SOME COMMENTS ON BAILLIE-PSW PSEUDOPRIMES

Zhuo Chen
Department of Mathematics and Statistics,
University of Minnesota, Duluth, Duluth, MN 55812

John Greene
Department of Mathematics and Statistics,
University of Minnesota, Duluth, Duluth, MN 55812
(Submitted April 2001-Final Revision July 2001)

1. INTRODUCTION

In [2], Pomerance, Selfridge and Wagstaff offered \$30 for a number n which is simultaneously a strong base 2-pseudoprime and a Lucas pseudoprime (with a discriminant specified in [2]). Since there is no known composite number that meets this criteria, even if the first condition is weakened to requiring only that n be a base 2-pseudoprime, it was suggested that this might be a reasonable test for "primality" which, though fallible, might be more reliable than current tests. Indeed since their article was published, both Mathematica and Maple have switched to some variation on this method.

In [3], an unpublished manuscript by Carl Pomerance (available on Jon Grantham's web site, www.pseudoprime.com/pseudo.html), Baillie is credited with first proposing such a combination test. In [2], Pomerance, Selfridge and Wagstaff show that there are no counterexamples less then $20 \cdot 10^9$. Subsequently, a composite number which is both a base 2-pseudoprime and a Lucas pseudoprime has been referred to as a Baillie-PSW pseudoprime.

Pomerance [3] gave a heuristic argument to show that there should be infinitely many such numbers. In fact, his argument suggest that for any $\varepsilon > 0$, the number of Baillie-PSW pseudoprimes $< x$ should exceed $x^{1-\varepsilon}$ for x sufficiently large depending on the choice of ε.

With time, the prize for such a number, n has grown to \$620, and the conditions have been relaxed to the following [4]:

1) $2^n \equiv (\text{mod } n)$,
2) $F_{n+1} \equiv (\text{mod } n)$
3) $n \equiv 2$ or $3 (\text{mod } 5)$,
4) n is composite (with explicit factorization provided).

In this paper, we present calculations related to the construction of Baillie-PSW pseudoprimes. We use a variation of the method Pomerance described. It should be pointed out that we have no example of such a number, although we are certain we could construct one if only we could search through a rather large space in which such an example will live.

2. PRELIMINARIES

The following are elementary facts related to base 2-pseudoprimes and Fibonacci pseudoprimes. These facts can be found in many books on factoring, cryptography or primality. For example, see [1 Sec. 10.14], [5, Chap. 2 Sec IV], or [6, pp. 107-115].

For each odd number $n > 1$, there is an integer $h > 0$ such that

$$\begin{array}{ll} 1) & 2^h \equiv 1 (\text{mod } n), \\ 2) & \text{if } 2^m \equiv 1 (\text{mod } n) \text{ then } h|m. \end{array}$$

This number h is called the order of 2 modulo n and is denoted $\text{ord}_n(2)$. Since $2^{\phi(n)} \equiv 1$ (mod n), it follows that $h|\phi(n)$. Similarly, for each odd number $n > 1$ there is a positive integer k such that

$$\begin{array}{ll} 1) & F_k \equiv 0 (\text{mod } n), \\ 2) & \text{if } F_m \equiv 0 (\text{mod } n) \text{ then } k|m. \end{array}$$

We are unaware of a standard notation for this index k. We refer to it as the Fibonacci order of n and denote it by $\text{ord}_f(n)$.

A composite number, n, is called a base 2-pseudoprime if $2^{n-1} \equiv 1 (\text{mod } n)$. This happens if and only if $\text{ord}_n(2)$ is a divisor of $n-1$. For primes p, $F_{p-\left(\frac{5}{p}\right)} \equiv 0 (\text{mod } p)$. If for an odd composite number n, $F_{n-\left(\frac{5}{n}\right)} \equiv 0 (\text{mod } n)$, we call n a Fibonacci pseudoprime. This happens if and only if $\text{ord}_f(n)$ is a divisor of $n - \left(\frac{5}{n}\right)$.

The following are obvious sufficient conditions for n to be a base 2-pseudoprime or a Fibonacci pseudoprime: Suppose that n is an odd, square free composite number.

$$\begin{array}{l} \text{If for each prime } p|n, \text{ord}_p(2) \text{divides } n-1 \\ \text{then } n \text{ is a base 2-pseudoprime.} \end{array} \tag{2.1}$$

$$\begin{array}{l} \text{If for each prime } p|n, \text{ord}_f(p) \text{divides } n - \left(\dfrac{5}{n}\right) \\ \\ \text{then } n \text{ is a Fibonacci pseudoprime.} \end{array} \tag{2.2}$$

As we mentioned in the introduction, Pomerance, Selfridge and Wagstaff offer \$620 for an example of a number $n \equiv 2$ or 3 (mod 5) such that n is both a base 2-pseudoprime and a Fibonacci pseudoprime. In this case, $n - \left(\frac{5}{n}\right) = n + 1$.

Here is a variation on Pomerance's method for searching for such a number: Let M and N be two highly composite numbers with $\text{GCD}(M, N) = 2$. Let P be the set of all primes p with the following properties:

$$\begin{array}{ll} 1) & p \text{ does not divide } MN, \\ 2) & \text{ord}_p(2) \text{ divides } M, \\ 3) & \text{ord}_f(p) \text{ divides } N. \end{array}$$

Define a function f on the subsets of P as follows:

$$f(A) = \prod_{p \in A} p.$$

If a subset, A, of P with cardinality at least 2 can be found such that

$$f(A) \equiv 2 \text{ or } 3 (\text{mod } 5),$$

$$f(A) \equiv 1 (\text{mod } M), \text{ and } f(A) \equiv -1 (\text{mod } N),$$

then as an easy consequence of (2.1) and (2.2), $f(A)$ will be a Baillie-PSW pseudoprime. If P is a large set compared with MN, then we expect lots of subsets A to exist. That is, assuming that the congruence classes of $f(A)$ are roughly uniformly distributed modulo M and N, one might expect

$$\frac{2^{|P|}}{\phi(MN)} \tag{2.3}$$

subsets A to have the desired properties.

In addition to Pomerance's manuscript, Grantham's site also contains a list of 2030 primes, constructed by Grantham and Red Alford. Grantham comments that he and Alford "highly suspect" that some subset product of these primes is a Baillie-PSW pseudoprime. The site does not give reasons. However, an analysis of the primes shows that each has the property that $p-1$ divides M and $p+1$ divides N, where $M = 2(13)^2(17)^2(29)^2(37)^2(41)^2(53)^2(61)\ldots(1249)$ and $N = 2^2(3)^7(7)^4(11)^3(19)^2(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2(71)\ldots(1187)$. Here, the only odd primes dividing M are congruent to 1 (mod 4) and the only odd primes dividing N are those congruent to 3(mod 4). In each case, there are exactly 100 such primes. For this choice of M and N, $\phi(MN) \cong 1.017659177 \times 10^{545} < 2^{1811}$. The problem, of course, is that a space of size 2^{2030} is hard to search even if one expects 2^{219} examples.

This current investigation began as a Master's project for the first author. The project was to look for much smaller numbers M and N for which $\frac{2^{|P|}}{\phi(MN)} > 1$. It was thought that using $\text{ord}_p(2)$ and $\text{ord}_f(p)$ instead of $p-1$ and $p+1$ would significantly reduce the size of M and N. We performed our calculations using five Pentium III PC's and three Apple PowerMac's. We used C/C++ on the PC's, employing only single precision arithmetic (but with 64 bit integers.) On the PowerMac's, we used Maple V^{TM}.

3. RESULTS WITHOUT USING ORD$_p$(2) OR ORD$_f$(p).

Based on the primes of Grantham's site and their implied numbers M and N, we searched for smaller M and N as follows. We attempted to partition the small primes between M and N a bit more evenly. We began with intial values

$$M_{\text{start}} = 2(7)^4(13)^2(19)^2(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2,$$

$$N_{\text{start}} = (2)^6(3)^6(11)^3(17)^2(29)^2(37)^2(41)^2(53)^2.$$

We put the powers of 2 and 3 in N_{start} because it was thought that this would be advantageouos when we considered $\text{ord}_p(2)$, as discussed in the next section. We chose to favor $\text{ord}_p(2)$ over $\text{ord}_f(p)$ because it was quicker to calculate $\text{ord}_p(2)$ than $\text{ord}_f(p)$. For a given value of n, we then construct an

$$M_{\text{tail}} = \text{ product of } n-9 \text{ primes, all congruent to } 3(\text{mod } 4),$$

$$N_{\text{tail}} = \text{ product of } n-7 \text{ primes, all congruent to } 1(\text{mod } 4).$$

We set $M = M_{\text{start}}M_{\text{tail}}$ and $N = 4N_{\text{start}}N_{\text{tail}}$. Thus, M and N are each divisible by exactly n odd primes. Next, we constructed the set

$$N_{\text{init}} = \{a : a \text{ is a divisor of } N_{\text{start}}\}$$

of all divisors of N_{start}. This set contains 47,628 elements. For each k, let

$$N_k = \{x : x \text{ is a divisor of } N_{\text{tail}} \text{ and } x \text{ has } k \text{ prime divisors}\}.$$

This set has $\binom{n-7}{k}$ elements. If $g(x,y) = 4xy - 1$, with $x \in N_{\text{init}}$ and $y \in N_k$ (setting $y = 1$ if $k = 0$), then $g(x,y) + 1$ is a divisor of N with exactly k prime divisors in common with N_{tail}. We proceed as follows: As k increases from 0, for each x in N_{init} and y in N_k, determine if $g(x,y) - 1$ is a divisor of M. If so, test if $g(x,y)$ is prime. If it is, add $g(x,y)$ to the list of pirmes in P_k. At the end, we construct the set $P = \cup_k P_k$. Technically, we should delete any primes $p|MN$ from the list. In the following tables, we have not done this. However, this will not affect our results since the number of such primes is small compared to the size of P.

Our first table gives the number of primes found for various values of n, k:

k\n	10	20	30	40	50	60	70	80	90	100
0	7	9	19	19	24	27	30	32	33	34
1	1	8	21	40	60	91	123	151	194	224
2	0	1	10	37	72	119	201	295	416	568
3	0	0	9	24	58	123	203	342	565	850
4	0	0	0	5	26	66	122	236	380	528
5	0	0	0	2	6	13	47	91		
6	0	0	0	0	0	3	7			
total	8	18	59	127	246	442	733	1147	1588	2204
needed	192	332	490	660	838	1023	1214	1410	1610	1813

Table 3.1

Some comments on this table: the empty entries indicate computations we did not undertake (there are about 37 million calculations needed for each element of N_{start} for entry (90,5), for example. Our construction ensures that each $P_k = P_k(n)$ satisfies $P_k(m) \subseteq P_k(n)$ if $m \leq n$. Thus, we know that we will find at least 91 primes for entry $n = 90, k = 5$. Hence, by $n = 90$, the number of primes in P grows past the expected number needed to cover all reduced residue classes. It should also be pointed out that the counts are not complete for the larger numbers n: we sped up calculations by using only the smallest entries from N_{init}. Based on numerical evidence, this missed some but not many primes. An interesting feature to the table is that although Alford's and Grantham's M and N seemed very contrived in that each was divisible by exactly 100 odd primes, it appears that they could not have decreased the number of primes by much.

We analyzed our data as follows. A number is called z-smooth if all its prime divisors are less than z. Riesel [6, page 164] gives a crude estimate of $u^{-u}x^u$ for the number of x-smooth numbers less than x^u. He indicates that this estimate is often good enough to approximate the run time of computer algorithms which make use of smooth numbers. We are seeking primes such that $p-1$ and $p+1$ are both z-smooth with respect to some z, and which also have factors from prescribed sets of primes. If one has a set of primes with asymptotic density $1/2$, then Riesel's argument leads to an estimate of $(2u)^{-u}x^u$ numbers less than x^u which are x-smooth and have all their prime divisors from that prescribed set.

We use the following model: Given two disjoint sets of n primes; $p_1, p_2, \ldots, p_n$, and $q_1, q_2, \ldots, q_n$ with all the p's and q's of about the same size, we select j of the primes from the q-list, multiply them together to get an m. We ask that $4m-1$ be prime and $4m-2$ factor over the p's. In fact, what we really need is for $2m-1$ to factor over the p's. In this case, $x^u \cong 2q_n^j$ and $x = p_n \cong q_n$. This gives

$$u \cong \frac{\ln 2 + j \ln q_n}{\ln q_n} = j + \frac{\ln 2}{\ln q_n} = j + \alpha,$$

where $\alpha = \ln(2)/\ln(q_n)$. Thus, the rough probability that $4m-2$ is smooth with factors dividing M is $(2j+2\alpha)^{-j-\alpha}$. We also require that $4m-1$ be prime, which happens with expected probability $\frac{2}{\ln(4m-1)}$. Thus, our estimate of the probability that a number of this form meet our requirements is $\frac{2(2u)^{-u}}{\ln(4q_n^j)}$, where $u = j + \frac{\ln 2}{\ln q_n}$. The expected number of primes of this form is $\frac{2(2u)^{-u}}{\ln(4q_n^j)}\binom{n}{j}$.

Obviously, our primes differ dramatically in size. Moreover, our numbers need more than smoothness – there are limits on the divisibility of our numbers by small primes. However, this model is still useful for making predictions and understanding overall patterns. For example, using $\binom{n}{j} \cong \frac{n^j}{j!} \cong \frac{n^j e^j}{\sqrt{2\pi j}\, j^j}$, we have

$$\frac{2(2u)^{-u}}{\ln(4q_n^j)}\binom{n}{j} \cong \frac{2^{1-u}u^{-u}n^j e^j}{\ln(4q_n^j)\sqrt{2\pi j}\, j^j}.$$

If we ignore the difference between j and u, this expression is approximately

$$\frac{2}{\ln(4q_n^j)\sqrt{2\pi j}}\left(\frac{en}{2j^2}\right)^j. \tag{3.1}$$

Thus, we expect no primes to be contributed by the cases where $j > \sqrt{en/2}$. For example looking at Table 3.1, when $n = 50$, we expect no primes for $k \geq 8$. In fact, we got none for $k = 6$ or 7 either. If we trust (3.1) to give good estimates of the numbers of primes for various k in Table 3.1, then for $k = 6$, we should have found $.37 \cong 0$ primes. In fact, we do not trust (3.1) for more than a crude analysis. For example, it predicts 1.59 primes for $n = 50, k = 5$ rather than the 6 we found, and it predicts 4.8 primes for $k = 4$ rather than our 26.

Suppose we accept $\frac{2(2u)^{-u}}{\ln(4q_n^j)}$ as a rough probability that a prime $g(x,y)$ has the desired properties, where $g(x,y) - 1$ has j prime divisors. For each entry (n, k) in Table 3.1, we solved the equation

$$\frac{\#\text{ of primes found}}{\#\text{ of cases looked at}} = \frac{2(2u)^{-u}}{\ln(4q_n^j)} \tag{3.2}$$

for j, where q_n is the largest prime divisor of MN. We take this "j" to be some kind of average number of prime factors. The results are recorded in the table below.

k\n	10	20	30	40	50	60	70	80	90	100
0	3.32	3.21	2.96	2.95	2.87	2.82	2.78	2.76	2.75	2.73
1	4.24	4.03	3.90	3.81	3.76	3.69	3.64	3.62	3.58	3.57
2	-	5.16	4.82	4.65	4.60	4.57	4.52	4.49	4.46	4.44
3	-	-	5.40	5.44	5.41	5.37	5.37	5.35	5.32	5.30
4	-	-	-	6.42	6.26	6.24	6.26	6.24	6.25	6.29
5	-	-	-	7.13	7.20	7.28	7.17			

Table 3.2

We did not compute values for $k = 6, n = 60$, 70 because we only did partial searches with $k = 6$. We ignored $n = 80, k = 5$ for the same reason. Based on the table, we expect the (5,90) entry to be roughly 7.2. We may use this to estimate the number of primes found for $k = 5, n = 90$. The result is that we expect some 171 primes in this case. Similarly, we expect maybe 46 primes when $k = 6$ (using $j = 8.2$) so that k from 0 to 6, we expect a total of 1805 primes when $n = 90$.

This table may be used to interpolate back to the point where the number of primes exactly matches the minimum number needed to cover all reduced residue classes. This point will be between $n = 80$ and $n = 90$. If we are cautious and use only $k = 0, \ldots, 6$ and j-values: 2.76, 3.62, 4.49, 5.34, 6.25, 7.20, 8.20, then the matching point occurs at $n = 88$. Using the most optimistic numbers for j reduces this to $n = 85$.

4. THE EFFECT OF USING ORD$_p$(2) OR ORD$_f$(p)

How much does it help to ask only that $\text{ord}_p(2)$ divide M rather than that $p-1$ divide M? Here is one model. Let $M' = 2^4(3^3)(11^2)(17)(29)M$ and search for primes as in Section 3, but for which $p - 1$ divides M'. Include p in P if $2^M \equiv 1 \pmod{p}$. The only additional primes picked up this way are primes in which $p-1$ does not divide M, but $p-1$ divides M' and $\text{ord}_p(2)$ divides M. We expect that $p-1$ will have exactly one factor of 11 in $\frac{10}{11^2}$ cases, and that this factor will not divide $\text{ord}_p(2)$ in $\frac{1}{11}$ of those cases. Similarly, exactly two factors of 11 should occur in $\frac{10}{11^3}$ cases, with both factors dropping out $\frac{1}{11^2}$ of the time. Thus, the 11's should increase the count by a factor of $(1+\frac{10}{11^3}+\frac{10}{11^5})$. Arguing likewise for the other divisors M'/M gives a multiplier of

$$\left(1+\frac{1}{8}+\frac{1}{32}+\frac{1}{128}+\frac{1}{512}\right)\left(1+\frac{2}{27}+\frac{2}{243}+\frac{2}{2187}\right)$$

$$\left(1+\frac{10}{1331}+\frac{10}{11^5}\right)\left(1+\frac{16}{17^3}\right)\left(1+\frac{28}{29^3}\right)\cong 1.278.$$

As can be seen, it is the smaller primes that contribute most to this number. This is why we chose to make N divisibile by both powers of 2 and powers of 3. In Table 4.1, we give the actual numbers of primes found for various n, k for which $p-1$ divides M', $\text{ord}_p(2)$ divides M, and $p+1$ divides N.

k\n	10	20	30	40	50	60	70	80	90	100
0	9	11	23	24	30	33	35	39	40	42
1	2	10	28	55	77	112	151	183	233	268
2	0	1	19	57	103	173	285	415	580	780
3	0	0	9	30	71	171	274	472	762	1144
4	0	0	0	9	35	91	190	359	564	736
5	0	0	0	2	8	20	70	134		
6	0	0	0	0	0	4	10			
total	11	22	79	177	324	604	1015	1602	2179	2970
ratio	1.38	1.22	1.34	1.39	1.32	1.37	1.38	1.39	1.37	1.35
needed	192	332	490	660	838	1023	1214	1410	1610	1813

Table 4.1

In the table, the actual multiplier (the ratio row) appears to be somewhat higher, closer to 1.37 with the data looked at so far. We do not have an explanation for this discrepancy.

Given the data above, it is natural to ask how low n can be and still have a sufficiently large number of primes to expect to cover the reduced residue classes of MN. According to the table, this happens by $n=80$. We estimated the number of primes with $n=75$ as follows: using the formula

$$\frac{\#\text{ of primes found}}{\#\text{ of cases looked at}}=\frac{2(2u)^{-u}}{\ln(4q_n^j)}$$

and solve for j with the data from $n = 70$ and $n = 80$ in table 4.1 (admittedly a questionable thing to do) we interpolated to get estimated values of j for $n = 75$. Here are our results:

n\k	0	1	2	3	4	5	6	7
70	2.734	3.580	4.417	5.291	6.140	7.066		
75	2.715	3.572	4.404	5.277	6.134	7.066	8.016	8.966
80	2.695	3.563	4.391	5.262	6.128			

Table 4.2

The row for $n = 75$ was obtained by averaging the results from 70 and 80, but rounding up to three decimal places. However, the prime list for $n = 80, k = 5$ was incomplete, so we used the value from $n = 70, k = 5$ for this entry. We estimated the entries for $k = 6$ and $k = 7$ by adding .95 to the previous entries. Based on this table, when $n = 75$, we should expect to find the following numbers of primes:

0	1	2	3	4	5	6	7	total	needed
37	165	344	360	263	103	28	6	1306	1311

Table 4.3

Since we were conservative in our estimates for $k = 5, 6, 7$, we decided to actually carry out the computer search for primes. We were lucky to exceed expectations. Here is our actual count of primes found for $n = 75$.

0	1	2	3	4	5	6	7	total	needed
35	165	349	356	279	116	25	1	1326	1311

Table 4.4

Of the total, six primes are divisors of MN, leaving a set P with 1320 elements. Thus, we expect a Baillie-PSW pseudoprime to exist at this level. Since we did not complete counts for $k = 6, 7$, it is remotely possible that there are enough primes at $n = 74$ as well.

Introducing the Fibonacci order with our M and N might be expected to have the following effect: Supposing we use an $N' = N(7)^3(13)^2(19)(23)$. We would then expect

$$\left(1+\frac{1}{1024}\right)\left(1+\frac{6}{7^3}+\frac{6}{7^7}+\frac{6}{7^7}\right)\left(1+\frac{12}{13^3}+\frac{12}{13^5}\right)\left(1+\frac{18}{19^3}\right)\left(1+\frac{22}{23^3}\right)\cong 1.027$$

times as many primes. In particular, for $n = 70, (1022)(1.027) \cong 1050$, still far short of the 1214 needed in this case. In actual calculations, we again appear to beat this estimate, picking up at least 40 additional primes for k between 0 and 3. However, we estimate fewer than 40 primes remain to be found, leaving us more than 100 short of our goal.

5. THE QUEST FOR $n = 70$

Given that we could find enough primes in our set P with $n = 75$, which corresponds to 75 odd primes dividing each of M and N, we attempted to push the computational limits of our computers to try to reduce this to $n = 70$. There are several ways to change the way M and N are constructed to try to increase the size of P. We have put powers of 2 and 3 in N so as to favor the existence of primes with $\mathrm{ord}_p(2)$ dividing M over $\mathrm{ord}_f(p)$ dividing N. Suppose we are a bit more equitable, and start with, say,

$$M_{\text{start}} = 2(3)^6(11)^3(17)^2(23)^2(31)^2(41)^2(47)^2(59)^2,$$

$$N_{\text{start}} = (2)^6(7)^4(13)^2(19)^2(29)^2(37)^2(43)^2(53)^2(61)^2.$$

One might expect this change to produce slightly more primes with $p-1|M, p+1|N$, decrease the number of primes added using $\mathrm{ord}_p(2)$, but increase the number of primes added using $\mathrm{ord}_f(p)$. In fact, for reasons we do not understand, this change slightly decreased the number of primes p with $p-1|M, p+1|N$. The increase in the number of primes added using $\mathrm{ord}_f(p)$ did not offset this decrease.

We only calculated these numbers for $0 \le k \le 4$. It is possible that things would improve for higher values of k. We considered it very unlikely, however, that searching higher k would yield enough additional primes to make a real difference. This being the case, we went back to our original set up, but increased the multiplicity of the smaller prime divisors of M and N. This increased the size of P, but also increased $\phi(MN)$, meaning that it increased the number of primes needed. We finally succeeded in obtaining enough primes with

$$M_{\text{start}} = 2(7)^5(13)^3(19)^3(23)^2(31)^2(43)^2(47)^2(59)^2(67)^2,$$

$$N_{\text{start}} = (2)^{12}(3)^8(11)^3(17)^3(29)^2(37)^2(41)^2(53)^2,$$

and M_{tail} and N_{tail} as before. That is, $M_{\text{tail}} = (71)(79)\dots(787)$, a product of 66 primes all congruent to 3(mod 4), and $N_{\text{tail}} = (61)(73)\dots(829)$, a product of 68 primes all congruent to 1 (mod 4). In this case, we obtained the following table:

k	0	1	2	3	4	5	6	7	total
p-1/p+1	30	137	232	242	137	51	7	1	837
$\mathrm{ord}_p(2)$	6	37	108	88	79	27	3		348
ord_f(p)	0	6	17	21	9	4			57
total	36	180	357	351	225	82	10	1	1242

Table 5.1

The needed number of primes increased from the original 1214 to 1240. Thus, $2^{|P|}$ is only about four times as big as $\phi(MN)$. We only did partial searches with $k = 4, 5$ for primes satisfying $\mathrm{ord}_f(p)|N$, and we suspect that there are more primes to find. Also, we were using only single precision arithmetic in our search on PC's (using 64-bit numbers, however) and at $k = 6, 7$ we were hampered by integer overflow problems, so we expect a few more primes here as well. Thus, we are confident that there is a Baillie-PSW pseudoprime to be found using this M and N.

It would be hard to push these calculations down to $n = 69$. The largest primes dividing M and N are 787 and 829 respectively. There are a total of 60 primes in our list requiring one or the other of these. Thus, our list would drop to 1182 primes if these were deleted. Since $\log_2 \phi(MN)$ would only drop to 1221, there would be a large gap to make up. We appeared to be getting diminishing returns from increasing the multiplicity of the smaller primes, so it is doubtful that this gap could be bridged.

6. CONCLUSIONS

To date, the \$620 appears to be safe. Unless an efficient scheme to search a space of size 2^{1500} is found, or an approach other than that suggested by Pomerance can be found, the problem of constructing a counterexample appears to be intractable. It should be mentioned that Pomerance has indicated a willingness to pay his share even for an existence proof [4]. There might be more hope here. For example, suppose we have an M, N, P. Let A be a subset of P, and let U be the set of all subset products of elements of A modulo MN. Given a prime $p \in P - A$, we might ask how big a set of subset products for $A \cup \{p\}$ is. Giving pU the obvious meaning, this set will clearly be $U \cup pU$ and since $|U| = |PU|$, $|U \cup pU| = 2|U| - |U \cap pU|$. If $x \in U \cap pU$, then for some sets of primes, $x = p_1 p_2 \ldots p_k \equiv p q_1 q_2 \ldots q_j$, with the p's and q's from A. This can only happen if $p \equiv p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1}$. Thus, if we can choose p so as to avoid the set

$$\{p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1} (\text{mod } MN) : p\text{'s and } q\text{'s are in } A\},$$

then $|U \cup pU| = 2|U|$. Obviously, we cannot pick p to meet this condition forever. If $|U| > \frac{1}{2}\phi(MN)$, there will be a representation $p \equiv p_1 p_2 \ldots p_k q_1^{-1} q_2^{-1} \ldots q_j^{-1}$. If the number of such representations of p is small, the intersection of U and pU will also be small. Thus, one might have a chance of proving that all reduced residue classes are covered at some stage.

If for some M and N, $|P|$ is much larger than $\log_2 \phi(MN)$, perhaps there is a way to exploit this size difference as well. For example, the authors would be interested in a proof or counterexample to the following claim:

Claim: Let m and n be relatively prime integers. Let A and B be disjoint sets of primes, with no prime dividing mn. Suppose that for each reduced residue class x of m and y of n there are nonempty subsets S, T of A and U, V of B such that

$$f(S) \equiv x (\text{mod } m) \text{ and } f(U) \equiv x (\text{mod } m),$$

$$f(T) \equiv y (\text{mod } n) \text{ and } f(V) \equiv y (\text{mod } n).$$

Then for each reduced residue class z of mn, there is a subset W of $A \cup B$ such that $f(W) \equiv z (\text{mod } mn)$.

The authors have not experimented with the claim enough to actually submit it as a conjecture. However, if such a claim were true, then it might be possible to use the prime factorization of MN to show that P covers all reduced residue classes of MN. This approach is wasteful of primes in P so the authors are currently calculating primes for the case $n = 100$, with the same M_{start} and N_{start} that were used for $n = 70$. This should give a very large set P compared to $\log_2 \phi(MN)$. As of this writing, the set P has 4838 primes, with $\log_2 \phi(MN) \cong 1838$. We estimate that $|P|$ may get as large as 5500. Various sets of primes we have found are available on the second author's web site, www.d.umn.edu/~jgreene.

REFERENCES

[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford University Press, New York, 1979.

[2] C. Pomerance, J.L. Selfridge, and S.S. Wagstaff, Jr. "The Pseudoprimes to $25 \cdot 10^9$." *Math. Comp.* **35** (1980): 1003-1026.

[3] C. Pomerance. "Are There Counter-Examples to the Baillie-PSW Primality Test?" Unpublished manuscript.

[4] C. Pomerance, private communication.

[5] P. Ribenboim. *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.

[6] H. Riesel. *Prime Numbers and Computer Methods for Factorization*, Second Edition, Birkhauser, Boston, 1994.

AMS Classification Numbers: 11N25, 11A07, 11B39

✠ ✠ ✠