Diophantine Equations Associated with Baillie-PSW Pseudoprimes

RICHARD J. McINTOSH
and
DIPRA MITRA
University of Regina, Canada

In 1980 Pomerance, Selfridge and Wagstaff offered \$30 for a number N which is simultaneuosly a strong base 2-pseudoprime and a (true) Lucas pseudoprime (with a discriminant specified in their paper). Baillie is credited with first proposing such a combination test. For this reason such pseudoprimes are called Baillie-PSW pseudoprimes. Pomerance gave a heuristic argument to show that there should be infinitely many such pseudoprimes. This combined probable prime test might be more reliable than other tests used at that time. Indeed since their article was published, both Mathematica and Maple have switch to some variation on this method. With time the prize for such a number N has grown to \$630.

If odd number N is a base 2-pseudoprime, then order$(2,p)|N-1$ for all primes $p|N$. If N is Lucas pseudoprime with discriminant D, then the rank (of apparition) $\rho(p)$ of the Lucas sequence $U_n(P,Q)$ (mod p) satisfies $\rho(p)|N-\epsilon(N)$ for all $p|N$, where $\epsilon(N)$ is the Jacobi symbol $\left(\frac{D}{N}\right)$. It is known that order$(2,p)|p-1$ and $\rho(p)|p-\epsilon(p)$. To avoid having to compute the order and rank of p, we look for odd squarefree numbers N satisfying (i) $p-1|N-1$ and (ii) $p-\epsilon(p)|N-\epsilon(N)$ for all $p|N$. This combined condition forces $\epsilon(p)=-1$. Hence the second condition becomes $p+1|N-\epsilon(N)$. If N is a true Lucas pseudoprime, then $\epsilon(N)=-1$ and N has an odd number of prime divisors p each satisfying $p+1|N+1$.

We now turn to the search for Carmichael numbers $N=p_1p_2\cdots p_d$, where $p_i+1|N+1$. (We will not require d to be odd.) Hence for each p dividing N we have $p-1|N-1$ and $p+1|N+1$. Since

$$N-1=(N/p)(p-1)+N/p-1$$

and

$$N+1=(N/p)(p+1)-N/p+1\,,$$

we must have both $p-1$ and $p+1$ dividing $N/p-1$, or equivalently, $(p^2-1)/2$ dividing $N/p-1$.

Let $N = \prod_{i=1}^{d} p_i$ with $p_1 < p_2 < \cdots < p_d$. Write $N = Pqrs$, where $P = \prod_{i=1}^{d-3} p_i$, $q = p_{d-2}$, $r = p_{d-1}$ and $s = p_d$. Define

$$f_q = \frac{N/q - 1}{(q^2-1)/2} = \frac{2Prs - 2}{q^2 - 1}\,,$$

$$f_r = \frac{2Pqs - 2}{r^2 - 1} \quad \text{and} \quad f_s = \frac{2Pqr - 2}{s^2 - 1}\,.$$

Then $f_s < f_r < f_q$ are all positive integers, none of which are 0 or 2 (mod P). Observe that

$$\begin{aligned} f_q f_r f_s &= \frac{(2Prs-2)(2Pqs-2)(2Pqr-2)}{(q^2-1)(r^2-1)(s^2-1)} \\ &= 8P^3\Big(1 - \frac{1}{Prs}\Big)\Big(1 - \frac{1}{Pqs}\Big)\Big(1 - \frac{1}{Pqr}\Big) \\ &\qquad \times \Big(1 + \frac{1}{q^2-1}\Big)\Big(1 + \frac{1}{r^2-1}\Big)\Big(1 + \frac{1}{s^2-1}\Big). \end{aligned}$$

If $q \geq 5P^{3/2}$, then $8P^3 < f_q f_r f_s < 8P^3 + 1$, which is impossible. Upper bounds for r and s can then be obtained using the definitions of f_r and f_s. We have established

Theorem 1. Let $N = Pqrs$ be defined as above. Then
(1) $q < 5P^{3/2}$,
(2) $r < 5P^{5/2}$,
(3) $s < 5\sqrt{2}P^{5/2}$.

It is not difficult to show that $1 \le f_s < 2P$, $3 \le f_r < 3P^{3/2}$ and $2P < f_q < 9P^3$.

Solving the system

$$\left\{\begin{array}{l}(q^2-1)f_q = 2Prs - 2\,,\\ (r^2-1)f_r = 2Pqs - 2\,,\\ (s^2-1)f_s = 2Prs - 2\end{array}\right\}$$

for q, r and s in terms of P, f_q, f_r and f_s we find that q^2 is root of a quartic polynomial

$$f_q\big[f_qf_rf_s - 8p^3\big]^3X^4 + C_3X^3 + C_2X^2 + C_1X + f_rf_s\big[f_rf_s(f_q-2)^2 - 4(f_r-2)(f_s-2)p^2\big]^2\,,$$

which implies that q is a factor of

$$f_rf_s(f_q-2)^2 - 4(f_r-2)(f_s-2)p^2\,.$$

We now turn to the easier problem of finding Carmichael numbers $N = p_1 p_2 \cdots p_d$, where $p_i + 1 | N - 1$, or equivalently, $p_i^2 - 1 | 2N - 2$. In the previous problem $\gcd(p_i - 1, p_j + 1) = 2$ for all i and j. This condition is no longer necessary, which makes it much easier to build such numbers N. Two examples are:

$$\begin{aligned} N &= 5002862939121639632040001 \\ &= 31 \times 53 \times 79 \times 89 \times 101 \times 151 \times 181 \times 251 \times 379 \\ &\qquad \times 647 \times 2549 \\ N &= 690134451842708980041692801 \\ &= 29 \times 37 \times 41 \times 43 \times 71 \times 101 \times 127 \times 151 \times 701 \\ &\qquad \times 1871 \times 3457 \times 5851 \end{aligned}$$

To build these examples, let M be a smooth number, say $M = 2^5 \cdot 3^4 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. Then construct a list of primes q_i such that $q_i \pm 1 | M$. For our M we get a list of 39 primes. There are $2^{39} - 1 = 549755813887$ nonempty subproducts of these primes, which fall into the $\phi(M) = 125411328000$ reduced residue classes modulo M. If we make the plausible assumption that the these subproducts fall into each reduced residue class with equal probability, then there should be about $2^{39}/\phi(M) \approx 4$ subproducts congruent to $1 \pmod{M}$. These subproducts $N = \prod p_i$ satisfy $p_i \pm 1 | M | N - 1$.

Note that the subproduct N does not necessarily have to be $1 \pmod{M}$. It suffices to have

$$N = \prod_{i=1}^{d} p_i \equiv 1 \pmod{L},$$

where

$$L = \operatorname{lcm}\left\{ \frac{p_i^2 - 1}{2} \right\}_{i=1}^{d}.$$

Choosing a smooth number M before searching for (or building) N may not be the best method if we are interested in N with the minimum number of prime factors, but we still have to restrict the growth of

$$L_k = \operatorname{lcm}\left\{ \frac{p_i^2 - 1}{2} \right\}_{i=1}^{k}$$

when choosing the p_i to form the product N.

To obtain bounds on the larger prime factors of N, we put $N = Pqr$, where $P = \prod_{i=1}^{d-2} p_i$, $q = p_{d-1}$ and $r = p_d$. Since $(p^2-1)/2$ must divide $N-1$ for all $p|N$, we define the quotients

$$t_q = \frac{2Pqr-2}{q^2-1} \quad \text{and} \quad t_r = \frac{2Pqr-2}{r^2-1}\,.$$

Then $t_r < t_q$ are positive integers, neither of which are 0 or 2 (mod P). It turns out that $1 \le t_r < 2P$ and $t_q t_r > 4P^2$. Moreover,

$$t_q t_r = 4P^2\Big(1-\frac{1}{Pqr}\Big)^2\Big(1+\frac{1}{q^2-1}\Big)\Big(1+\frac{1}{r^2-1}\Big)\,,$$

which leads to

Theorem 2. Let $N = Pqr$ be defined as above. Then
(1) $q < 3P$,
(2) $r < 2Pq < 6P^2$.

The analogous theorem for Carmichael numbers has $q < 2P^2$ and $r < P^3$.