Dickson Pseudoprimes and Primality Testing*)

Winfried B. Müller
Institut für Mathematik
Universität Klagenfurt
A-9022 Klagenfurt
Austria

Alan Oswald
School of Computing and Mathematics
Teesside Polytechnic
Middlesbrough, Cleveland TS1 3BA
Great Britain

Abstract: The paper gives a general definition for the concept of strong Dickson pseudoprimes which contains as special cases the Carmichael numbers and the strong Fibonacci pseudoprimes. Furthermore, we give necessary and sufficient conditions for two important classes of strong Dickson pseudoprimes and deduce some properties for their elements. A suggestion of how to improve a primality test by Baillie&Wagstaff concludes the paper.

1. Carmichael Numbers

Fermat's Little Theorem plays an important role in many primality tests and in motivating the concept of pseudoprimes. An equivalent formulation of this theorem states that for any prime n and an arbitrary integer b one has

$$b^n \equiv b \bmod n. \tag{1}$$

An odd composite number n for which $b^n \equiv b \bmod n$ for a certain integer b is called a *pseudoprime to the base* b (abbreviated *psp*(b)). If n is not a prime then it is still possible, but not very likely, that (1) holds for a randomly chosen integer b, and even less likely, that (1) holds for all integers b. An odd composite integer n such that $b^n \equiv b \bmod n$ for every $b \in \mathbb{Z}$ is called a *Carmichael number*. An odd composite integer n is a Carmichael number if and only if n is square-free and $(p-1) \mid (n-1)$ for every prime p dividing n (cf. KOBLITZ [7]). The smallest Carmichael number is $n = 561 = 3 \cdot 11 \cdot 17$. CHERNICK [1] gave a method for obtaining Carmichael numbers with three prime factors. For a positive integer t the number $n = (6t+1)(12t+1)(18t+1)$ is a Carmichael number if all three factors of n are prime. A fast method for finding (also very large) Carmichael numbers of this form is due to DUBNER [2]. A table with all Carmichael numbers $\leq 10^{12}$ was calculated by JAESCHKE [6]. However, it is not known if there are infinitely many Carmichael numbers.

*) This work peformed in part at the University of Klagenfurt was supported by the Forschungskommission of the University of Klagenfurt and by the Österreichischer Fonds zur Förderung der wissenschaftlichen Forschung under project no. P6174.

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 512-516, 1991.

2. Generalizations of Fermat's Little Theorem

Let b, c be nonzero integers and α, β be the roots of the polynomial $x^2 - bx + c$. Assume that $d = b^2 - 4c \neq 0$. Then the sequences

$$U_n(b,c) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n(b,c) := \alpha^n + \beta^n, \quad n \geq 0$$

are called the *Lucas sequences associated to the pair* (b,c) (cf. RIBENBOIM [14]). If n is an odd prime and $\gcd(n,d) = 1$, then

$$U_{n-(d/n)} \equiv 0 \bmod n, \tag{2}$$

where (d/n) is the Jacobi symbol. An odd composite integer n such that (2) holds is called a *Lucas pseudoprime with parameters* (b,c) (abbreviated *lpsp*(b,c)).
Comparing probable prime tests based on Fermat's Theorem (1) and on the Lucas test (2) one obtains e.g. 22 *psp*(2)s and only 9 *lpsp*$(1,c)$s less than 10^4, where $c = \frac{1}{4}(1-d)$ and d is the first element of the sequence $5, -7, 9, -11, 13, \cdots$ for which $(d/4) = -1$. As by test (1) with different bases b at least the Carmicheal numbers cannot be exposed as composite, BAILLIE AND WAGSTTAFF [3] suggested a primality test combining Fermat's Theorem with Lucas pseudoprimes. They proved that all of the 21853 *psp*(2)s under $25 \cdot 10^9$ fail the Lucas test (2), where b and c are chosen as above.

At EUROCRYPT'88 DI PORTO AND FILIPPONI [4] proposed another method for finding large probable primes based on the fact that for any prime number n and an arbitrary integer b there holds

$$V_n(b,-1) \equiv b \bmod n. \tag{3}$$

Composite odd integers n with $V_n(1,-1) \equiv 1 \bmod n$ are called *Fibonacci pseudoprimes* (abbreviated *fpsp*$(1,-1)$) and have been studied already by SINGMASTER [15]. FILIPPONI [5] verified experimentally that there exist only 7 *fpsp*$(1,-1)$ under 10^4 and 852 *fpsp*$(1,-1)$ less than 10^8. Numerical tests on odd composite integers n up to 10^{100} suggest that very few such numbers satisfy a combination of congruences $V_n(b,-1) \equiv b \bmod n$ for several b.
According to LIDL, MÜLLER AND OSWALD [10] an odd composite number n is called a *strong Fibonacci pseudoprime* if n satisfies the congruence (3) for every $b \in \mathbb{Z}$. In contrast to Fermat's Theorem there are no strong Fibonacci pseudoprimes $n \leq 10^{13}$ (cf. [10]). In particular, there is no odd composite integer $n \leq 10^8$ which satisfies (2) for all $b \in \mathbb{Z}$ with $1 \leq b \leq 8$ (cf. [5]). However, the question of existence of strong Fibonacci pseudoprimes n has not yet been answered.

3. Strong Dickson Pseudoprimes

By using *Waring's formula* it can be verified that

$$V_n(b,c) = \alpha^n + \beta^n = \sum_{i=0}^{[n/2]} \frac{n}{n-i} \binom{n-i}{i} (-c)^i \, b^{n-2i} =: g_n(b,c), \tag{4}$$

where $[n/2]$ denotes the greatest integer $i \leq \frac{n}{2}$. The polynomial $g_n(x,c)$ is called the *Dickson polynomial of parameter c and degree n.* It is not difficult to show that the coefficients of $g_n(x,c)$ are integers for any positive integer n and any $c \in \mathbb{Z}$.
Properties of Dickson polynomials and their application in cryptography have been studied in great detail (cf. LIDL AND MÜLLER [8], MÜLLER [11], MÜLLER AND NÖBAUER R. [12]). From (4) it can be seen immediately that for any prime n and an arbitrary $b \in \mathbb{Z}$ there holds

$$V_n(b,c) = g_n(b,c) \equiv b \bmod n. \tag{5}$$

Generalizing the definition of strong Fibonacci pseudoprimes, we call an odd composite integer n a *strong Dickson pseudoprime of the kind c* (in short: a *strong c-Dickson pseudoprime*) if $g_n(b,c) \equiv b \bmod n$ for all $b \in \mathbb{Z}$.
Obviously, the strong 0-Dickson pseudoprimes are exactly the Carmichael numbers and the strong (-1)-Dickson pseudoprimes the strong Fibonacci pseudoprimes.

The following theorem gives a reformulation of Theorem 1 in [10].

Theorem 1: *An odd integer n is a strong* (-1)*-Dickson pseudoprime if and only if*
(i) *n is Carmichael number,*
(ii) $2(p_i+1) \mid (n-1)$ *or* $2(p_i+1) \mid (n-p_i)$ *for every prime* p_i *dividing n.*

Improving the results on the minimal number of prime factors of strong (-1)-Dickson pseudoprimes given in [10] we state

Corollary 1: *Any strong* (-1)*-Dickson pseudoprime* $n \equiv 1 \bmod 4$ *must be the product of at least four distinct primes.*
Any strong (-1)*-Dickson pseudoprime* $n \equiv 3 \bmod 4$ *must be the product of at least five distinct primes.*

Proof: For the first statement, let $n = p_1p_2p_3$, whereby p_1, p_2, p_3 are primes with $p_1 < p_2 < p_3$. If n is a strong (-1)-Dickson pseudoprime with $(p_3-1) \mid (n-1)$ and $2(p_3+1) \mid (n-1)$ then $(p_3^2-1) \mid (n-1)$, i.e. $(p_3^2-1) \mid (p_1p_2p_3-1)$. Hence $(p_3^2-1) \mid (p_1p_2-p_3)$, which yields a contradiction.
If n is a strong (-1)-Dickson pseudoprime with $(p_3-1) \mid (n-1)$ and $2(p_3+1) \mid (n-p_3)$

then $(p_3 - 1) \mid (p_1p_2 - 1)$ and $2(p_3 + 1) \mid (p_1p_2 - 1)$. Hence $(p_3^2 - 1) \mid (p_1p_2 - 1)$, which yields a contradiction too.
The second statement was proved already as Corollary 4 in [10]. □

The following necessary und sufficient conditions for strong (+1)-Dickson pseudoprimes can be derived similarly as for (−1)-Dickson pseudoprimes in [10], using a formula for the number of fixed points of the permutation $x \to g_n(x, 1)$ on $\mathbb{Z}/(n)$ given in [13].

Theorem 2. *An odd integer n is a strong (+1)-Dickson pseudoprime if and only if*
(i) *n is square-free,*
(ii) *$((p_i - 1) \mid (n - 1)$ or $(p_i - 1) \mid (n - p_i))$ for every prime p_i dividing n,*
(iii) *$((p_i + 1) \mid (n - 1)$ or $(p_i + 1) \mid (n - p_i))$ for every prime p_i dividing n.*

Corollary 3. *Any strong (−1)-Dickson pseudoprime is also a strong (+1)-Dickson pseudoprime.*

Lemma 1. *A Carmichael number of the form*

$$n = (6t + 1)(12t + 1)\prod_{i=1}^{r-2}(9 \cdot 2^i t + 1) \text{ with } t, r \in \mathbb{Z},\ t \geq 1,\ r \geq 3$$

(cf. [14]) is not a strong (−1)-Dickson pseudoprime.

Proof. If n is a strong (−1)-Dickson pseudoprime then $(p + 1) \mid (n - 1)$ for each prime p dividing n (Theorem 1(ii)). Now $(12t + 1) + 1 = 2(6t + 1)$ and so $(6t + 1) \mid (n - 1)$. But $(6t + 1) \mid n$ and this is a contradiction. □

4. Conclusions and Remarks

It is an open problem if there exist strong c-Dickson pseudoprimes for $c \neq 0$. The numerical evidence collected so far indicates that there are very few odd composite integers n satisfying a combination of congruences $V_n(b, +1) \equiv b \bmod n$ for several arbitrarily chosen b. In accordance with Corollary 3, even fewer integers n satisfy the congruences $V_n(b, -1) \equiv b \bmod n$ for several b (cf. LIDL AND MÜLLER [9]). The scarcity of odd composite integers passing only a small number of tests by congruence (5) with different parameters c suggests a fast probabilistic primality test combining such tests. In general, one needs less tests to disclose an odd composite integer n as not prime using congruence (5) with negative parameters c rather than positive ones. E.g., there are only 24 composed odd numbers under 10^6 passing test (5) with $(b, c) = (3, -3)$ and up to $3.7\text{x}10^6$ only the composed odd number 1 909 001 with the factor 461 passes the tests (5) for $(b, c) =$

$(1,-1)$ and $(b,c) = (3,-3)$. But this number is disclosed by the test with $(b,c) = (2,-1)$ too. Hence, a combination of several tests by congruence (5) with a few different negative parameters c seems to be more efficient than the proposed primality test by Baillie&Wagstaff combining tests by congruence (1) and (2). Numerical evidence for this statement for the numbers up to 10^9 is in progress.

References

[1] CHERNICK J.: On Fermat's simple theorem. Bull.Amer.Math.Soc. **45**, 269–274 (1939).

[2] DUBNER H.: A New Method for Producing Large Carmichael Numbers. Math.Comp. **53**, No. 187, 411–414 (1989).

[3] BAILLIE, R., WAGSTAFF JR., S.S.: Lucas pseudoprimes. Math.Comp. **35**, 1391–1417 (1980).

[4] DI PORTO, A., FILIPPONI, P.: A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers. In: Advances in Cryptology – Eurocrypt'88, Lecture Notes in Computer Science **330**, Springer–Verlag, New York–Berlin–Heidelberg, pp. 211–223, 1988.

[5] FILIPPONI, P.: Table of Fibonacci Pseudoprimes to 10^8. Note Recensioni Notizie **37**, No. 1–2, 33–38 (1988).

[6] JAESCHKE, G.: Math.Comp. **55**, No. 191, 383–389 (1990).

[7] KOBLITZ, N.: A Course in Number Theory and Cryptography. Springer–Verlag, New York–Berlin–Heidelberg, 1987.

[8] LIDL, R., MÜLLER, W.B.: Permutation polynomials in RSA-cryptosystems. Advances in Cryptology - Crypto '83 (ed. D.Chaum), New York, Plenum Press, pp. 293–301, 1984.

[9] LIDL, R., MÜLLER, W.B.: Generalizations of the Fibonacci Pseudoprimes Test. To appear in Discrete Mathem. **92** (1991).

[10] LIDL, R., MÜLLER, W.B., OSWALD A.: Some Remarks on Strong Fibonacci Pseudoprimes. Applicable Algebra in Engineering, Communication and Computing (AAECC) **1**, 59–65 (1990).

[11] MÜLLER, W.B.: Polynomial Functions in Modern Cryptology. In: Contributions to General Algebra **3**, Teubner–Verlag, Stuttgart, pp. 7–32, 1985.

[12] MÜLLER, W.B., NÖBAUER R.: Cryptanalysis of the Dickson-scheme. In: Advances in Cryptology – Eurocrypt'85, Lecture Notes in Computer Science **219**, Springer–Verlag, New York–Berlin–Heidelberg, pp. 50–61, 1986.

[13] NÖBAUER, W.: Über die Fixpunkte der Dickson–Permutationen. Sb.d.Österr.Akad.-d.Wiss., math.-nat.Kl., Abt.II, Bd. **193**, 115–133 (1984).

[14] RIBENBOIM, P.: The Book of Prime Number Records. Springer–Verlag, New York–Berlin–Heidelberg, 1988.

[15] SINGMASTER, D.: Some Lucas pseudoprimes. Abstracts Amer.Math.Soc. **4**, No.83T-10-146, p.197 (1983).