BUILDING PSEUDOPRIMES WITH A LARGE NUMBER OF PRIME FACTORS

D. Guillaume [*] F. Morain [†‡]

February 3, 1995

Abstract

We extend the method due originally to Löh and Niebuhr for the generation of Carmichael numbers with a large number of prime factors to other classes of pseudoprimes, such as Williams's pseudoprimes and elliptic pseudoprimes. We exhibit also some new Dickson pseudoprimes as well as superstrong Dickson pseudoprimes.

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 [32]). We denote by $\mathcal{C}(x)$ the number of Carmichael numbers up to x. Many properties of these numbers are described in [35].

Recent tables of Carmichael numbers include that of Keller up to 10^{13} (see [17]), that of Jaeschke [16] 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 [30]) and more recently up to 10^{16} (email to the NMBRTHRY mailing list, April 1993).

Yorinaga [40, 41] has found many Carmichael numbers using several methods including Chernick's "extension theorem" (see Section 2). In particular, he found Carmichael numbers with 12 and up to 18 prime factors. Pinch found the smallest Carmichael numbers with up to 20 prime factors [30]. Wagstaff [37] used the so-called "universal forms" of Chernick [6] to find large Carmichael numbers. Woods and Huenemann [39] gave larger numbers using the extension Theorem. Dubner [9] found even larger Carmichael numbers using a modification of the universal forms, culminating in a 3710-digit number, and more recently in a 8060-digit number (email sent to the NMBRTHRY

[*]19 rue Grange Dame Rose 78140 Vélizy, France

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

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

Keywords: Carmichael numbers, pseudoprimes, Lucas pseudoprimes, elliptic pseudoprimes, strong Dickson pseudoprimes.

mailing list, July 1994). Löh and Niebuhr [27, 28] have built numbers with up to 1,101,518 factors (this particular result was communicated to us by Keller). Recently, Zhang [42] 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, spurred by the work of Zhang [42], Alford, Granville and Pomerance had just proved that there is an infinite number of Carmichael numbers [1]. Then, around May 15, 1992, we heard about 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 Carmichael numbers with 1,101,518 prime factors), we think we shed some light on their method, including an analysis of it and some refinements. Moreover, we generalize it to other classes of pseudoprime numbers. A preversion of this article was published as [15].

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 and superstrong Dickson pseudoprimes and we give some examples of such numbers (only one such number was known, it was found by Pinch). We conclude with some remarks on problems related to Carmichael numbers: we discuss Lehmer's problem and Giuga's problem.

2 Background

In what follows, $p_1, p_2, \ldots, p_i$ denote prime numbers. 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*

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

An alternative statement is that

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

where λ denotes Carmichael's function (see [36]). Recall that $\lambda(p^e) = \varphi(p^e)$ for p an odd prime or $p = 2$ and $e \leq 2$ (φ is Euler's totient function), $\lambda(2^e) = 2^{e-2}$ 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

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

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 An algorithm for building Carmichael numbers

3.1 The idea

The idea of [27, 42, 14, 1] is to search for Carmichael numbers C with $\lambda(C)$ dividing a fixed number Λ.

Let

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

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

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

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, where $r < t$ and $u = t - r$ is 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. Löh and Niebuhr used this idea to find many Carmichael numbers, the largest of which has 1101518 prime factors and was obtained with $\Lambda = 2^{14} \times 3^7 \times 5^4 \times 7^2 \times 11^2 \times 13^2 \times 17 \times 19 \times 23 \times 29 \times 31 \times 37 \times 41 \times 43 \times 47$. Their program uses backtracking in the search for the θ_i's.

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 one asks: 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

$$\binom{t}{u} \geq \mathrm{Card}((\mathbf{Z}/\Lambda\mathbf{Z})^\times) = \varphi(\Lambda). \tag{3}$$

Though heuristic, numerous computations indicated that meeting this condition was also sufficient to determine a Carmichael number with $t-u$ prime factors. Thus, we select u as the minimum value for which (3) holds. Note that (3) suggests we choose Λ with a "small" value of $\varphi(\Lambda)$.

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; those numbers were first studied by Ramanujan [34]; see also [29]).

3.4 Remarks

3.4.1 Using outside primes

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

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

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 [16]). Given a set $(p_1, \ldots, p_{r-1})$, we let p_r run through the arithmetic progression $a + XK$. Very often, a is itself a prime and we hope that $a - 1 \mid R - 1$. We note also that if some q divides all the numbers $p_i - 1$, for $1 \leq i \leq r-1$, 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 Carmichael number.

3.4.2 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 ($h \geq 0$), 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 he obtained is a 1305-factor number with 8340 decimal digits.

3.4.3 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 we replace S with

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

For instance, if a is a quadratic residue modulo p, then $p \in S_a(\Lambda)$ only if $(p-1)/2 \mid \Lambda$.

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

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

These sequences have many properties (see [21] or [35]), including arithmetical ones. Let $\epsilon(N)$ denote the Jacobi symbol $\left(\frac{\Delta}{N}\right)$.

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

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

A *Lucas pseudoprime* for parameters (P,Q) is an odd composite integer N which satisfies $U_{N-\epsilon(N)} \equiv 0 \bmod N$.

Let Δ be a fixed integer. Williams [38] 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 *The integer N is a Δ–Lpsp if and only if N is a squarefree product of primes p_1, ..., 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 θ_i of $S_\Delta(\Lambda)$ such that

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

If so, we put $N = P(S_\Delta)/(\theta_1 \cdots \theta_u)$ 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 $t = \text{Card}(S_7(\Lambda)) = 109$. 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 we found is built up from $S_{43}(\Lambda^*)$ with $\Lambda^* = 2^7 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29$. The set $S_{43}(\Lambda^*)$ contains 5047 primes. One would have had to examine all combinations of 5 elements of $S_{43}(\Lambda^*)$. There are more than 2.7×10^{16} of these. We reduced that number by using the following trick. One remarks that $P(S_{43})/4639 \equiv 1 \bmod (2^4, 3^3, 5^2, 7, 23, 29)$. So, we decide to keep those primes of $S_{43}(\Lambda^*)$ that are congruent to $\pm 1 \bmod (2^4, 3^3, 5^2, 7, 23, 29)$. There are 71 of these and now one has to examine all combinations of 8 primes from this new set. There are only 1.06×10^{10} such combinations, which is greater than $\varphi(\Lambda)/\varphi(2^4 \times 3^3 \times 5^2 \times 7 \times 23 \times 29) \approx 96.77 \times 10^5$. 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. In this case, we also found that:

$$K = P(S_{43})/(4639 \times 121393999 \times 409704751 \times 1182383999 \times 9429512399 \times 66006586799 \times 137005268399 \times 274010536801 \times 2025295272001)$$

satisfies $K \equiv -1 \bmod \Lambda$, but $\epsilon(K) = -\epsilon(P(S_{43})) \prod_i \epsilon(\theta_i)$, so K is not a 43-Lpsp.

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 such that $\left(\frac{-D}{N}\right) = -1$. 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's 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 $N \equiv -1 \bmod \Lambda$ since we must have

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

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

4.3.1 Definition and properties

Let c be an integer. The Dickson polynomial of parameter c and degree n is defined as (see [8, 20, 23])

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

An odd composite integer N is called a *strong Dickson pseudoprime* (sDpp(c) in short) if for all m in $\mathbf{Z}$:

$$g_N(m, c) \equiv m \bmod N. \tag{4}$$

A *strong Fibonacci pseudoprime* (sF-psp in short) is simply an sDpp(-1): these numbers were first introduced and studied in [33].

Extending a result of [25], Kowol proved the following [19]

Theorem 4.3 *Let $N = p_1 p_2 \ldots p_r$ be the prime factorization of an odd, squarefree number N prime to c and e_i denote the order of c modulo p_i. Then N is a sDpp(c) if and only if for all i, one has*

(i) $p_i - 1 \mid N-1$ if $c \not\equiv 1 \bmod p_i$; $p_i - 1 \mid N-1$ or $p_i - 1 \mid N+1$ if $c \equiv 1 \bmod p_i$;

(ii) $e_i(p_i+1) \mid N-1$ or $e_i(p_i+1) \mid N-p_i$.

For $c = -1$, one obtains that any sF-psp N is a Carmichael number for which $2(p_i + 1) \mid N - 1$ (type I) or $2(p_i + 1) \mid N - p_i$ for all i (type II). Other characterisations of sDpp(c) are given in [23, Chapter 7].

Following [24], if N is a sDpp(c) for all c such that $\gcd(c, N) = 1$, then N is called *superstrong Dickson pseudoprime* (ssDpp in short). The authors prove:

Theorem 4.4 *An odd composite N is a ssDpp if and only if*
(i) N is a Carmichael number,
(ii) for all prime factor p of N, one has $(p^2 - 1) \mid N - 1$ or $(p^2 - 1) \mid N - p$.

4.3.2 Building sF-psp's

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

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

The set S has 40 elements which are given in Table 1. 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 $2(p + 1) | N - 1$ for all prime $p \mid N$.

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 now examine every combination $\theta_1, \ldots, \theta_{11}$ of numbers of S and hope that $\theta_1 \cdots \theta_{11}$ is congruent to $1/(p_1 p_2 p_3 p_4)$ where the p_j's are distinct elements of S which are different from the θ_i's. After several nights of CPU on a DecAlpha, we finally found that

$$sF_1 = 29 \times 31 \times 37 \times 43 \times 53 \times 67 \times 79 \times 89 \times 97 \times 151 \times 181 \times 191 \times 419 \times 881 \times 883$$

is a sF-psp. Note that

$$sF_1 - 1 = 2^7 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 1949 \times 894811 \times 3456585949$$

and

$$sF_1 + 1 = 2 \times 142591 \times 351256343 \times 58838638438298777.$$

By construction, sF_1 is of type I and it turns out to be a ssDpp. Note that if $p - 1 \mid N - 1$ and $2(p + 1) \mid N - 1$, then with high probability $p^2 - 1 \mid N - 1$ (it is true when $p \equiv 3 \bmod 4$). Looking for ssDpp's with some prescribed number of factors yielded the results given in Table 2. It should be pointed out that these results are not exhaustive. Finding more numbers would simply require more computing time.

4.3.3 Building sDpp's

Following a suggestion of one of the referees, we searched for a sDpp(2) not being a ssDpp. With the same value of Λ, we built

$$S_2 = \{p \text{ prime}, p - 1 \mid \Lambda, e_p(p + 1) \mid \Lambda, p \nmid \Lambda\}$$

where $\epsilon(p)$ is the order of 2 modulo p. It turns out that S_2 is just $S \cup \{127, 6271\}$. It is enough to find a N such that $N \equiv 1 \bmod \Lambda$ and which has 127 or 6271 as a prime factor, in order not to have room for $2(p+1) \nmid N-1$ for instance. Looking at combinations of 23 factors, we find that

$$SD_1 = 346720544736455641553421473905553096835977061105232 68445622401$$

$$= 23\times29\times31\times37\times53\times89\times97\times101\times103\times109\times191\times199\times239\times271\times307\times419\times449\times571\times881$$

$$\times883\times911\times3457\times5851\times6271\times11969$$

is a sDpp and

$$SD_1 - 1 = 2^7\times3^3\times5^2\times7^2\times11\times13\times17\times19\times41\times22801291\times24667267$$

$$\times1623836866783\times 4735048896899885541041.$$

It is a not a sF-psp, since

$$2(6271+1) = 2^8\times7^2$$

nor a ssDpp, since

$$6271^2 - 1 = 2^8\times3\times5\times7^2\times11\times19.$$

The same conclusion holds for the numbers in Table 3. On the other hand, we found that

$$SD_2 = 191386131075177646988474204313974440985419 10401$$

$$= 43\times67\times71\times97\times109\times113\times131\times191\times197\times199\times307\times379\times419\times449\times701\times883\times911\times1871\times3457$$

is a sDpp(2) and a sF-psp, but not a ssDpp, since:

$$SD_2 - 1 = 2^7\times3^3\times5^2\times7^2\times11\times13^2\times17\times19\times13063\times576336071223646842618945178879$$

and

$$3457^2 - 1 = 2^8\times3^3\times7\times13\times19$$

hence does not divide $SD_2 - 1$.

During our search, more ssDpp's showed up. They are listed in Table 4.

Remark. Our method is convenient when we impose $e_p(p+1) \mid N-1$, but it cannot be used if we insist on $e_p(p+1) \mid N-p$.

5 Some negative results

Let us turn our attention to numbers that our method has so far been unable to tackle.

5.1 A question of Williams

In [38], 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 two composite numbers Λ_+ and Λ_- with a large number of divisors, such that $\gcd(\Lambda_-, \Lambda_+) \mid 2$, and find a large set of primes p such that $p-1 \mid \Lambda_-$ and simultaneously $p+1 \mid \Lambda_+$. Experiments made so far show that it is hard to get values of $\Lambda_\pm$ reasonably small for our method to work rapidly.

In [32], 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.

5.2 Lehmer's problem

In [22] Lehmer raised the following question: does there exist a composite integer N for which

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

Such a number must be a Carmichael number. In view of [26, 18, 7] (see also [35]), such a number N 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 zeroes, which we can spot at once.

5.3 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 [35]). By [2], such an N must be greater than 10^{1700}. We did not find any Carmichael number built with our method that satisfies this property.

6 Conclusions

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. In [1], it is proved that there exists an infinite number of Λ for which this result is true. Hence, there is an infinite number of Carmichael numbers.

We have described an algorithm that can build Carmichael numbers with many factors without using Chernick's forms. We have generalized this method to the construction of numbers with similar properties. We think that there is hope for some extension of this work that can solve more difficult problems.

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 [10] and A. Schinzel for his great culture on Davenport's problem; L. Reboul who brought Giuga's problem to our attention; R. Lercier who helped factoring some of the numbers involved; 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; P. Dumas for reading the manuscript. Many thanks also to C. Pomerance, who sent us [42] as well as a preprint of his work, and for his interest in our paper. Finally, we thank the referees for their precise reading and many suggestions concerning this work.

References

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Math. 139*, 3 (May 1994), 703–722.

[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* (Apr. 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 (Jan. 1989), 231–245.

[13] D. M. Gordon and C. Pomerance. The distribution of Lucas and elliptic pseudoprimes. *Math. Comp. 57*, 196 (Oct. 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] D. Guillaume and F. Morain. Building Carmichael numbers with a large number of prime factors and generalization to other numbers. Research Report 1741, INRIA, Aug. 1992.

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

[17] W. Keller. The Carmichael numbers to 10^{13}. *AMS Abstracts 9* (1988), 328–329. Abstract 88T-11-150.

[18] 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.

[19] G. Kowol. On strong Dickson pseudoprimes. *AAECC 3* (1992), 129–138.

[20] H. Lausch and W. Nöbauer. *Algebra of polynomials*. North Holland, Amsterdam, 1973.

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

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

[23] R. Lidl, G. L. Mullen, and G. Turnwald. *Dickson polynomials*, vol. 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, 1993.

[24] R. Lidl and W. B. Müller. Primality testing with Lucas functions. In *Auscrypt '92* (1992), vol. 718 of *Lect. Notes in Computer Science*, Springer–Verlag, pp. 539–542.

[25] R. Lidl, W. B. Müller, and A. Oswald. Some remarks on strong Fibonacci pseudoprimes. *AAECC 1* (1990), 59–65.

[26] 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.

[27] G. Löh. Carmichael numbers with a large number of prime factors. *AMS Abstracts 9* (1988), 329. Abstract 88T-11-151.

[28] G. Löh and W. Niebuhr. Carmichael numbers with a large number of prime factors, II. *AMS Abstracts 10* (1989), 305. Abstract 89T-11-131.

[29] J.-L. Nicolas. On highly composite numbers. In *Ramanujan revisited* (1988), G. Andrews, R. Askey, B. Berndt, K. Ramanathan, and R. Rankin, Eds., Academic Press, pp. 215–244.

[30] R. Pinch. The Carmichael numbers to 10^{15}. *Math. Comp. 61*, 203 (July 1993), 381–392.

[31] R. Pinch. The pseudoprimes up to 10^{13}. Preprint, 1995.

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

[33] 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.

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

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

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

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

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

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

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

[41] M. Yorinaga. Carmichael numbers with many prime factors. *J. Okayama Univ. 22* (1980), 169–184.

[42] M. Zhang. Searching for large Carmichael numbers. To appear in *Sichuan Daxue Xuebao*, Dec. 1991.

p	$p \bmod 4$	$p-1$	$p+1$
23	3	2×11	$2^3 \times 3$
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
41	1	$2^3 \times 5$	$2 \times 3 \times 7$
43	3	$2 \times 3 \times 7$	$2^2 \times 11$
53	1	$2^2 \times 13$	2×3^3
67	3	$2 \times 3 \times 11$	$2^2 \times 17$
71	3	$2 \times 5 \times 7$	$2^3 \times 3^2$
79	3	$2 \times 3 \times 13$	$2^4 \times 5$
89	1	$2^3 \times 11$	$2 \times 3^2 \times 5$
97	1	$2^5 \times 3$	2×7^2
101	1	$2^2 \times 5^2$	$2 \times 3 \times 17$
103	3	$2 \times 3 \times 17$	$2^3 \times 13$
109	1	$2^2 \times 3^3$	$2 \times 5 \times 11$
113	1	$2^4 \times 7$	$2 \times 3 \times 19$
131	3	$2 \times 5 \times 13$	$2^2 \times 3 \times 11$
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	$2 \times 5 \times 19$	$2^6 \times 3$
197	1	$2^2 \times 7^2$	$2 \times 3^2 \times 11$
199	3	$2 \times 3^2 \times 11$	$2^3 \times 5^2$
239	3	$2 \times 7 \times 17$	$2^4 \times 3 \times 5$
271	3	$2 \times 3^3 \times 5$	$2^4 \times 17$
307	3	$2 \times 3^2 \times 17$	$2^2 \times 7 \times 11$
379	3	$2 \times 3^3 \times 7$	$2^2 \times 5 \times 19$
419	3	$2 \times 11 \times 19$	$2^2 \times 3 \times 5 \times 7$
449	1	$2^6 \times 7$	$2 \times 3^2 \times 5^2$
571	3	$2 \times 3 \times 5 \times 19$	$2^2 \times 11 \times 13$
701	1	$2^2 \times 5^2 \times 7$	$2 \times 3^3 \times 13$
881	1	$2^4 \times 5 \times 11$	$2 \times 3^2 \times 7^2$
883	3	$2 \times 3^2 \times 7^2$	$2^2 \times 13 \times 17$
911	3	$2 \times 5 \times 7 \times 13$	$2^4 \times 3 \times 19$
1429	1	$2^2 \times 3 \times 7 \times 17$	$2 \times 5 \times 11 \times 13$
1871	3	$2 \times 5 \times 11 \times 17$	$2^4 \times 3^2 \times 13$
2549	1	$2^2 \times 7^2 \times 13$	$2 \times 3 \times 5^2 \times 17$
3457	1	$2^7 \times 3^3$	$2 \times 7 \times 13 \times 19$
4159	3	$2 \times 3^3 \times 7 \times 11$	$2^6 \times 5 \times 13$
5851	3	$2 \times 3^2 \times 5^2 \times 13$	$2^2 \times 7 \times 11 \times 19$
11969	1	$2^6 \times 11 \times 17$	$2 \times 3^2 \times 5 \times 7 \times 19$

Table 1: Factorizations of the numbers $p \pm 1$, $p \in S$.

sF_2	$=$	$23 \times 29 \times 31 \times 41 \times 43 \times 53 \times 71 \times 89 \times 97 \times 103 \times 131 \times 151 \times 199 \times 379$
		$\times 449 \times 1429 \times 3457 \times 4159$
	$=$	$167872834324702870101415827333360777600 1,$
$sF_2 - 1$	$=$	$2^8 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 179 \times 47959981812343004566439 11$
$sF_2 + 1$	$=$	$2 \times 211 \times 3571 \times 22059377 \times 5049924427404593054501927 3;$
sF_3	$=$	$23 \times 31 \times 43 \times 71 \times 101 \times 103 \times 109 \times 131 \times 151 \times 181 \times 191 \times 199 \times 271$
		$\times 307 \times 419 \times 571 \times 881 \times 911 \times 1429 \times 1871 \times 5851 \times 11969$
	$=$	$100475634258813355372562964822982699764176971487396 1601,$
$sF_3 - 1$	$=$	$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 37 \times 154277$
		$\times 900138764131213330748469224289686471,$
$sF_3 + 1$	$=$	$2 \times 5023781712940667768628148241149134988208848574369808 01;$
sF_4	$=$	$23 \times 31 \times 37 \times 41 \times 53 \times 67 \times 97 \times 101 \times 109 \times 151 \times 181 \times 191 \times 197 \times 239$
		$\times 271 \times 379 \times 419 \times 449 \times 571 \times 701 \times 911 \times 1429 \times 2549 \times 5851$
	$=$	$151381197297673254570192926273745833804231848549434336001,$
$sF_4 - 1$	$=$	$2^8 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 1669 \times 10099 \times 13151 \times 912879571 \times$
		$13591749631 \times 28147589755189,$
$sF_4 + 1$	$=$	$2 \times 3847 \times 3225815741 \times 17729977627 \times 3440107463585536205297514587909 69;$
sF_5	$=$	$53 \times 97 \times 103 \times 109 \times 113 \times 131 \times 151 \times 181 \times 191 \times 197 \times 239 \times 307 \times 911 \times 4159 \times 11969$
	$=$	$292359777010783081214520835626016320 1,$
$sF_5 - 1$	$=$	$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17^2 \times 19 \times 16217 \times 65497 \times 827996294845451,$
$sF_5 + 1$	$=$	$2 \times 59 \times 569 \times 435435013867300767350571677377 31$
sF_6	$=$	$31 \times 43 \times 67 \times 79 \times 89 \times 101 \times 113 \times 131 \times 151 \times 181 \times 191 \times 197 \times 199 \times 239 \times 307 \times 379$
		$\times 419 \times 881 \times 883 \times 1429 \times 1871 \times 4159 \times 5851$
	$=$	$113305896421334645086410254311835758939267876567182230401,$
$sF_6 - 1$	$=$	$2^7 \times 3^4 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 16763$
		$\times 1152208644008809361616459954259952325740 9,$
$sF_6 + 1$	$=$	$2 \times 3156667 \times 1794707779143866696842116294050588151035061293560 3;$
sF_7	$=$	$29 \times 37 \times 41 \times 53 \times 67 \times 71 \times 101 \times 109 \times 131 \times 151 \times 197 \times 271 \times 379 \times 449 \times 571 \times 701$
		$\times 881 \times 883 \times 2549 \times 3457 \times 4159 \times 5851 \times 11969$
	$=$	$175366494640126071313801036607482382631300945388043955264 01,$
$sF_7 - 1$	$=$	$2^8 \times 3^5 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 83 \times 277 \times 1913 \times 6927997$
		$\times 163510336095614001346453074720 37,$
$sF_7 + 1$	$=$	$2 \times 383 \times 4657 \times 574933 \times 855055641043469277579542991408900217374798718 7;$
sF_8	$=$	$29 \times 31 \times 41 \times 43 \times 53 \times 89 \times 97 \times 103 \times 109 \times 113 \times 151 \times 181 \times 191 \times 197 \times 199 \times 379$
		$\times 571 \times 701 \times 881 \times 883 \times 3457 \times 4159 \times 11969$
	$=$	$382363200130771519387481158312471260006204175039799040 1,$
$sF_8 - 1$	$=$	$2^9 \times 3^3 \times 5^2 \times 7^3 \times 11 \times 13 \times 17 \times 19 \times 560459 \times 18793424755271$
		$\times 663009722481325323689 03,$
$sF_8 + 1$	$=$	$2 \times 263 \times 194491727256119029050241 \times 373756892514403658245908114 47;$

Table 2: Superstrong pseudoprimes.

SD_3	$=$	$4380491923490462132535639231582036921990853743062350956480 1$
	$=$	$29 \times 37 \times 41 \times 43 \times 53 \times 67 \times 79 \times 101 \times 103 \times 109 \times 113 \times 127 \times 131 \times 181 \times 191$
		$\times 197 \times 271 \times 379 \times 419 \times 449 \times 881 \times 1871 \times 2549 \times 5851 \times 11969,$
$SD_3 - 1$	$=$	$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13^2 \times 17 \times 19 \times 331 \times 65269 \times 53301583 \times 74571437$
		$\times 3158686907 \times 63529728175703;$
SD_4	$=$	$954698978134774825721674550351897176978472782793789785074787201$
	$=$	$23 \times 43 \times 53 \times 79 \times 89 \times 101 \times 103 \times 109 \times 127 \times 131 \times 181 \times 191 \times 239 \times 379$
		$\times 419 \times 449 \times 571 \times 701 \times 881 \times 883 \times 911 \times 1871 \times 5851 \times 6271 \times 11969,$
$SD_4 - 1$	$=$	$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 149 \times 983 \times 6899 \times 32783 \times 373773077$
		$\times 394307860438280535526066544731;$
SD_5	$=$	$1176731092464815813274493585871607921910014961008440544 01$
	$=$	$23 \times 31 \times 41 \times 43 \times 53 \times 71 \times 89 \times 97 \times 103 \times 113 \times 151 \times 191 \times 197 \times 239$
		$\times 307 \times 379 \times 419 \times 449 \times 571 \times 701 \times 911 \times 1429 \times 2549 \times 6271,$
$SD_5 - 1$	$=$	$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 73 \times 257 \times 106018073632710285797$
		$\times 3025470720618148931 33;$
SD_6	$=$	$5067632018925233621223137791564876359336876484310401$
	$=$	$89 \times 97 \times 101 \times 103 \times 127 \times 131 \times 151 \times 199 \times 239 \times 419 \times 449 \times 701$
		$\times 911 \times 1429 \times 2549 \times 3457 \times 4159 \times 6271 \times 11969,$
$SD_6 - 1$	$=$	$2^7 \times 3^4 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 43 \times 103710460921$
		$\times 193706598291387085241239 1189.$

Table 3: Another list of sDpp(2) not ssDpp nor sF-psp.

SSD_1	=	$1074882431319136003549198441438798911316479057935049983240193849601$
	=	$23 \times 41 \times 53 \times 79 \times 89 \times 97 \times 101 \times 103 \times 131 \times 181 \times 191 \times 199 \times 379 \times 449$
		$\times 571 \times 883 \times 911 \times 1429 \times 1871 \times 2549 \times 3457 \times 4159 \times 5851 \times 6271 \times 11969,$
$SSD_1 - 1$	=	$2^8 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17^3 \times 19 \times 1181 \times 1367 \times 156069923$
		$\times 9012487785751 \times 418795904873876486096 2873;$
SSD_2	=	$24895242257529369939494836061417642873443567601032584888000001$
	=	$31 \times 37 \times 53 \times 67 \times 89 \times 97 \times 109 \times 113 \times 127 \times 151 \times 191 \times 197 \times 199 \times 271$
		$\times 307 \times 419 \times 449 \times 571 \times 701 \times 881 \times 883 \times 911 \times 3457 \times 4159 \times 6271,$
$SSD_2 - 1$	=	$2^9 \times 3^5 \times 5^6 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 1913$
		$\times 29578114536385529297368157965850 19111669689;$
SSD_3	=	$254001515679547435472695745304581614282962275650520910938880 1$
	=	$23 \times 29 \times 37 \times 41 \times 43 \times 53 \times 89 \times 101 \times 113 \times 131 \times 181 \times 191 \times 197 \times 199$
		$\times 239 \times 271 \times 379 \times 419 \times 571 \times 1429 \times 1871 \times 2549 \times 4159 \times 5851 \times 6271,$
$SSD_3 - 1$	=	$2^9 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 251 \times 1181$
		$\times 109547965266333621745142576529380 18179513703$
SSD_4	=	$304191826382731265490322742438856177808461290542630846041316224 01$
	=	$29 \times 41 \times 53 \times 71 \times 79 \times 89 \times 97 \times 101 \times 103 \times 151 \times 197 \times 199 \times 239 \times 307$
		$\times 379 \times 701 \times 881 \times 911 \times 1429 \times 1871 \times 2549 \times 3457 \times 5851 \times 6271 \times 11969,$
$SSD_4 - 1$	=	$2^9 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 17959583$
		$\times 216542386161673875179675095786743306 2492352583;$
SSD_5	=	$346276812416978888598012957326772337339310477097186918044928 01$
	=	$31 \times 37 \times 43 \times 53 \times 67 \times 79 \times 97 \times 101 \times 109 \times 127 \times 181 \times 197 \times 199 \times 239$
		$\times 271 \times 379 \times 419 \times 449 \times 701 \times 911 \times 1429 \times 2549 \times 3457 \times 5851 \times 11969,$
$SSD_5 - 1$	=	$2^10 \times 3^3 \times 5^2 \times 7^2 \times 11^2 \times 13 \times 17 \times 19 \times 4253955970447$
		$\times 473041633909644665321595636817369087;$
SSD_6	=	$9735675423832482264137740738568890558006247355287432681267404801$
	=	$29 \times 31 \times 41 \times 43 \times 79 \times 97 \times 101 \times 109 \times 131 \times 181 \times 191 \times 197 \times 199 \times$
		$271 \times 449 \times 571 \times 881 \times 911 \times 1429 \times 1871 \times 2549 \times 3457 \times 4159 \times 6271 \times 11969,$
$SSD_6 - 1$	=	$2^13 \times 3^5 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 110477 \times 3043627 \times 51281917$
		$\times 30346063051 \times 1651829861857529985 59;$
SSD_7	=	$1513811972976732545701929262737458338042318485494343360 01$
	=	$23 \times 31 \times 37 \times 41 \times 53 \times 67 \times 97 \times 101 \times 109 \times 151 \times 181 \times 191 \times 197 \times 239$
		$\times 271 \times 379 \times 419 \times 449 \times 571 \times 701 \times 911 \times 1429 \times 2549 \times 5851,$
$SSD_7 - 1$	=	$2^8 \times 3^3 \times 5^3 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 1669 \times 10099 \times 13151 \times 912879571$
		$\times 13591749631 \times 28147589755189;$
SSD_8	=	$21216273054891509455785488410749082705994904225680233344 01$
	=	$23 \times 29 \times 37 \times 41 \times 43 \times 79 \times 97 \times 101 \times 109 \times 151 \times 181 \times 191 \times 197 \times 199$
		$\times 239 \times 419 \times 449 \times 881 \times 883 \times 911 \times 1429 \times 2549 \times 4159 \times 5851,$
$SSD_8 - 1$	=	$2^9 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 17359 \times 18041 \times 618421$
		$\times 14005260273857704109401 782315491;$
SSD_9	=	$24628855951004657197699091010182424855141766563690498466560 1$
	=	$29 \times 31 \times 37 \times 41 \times 43 \times 97 \times 101 \times 103 \times 113 \times 151 \times 191 \times 199 \times 239 \times 271$
		$\times 307 \times 379 \times 571 \times 701 \times 1429 \times 1871 \times 2549 \times 4159 \times 6271 \times 11969,$
$SSD_9 - 1$	=	$2^9 \times 3^3 \times 5^2 \times 7^2 \times 11 \times 13 \times 17 \times 19 \times 13831 \times 25633 \times 179527$
		$\times 49471271486964608551498352 63214521.$

Table 4: Another list of superstrong pseudoprimes.