#A59 INTEGERS 14 (2014)

CARMICHAEL NUMBERS WITH $(p+1) \mid (n-1)$

Richard J. McIntosh
Department of Mathematics and Statistics, University of Regina, Regina, Saskatchewan, Canada
Richard.McIntosh@uregina.ca

Received: 7/23/13, Revised: 7/19/14, Accepted: 9/17/14, Published: 10/30/14

Abstract

A Carmichael number N is a super-Carmichael (sC) number if $(p \pm 1) \mid (N-1)$ for all $p|N$. These numbers are somewhat related to the strong Fibonacci pseudoprimes. The smallest such number, $17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$, was discovered by Richard Pinch. In this paper we prove that an sC number must have at least four prime factors and there are only finitely many sC numbers $N = \prod_{i=1}^{d} p_i$ with a given set of $d-3$ prime factors $p_1, \ldots, p_{d-3}$. Four methods for finding sC numbers are given. We report that if there are any sC numbers with exactly four prime factors, then the smallest prime factor is greater than 4000.

1. Introduction

The Baillie-PSW test [3, 14] is a probable prime test based on a combination of a strong Fermat probable prime test and a strong Lucas probable prime test. Many computer algebra systems and software packages use some version of this test. A Lucas sequence is chosen such that the Jacobi symbol $(D|N) = -1$, where N is the number to be tested for primality and D is the discriminant of the Lucas sequence. If one does not require $(D|N) = -1$, then a counterexample N may be an odd squarefree composite number such that $(p \pm 1) \mid (N-1)$ for all primes $p \mid N$. We call such numbers *super-Carmichael* (sC) numbers. They are somewhat related to the strong Fibonacci pseudoprimes. The smallest such number, $17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$, discovered by Pinch [11, 2 Section 4], is a strong Fibonacci pseudoprime. There are infinitely many Carmichael numbers [1] (i.e., infinitely many squarefree numbers N such that $p-1 \mid N-1$ for all primes $p|N$) and there are infinitely many squarefree numbers N such that $p+1 \mid N-1$ for all primes $p|N$ [2, 15]. Whether or not the intersection of these sets is infinite is still an open problem. In this paper we prove that an sC number must have at least four prime factors and there are only finitely many (possibly none) sC numbers $N = \prod_{i=1}^{d} p_i$ with a given set of $d-3$ prime factors $p_1, \ldots, p_{d-3}$. This leads to a method for the search of sC numbers. We report that if there are any sC numbers with exactly four prime factors, then $p_1 > 4000$ and $N > 10^{24}$.

2. Some Properties and Theorems for Super-Carmichael Numbers

Let $N = \prod_{i=1}^{d} p_i$ with primes $p_1 < p_2 < \cdots < p_d$ be an sC number. Since $(p_j \pm 1)$ divides $N-1$, it follows that p_i does not divide $p_j \pm 1$ for all i and j. This forces $p_1 \geq 5$. We call a set of two or more distinct odd primes *compatible* if p_i does not divide $p_j \pm 1$ for all i and j. For each prime p dividing N we have

$$N - 1 = (p-1)\left(\frac{N}{p} + 1\right) + \frac{N}{p} - p$$

and

$$N - 1 = (p+1)\left(\frac{N}{p} - 1\right) - \frac{N}{p} + p\,,$$

which implies that

$$\frac{p^2-1}{2} \;\Big|\; \frac{N}{p} - p\,. \tag{2.1}$$

Since $(p_i^2 - 1)/2 \equiv 0 \pmod{12}$, it follows that $N \equiv 1 \pmod{12}$. The divisibility in (2.1) is strong enough to deduce that there are only finitely many sC numbers $N = \prod_{i=1}^{d} p_i$ with a given set of $d-3$ prime factors $p_1, \ldots, p_{d-3}$. To accomplish this write $N = Pqrs$, where $P = \prod_{i=1}^{d-3} p_i$, $q = p_{d-2}$, $r = p_{d-1}$ and $s = p_d$. Then

$$t_q := \frac{2Prs - 2q}{q^2 - 1}\,, \qquad t_r := \frac{2Pqs - 2r}{r^2 - 1}\,, \qquad t_s := \frac{2Pqr - 2s}{s^2 - 1} \tag{2.2}$$

are positive integers with $t_q > t_r > t_s$, $t_q > 2P$ and $t_s < 2P$.

We will now show that q satisfies a polynomial of degree at most eight whose coefficients depend on t_q, t_r, t_s and P, where $P \geq 1$. We begin with the equations

$$t_q(q^2-1) + 2q = 2Prs \tag{2.3}$$

$$t_r(r^2-1) + 2r = 2Pqs \tag{2.4}$$

$$t_s(s^2-1) + 2s = 2Pqr \tag{2.5}$$

obtained from (2.2). Observe that $\gcd(t_q t_r t_s, Pqrs) = 1$. Eliminating s from (2.3) and (2.4) yields

$$(t_r r^2 + 2r - t_r)r = (t_q q^2 + 2q - t_q)q\,,$$

which expands to the r-cubic polynomial

$$t_r r^3 + 2r^2 - t_r r - (t_q q^2 + 2q - t_q)q = 0\,. \tag{2.6}$$

From (2.3) we obtain

$$s = \frac{t_q(q^2-1)+2q}{2Pr}\,.$$

Substituting this into (2.5) gives the r-cubic polynomial

$$8P^3qr^3 + 4P^2t_sr^2 - 4P(t_qq^2+2q-t_q)r - t_s(t_qq^2+2q-t_q)^2 = 0\,. \tag{2.7}$$

Subtracting $8P^3q$ times (2.6) from t_r times (2.7) yields the r-quadratic polynomial

$$\begin{aligned}4P^2(t_rt_s-4Pq)r^2 &- 4Pt_r(t_qq^2+2q-t_q-2P^2q)r\\ &-t_rt_s(t_qq^2+2q-t_q)^2 - 8P^3q^2(t_qq^2+2q-t_q) = 0.\end{aligned} \tag{2.8}$$

Since q does not divide t_rt_s, the leading coefficient of this polynomial is nonzero. Equation (2.8) can be used to remove the terms involving r^2 and r^3 from (2.6). This yields an r-linear polynomial $Ar - B = 0$, where

$$\begin{aligned}B &= (t_qq^2+2q-t_q)(t_qq^2+2q-t_q-2P^2q)\\ &\quad\times\big[(t_qt_rt_s-8P^3)t_rq^2 + 2(t_r^2-4P^2)t_sq - (t_qt_r-2Pt_s)t_rt_s\big].\end{aligned}$$

For the time being we will assume that B, and hence A, are nonzero. We can now express $r = B/A$ as a rational function of t_q, t_r, t_s, P and q. Substituting this expression for r into (2.8) and removing the nonzero factor

$$(t_qq^2+2q-t_q)^2(t_rt_s-4Pq)^2 = (2Prs)^2\left(\frac{4(Pqrs-1)(Pq-rs)}{(r^2-1)(s^2-1)}\right)^2,$$

we obtain an 8th degree q-polynomial

$$C_8q^8 + C_7q^7 + \cdots + C_0 = 0\,, \tag{2.9}$$

whose coefficients are polynomials in t_q, t_r, t_s and P. The leading coefficient of this polynomial is

$$C_8 = t_q(t_qt_rt_s - 8P^3)^3\,;$$

the other coefficients are too cumbersome to write down.

Now suppose that $B = 0$. Since q does not divide t_q, it follows that

$$(t_qt_rt_s-8P^3)t_rq^2 + 2(t_r^2-4P^2)t_sq - (t_qt_r-2Pt_s)t_rt_s = 0\,. \tag{2.10}$$

Observe that $t_r \mid 8P^2qt_s$ and $t_s \mid 8P^3q^2t_r$. Since $\gcd(t_qt_rt_s, Pqrs) = 1$, it follows that $t_r \mid 8t_s$ and $t_s \mid 8t_r$, which implies that $t_r/t_s = 2, 4$ or 8.

Theorem 1. *There are no super-Carmichael numbers with exactly three prime factors.*

Proof. This is the case $P = 1$. Let $N = qrs$, where $q < r < s$ are primes. Then $s^2 - 1 > qr$. From the definition of t_s we have $t_s(s^2-1) = 2qr - 2s < 2qr$, which forces $t_s = 1$ and $s^2 = 2qr - 2s + 1 < 2qr < 2qs$. Therefore $s < 2q$ and $t_r(r^2 - 1) = 2qs - 2r < 4q^2 - 2r < 4(q^2 - 1)$, which implies that $t_r < 4$. Since $t_s < t_r$, we must have $t_r = 2$ or $t_r = 3$. Observe that $s^2 < 2qr$, $q^2s^2 < 2q^3r < 2r^4$, $qs < \sqrt{2}r^2$, $2qs < \sqrt{8}r^2 < 3r^2+2r-3$. Hence $t_r(r^2-1) = 2qs-2r < 3(r^2-1)$. This forces $t_r = 2$. Since $r < s < 2q$ and $q \geq 5$, we have $t_q(q^2-1) = 2rs-2q < 8q^2-2q < 8(q^2-1)$, and so $t_q < 8$. Hence $t_qq^3 = q(2rs-2q+t_q) = 2N-(2q-t_q)q < 2N$. Since $s^2 < 2qr$, it follows that $s^3 < 2qrs = 2N$. Since $t_r = 2$, we have $2(r^2-1) = 2qs-2r$, $r^3 = qrs - r^2 + r = N - r(r-1) < N$. Therefore $N^3 = q^3r^3s^3 < 2q^3N^2$, which implies that $2N < 4q^3$. We now have $t_qq^3 < 2N < 4q^3$, which forces $t_q = 3$ because $2 = t_r < t_q$.

With $t_s = 1$, $t_r = 2$, $t_q = 3$ and $P = 1$, equation (2.6) becomes

$$2r^3 + 2r^2 - 2r - (3q^2 + 2q - 3)q = 0 \tag{2.11}$$

and equation (2.8) becomes

$$4(2q-1)r^2 + 12(q^2-1)r - (q^2 - 2q + 3)(3q^2 + 2q - 3) = 0\,. \tag{2.12}$$

Using (2.12) to remove the terms in (2.11) involving r^2 and r^3 we obtain

$$(q+1)(6q^2 + 19q - 29)r - 3(q^2+2)(3q^2 + 2q - 3) = 0\,.$$

Therefore

$$r = \frac{3(q^2+2)(3q^2+2q-3)}{(q+1)(6q^2+19q-29)}\,.$$

Substituting this into (2.12) we get

$$(3q^4 - 16q^3 - 78q^2 - 168q - 1)(3q^2 + 2q - 3)^2(2q-1)^2 = 0\,.$$

Since $(3q^2 + 2q - 3)^2(2q-1)^2 > 0$, it follows that

$$3q^4 - 16q^3 - 78q^2 - 168q - 1 = 0\,,$$

or

$$(3q^3 - 16q^2 - 78q - 168)q = 1\,, \qquad \square$$

which is impossible.

Throughout the rest of this paper we will assume that $P > 1$. This really means $P \geq p_1 \geq 5$.

Theorem 2. *Given $P = \prod_{i=1}^{d-3} p_i$ with primes $p_1 < p_2 < \cdots < p_{d-3}$, there are only finitely many super-Carmichael numbers $N = Pqrs$ with primes $p_{d-3} < q < r < s$.*

Remark. The analogous theorem for Carmichael numbers has only finitely many Carmichael numbers if all but the largest two prime factors are assigned. This was proved by Beeger [4] for the case $d = 3$ and by Duparc [5] in general. (See also [11].)

Proof. The idea of the proof is to show that if q is chosen too large, then the product $t_qt_rt_s$ falls between $8P^3-1$ and $8P^3$, or between $8P^3$ and $8P^3+1$. The boundedness of this product follows from

$$\begin{aligned}
t_qt_rt_s &= \frac{(2Prs-2q)(2Pqs-2r)(2Pqr-2s)}{(q^2-1)(r^2-1)(s^2-1)}\\
&= 8P^3\Big(1-\frac{q}{Prs}\Big)\Big(1-\frac{r}{Pqs}\Big)\Big(1-\frac{s}{Pqr}\Big)\Big(1+\frac{1}{q^2-1}\Big)\Big(1+\frac{1}{r^2-1}\Big)\Big(1+\frac{1}{s^2-1}\Big)\\
&< 8P^3\Big(1+\frac{1}{q^2-1}\Big)^3\\
&\le 8P^3\Big(1+\frac{1}{7^2-1}\Big)^3.
\end{aligned}$$

Therefore, given P, there are only finitely many values for t_q, t_r and t_s. Also, if $q > 5P^{3/2}$, then

$$t_qt_rt_s < 8P^3\Big(1+\frac{1}{q^2-1}\Big)^3 < 8P^3+1\,.$$

From the definition of t_s we get $s^2 < 2Pqr$, $(s/r)^2 < 2Pq/r < 2P$ and $s/r < \sqrt{2P}$. To obtain a lower bound for $t_qt_rt_s$ we begin with

$$\begin{aligned}
t_qt_rt_s &= \frac{(2Prs-2q)(2Pqs-2r)(2Pqr-2s)}{(q^2-1)(r^2-1)(s^2-1)}\\
&= 8P^3\Big(1-\frac{q}{Prs}\Big)\Big(1-\frac{r}{Pqs}\Big)\Big(1-\frac{s}{Pqr}\Big)\Big(1+\frac{1}{q^2-1}\Big)\Big(1+\frac{1}{r^2-1}\Big)\Big(1+\frac{1}{s^2-1}\Big)\\
&> 8P^3\Big(1-\frac{1}{Ps}\Big)\Big(1-\frac{1}{Pq}\Big)\Big(1-\frac{s}{Pqr}\Big)\\
&> 8P^3\Big(1-\frac{1}{Pq}\Big)^2\Big(1-\frac{\sqrt{2}}{\sqrt{P}q}\Big).
\end{aligned}$$

Since $P \ge 5$, we find that if $q > 20P^{5/2}$, then $t_qt_rt_s > 8P^3-1$.

Since P does not divide $t_qt_rt_s$, we get $t_qt_rt_s \ne 8P^3$. Therefore if $q > 20P^{5/2}$, then $8P^3-1 < t_qt_rt_s < 8P^3$ or $8P^3 < t_qt_rt_s < 8P^3+1$, which is impossible. Hence $q < 20P^{5/2}$, which proves that given P there are only finitely many values for q. Since $r^2 < s^2 < 2Pqr$, we get $r < 2Pq$ and $s < \sqrt{2Pqr} < 2Pq$, which completes the proof that given P there are only finitely many values for q, r and s. □

Remark. Based on the many sC numbers we have encountered, it appears that $t_qt_rt_s > 8P^3$ and $s^5 < N$, but we have no idea how to prove this. This would imply that all sC numbers have at least six prime factors. If we relax some of the conditions and define $P = 239$, $q = 29$, $r = 71$ and $s = 701$, then t_q, t_r and t_s are positive integers and $t_qt_rt_s < 8P^3$.

3. Organization of a Search

Before initiating a search we went through the list [**9**] of all base 2 Fermat pseudoprimes below 2^{64} and checked if any of these are sC numbers and found the following six examples:

$$\begin{aligned}
&17\cdot 31\cdot 41\cdot 43\cdot 89\cdot 97\cdot 167\cdot 331\,,\\
&41\cdot 53\cdot 79\cdot 103\cdot 239\cdot 271\cdot 509\,,\\
&17\cdot 37\cdot 41\cdot 71\cdot 79\cdot 97\cdot 113\cdot 131\cdot 191\,,\\
&17\cdot 61\cdot 71\cdot 89\cdot 197\cdot 311\cdot 769\cdot 2729\,,\\
&19\cdot 41\cdot 43\cdot 71\cdot 89\cdot 127\cdot 199\cdot 449\cdot 991\,,\\
&29\cdot 37\cdot 79\cdot 181\cdot 191\cdot 449\cdot 701\cdot 3457\,.
\end{aligned}$$

The first three were discovered by Pinch [12, Section 5]. We also found 13 squarefree base 2 Fermat pseudoprimes satisfying $(p+1)\mid(N-1)$ for all primes $p\mid N$ including the following two examples each with 6 prime factors:

$$11\cdot 29\cdot 71\cdot 79\cdot 181\cdot 251\,,\quad 13\cdot 251\cdot 683\cdot 3571\cdot 5281\cdot 11119\,.$$

Note that the squares of the Wieferich primes 1093 and 3511 are base 2 Fermat pseudoprimes satisfying $(p+1)\mid(N-1)$ for all primes $p\mid N$.

One way to conduct a search for sC numbers with d prime factors is to run $P=\prod_{i=1}^{d-3}p_i$ through products of $d-3$ compatible primes up to a some preassigned bound M. The inner three loops have t_s, t_r and t_q running through ranges determined by

$$\begin{aligned}
&t_s<2P\,,\\
&t_r>t_s\,,\\
&t_q>t_r\,,\\
&t_q>2P\,,\\
&\gcd(t_st_rt_q,P)=1\,,\\
&t_st_rt_q>8P^3\left(1-\tfrac{1}{Pq_1}\right)\left(1-\tfrac{1}{Ps_1}\right)\left(1-\tfrac{\sqrt{2}}{\sqrt{P}q_1}\right),\\
&t_st_rt_q<8P^3\left(1+\tfrac{1}{q_1^2-1}\right)\left(1+\tfrac{1}{r_1^2-1}\right)\left(1+\tfrac{1}{s_1^2-1}\right),
\end{aligned}$$

where q_1, r_1 and s_1 are the next three primes greater than p_{d-3}. Inside of these loops, if $t_r/t_s=2$, 4 or 8, then the polynomial (2.10) is tested for prime integer roots $q>p_{d-3}$ using the MAPLE subroutine isolve. If there are any, then for these values of q we test if (2.8) has a prime integer solution $r>q$. If so, then we put $s=(t_qq^2+2q-t_q)/(2Pr)$ and check if s is a prime $>r$ and verify all divisibility conditions necessary for $N=Pqrs$ to be an sC number. If (2.10) does not give rise to a sC number or t_r/t_s is not equal to 2, 4 or 8, then the polynomial (2.9) is tested for prime integer roots $q>p_{d-3}$. If there are any, then we compute $r=B/A$ and $s=(t_qq^2+2q-t_q)/(2Pr)$, and check the primality of r and s, and all divisibility conditions necessary for $N=Pqrs$ to be an sC number. This method worked well for $d=4$. In this case the variable $P=p_1$ runs through the primes ≥ 5. We report that if there are any sC numbers with exactly four prime factors, then the smallest prime factor must be greater than 4000 and $N>10^{24}$ (see below).

To increase the lower bound for sC numbers with exactly four prime factors we initiated a search looping t_s and s through appropriate ranges. More precisely, suppose $N = pqrs < X$, where $p < q < r < s$ are primes, $t_s := (2pqr - 2s)/(s^2 - 1)$ is an integer and X is some preassigned bound. Then $t_s < 2p < 2X^{1/4}$ and $s < (2X/t_s)^{1/3} + 1$ since $(s-1)^3 t_s < (s^3 - s)t_s = 2N - 2s^2 < 2X$. In the outer loop t_s ranges through the positive integers $< 2X^{1/4}$ and in the inner loop s ranges through the odd primes $< (2X/t_s)^{1/3} + 1$. Before checking if $n := t_s(s^2 - 1)/2 + s = N/s$ is a product of three primes $p < q < r$ with $r < s$ it is best to first check that $N = ns$ is a base 2 Fermat pseudoprime. If n is a product of three primes $p < q < r$ with $r < s$, then the divisibility conditions for N to be an sC number are checked. With $X = 10^{24}$ we found no sC numbers with exactly four prime factors.

Another way to conduct a search for sC numbers is to modify the method used by Pinch [**11**] to find all Carmichael numbers less than some preassigned bound X. Assume that $N = \prod_{i=1}^{d} p_i$ is an sC number less than X and with exactly d prime factors. One obtains all such N by first looping through all compatible sets of $d - 1$ primes such that $p_1 p_2 \cdots p_{j-1} p_j^{d+1-j} < X$, $j = 1, 2, \ldots, d - 1$. At search level $d - 1$ let $P = \prod_{i=1}^{d-1} p_i$, $L = \mathrm{lcm}\{(p_i^2 - 1)/2\}_{i=1}^{d-1}$, and solve the congruence $Pp \equiv 1 \pmod{L}$ for p, where $0 < p < L$. Next, check if p satisfies the following conditions: (i) $p_{d-1} < p < \sqrt{2P}$, (ii) p is prime, and (iii) $(p^2 - 1)/2$ divides $P - p$. If all of these conditions are satisfied, then $N = Pp$ is an sC number. If $(p + L)^2 < 2P$, then increment p by L and retest the above conditions. We completed this search with $5 \leq d \leq 12$ for various values of X between 10^{16} and 10^{24}. Before testing condition (iii) we checked if $N = Pp$ is a base 2 Fermat pseudoprime. Four more sC numbers slightly beyond 2^{64} were found. They are:

$$\begin{aligned}
&17 \cdot 29 \cdot 37 \cdot 41 \cdot 151 \cdot 199 \cdot 449 \cdot 571 \cdot 5851\,,\\
&41 \cdot 53 \cdot 79 \cdot 137 \cdot 139 \cdot 181 \cdot 239 \cdot 271 \cdot 1429\,,\\
&13 \cdot 17 \cdot 19 \cdot 29 \cdot 41 \cdot 89 \cdot 97 \cdot 127 \cdot 199 \cdot 251 \cdot 449\,,\\
&17 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 109 \cdot 199 \cdot 419 \cdot 881\,.
\end{aligned}$$

We found no reason why any prime $p_1 \geq 5$ could not be the smallest prime factor of some sC number N. However, since the prime factors of N must be compatible, sC numbers with p_1 very small are more likely to be large. For this reason we decided to try a method based on a probabilistic argument by Erdös [8] for constructing Carmichael numbers. This method begins by choosing a number M with many small factors. Next, a list $\mathcal{P}$ of the primes p not dividing M such that $p \pm 1$ divides M is constructed. It is reasonable to assume that the subproducts of the primes in $\mathcal{P}$ are roughly equidistributed (mod M) among the $\phi(M)$ reduced residue classes (mod M). If $2^{|\mathcal{P}|} > \phi(M)$, where $|\mathcal{P}|$ is the cardinality of $\mathcal{P}$, then there is a good chance that some subproduct N of the primes in $\mathcal{P}$ will be congruent to 1(mod M). This number N will be an sC number because for every prime $p|N$ we have $p \pm 1 \mid M \mid N - 1$. The relatively large sC number

$$\begin{aligned}
7 \quad &\cdot 37 \cdot 53 \cdot 59 \cdot 109 \cdot 131 \cdot 191 \cdot 229 \cdot 571 \cdot 683 \cdot 919 \cdot 929\\
&\cdot 1151 \cdot 1451 \cdot 1871 \cdot 4751 \cdot 7019 \cdot 7039 \cdot 7129 \cdot 51679 \cdot 244529
\end{aligned}$$

was discovered using $M = 2^7 \cdot 3^4 \cdot 5^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$, which has $|\mathcal{P}| = 51$ and $2^{|\mathcal{P}|} \approx \phi(M)$. With $M = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ the sC number

$$11 \cdot 41 \cdot 47 \cdot 79 \cdot 127 \cdot 137 \cdot 151 \cdot 181 \cdot 233 \cdot 271 \cdot 701 \cdot 911 \cdot 919 \cdot 1103 \cdot 1217 \cdot 9281 \cdot 13339$$

was discovered. To speed up the search for a subproduct $N \equiv 1 \,(\mathrm{mod}\ M)$ let $\mathcal{A}$ be a set of the 15 or so largest primes in $\mathcal{P}$ and let S be the list of inverses (mod M) of all subproducts of $\mathcal{A}$. Next, search through the subproducts of the primes in $\mathcal{P}$ that are not in $\mathcal{A}$ and contain the prime p_1, testing for a match (mod M) in S. With $|\mathcal{A}| = 15$, searching a space of size 2^{50} in reasonable time was the limit of our MAPLE program. Searching for an sC number with $p_1 = 5$ is well beyond this limit.

We found it necessary to modify the above method in the search for sC numbers N with a small number of prime factors. Suppose that the prime factors of N lie in $\mathcal{P}$. If $L := \mathrm{lcm}\{(p^2-1)/2 : p|N\}$ is a proper divisor of M, then N may not be discovered by the above method. To remedy this problem without slowing down the program too much, we first selected the subproducts of $\mathcal{P}$ that are congruent to $1(\mathrm{mod}\ M_1)$, where M_1 is a proper divisor of M with very small prime factors, say $M_1 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ (we are assuming that $M_1|L$). This will eliminate most of the subproducts of $\mathcal{P}$. Next, we check if the subproduct N is a base 2 Fermat pseudoprime, and if so, then we compute L and test if $N \equiv 1 \,(\mathrm{mod}\ L)$. Using this modification we rediscovered several sC numbers having a small number of prime factors, and found a new one with exactly 10 prime factors:

$$41 \cdot 53 \cdot 67 \cdot 103 \cdot 151 \cdot 379 \cdot 571 \cdot 701 \cdot 2393 \cdot 5851 \,.$$

This number N has 2^4 not dividing $N-1$. In our original program all the integers M that were selected were divisible by larger powers of 2, which explains why this sC number was missed. The number $41 \cdot 53 \cdot 79 \cdot 137 \cdot 139 \cdot 181 \cdot 239 \cdot 271 \cdot 1429$, discovered earlier using the algorithm of Pinch, has 23 dividing L and 19 not dividing $N-1$. This number was rediscovered by our modified Erdös program.

4. Williams Numbers

In the Baillie-PSW primality test a Lucas sequence is chosen so that the Jacobi symbol $(D|N) = -1$, where N is the number to be tested for primality and D is the discriminant of the Lucas sequence. Pomerance [**13**] gave a heuristic argument suggesting that there are infinitely many counterexamples, but no one has ever found one. Based on his argument it is highly probable that there exist odd squarefree composite numbers N with the property that $p-1 \mid N-1$ and $p+1 \mid N+1$ for all primes $p|N$. Echi [7] calls such numbers Williams numbers (more precisely, 1-Williams numbers). There are infinitely many Carmichael numbers [**1**] (i.e. infinitely many squarefree numbers N such that $p-1 \mid N-1$ for all primes $p|N$) and there are infinitely many squarefree numbers N such that $p+1 \mid N+1$ for all primes $p|N$ [**6**,

15]. Whether or not the intersection of these sets is infinite, or even nonempty, is still an open problem. A study of Williams numbers was undertaken by McIntosh and Mitra [**10**]. One of the reasons that Williams numbers appear to be much more rare than sC numbers is that the definition of a compatible set of primes for Williams numbers requires $\gcd(p_i - 1, p_j + 1) = 2$ for all i and j.

Acknowledgement. Support by the Natural Sciences and Engineering Research Council of Canada is gratefully acknowledged. The author thanks Carl Pomerance for bringing to his attention several interesting papers on this subject.

References

[1] W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* (2) **139** (1994), 703–722.

[2] W.R. Alford, A. Granville and C.Pomerance, On the difficulty of finding reliable witnesses, *Algorithmic Number Theory Proceedings (ANTS-I)*, L.M. Adleman and M.-D. Huang, eds., Lecture Notes in Computer Sci. **877** (1994), Springer-Verlag, Berlin, pp. 116.

[3] R. Baillie and S.S. Wagstaff, Jr., Lucas pseudoprimes, *Math. Comp.* **35** (1980) 1391–1417.

[4] N.G.W.H. Beeger, On composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n, *Scripta Math.* **16** (1950) 133–135.

[5] H.J.A. Duparc, On Carmichael numbers, *Simon Stevin* **29** (1952) 21–24.

[6] A. Ekstrom, C. Pomerance and D.S. Thakur, Infinitude of elliptic Carmichael numbers, *J. Aust. Math. Soc.* **92** (2012) 45–60.

[7] O. Echi, Williams numbers, *C. R. Math. Acad. Sci. Soc. R. Can.* **29** (2007) no. 2, 41–47.

[8] P. Erdös, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** (1956) 201–206.

[9] J. Feitsma, List of all base 2 Fermat pseudoprimes below 2^{64} computed by J. Feitsma and edited by W. Galway (2013), www.cecm.sfu.ca/Pseudoprimes

[10] R.J. McIntosh and D. Mitra, Carmichael Numbers with $p + 1 | n + 1$, *J. Number Theory*, to appear.

[11] R.G.E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (1993) 381–391.

[12] R.G.E. Pinch, Absolute quadratic pseudoprimes, unpublished manuscript (2006), http://s369624816.websitehome.co.uk/rgep/p20.pdf

[13] C. Pomerance, Are there counterexamples to the Baillie-PSW primality test?, Unpublished manuscript (1984), www.pseudoprime.com/dopo.pdf

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

[15] T. Wright, There are infinitely many elliptic Carmichael numbers, to appear.