Building Carmichael numbers with a large number of prime factors and generalization to other numbers

D. Guillaume, François Morain

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tél.:(1) 39 63 55 11

Rapports de Recherche

1992

25ème anniversaire

N° 1741

Programme 2
Calcul Symbolique, Programmation
et Génie logiciel

BUILDING CARMICHAEL NUMBERS WITH A LARGE NUMBER OF PRIME FACTORS AND GENERALIZATION TO OTHER NUMBERS

Dominique GUILLAUME
François MORAIN

Août 1992

RR-1741

BUILDING CARMICHAEL NUMBERS WITH A LARGE NUMBER OF PRIME FACTORS AND GENERALIZATION TO OTHER NUMBERS

Dominique GUILLAUME *
François MORAIN † ‡ §

Abstract. We extend the method of Löh and Niebuhr for the generation of Carmichael numbers with a large number of prime factors to other classes of pseudoprimes. In particular, we exhibit the first known strong Fibonacci pseudoprimes. The method can be viewed as a simplified version, yet practical, of the method used by Alford, Granville and Pomerance to prove that there is an infinite number of Carmichael numbers.

CONSTRUCTION DE NOMBRES DE CARMICHAEL AVEC UN GRAND NOMBRE DE FACTEURS PREMIERS ET GENERALISATION A D'AUTRES NOMBRES

Résumé. Nous étendons la méthode de construction de nombres de Carmichael avec un grand nombre de facteurs premiers, due à Löh et Niebuhr, à d'autres classes de nombres pseudopremiers. En particulier, nous donnons les premiers exemples connus de nombres pseudopremiers de Fibonacci forts. La méthode peut être vue comme une version simplifiée et pratique, de la méthode utilisée par Alford, Granville et Pomerance pour prouver qu'il existe une infinité de nombres de Carmichael.

* 19 rue Grange Dame Rose 78140 Vélizy, France

† LIX, Laboratoire d'Informatique de l'Ecole Polytechnique Ecole, Polytechnique, 91128 Palaiseau Cedex, France

‡ Projet ALGORITHMES, INRIA, Domaine de Voluceau, B. P. 105, 78153 LE CHESNAY CEDEX (France).

§ On leave from the French Department of Defense, Délégation Générale pour l'Armement.

BUILDING CARMICHAEL NUMBERS WITH A LARGE NUMBER OF PRIME FACTORS AND GENERALIZATION TO OTHER NUMBERS

D. Guillaume * F. Morain †‡§

June 30, 1992

Abstract

We extend the method of Löh and Niebuhr for the generation of Carmichael numbers with a large number of prime factors to other classes of pseudoprimes. In particular, we exhibit the first known strong Fibonacci pseudoprimes. The method can be viewed as a simplified version, yet practical, of the method used by Alford, Granville and Pomerance to prove that there is an infinite number of Carmichael numbers.

1 Introduction

A Carmichael number C is a composite integer for which the identity

$$a^{C-1} \equiv 1 \bmod C$$

holds for all values of a prime to C. These numbers are of interest in the study of pseudoprimality tests, where they can be seen as worst cases for the Fermat compositeness test (see [29]). We denote by $\mathcal{C}(x)$ the number of Carmichael numbers up to x. Many properties of these numbers are described in [32].

Recent tables of Carmichael numbers include that of Keller up to 10^{13} (see [16]), that of Jaeschke [15] up to 10^{12} (Jaeschke gave $\mathcal{C}(10^{12}) = 8238$ but the correct value was found by Keller: $\mathcal{C}(10^{12}) = 8241$; this is in agreement with our own calculations and that of Pinch) and by Pinch up to 10^{15} (see [28]).

Yorinaga [39] has found many Carmichael numbers using several methods including Chernick's "extension Theorem" (see Section 2). In particular, he found numbers with 12 and up to 15 prime factors. Pinch found the smallest numbers with up to 20 factors [28]. Wagstaff [36] used the so-called "universal forms" of Chernick [6] to find large Carmichael numbers. Woods and Huenemann [38] gave larger numbers using the extension Theorem. Dubner [9] found even larger Carmichael

*19 rue Grange Dame Rose 78140 Vélizy, France

†LIX, Laboratoire d'Informatique de l'Ecole Polytechnique Ecole Polytechnique, 91128 Palaiseau Cedex, France

‡Institut National de Recherche en Informatique et en Automatique (INRIA), Domaine de Voluceau, B. P. 105 78153 LE CHESNAY CEDEX (France).

§On leave from the French Department of Defense, Délégation Générale pour l'Armement.

numbers using a modification of the universal forms, culminating in a 3710-digit number (Dubner informed the second author that he found a 6025-digit number with his method). Löh and Niebuhr have built numbers with up to 10058 factors and 81488 digits [23, 24]. Recently, Zhang has built a Carmichael number with 1305 prime factors and 8340 digits.

The purpose of this paper is to analyze the method used by Löh and Niebuhr and to extend it to other classes of numbers.

By one of these coincidences frequently occurring in Science, Carmichael numbers were studied simultaneously by many people with many striking independent results. We began to work on that topic around August 1991. At the end of 1991, we had built Carmichael numbers with up to 5000 prime factors, as well as other numbers that will be described later. The paper was finished at the end of January, 1992 (this formed [14]). At this point, we learned that, following the work of Zhang [40], Alford, Granville and Pomerance had just proved that there is an infinite number of Carmichael numbers [1]. Then, around May 15, 1992, we heard from the work of Keller and Löh and Niebuhr. (We note that very few people were aware of this work.) Though part of our work is subsumed by that of Löh and Niebuhr (according to a private communication of Keller, they have built numbers with 125,000 and 500,000 prime factors), we think we shed some light on their method, including an analysis of it and some refinements. Moreover, we generalized it to other classes of pseudoprime numbers.

The paper is organized as follows. First, we recall some basic facts on Carmichael numbers. Next, we present the algorithm of Löh and Niebuhr. We compare the method with that of Zhang. Then, we generalize this work to other classes of numbers, such as Williams's numbers and elliptic pseudoprimes. Also, we address the problem of finding *strong Fibonacci pseudoprimes* and we give the first known examples of such numbers. We conclude with some remarks on problems related to Carmichael numbers: we discuss Lehmer's problem and Giuga's problem. We also state some conjectures related to the major result of Pomerance.

2 Background

The defining property of Carmichael numbers is equivalent to [6, Theorem 1]

Theorem 2.1 *A Carmichael number C is an odd squarefree composite number, $C = p_1 \cdots p_r$ with $r \geq 3$ such that*

$$C - 1 \equiv 0 \bmod (p_i - 1) \text{ for } 1 \leq i \leq r. \tag{1}$$

An alternative statement is that

$$\lambda(C) \mid C - 1$$

where λ denotes Carmichael's function (see [33]). Recall that $\lambda(p^e) = \varphi(p^e)$ for p an odd prime (φ is Euler's totient function) or $p = 2$ and $e \leq 2$, $\lambda(2^e) = 2^{e-2}$ for $e > 2$ and

$$\lambda\left(\prod_{i=1}^{r} p_i^{e_i}\right) = \operatorname{lcm}(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r})).$$

From this, we easily derive the property that

$$p_j \not\equiv 1 \bmod p_i \text{ for } 1 \leq i < j \leq r. \tag{2}$$

For convenience, we cite Chernick's "extension" Theorem, which makes it possible to construct larger Carmichael numbers from a known one.

Theorem 2.2 *Let $C = p_1 \cdots p_r$ be a Carmichael number and $L = \lambda(C) = \mathrm{lcm}(p_1 - 1, \ldots, p_r - 1)$. Put $D = (C-1)/L$. If there is a divisor F of D for which $p = FL + 1$ is a prime distinct from the p_i's, then pC is a Carmichael number.*

3 The algorithm

3.1 The idea

The idea of [23, 40, 14, 1] is to search for Carmichael numbers C with a fixed value of $\Lambda = \lambda(C)$.

Let

$$S(\Lambda) = \{p, p \text{ prime}, p \nmid \Lambda, p - 1 \mid \Lambda\}.$$

It is clear that a squarefree product N of elements of $S(\Lambda)$ satisfies

$$\lambda(N) \mid \Lambda$$

as well as property (2). Suppose one wants to find Carmichael numbers with r factors built up with the primes of $S := S(\Lambda)$. It is enough to look for r distinct elements $p_1, \ldots, p_r$ of S such that

$$C := p_1 \times \cdots \times p_r \equiv 1 \bmod \Lambda.$$

If this is the case, we have $C \equiv 1 \bmod \lambda(C)$ since $\lambda(C) \mid \Lambda$.

3.2 An informal description of the algorithm

Let $t = \mathrm{Card}(S)$ and

$$P(S) = \prod_{p \in S} p.$$

Suppose one is looking for a Carmichael number with r prime factors, $r < t$ and $u = t - r$ small. One looks for u primes of S, say $\Theta = \{\theta_1, \ldots, \theta_u\}$ such that

$$\Pi(\Theta) := P(S)/(\theta_1 \cdots \theta_u) \equiv 1 \bmod \Lambda.$$

We examine all u-tuples of primes θ_i in S in order to find a good one. Let us describe the program.

procedure FindCarmichael$(S(\Lambda), r)$

(* one wants r-factor numbers *)

1. Set $t = \mathrm{Card}(S)$, $u = t - r$.
2. Compute $P_\Lambda = \prod_{p \in S} p \bmod \Lambda$.
3. For all u-tuples of distinct primes $\theta_1, \ldots, \theta_u$, check whether

$$\theta_1 \times \theta_2 \times \cdots \times \theta_u \equiv P_\Lambda \bmod \Lambda. \tag{3}$$

Löh and Niebuhr used this idea to find a 81488-digit number with 10058 prime factors.

3.3 A rough analysis; choice of Λ

One can see the situation as follows. One builds the sets of squarefree products of u elements of S

$$S_u = \{p_1 \cdots p_u \bmod \Lambda, p_i \neq p_j, p_i \in S\}$$

and we ask: When does S_u contain the residue $P_\Lambda := P(S) \bmod \Lambda$? It certainly does if $S_u = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$. A necessary condition for that is of course

$$\binom{t}{u} > \mathrm{Card}((\mathbf{Z}/\Lambda\mathbf{Z})^\times) = \varphi(\Lambda). \tag{4}$$

Experiments show that this condition is sufficient in practice. (A more careful study of this problem is carried out in section 5.) Let u_0 denote the first u satisfying (4). As a consequence, when $u \geq u_0$, the probability that $p_1 \cdots p_u \equiv P_\Lambda \bmod \Lambda$ is (of the order of magnitude of) $1/\varphi(\Lambda)$. This suggest to choose Λ with a "small" value of $\varphi(\Lambda)$. This we will explain below.

Since one wants Carmichael numbers with many factors, a good Λ is one for which the set $S(\Lambda)$ contains many prime numbers. Therefore, Λ must have many divisors. For the sake of simplicity, one chooses the set

$$\mathcal{Q} = \{q_1 = 2, \ldots, q_s\}$$

with q_i the i-th prime and an s-tuple of positive integers $\mathcal{A} = (A_1, \ldots, A_s)$, from which we compute

$$\Lambda(\mathcal{Q}, \mathcal{A}) = q_1^{A_1} \cdots q_s^{A_s}.$$

The set S is then

$$S(\mathcal{Q}, \mathcal{A}) = \left\{ p \text{ prime } \mid p \notin \mathcal{Q} \text{ and } p - 1 = \prod_{i=1}^{s} q_i^{\alpha_i}, 0 \leq \alpha_i \leq A_i \right\}.$$

An advantage of this construction is that proving the primality of such numbers p is quite simple since the factorization of $p - 1$ is known (see [3]).

Löh decided to choose the values of the exponents $\mathcal{A}$ that yield highly composite values of Λ (recall that a *highly composite number* n is such that $m < n$ implies that m has fewer divisors than n; these numbers were first studied by Ramanujan [31], see also [27]). In our implementation, we preferred *highly prime* values of Λ, that is these numbers n for which $S(n)$ has more elements than $S(m)$ for $m < n$.

3.4 Description of our implementation

We suppose that a pair $(\mathcal{Q}, \mathcal{A})$ is given and therefore, we drop any mention of these in the following, in order to simplify the notations.

Property (3) is checked by means of the Chinese Remainder Theorem by replacing Λ by a suitable product $m_1 \times \cdots \times m_k$ of integers $m_i < 2^{16}$ and $m_1 > m_2 > \cdots > m_k$. We check

$$\Pi(\Theta) \equiv 1 \bmod m_j$$

or

$$\theta_1 \times \cdots \times \theta_u \equiv P(S) \bmod m_j := \rho_j$$

a quantity that is precomputed and that depends only on $\mathcal{Q}$ and $\mathcal{A}$.

It should be noted that we first look for θ's such that their product satisfies $\theta_1 \times \cdots \times \theta_u \equiv \rho_1 \bmod m_1$ and we check the remaining congruences only if needed. This does not occur too frequently, since m_1 is the largest modulus and that it captures almost all the information.

As such, the algorithm (named ALGORITHM0) needs to examine all u-tuples of primes in S. The cost is

$$O\left(\binom{t}{u}(u\mathcal{M})\right)$$

where $\mathcal{M}$ is the cost of a multiplication modulo a 16-bit number. Asymptotically, this cost is

$$C_0(t) = O(t^u).$$

We can do better.

3.4.1 First improvement

ALGORITHM1 is as follows. What we do is to examine all $(u-1)$-tuples and find θ_u such that

$$\theta_u \equiv P(S)/(\theta_1 \cdots \theta_{u-1}) \bmod \Lambda.$$

If θ_u is in S and different from the previous θ_i's, we have found a Carmichael number. (Note that θ_u is also computed by using the Chinese Remainder Theorem.) For this to be efficient, we sort S. The cost of the precomputations is $O(t \log t)$ and the time required for the algorithm is

$$O\left(\binom{t}{u-1}((u-1)\mathcal{M} + c_1 \log t)\right)$$

where $c_1 \log t$ is the cost of testing whether θ_u is in S. Asymptotically, the cost of the algorithm is

$$C_1(t) = O(t^{u-1} \log t).$$

The number of combinations is reduced, but we increased the space needed.

3.4.2 Second improvement

The best we can do in the same direction is to compute S_2, sort it, which takes $O(t^2 \log t)$ operations and then look for an $(u-2)$-tuple $(\theta_1, \ldots, \theta_{u-2})$ such that

$$P(S)/(\theta_1 \times \cdots \times \theta_{u-2}) \bmod \Lambda$$

is in S_2. When this is so, there exists p and q in S such that

$$P(S)/(\theta_1 \times \cdots \times \theta_{u-2}) \equiv p \times q \bmod \Lambda$$

and we have a Carmichael number, provided p and q are different from the θ_i's. The asymptotic cost of the algorithm (named ALGORITHM2) is now

$$C_2(t) = O(t^{u-2} \log t).$$

This is the best we can do, since u is always less than 6 and that storage is now $O(t^2)$ which can be quite large.

Remarks. In practice, we have slightly less than $t(t-1)/2$ numbers in S_2 since there are some pairs (p_1, p_2) in S which yields the same value of $p_1 p_2 \bmod \Lambda$. This is a minor nuisance, but it has to be taken into account when looking for p and q in the process described above.

3.4.3 Third improvement

Let us consider the following example. The largest number we found (before learning about Löh) was obtained with $\Lambda^* = 2^7 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29$. For this, $S(\Lambda)$ has 5111 elements. Our method would have required to examine all 5-tuples of primes in $S(\Lambda)$, that is approximately 29×10^{15} numbers. In order to decrease this number, we used the following idea. Since $P(S)/3697 \equiv 1 \bmod (2^3 \times 3^2 \times 5^2 \times 11 \times 29)$, we decide to keep those elements of S congruent to 1 mod 574200 and ± 1 mod 17, making a subset of 117 primes. Looking at every combination of numbers 6 by 6 (there are less than 3×10^9 combinations), one finds 13 Carmichael numbers with more than 37000 decimal digits, the largest of which is

$$P/(3697 \times 195228001 \times 634491001 \times 5075928001 \times 8553283201 \times 17960976001 \times 545271804001),$$

a 37425-digit number with 5105 prime factors.

3.5 Remarks

3.5.1 Using outside primes

While working out our ideas, we tried to modify the algorithm so as to produce Carmichael numbers all of which prime factors where in $S(\Lambda)$ but for one. More precisely, we look for $C = p_1 \times \cdots \times p_{r-1} \times p_r = Rp_r$ with p_r satisfying

$$p_r R \equiv 1 \bmod \operatorname{lcm}(K, p_r - 1)$$

with $K = \lambda(R)$. Equivalently $p_r \equiv 1/R := a \bmod K$ and $(R-1)/g \equiv 0 \bmod (p_r - 1)/g$ where $g = \gcd(a-1, K, R-1)$ (see [15]). Given a set $(p_1, \ldots, p_{r-1})$, we let p_r run through the arithmetic progression $a + XR$. Very often, a is itself a prime and we hope that $a - 1 \mid R - 1$. We note also that if a q divides all the numbers $p_i - 1$, for $1 \le i \le r-1$, then q divides $R-1$ and also $a-1$, which increases somewhat the probability that $a - 1 \mid R - 1$. Thus, we force the $p_i - 1$ to have all the q's in common. We found a 252-factor number, computed from $S(\{2,3,5,7\},(7,6,3,3))$, a set of 257 prime numbers. We took as the set

$$\{p_1, \ldots, p_{251}\} = S \backslash \{972001, 1088641, 5334337, 14817601, 100018801, 571536001\}.$$

For these numbers, we have $K = 4000752000 = 2^7 \times 3^6 \times 5^3 \times 7^3$ and $a = 813401$ which happens to be a prime dividing $R-1$, so that $p_{252} = a$. This yields a 1157-digit number.

3.5.2 Comparison with Zhang's method

Zhang uses also highly composite values of Λ. Then, he partitions $S(\Lambda)$ as $\Sigma_1 \cup \Sigma_2$ where Σ_2 contains $t - n$ primes. For a subset T of Σ_2 with $t - n - h$ elements ($h \ge 0$), he computes

$$f = \prod_{p \in T} p$$

and

$$g \equiv 1/f \bmod \Lambda.$$

If g is squarefree and has all its prime factors in Σ_1, then fg is a Carmichael number. From a numerical point of view, the largest Carmichael number obtained is a 1305-factor number with 8340 decimal digits.

3.5.3 Generalization to the generation of pseudoprimes

If we just want pseudoprimes to base a, it is easy to modify the construction of the set S. Let $l_a(p)$ denote the order of a modulo p. Then S should be chosen as

$$S(\Lambda) = \{p, p \text{ prime}, p \nmid \Lambda, l_a(p) \mid \Lambda\}.$$

4 Generalization to other classes of numbers

4.1 Williams numbers

4.1.1 Theory

Let P and Q be two integers such that the quantity $\Delta = P^2 - 4Q$ is a non-zero integer (Δ is called the discriminant). Let α and β be the roots of the equation $X^2 - PX + Q = 0$. Then, the Lucas sequences are defined as

$$V_n(P,Q) = \alpha^n + \beta^n, U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

These sequences have many properties (see [19] or [32]), including arithmetical ones. In particular

Theorem 4.1 *Let p be an odd prime such that $p \nmid Q$. Then*

$$U_{p-\epsilon(p)}(P,Q) \equiv 0 \bmod p$$

where $\epsilon(p)$ is the Legendre symbol $\left(\frac{\Delta}{p}\right)$.

A *Lucas pseudoprime* for parameters (P,Q) is an odd composite integer N which satisfies $U_{N-\epsilon(N)} \equiv 0 \bmod N$. (Here $\epsilon(N)$ is the Jacobi symbol $\left(\frac{\Delta}{N}\right)$.)

Let Δ be a fixed integer. Williams [37] studied the properties of the numbers N for which

$$U_{N-\epsilon(N)} \equiv 0 \bmod N$$

for all choices of integers (P,Q) such that $(P,Q) = 1$, $P^2 - 4Q = \Delta$ and $(N, \Delta Q) = 1$. Let us call such a number a Δ–Lucas pseudoprime (or Δ–Lpsp in short). The following Theorem is then proved.

Theorem 4.2 *If N is a Δ–Lpsp, then N is a squarefree product of primes $p_1, \ldots, p_k$ such that*

$$p_i - \epsilon(p_i) \mid N - \epsilon(N).$$

4.1.2 Practice

The modified algorithm is as follows. Fix an integer Δ and a number Λ. Build the set

$$S_\Delta(\Lambda) = \{p \text{ prime}, p - \epsilon(p) \mid \Lambda, p \nmid \Lambda\}.$$

As before, denote by t the cardinality of $S_\Delta(\Lambda)$ and

$$P(S_\Delta) = \prod_{p \in S_\Delta(\Lambda)} p.$$

Let u be a small integer. We look for a squarefree product of u elements of $S_\Delta(\Lambda)$ such that

$$\theta_1 \times \cdots \times \theta_u \equiv \pm P(S_\Delta) \bmod \Lambda.$$

If so, we put $N = P(S_\Delta)/(\theta_1 \times \cdots \times \theta_u)$ and if $\epsilon(N) = \epsilon(P(S_\Delta)) \prod_i \epsilon(\theta_i)$, we have found a Δ–Lpsp.

Take for example $\Delta = 7$ and $\Lambda = 2^{10} \times 3^7 \times 5^3$. Then $t = \mathrm{Card}(S_7(\Lambda)) = 109$. We look for $u = 5$ numbers to exclude from the product $P(S_7)$. We find that

$$P(S_7) \equiv 17 \times 359 \times 1459 \times 23039 \times 143999 \bmod \Lambda$$

and $\epsilon(P(S_7)) = +1 = \epsilon(17)\epsilon(359)\epsilon(1459)\epsilon(23039)\epsilon(143999) = (-1) \times (-1) \times (+1) \times (-1) \times (-1) = +1$. The corresponding number N is a 427-digit number.

The largest number is built up from $S_{43}(\Lambda^*)$ which contains 5047 primes. One excludes 4639 and looks for combinations of 8 out of the 71 primes that are congruent to ± 1 mod $(2^4, 3^3, 5^2, 7, 23, 29)$. One finds 24 numbers which are 43-Lpsp, the largest of which is

$$P(S_{43})/(4639 \times 6303151 \times 1008503999 \times 1714456801 \times 2867933249 \times 5150574001 \times 18241820351$$
$$\times 4290428141999 \times 18632716502401),$$

a 36869-digit number with 5038 prime factors.

4.2 Elliptic pseudoprimes

4.2.1 Theory

For the definition of *elliptic pseudoprimes*, we refer to [12] (see also [13]). For our purpose, it is enough to cite the following result. Let D be an integer among $\{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.

Proposition 4.1 *Let N be a squarefree composite number. If for all prime p dividing N, one has $\left(\frac{-D}{p}\right) = -1$ and $p + 1 \mid N + 1$, then N is a D-elliptic pseudoprime (in short D-ellpsp).*

4.2.2 Practice

The algorithm is exactly that used for Williams numbers. For a given D, the set $S_D(\Lambda)$ is

$$S_D(\Lambda) = \{p \text{ prime}, \left(\frac{-D}{p}\right) = -1, p + 1 \mid \Lambda, p \nmid \Lambda\}.$$

We have to find a squarefree N with an odd number of prime factors that satisfies $N \equiv -1$ mod Λ since we must have

$$\left(\frac{-D}{N}\right) = \prod_{p \mid N} \left(\frac{-D}{p}\right) = -1.$$

For example, taking the value of Λ used in Section 2 and taking $D = 43$, we find that $\#S_{43}(\Lambda) = 1095$. We find that

$$P(S_{43}(\Lambda))/(71 \times 4009823 \times 36837503 \times 42325919 \times 214885439 \times 504092159)$$

is a 7015-digit 43-ellpsp.

For $\Lambda = \Lambda^*$, one finds that $S_{43}(\Lambda)$ has 2470 elements. After exclusion of 113 and with those primes congruent to ± 1 mod $(3^3, 7, 11, 13, 17)$, one finds that

$$P(S_{43}(\Lambda^*))/(113 \times 41887 \times 2475199 \times 8576567 \times 373080707 \times 1867941503 \times 3331520191 \times 7461614159 \times 22882283423)$$

is a 18026-digit number with 2461 prime factors.

4.3 Strong Fibonacci pseudoprimes

4.3.1 Definition and properties

In 1988, Di Porto and Filipponi introduced a new class of pseudoprimes called *Fibonacci pseudoprimes of the m-th kind* [30]. Let c be an integer. The Dickson polynomial of parameter c and degree n is defined as (see [8, 18])

$$g_n(x, c) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-c)^i x^{n-2i}.$$

An odd composite integer N is called a *Fibonacci pseudoprime of the m-th kind* if

$$g_N(m, -1) \equiv m \bmod N. \tag{5}$$

A number N satisfying (5) for all m such that $1 \leq m \leq M$ is called *M-strong Fibonacci pseudoprime.* Then, an $N - 1$-strong Fibonacci pseudoprime is simply called *strong Fibonacci pseudoprime.*

In [21], the following theorem is proved.

Theorem 4.3 *An odd integer N is a strong Fibonacci pseudoprime if and only if N is a Carmichael number and N is either the product of an arbitrary number of prime factors $p_i \equiv 1 \bmod 4$ such that*

$$(p_i + 1) \mid N - 1 \text{ or } (p_i + 1) \mid N + 1$$

and of an even number of primes $p_i \equiv 3 \bmod 4$ which satisfy

$$2(p_i + 1) \mid N - 1$$

(this forms type I) or N is the product of an odd number of primes $p_i \equiv 3 \bmod 4$ such that

$$2(p_i + 1) \mid N - p_i$$

(this forms type II).

However, no number of this form was found. A proof that no such number exist would have led to a new characterization of prime numbers.

4.3.2 Computations

Since an SF-psp is a Carmichael number, we start by building a Carmichael number as described above. We put $\Lambda = 2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19$ and build

$$S = \{p, p \text{ prime}, p-1 \mid \Lambda, 2(p+1) \mid \Lambda\}.$$

We find that $\text{Card}(S) = 40$. We now apply the method of section 3 and find a squarefree product of elements, call it N, such that $N \equiv 1 \bmod \Lambda$. By construction, one has $p-1 \mid N-1$ and $2(p+1) \mid N-1$.

Using the same argument as in section 3, the smallest value of u for which

$$\binom{40}{u} > \varphi(\Lambda) \approx 33.44 \times 10^9$$

is $u = 15$. We examine every combination of 14 numbers of S and try to find a suitable 15-th prime in S. We finally found that

$$\begin{aligned} N &= 29 \times 31 \times 37 \times 43 \times 53 \times 67 \times 79 \times 89 \times 97 \times 151 \times 181 \times 191 \times 419 \times 881 \times 883 \\ &= 589398328999039533470003707 2001 \end{aligned}$$

is a SF-psp. Note that

$$N - 1 = 2^7 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 1949 \times 894811 \times 3456585949$$

and

$$N + 1 = 2 \times 142591 \times 351256343 \times 58838638438298777.$$

The factorizations are listed in Table 1. By construction, N is of type I and moreover, all prime factors p of N are such that $p-1 \mid N-1$ and $p+1 \mid N-1$. We found some other numbers, also of type I:

$$\begin{aligned} SF_2 &= 23 \times 29 \times 31 \times 41 \times 43 \times 53 \times 71 \times 89 \times 97 \times 103 \times 131 \times 151 \times 199 \times 379 \\ &\quad \times 449 \times 1429 \times 3457 \times 4159 \\ &= 167872834324702870101415827333360777 6001, \\ SF_3 &= 23 \times 31 \times 43 \times 71 \times 101 \times 103 \times 109 \times 131 \times 151 \times 181 \times 191 \times 199 \times 271 \\ &\quad \times 307 \times 419 \times 571 \times 881 \times 911 \times 1429 \times 1871 \times 5851 \times 11969 \\ &= 1004756342588133553725629648229826997641769714873961601, \\ SF_4 &= 23 \times 31 \times 37 \times 41 \times 53 \times 67 \times 97 \times 101 \times 109 \times 151 \times 181 \times 191 \times 197 \times 239 \\ &\quad \times 271 \times 379 \times 419 \times 449 \times 571 \times 701 \times 911 \times 1429 \times 2549 \times 5851 \\ &= 151381197297673254570192926273745833804231848549434336001. \end{aligned}$$

Shortly after our discovery, Pinch (private communication) found the smallest SF-psp by inspection of his tables of Carmichael numbers up to 10^{15} (see [28]). With his kind permission, we list it here. It is

$$SF' = 443372888629441 = 17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331.$$

The number found by Pinch has also the same property. It seems harder to build SF-psp's which are of type II.

p	$p \bmod 4$	$p-1$	$p+1$
29	1	$2^2 \times 7$	$2 \times 3 \times 5$
31	3	$2 \times 3 \times 5$	2^5
37	1	$2^2 \times 3^2$	2×19
43	3	$2 \times 3 \times 7$	$2^2 \times 11$
53	1	$2^2 \times 13$	2×3^3
67	3	$2 \times 3 \times 11$	$2^2 \times 17$
79	1	$2 \times 3 \times 13$	$2^4 \times 5$
89	1	$2^3 \times 11$	$2 \times 3^2 \times 5$
97	1	$2^5 \times 3$	2×7^2
151	3	$2 \times 3 \times 5^2$	$2^3 \times 19$
181	1	$2^2 \times 3^2 \times 5$	$2 \times 7 \times 13$
191	3	$2 \times 5 \times 19$	$2^6 \times 3$
419	3	$2 \times 11 \times 19$	$2^2 \times 3 \times 5 \times 7$
881	1	$2^4 \times 5 \times 11$	$2 \times 3^2 \times 7^2$
883	3	$2 \times 3^2 \times 7^2$	$2^2 \times 13 \times 17$

Table 1: Factorization of $p-1$ for the first known SF-psp

4.4 Some negative results

Let us end this section with numbers that our method cannot tackle.

4.4.1 A question of Williams

In [37], Williams asked the following: Does there exist a Carmichael number C such that C is Δ–Lpsp for a fixed Δ with $\left(\frac{\Delta}{C}\right) = -1$? If such a number exists, then for all primes p dividing C, one must have $p-1 \mid C-1$ and $p+1 \mid C+1$.

For our method to work, we would need a set of primes p such that $p-1 \mid \Lambda_-$ and simultaneously $p+1 \mid \Lambda_+$ with $\gcd(\Lambda_-, \Lambda_+) \mid 2$. Experiments made so far show that it is hard to get values of $\Lambda_\pm$ reasonably small for our method to work rapidly.

In [29], the authors offer some money for the exhibition of a number N which is strong pseudoprime to base 2 as well as a Lucas pseudoprime for the "first natural" discriminant. For this, we would need the same construction as above, but this time we insist on $l_2(p) \mid \Lambda_-$. Even this seems out of reach for our method.

4.4.2 Lehmer's problem

In [20] Lehmer raised the following question: does there exist composite integers for which

$$\varphi(N) \mid N-1$$

where φ is Euler function. In view of [22, 17, 7] (see also [32]), such a number N, being a Carmichael number, must have a large number of prime factors (at least 14 and many more if $3 \mid N$). It is tempting to look at our numbers and test whether they satisfy the condition. However, a look at

the power of 2 dividing $N-1$ ordinarily shows that this cannot be the case. More precisely, if N has r factors, then 2^r must divide $N-1$. Moreover, if 5 divides $p-1$ for many p's dividing N, then N must have many trailing zeros, which we can spot at once.

4.4.3 Giuga's problem

In [11], Giuga asked whether there exist composite integers N such that

$$N \mid 1^{N-1} + 2^{N-1} + \cdots + (N-1)^{N-1} + 1.$$

Equivalently, N must be a Carmichael number and satisfy

$$p \mid N \Rightarrow \frac{N-1}{p-1} \equiv 1 \bmod p^2.$$

(See [32]). By [2], such an N must be greater than 10^{1700}. We did not found any Carmichael number built with our method that satisfies this property.

5 Speculations

Let us come back to the idea of the algorithm. We can see the situation as follows. We build the sets

$$S_u = \{p_1 \ldots p_u \bmod \Lambda, p_i \neq p_j, p_i \in S\}$$

and we wonder when S_u contains 1 or a particular residue. Our main conjecture is the following:

Conjecture 5.1 *With the preceding notations, there exists an infinite number of Λ for which there exists an integer u less than $t = \mathrm{Card}(S(\Lambda))$ satisfying $1 \in S_u$.*

If this conjecture is true, then there exists a Carmichael number with u factors, since we have proved the existence of a u-tuple of primes in S of product 1.

The best we can say is that if there exists u such that $S_u = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$, the problem is solved. A necessary condition on u is that

$$\binom{t}{u} > \varphi(\Lambda).$$

We are led to:

Conjecture 5.2 *With the same notations, if for $u > 2$, one has*

$$\binom{t}{u} > \varphi(\Lambda)$$

then $S_u = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$. Moreover, the expected number of Carmichael numbers is $\binom{t}{u}/\varphi(\Lambda)$, so that the total number of Carmichael numbers built up from $S(\Lambda)$ should be about $2^t/\varphi(\Lambda)$.

Note that the preceding conjecture is false if we consider arbitrary subsets S of $(\mathbf{Z}/\Lambda\mathbf{Z})^\times$. In particular, if S is included in a proper subgroup of $(\mathbf{Z}/\Lambda\mathbf{Z})^\times$, then this is trivially false. However, this does not necessarily contradict the first conjecture.

The first conjecture is closely related to the Davenport problem: *Given a finite Abelian group G, what is the maximal value of n for which there exists a sequence $a_1, \ldots, a_n$ in G such that $\prod_{i \in I} a_i \neq 1$ for all non-empty subset I of $\{1, \ldots, n\}$*. Let's call this maximal value $\sigma(G)$. The best bound on $\sigma(G)$ can be found in [34, 35, 25, 26].

Theorem 5.1 *Let $|G|$ denote the cardinality of G and m the maximal order of an element in G. Then*

$$\sigma(G) \leq m(1 + \log(|G|/m)). \tag{6}$$

In our case, $G = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$, $|G| = \varphi(G)$ and $m = \lambda(\Lambda)$. Let $\varpi(\Lambda) = \lambda(\Lambda)(1 + \log(\varphi(\Lambda)/\lambda(\Lambda)))$. It follows that if $|S(\Lambda)| > \varpi(\Lambda)$, then there exists a Carmichael number built up from the elements of $S(\Lambda)$. However, this is not possible, since $|S(\Lambda)|$ is usually much smaller than $\lambda(\Lambda)$ itself.

One of the great achievements of [1] has been to replace $S(\Lambda)$ with $S'(\delta\Lambda) = \{p \text{ prime }, \delta \mid p - 1 \mid \delta\Lambda\}$ for some integer δ prime to Λ. Then, $S'(\delta\Lambda)$ is contained in a subgroup of $(\mathbf{Z}/(\delta\Lambda)\mathbf{Z})^\times$ which is isomorphic to $(\mathbf{Z}/\Lambda\mathbf{Z})^\times$. Hence, if δ is large enough, then $|S'(\delta\Lambda)|$ will be greater than the bound (6) and we will be sure to get a Carmichael number out of one of the sequences of products of $S'(\delta\Lambda)$.

6 Conclusions

We have described an algorithm that can build Carmichael numbers with many factors without using Chernick's forms. By the way we are doing this, it should be clear that building Carmichael numbers is quite easy, and we have found lots of numbers with 1000 factors and so on; 500-factor numbers are trivial to build.

Acknowledgments. We thank J.-L. Nicolas for his invaluable help and support while working out the results and writing the paper; G. Tenenbaum for pointing out to [10] and A. Schinzel for his great culture on Davenport's problem; L. Reboul who brought Giuga's problem to our attention; R. Pinch for making his table available; W. Keller for sending us the references to the work of Löh and Niebuhr; P. Flajolet for his help and support during our cutting the original manuscript into pieces. Many thanks also to C. Pomerance, who sent us [40] as well as a preprint of his work, and for his interest in our paper. Also, we have to thank the Centre de Calcul de l'Ecole Polytechnique for the use of their machines.

References

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. Preprint, April 3rd 1992.

[2] E. Bedocchi. Note on a conjecture on prime numbers. *Rev. Math. Univ. Parma 4*, 11 (1985), 229–236.

[3] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp. 29*, 130 (1975), 620–647.

[4] R. D. CARMICHAEL. Note on a new number theory function. *Bull. AMS XVI* (1910), 232–238.

[5] R. D. CARMICHAEL. On composite numbers P which satisfy the fermat congruence $a^{P-1} \equiv 1 \bmod P$. *American Mathematical Monthly XIX* (1912), 22–27.

[6] J. CHERNICK. On Fermat's simple theorem. *Bull. AMS 45* (April 1939), 269–274.

[7] G. L. COHEN AND P. HAGIS, JR. On the number of prime factors of n if $\phi(n) \mid (n-1)$. *Nieuw Archief voor Wiskunde (3) XXVIII* (1980), 177–185.

[8] L. E. DICKSON. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group I. *Ann. Math. 11* (1896), 65–120.

[9] H. DUBNER. A new method for producing large Carmichael numbers. *Math. Comp. 53*, 187 (July 1989), 411–414.

[10] P. ERDŐS, C. POMERANCE, AND E. SCHMUTZ. Carmichael's lambda function. *Acta Arithmetica LVIII*, 4 (1991), 363–385.

[11] G. GIUGA. Su una presumibile proprietà caratteristica dei numeri primi. *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. 3*, 14 (83) (1950), 511–528.

[12] D. M. GORDON. On the number of elliptic pseudoprimes. *Math. Comp. 52*, 185 (January 1989), 231–245.

[13] D. M. GORDON AND C. POMERANCE. The distribution of Lucas and elliptic pseudoprimes. *Math. Comp. 57*, 196 (October 1991), 825–838.

[14] D. GUILLAUME AND F. MORAIN. Building Carmichael numbers with a large number of prime factors. Research Report LIX/RR/92/01, Ecole Polytechnique–LIX, Feb. 1992.

[15] G. JAESCHKE. The Carmichael numbers to 10^{12}. *Math. Comp. 55*, 191 (July 1990), 383–389.

[16] W. KELLER. The Carmichael numbers to 10^{13}. *AMS Abstracts 9* (1998), 328–329.

[17] M. KISHORE. On the number of distinct prime factors of n for which $\phi(n) \mid n-1$. *Nieuw Archief voor Wiskunde (3) XXV* (1977), 48–53.

[18] H. LAUSCH AND W. NÖBAUER. *Algebra of polynomials.* North Holland, Amsterdam, 1973.

[19] D. H. LEHMER. An extended theory of Lucas' functions. *Annals of Math. 31* (1930), 419–448. Series (2).

[20] D. H. LEHMER. On Euler's totient function. *Bull. AMS 38* (1932), 745–751.

[21] R. LIDL, W. B. MÜLLER, AND A. OSWALD. Some remarks on strong Fibonacci pseudoprimes. *Applicable Algebra in Engineering, Communication and Computing 1* (1990), 59–65.

[22] E. LIEUWENS. Do there exist composite numbers M for which $k\phi(M) = M-1$ holds? *Nieuw Archief voor Wiskunde (3) XVIII* (1970), 165–169.

[23] G. Löh. Carmichael numbers with a large number of prime factors. *AMS Abstracts 9* (1998), 329.

[24] G. Löh and W. Niebuhr. Carmichael numbers with a large number of prime factors, II. *AMS Abstracts 10* (1989).

[25] H. Mann. Additive group theory – a progress report. *Bull. AMS 79*, 6 (Nov. 1973), 1069–1075.

[26] R. Meshulam. An uncertainty inequality and zero subsums. *Discrete Mathematics 84* (1990), 197–200.

[27] J.-L. Nicolas. On highly composite numbers. In *Ramanujan revisited* (1988), Academic Press, pp. 215–244.

[28] R. Pinch. The Carmichael numbers to 10^{15}. In preparation, January 1992.

[29] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to 25.10^9. *Math. Comp. 35*, 151 (1980), 1003–1026.

[30] A. D. Porto and P. Filipponi. A probabilistic primality test based on the properties of certain generalized Lucas numbers. In *Advances in Cryptology - EUROCRYPT '88* (1988), C. G. Günther, Ed., vol. 330 of *Lect. Notes in Computer Science*, Springer-Verlag, pp. 211–223. Proceedings Eurocrypt '88, Davos (Switzerland), May 25-27, 1988.

[31] S. Ramanujan. Highly composite numbers. *Proc. London Math. Soc. 2*, 14 (1915), 347–409.

[32] P. Ribenboim. *The book of prime number records*, 2nd ed. Springer, 1989.

[33] H. Riesel. *Prime numbers and computer methods for factorization*, 2nd ed., vol. 57 of *Progress in Mathematics*. Birkhäuser, 1985.

[34] P. van Emde Boas. A combinatorial problem on finite abelian groups, II. Tech. Rep. ZW-007, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969. 60 pp.

[35] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups, III. Tech. Rep. ZW-008, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969.

[36] S. S. Wagstaff, Jr. Large Carmichael numbers. *Math. J. Okayama Univ. 22* (1980), 33–41.

[37] H. C. Williams. On numbers analogous to the Carmichael numbers. *Canadian Math. Bull. 20*, 1 (1977), 133–143.

[38] D. Woods and J. Huenemann. Larger Carmichael numbers. *Comp. & Maths. with Appls. 8*, 3 (1982), 215–216.

[39] M. Yorinaga. Numerical computations of Carmichael numbers. *Mathematical Journal of Okayama University 20*, 2 (1978), 151–163.

[40] M. Zhang. Searching for large Carmichael numbers. Preprint, Dec. 1991.

ISSN 0249-6399