

These two congruences and those of Table 2 can be together written

$$p_1 \equiv 356\,794\,315\,112\,467 \text{ modulo } 608\,500\,527\,054\,420.$$

Table 2.

for $b = 3$:	$p_1 \equiv 7$	$\pmod{12}$
for $b = 5$:	$p_1 \equiv 7$	$\pmod{20}$
for $b = 7$:	$p_1 \equiv 15$	$\pmod{28}$
for $b = 11$:	$p_1 \equiv 23$	$\pmod{44}$
for $b = 13$:	$p_1 \equiv 11$	$\pmod{52}$
for $b = 17$:	$p_1 \equiv 11$	$\pmod{68}$
for $b = 19$:	$p_1 \equiv 39$	$\pmod{76}$
for $b = 23$:	$p_1 \equiv 39$	$\pmod{92}$
for $b = 29$:	$p_1 \equiv 43$	$\pmod{116}$
for $b = 31$:	$p_1 \equiv 63$	$\pmod{124}$

Take $p_1 = 356\,794\,315\,112\,467$, we find the following number, which passes the Axiom test:

$$n = 16\,293\,065\,699\,588\,634\,810\,831\,933\,763\,781\,141\,498\,750\,450\,660\,078\,823\,067.$$

4.4. LARGE EXAMPLE

The same method has been used with a large set of bases in order to construct the 397-digit Carmichael number

$$n = p_1[313(p_1 - 1) + 1][353(p_1 - 1) + 1],$$

where

$$p_1 = 29\,674\,495\,668\,685\,510\,550\,154\,174\,642\,905\,332\,730\,771\,991\,799\,853\,043\,350\,995\,075\,531$$
$$276\,838\,753\,171\,770\,199\,594\,238\,596\,428\,121\,188\,033\,664\,754\,218\,345\,562\,493\,168\,782\,883$$

which is a strong pseudoprime to all prime bases up to 300.

5. Extensions

The following Chernick extension theorem (Chernick, 1939) allows, from one Carmichael number, to build others.

THEOREM 5.1. *Let $c = p_1 p_2 \cdots p_s$ be a Carmichael number and put*

$$\Lambda = \lambda(c) = \operatorname*{lcm}_{1 \le i \le s} (p_i - 1).$$

If p_{s+1} is a prime not dividing c and such that

$$\Lambda | p_{s+1} - 1 | c - 1, \tag{8}$$

then $c' = cp_{s+1}$ is also a Carmichael number.

5.1. EXTENSIONS OF STRONG PSEUDOPRIMES

We have constructed lures for the Rabin test, with an odd number of prime factors. The following theorem will allow us to build from them, lures with an even number of prime factors.

THEOREM 5.2. *Suppose that $n = p_1 p_2 \cdots p_h$ is a product of distinct odd primes and that the coefficients k_i and m_i defined in Lemma 3.1 are integers (hence n is a Carmichael number). Suppose also that the hypotheses of Lemma 3.2 are valid, that is the k_i are odd and*

$$\left(\frac{b}{p_i}\right) = -1 \qquad \text{for all } i \text{ such that } 1 \leq i \leq h.$$

Put

$$\Lambda = \lambda(n) = \operatorname*{lcm}_{1 \leq i \leq h} (p_i - 1).$$

If p_{h+1} is a prime not dividing n such that

$$\Lambda | p_{h+1} - 1 | n - 1, \tag{9}$$

and $(b/p_{h+1}) = -1$, then the product $n' = np_{h+1}$ is also a Carmichael number, and a strong pseudoprime to the base b.

PROOF. The fact that n' is a Carmichael number follows from Theorem 5.1; we must show that it is a spsp(b). From Theorem 5.1, we have $p_1 - 1 \mid n - 1$. So, there is a positive integer t such that

$$\frac{(n'-1)/2^t}{(p_1-1)/2}$$

is an odd integer, for all i. We will show that $b^{(n'-1)/2^t} \equiv -1$ modulo n' and this will imply that n' will be a strong pseudoprime to the base b. As we have $b^{(p_i-1)/2} \equiv -1$ modulo p_i for $1 \leq i \leq h+1$, it is sufficient to show that the integer (this is an integer, by Theorem 5.1)

$$\frac{(n'-1)/2^t}{(p_i-1)/2}$$

is odd. By Lemma 2.1, we must show that $v_2(p_i - 1) = v_2(p_1 - 1)$. The coefficients k_i are odd, so this equality holds for $i \leq h$. From Lemma 2.1, we have $v_2(\Lambda) = v_2(n-1)$. So, by (9), it holds also for $i = h + 1$. This completes the proof. □

5.2. EXAMPLE

As an example, take n from (6). There are exactly two primes satisfying the conditions of the Theorem 5.2:

$$152\,690\,003\,467 \qquad \text{and} \qquad 5\,576\,391\,616\,581\,787.$$

So, here are two numbers which are the product of four prime factors but pass the Maple test:

$$1\,913\,321\,727\,956\,758\,256\,045\,006\,260\,999\,587\,791\,041 =$$
$$286\,472\,803 \cdot 3\,724\,146\,427 \cdot 11\,745\,384\,883 \cdot 152\,690\,003\,467,$$

$$69\,876\,422\,826\,251\,144\,928\,143\,383\,863\,659\,397\,076\,940\,401 =$$
$$286\,472\,803 \cdot 3\,724\,146\,427 \cdot 11\,745\,384\,883 \cdot 5\,576\,391\,616\,581\,787.$$

6. Building Strong Lucas Pseudoprimes

Here, our aim is to build true (i.e. such that $\varepsilon(n) = -1$) strong Lucas pseudoprimes, for several chosen pairs (P, Q).

6.1. CLASSICAL RESULTS

We recall here two basic results, which can be found in Williams (1977), Baillie and Wagstaff (1980) or Ribenboim (1988). The first one is analogous to Fermat's little theorem.

THEOREM 6.1. *Let p be an odd prime not dividing D and denoting $\varepsilon(p)$ as the Legendre symbol (D/p). If $\varepsilon(p) = 1$, assume moreover that p does not divide Q. We then have*

$$p \mid U_{p-\varepsilon(p)}.$$

THEOREM 6.2. *Let p be a prime not dividing $2QD$. Then we have the following equivalences, where $\varepsilon(p)$ denotes the Legendre symbol (D/p),*

$$p \mid U_{(p-\varepsilon(p))/2} \iff \left(\tfrac{Q}{p}\right) = 1,$$
$$p \mid V_{(p-\varepsilon(p))/2} \iff \left(\tfrac{Q}{p}\right) = -1.$$

6.2. STRONG LUCAS PSEUDOPRIMES

We now use the notations of the Section 2 with $\varepsilon = -1$. Here, the analogue of Lemma 3.1 takes the following form.

LEMMA 6.1. *Let $D = P^2 - 4Q$ and $n = p_1 p_2 \cdots p_h$ be a product of distinct odd primes. Assume that $\gcd(n, QD) = 1$ and that the coefficients*

$$k_i = \frac{p_i + 1}{p_1 + 1}, \qquad m_i = \frac{\prod_{j \neq i} p_j - 1}{p_i + 1}, \qquad \textit{for } 1 \leq i \leq h$$

are integers. Assume also that

$$\left(\frac{D}{p_i}\right) = -1 \qquad \textit{for all } i \textit{ such that } 1 \leq i \leq h.$$

Then, we have the relation $p \mid U_{n+1}$.

PROOF. From Theorem 6.1 we know that $p_i \mid U_{p_i+1}$ for each p_i. So, by (1), $\alpha^{p_i+1} \equiv \beta^{p_i+1}$ modulo p_i. By Lemma 2.2, the ratios $(n+1)/(p_i+1)$ are integers. From this, we see that $\alpha^{n+1} \equiv \beta^{n+1}$ modulo each p_i, which means that n divides U_{n+1}. □

LEMMA 6.2. *With the assumptions of Lemma 6.3, suppose moreover that the k_i are odd and that*

$$\left(\frac{Q}{p_i}\right) = -1 \qquad \textit{for all } i \textit{ such that } 1 \leq i \leq h.$$

Then n is a strong Lucas pseudoprime with respect to the parameters P and Q.

PROOF. As the k_i are odd, the Lemma 2.1 shows that the ratios $(\frac{n+1}{2})/(\frac{p_i+1}{2})$ are odd. From Theorem 6.2, and because $Q = \alpha\beta$, we find

$$\alpha^{(p_i+1)/2} \equiv -\beta^{(p_i+1)/2} \text{ modulo } p_i.$$

Hence, $\alpha^{(n+1)/2} \equiv \beta^{(n+1)/2}$ modulo each p_i, which means, again by Theorem 6.2, that n divides $V_{(n+1)/2}$. □

7. Example

We apply this method to the following set of parameters (P, Q, D):

$$(1,-1,5),\ (1,2,-7),\ (1,-3,13),\ (1,-4,17),\ (3,-1,13),\ (3,5,-11),\ (5,2,17),\ (5,8,-7). \tag{10}$$

In order to satisfy the Legendre symbols conditions of Lemmas 6.3 and 6.4 we can choose

$$\left(\frac{-1}{p_i}\right) = \left(\frac{2}{p_i}\right) = \left(\frac{-3}{p_i}\right) = \left(\frac{5}{p_i}\right) = \left(\frac{-7}{p_i}\right) = \left(\frac{-11}{p_i}\right) = \left(\frac{13}{p_i}\right) = \left(\frac{17}{p_i}\right) = -1$$

for all $i = 1, 2, 3$. Choosing $k_2 = 23$ and $k_3 = 31$, these relations are satisfied as soon as the congruences shown in Table 3 hold.

Table 3.

$p_1 \equiv 3$	(mod 8)
$p_1 \equiv 11$	(mod 12)
$p_1 \equiv 7$	(mod 20)
$p_1 \equiv 27$	(mod 28)
$p_1 \equiv 43$	(mod 44)
$p_1 \equiv 11$	(mod 52)
$p_1 \equiv 23$	(mod 68)

To make the coefficients m_2, m_3 integers, we choose

$$p_1 \equiv 3 \text{ modulo } 23 \qquad \text{and} \qquad p_1 \equiv 27 \text{ modulo } 31.$$

Collecting all these congruences, we find

$$p_1 \equiv 375\,566\,267 \qquad \text{modulo } 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 31.$$

Let $p_1 = 7\,655\,438\,867$. The integers p_1, $p_2 = 23(p_1 + 1) - 1$ and $p_3 = 31(p_1 + 1) - 1$ are all prime, so their product

$$n = 319\,889\,369\,713\,946\,602\,502\,766\,595\,032\,347$$

is a strong Lucas pseudoprime to the parameters listed in (10). In fact, it is also a strong Lucas pseudoprime with respect to other parameters (P, Q, D) such as

$$(1,1,-3), \quad (1,-11,45), \quad (3,1,5), \quad (3,4,-7), \quad (5,9,11), \quad (5,13,-27).$$

8. Conclusion

The Rabin–Miller primality test provides a quite high security which is sufficient for most purposes, but it appears that it is somewhat vulnerable for deliberated attacks. The theoretical results of Alford *et al.* (1994) give strength to this observation. They imply that, for any given set of bases, there exist infinitely many Carmichael numbers which are strong pseudoprimes to all the bases of this set. However, further improvements of the Rabin–Miller test can make it even more secure. As an example, the new release 2.0 of Axiom uses more bases for large numbers: it uses about k bases for $2k$-decimal digits numbers and would be more difficult to break.

The situation is similar for the strong Lucas test. However, these two kinds of test can be combined, for example, as proposed in Pomerance *et al.* (1980) and then in Baillie and Wagstaff (1980). The resulting test seems much more difficult to break. Numerous packages now provide such a test, including Maple release V.3.

References

Alford, R., Granville, A., Pomerance, C. (1994). *On the difficulty of finding reliable witnesses.* Lecture Notes in Computer Science.

Arnault, F. (1995). *Rabin–Miller primality test: Composite numbers which pass it.* Mathematics of Computation, **64** (209) 355–361.

Arnault, F. (submitted). *The Rabin–Monier theorem for Lucas pseudoprimes.*

Baillie, R., Wagstaff S. Jr. (1980). *Lucas pseudoprimes.* Mathematics of Computation, **35**, (152) 1391–1417.

Char, B., Geddes, K., Gonnet, G., Leong, B., Monagan, M., Watt, S. (1991). *Maple V Library Reference Manual.* Springer-Verlag and Waterloo Maple Publishing.

Chernick, J. (1939). *On Fermat's simple theorem.* Bulletin of the American Mathematical Society, **45**, 269–274.

Davenport, J. H. (1992). *Primality Testing Revisited.* In (Wang, P. S., ed.) Proceedings of ISSAC'92 New York, ACM. (Revised in Axiom Technical Report no 6, NAG 1993.)

Jaeschke, G. (1993). *On strong pseudoprimes to several bases.* Mathematics of Computation, **61**, (204), 915–926.

Jenks, R., Sutor, R. (1992). *Axiom, The Scientific Computation System.* Springer-Verlag.

Knuth, D. E. (1973). *The Art of Computer Programming. Part 2: Semi-numerical algorithms.* Addison-Wesley.

Monier, L. (1980). *Evaluation and comparison of two efficient primality testing algorithms.* Theoretical Computer Science, **11**, 97–108.

Pomerance, C., Selfridge, J. L., Wagstaff, S. S. (1980). *The pseudoprimes to* $25 \cdot 10^9$. Mathematics of Computation, **35,** (151), 1003–1026.

Rabin, M. O. (1980). *Probabilistic algorithms for testing primality.* Journal of Number Theory, **12,** 128–138.

Ribenboim, P. (1988). *The Book of Prime Number Records.* Springer-Verlag.

Williams, H. C. (1977). *On numbers analogous to the Carmichael numbers.* Canadian Bulletin of Mathematics, **20,** 133–143.