THE PSEUDOPRIMES UP TO 10^{12}

R.G.E. Pinch

Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge

8 September 1992

Abstract. There are 38975 Fermat pseudoprimes (base 2) up to 10^{11} and 101629 up to 10^{12}: we describe the calculations and give some statistics. The numbers were generated by a variety of strategies, the most important being a back-tracking search for possible prime factorisations, and the computations checked by searching selected ranges of integers directly using a sieving technique.

0. Introduction.

A *(Fermat) pseudoprime (base 2)* is a composite number N with the property that $2^{N-1} \equiv 1 \mod N$.

For background on pseudoprimes and primality tests in general we refer to Koblitz [2], Ribenboim [9] and [10] or Riesel [11]. Previous tables of pseudoprimes were computed by Pomerance, Selfridge and Wagstaff [5].

We have shown that there are 38975 pseudoprimes up to 10^{11}, and 101629 up to 10^{12}; all have at most 8 prime factors. Let $P(X)$ denote the number of pseudoprimes less than X and let $P(d, X)$ denote the number with exactly d prime factors. In Table 1 we give the values of $P(X)$ and $P(d, X)$ for $d \leq 8$ and X in powers of 10 up to 10^{12}.

The pseudoprimes were generated by a variety of strategies, the most important being a back-tracking search for possible prime factorisations, and the computations checked by searching selected ranges of integers directly using a sieving technique, together with a "large prime variation".

We also used the same methods to calculate the smallest pseudoprimes with d prime factors for d up to 16. The results are given in Table 2.

1. Some properties of pseudoprimes.

In this section we discuss some elementary properties of pseudoprimes.

For any odd m we let $f(m)$ denote the multiplicative order of 2 modulo m, that is, the least power $f \geq 1$ such that $2^f \equiv 1 \mod m$. If $m = \prod_i p_i^{a_i}$ then $f(m) = \operatorname{lcm}\{f(p_i^{a_i})\}$. Clearly N is a pseudoprime if and only if $f(N)$ divides $N-1$. Further define $w(p)$ to be the largest exponent such that $p^w \mid 2^{p-1} - 1$.

Proposition 1. *Fix an odd prime p and put $f = f(p)$, $w = w(p)$. If $a \leq w$ then $f(p^a) = f$. If $a \geq w$ then $f(p^a) = p^{a-w} f$.*

Proof. The multiplicative group modulo p^a is cyclic of order $p^{a-1}(p-1)$, and reduction modulo p maps this group onto the multiplicative group modulo p, which is cyclic of order $p-1$. We conclude that $f \mid f(p^a)$, and further that the quotient $f(p^a)/f$ is a power of p.

Clearly if $a \leq w$ then $2^{p^a} \equiv (2^p)^{p^{a-1}} \equiv 2^{p^{a-1}} \equiv \ldots \equiv 2 \mod p^a$, so $f(p^a) = f$.

We now claim that for $a \geq w$,

$$2^{p^{a-w} f} = 1 + p^a X_a$$

where X_a is an integer with $X_a \equiv X_w \mod p$. Since X_w is prime to p by definition of w, X_a is prime to p. It follows immediately that the power of p dividing $f(p^a)$ is p^{a-w} and this will complete the proof of the Proposition.

1991 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A51.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

We proceed by induction. The case $a = w$ is immediate. Suppose now that $a \geq w$ and

$$2^{p^{a-w}f} = 1 + p^a X_a$$

with X_a an integer, $X_a \equiv X_w \mod p$. We have

$$2^{p^{a+1-w}f} = (1 + p^a X_a)^p = 1 + p^{a+1} X_a + R$$

where R denotes the sum of the remaining terms of the binomial expansion. Since p divides the binomial coefficient $\binom{p}{r}$ for $1 \leq r \leq p-1$, we see that the power of p dividing the term $\binom{p}{r}(p^a X_a)^r$ in R is at least p^{1+ar} for $1 \leq r \leq p-1$ and at least p^{ap} for the final term. Now $p \geq 3$, so every term in R is divisible by p^{1+2a}. Now $a \geq w \geq 1$, so $1 + 2a \geq a + 2$, and $p^{a+2} \mid R$; hence

$$2^{p^{a+1-w}f} = 1 + p^{a+1} X_{a+1}$$

where $X_{a+1} \equiv X_a \mod p$. This completes the induction step and the claim is proved. □

We note that if p^a divides a pseudoprime N then $f(p^a)$ must divide $N-1$ and so be prime to p. Hence we must have $w(p) \geq a$ and consequently p^a is itself a pseudoprime.

In practice it seems rare to have $w(p) > 1$. We shall return to this point in section 6.

2. Organisation of the search.

We assume throughout that we are searching for pseudoprimes less than some bound X: in our computations we took $X = 10^{12}$.

Proposition 2. *Let N be a pseudoprime less than X with exactly d prime factors $p_1 \leq \cdots \leq p_d$.*

1. *For each i, $f(p_i) \mid N - 1$.*
2. *Each p_i satisfies $N \equiv p_i \mod p_i f(p_i)$ and $p_i f(p_i) < X$.*
3. *For $r < d$ put $P_r = \prod_{i=1}^{r} p_i$. Then $p_{r+1} < (X/P_r)^{1/(d-r)}$ and p_{r+1} is prime to $f(p_i)$ for all $i \leq r$.*

Proof. Part (1) follows immediately from the condition $2^{N-1} \equiv 1 \mod p_i$.

Since $f(p_i) \mid p_i - 1$, we have $N \equiv 1 \equiv p_i \mod f(p_i)$, $N \equiv p_i \mod p_i$ and p_i prime to $f(p_i)$, so (2) follows.

The p_i are in increasing order so the inequality in (3) is trivial. Since $f(N) \mid N - 1$, we have $f(N)$ prime to N; but $f(p_i) \mid f(N)$ and $p_i \mid N$, so the remainder of (3) follows. □

We consider three classes of pseudoprimes and adopt a different strategy for each. For pseudoprimes with a repeated prime factor we use the strategy of section 6 and for square-free pseudoprimes with a prime factor greater then $X/1000$ we use the strategy of section 5. The remaining class of square-free pseudoprimes is the most numerous and here we apply the main strategy, consisting of a precomputation and the main search, described in the next two sections.

3. The precomputation.

The main strategy is considerably improved by a precomputation, which is also proves to be of value in the sieving methods of section 7. Let $\mathcal{A}[F,Y]$ denote the set of primes $q \leq Y$ for which $f(q) \leq F$, and let $\mathcal{B}[X]$ denote the set of primes q for which $qf(q) \leq X$. By Proposition 2(2), the prime factors of the pseudoprimes up to X are all elements of $\mathcal{B}[X]$.

We initially obtained the list $\mathcal{A}[1000,\infty]$ from the list of factors of numbers of the form $2^f - 1$ with $f \leq 1000$ in Brillhart et al [1] (the "Cunningham tables"). We obtain other lists $\mathcal{A}[F,Y]$ in two parts. For values of f less than 1000, we take the values of $q \leq Y$ from the list $\mathcal{A}[1000,\infty]$. For values of f between 1000 and F, we proceed as follows. For each f, let q run over all integers $\equiv 1 \mod f$ for which $2^f \equiv 1 \mod q$. The values of q which are prime are then added to the list, the correct order of 2 modulo q being obtained by considering the values of $2^e \bmod q$ for e dividing f. We obtain the list $\mathcal{B}[X]$ from a union of suitable $\mathcal{A}[F,Y]$.

The dominant term in the time taken to perform the precomputation is the time taken to run form the list of q with $q \equiv 1 \mod f$ and to compute $2^f \bmod q$, namely

$$\sum_{f=1000}^{F} \left\lceil \frac{Y}{f} \right\rceil \log f \sim \int_{1000}^{F} \frac{Y}{f} \log f \mathrm{d}f = \left[\tfrac{1}{2} Y (\log f)^2\right]_{1000}^{F} \sim \tfrac{1}{2} Y \left[(\log F)^2 - 47.71\right].$$

Taking $F = 10^4$, $Y = 10^9$ gives about $1.9 \cdot 10^{10}$ elementary operations; taking $F = 10^5$, $Y = 10^8$ gives about $8.5 \cdot 10^9$ operations. We computed the order of 2 for primes up to 10^7 directly. We find that $\mathcal{A}\left[10^4, 10^9\right]$ has 9131 elements; $\mathcal{A}\left[10^5, 10^8\right]$ has 59280; $\mathcal{A}\left[10^6, 10^7\right]$ has 44296; and $\mathcal{A}\left[10^6, 10^8\right]$ has 375615. From the Cunningham tables, list $\mathcal{A}\left[1000, \infty\right]$ has 4000 elements, the largest being

$$267823007376498379256993682056860433753700498963798805883563.$$

In total, $\mathcal{B}\left[10^{12}\right]$ has 145270 elements.

4. The main strategy.

Assume throughout that N is a pseudoprime, less than the pre-assigned bound X and with exactly d prime factors, all distinct and less than $X/1000$. We obtain all such N as lists of prime factors $p_1, \ldots, p_d$ by a back-tracking search. For suitable choices of F and Y we make use of the precomputed lists $\mathcal{A}\left[F, Y\right]$.

We produce successive lists of $p_1, \ldots, p_{d-1}$ recursively, looping at each search level over all the primes permitted by Proposition 2(3).

At search level $d-1$ put $P = \prod_{i=1}^{d-1} p_i$ and $L = f(P) = \operatorname{lcm}\{f_1, \ldots, f_{d-1}\}$. We look for primes q such that $N = Pq$ is a pseudoprime; that is, we require $2^{Pq-1} \equiv 1 \mod q$ and $2^{Pq-1} \equiv 1 \mod P$. The first condition is equivalent to $Pq \equiv 1 \mod f(q)$ and the second to $Pq \equiv 1 \mod L$. But $q \equiv 1 \mod f(q)$, so we require $f(q) \mid P - 1$ and $Pq \equiv 1 \mod L$. We consider the possible q with $f(q) = q$ in two ways.

For every factor f of $P - 1$ which satisfies $f \leq F$, we let q run over the primes from $\mathcal{A}\left[F, Y\right]$ for which $q \leq X/P$ and $f(q) = f$. If $Pq \equiv 1 \mod L$ then $N = Pq$ is a pseudoprime.

For factors f of $P - 1$ with $f > F$, or for values of q greater than X/P, we let q run over the integers satisfying $P \equiv 1 \mod f$ and $f(q) = f$. These conditions imply that $Pq \equiv 1 \mod f$ and $Pq \equiv 1 \mod L$, so it is sufficient to run over the q satisfying $Pq \equiv 1 \mod \operatorname{lcm}\{f, L\}$. If q is prime and $2^f \equiv 1 \mod q$ then $N = Pq$ is a pseudoprime.

We observe that small f are likely to occur often as factors of the $P - 1$ and so the precomputation of the $\mathcal{A}\left[F, Y\right]$ gives a considerable saving in this final stage.

We note that testing candidates for p_i for primality is required at every stage of the calculation. We found that using a table of primes up to a suitable limit produced a considerable saving in time.

Applying the main search with $X = 10^{12}$ we used $\mathcal{A}\left[10^4, 10^9\right]$ as the auxiliary list of primes.

5. Pseudoprimes with a large factor.

Suppose that $N = Pq$ is a square-free pseudoprime less than X with a prime factor q greater than $X/1000$; so we are assuming that $P < 1000$. We have $f(q) \mid P - 1$, so $f(q) < 1000$, that is $q \mid 2^f - 1$ for some $f < 1000$. We use the list $\mathcal{A}\left[1000, \infty\right]$ of primes dividing such numbers described in section 3. For each q in this list, and for each $P < X/q$ with $P \equiv 1 \mod f(q)$, we test whether $2^{Pq} \equiv 2 \mod P$: if so, then $N = Pq$ is a pseudoprime. There are 9 pseudoprimes up to 10^{12} with a prime factor greater than 10^9.

6. Pseudoprimes with a repeated prime factor.

Suppose now that N is a pseudoprime divisible by a repeated prime factor p^r with $r \geq 2$.

Lehmer [3] has shown that the only primes $p < 6.10^9$ satisfying this condition are $p = 1093$ and $p = 3511$, each in case with $w(p) = 2$. Since we require $p^2 < 10^{12}$, we restrict our attention to these two values of p. (In fact it is easy to check that these are the only two such p up to 10^6.) We have $f(1093^2) = 364$ and $f(3511^2) = 1755$. For each value of p we consider numbers $Q \equiv 1 \mod f(p^2)$ such that $N = p^2 Q \leq X$ and for each such N test directly whether $2^N \equiv 2 \mod N$.

We took $X = 10^{13}$. The resulting pseudoprimes are given in Table 3. There are 23 pseudoprimes up to 10^{12} with a repeated factor and 54 up to 10^{13}.

7. Checking ranges by sieving.

We used a sieving technique to verify that the list of pseudoprimes produced by the method of section 2 was complete in certain ranges.

Suppose that we wish to list those pseudoprimes in a range up to X which are divisible only by primes in some list $\mathcal{L}$ of primes, say all less than Y. Clearly we may assume that $Y \leq X$. We form a table indexed by the integers up to X and initially set each entry in the table to zero. For each p in $\mathcal{L}$ we add $\log p$ into the table entries corresponding to numbers t with $t \equiv 0 \mod p$ and $t \equiv 1 \mod f(p)$: that is, $t \equiv p \mod pf(p)$. At the end of this process we output any N for which the corresponding table entry is equal to $\log N$. Such an N has the property that all the prime factors p of N are in $\mathcal{L}$ and that $N \equiv 1 \mod f(p)$ for every p dividing N: that is, N is a pseudoprime whose prime factors are all in $\mathcal{L}$.

From Proposition 2(2) we note that taking $\mathcal{L} = \mathcal{B}[X]$ in the sieve will give all the pseudoprimes up to X.

To estimate the time taken to sieve over a range we need the following result.

Proposition 3. *Fix an integer b and let $f(p)$ denote the order of b in the multiplicative group modulo p for b prime to p. The sum, taken over primes p not dividing b,*

$$\sum_p \frac{1}{pf(p)}$$

is convergent.

Proof. Since the terms in the series are positive, the sum is convergent if any re-arrangement of it is convergent. Write

$$\sum_p \frac{1}{pf(p)} = \sum_f \frac{1}{f} \sum_{f(p)=f} \frac{1}{p}.$$

If b has order f modulo p, then p divides $b^f - 1$ and $p \equiv 1 \mod f$. Let p_i denote the k, say, distinct prime factors of $b^f - 1$ which satisfy $p_i > b$ and $p_i \equiv 1 \bmod f$: the p_i will include all the primes $p > b$ with $f(p) = f$. We have $k < f$ since all $p_i > b$, and $p_i \geq 1 + if$. So

$$\sum_{\substack{f(p)=f \\ p>b}} \frac{1}{p} \leq \sum_{i=1}^{k} \frac{1}{p_i} < \sum_{i=1}^{f} \frac{1}{if} < \frac{1}{f}(1 + \log f).$$

Hence

$$\sum_{p>b} \frac{1}{pf(p)} < \sum_f \frac{1 + \log f}{f^2}$$

and the latter sum is convergent. $\square$

We shall use this result with $b = 2$. In this case the numerical value of the sum, computed over the primes p up to 10^7, is approximately 0.40067.

The time taken to sieve over all the numbers up to X will be bounded by

$$X + \sum_{p \in \mathcal{L}} \left\lceil \frac{X}{pf(p)} \right\rceil \leq X + X \sum_p \frac{1}{pf(p)} + \pi(Y) = \mathrm{O}(X),$$

which is an improvement over a direct search for pseudoprimes: testing the condition $2^{N-1} \equiv 1 \mod N$ for all N up to X would already take time $\mathrm{O}(X \log X)$.

In practice, we found that the contribution of order $\pi(Y)$ from considering elements p of $\mathcal{L}$ for which there are few or no multiples of $pf(p)$ in the range outweighs the contribution of order X from scanning the table and so it is beneficial to reduce the size of the list $\mathcal{L}$ as much as possible.

We therefore consider a "large prime variation". After sieving with $\mathcal{L}$ the list of primes up to some limit Y, we use a further technique to deal with those pseudoprimes which have a prime factor q greater than Y. For each prime $q > Y$ in $\mathcal{B}[X]$, we consider all numbers P up to X/q which are $\equiv 1 \mod f(q)$. The procedure now follows that of section 5. For each such P we test whether $2^{Pq} \equiv 2 \mod P$. If so, $N = Pq$ is a pseudoprime.

8. Comparison with existing tables.

We have checked our tables against those of Pomerance, Selfridge and Wagstaff [5], who obtained the 21853 pseudoprimes up to 25.10^9. We extracted the Carmichael numbers from our tables and compared them against the tables of [4]. In each case there was no discrepancy.

9. Some details of the calculations.

We ran the search procedure of the main strategy, sections 3 and 4, with upper limits of $X = 10^n$ for each value of n up to 12 and each value of d up to 8 independently. As a consequence the list of pseudoprimes up to 10^{11} was in effect computed twice, that up to 10^{10} three times and so on, providing additional checks on the computations. The computer programs were written in C and run on Sun 3/60 and Sparc workstations. The restriction of the search to prime factors less than $X/1000$, that is, less than 10^9, meant that 32-bit integer arithmetic could be used throughout. As a check, both on the programs and the results, some of the runs, including all those up to 10^{12}, were duplicated using the rather strict Norcroft C compiler on an IBM 3084 mainframe. A total of about 200 hours of CPU time was required. All the results were consistent.

The methods of sections 5 and 6 were implemented using Pari/GP on a Sparc workstation. Less than an hour was required for this part of the computation.

We used the sieving process of section 7 to check the search process up to 10^{12}: this was the most expensive part of the computation, requiring about 300 hours of CPU time on an IBM 3084. The results were consistent with those obtained by the methods of sections 2 and 3.

As a further check, we ran the "large prime variation" for pseudoprimes up to 10^{12} with a prime factor q in $\mathcal{B}\left[10^{12}\right]$ with $q > 10^7$: there are 39463 such primes. The lists matched those found by the search process: there were 3145 such pseudoprimes up to 10^{12}.

10. Statistics.

Let $P(X)$ denote the number of pseudoprimes less than X, and $P(d,X)$ denote the number which have exactly d prime factors. In Table 1 we give $P(d,X)$ and $P(X)$ for values of X up to 10^{12}. No pseudoprime in this range has more than 8 prime factors. We have $P\left(10^{12}\right) = 101629$.

In Table 2 we give the smallest pseudoprime with d prime factors for d up to 17.

In Table 4 we give the number of pseudoprimes in each class modulo m for m up to 12.

In Tables 5 and 6 we give the number of pseudoprimes divisible by primes p up to 97. In Table 5 we count all pseudoprimes divisible by p: in Table 6 we count only those for which p is the smallest prime factor.

The largest prime factor of a pseudoprime up to 10^{12} is 8831418697, dividing

$$733007751851 = 83 \cdot 8831418697$$

and the largest prime to occur as the smallest prime factor of a pseudoprime in this range is 964897, dividing

$$969818939597 = 964897 \cdot 1005101.$$

Define $\alpha(x)$ by $P(x) = \exp(\log(x)^\alpha)$ and $\beta(x)$ by $P(x) = x\ell(x)^{-\beta}$, where

$$\ell(x) = \exp\left(\frac{\log x \log\log\log x}{\log\log x}\right).$$

Pomerance [6,7,8] showed that $\alpha \geq 85/207 > 0.4106$ and $\beta \geq \frac{1}{2}$ for x sufficiently large: he conjectured that β tends to 1. Clearly if β is even bounded then α tends to 1.

In Table 8 we tabulate the values of α and β for various values of x up to 10^{12}. We see that α is increasing over the range, but β is not obviously converging.

Define an odd composite integer N to be an *Euler pseudoprime* if

$$2^{(N-1)/2} \equiv \left(\frac{2}{N}\right)$$

where $\left(\frac{2}{N}\right)$ is the Jacobi symbol. We further define N to be a *strong*, or *Miller–Rabin pseudoprime* if it passes the following test. Put $N - 1 = 2^a b$ with b odd, and form the sequence $2^b, 2^{2b}, \ldots, 2^{2^a b} = 2^{N-1}$

modulo N. The test is passed if either the first term is $1 \bmod N$ or there are two consecutive terms $-1 \bmod N$, $1 \bmod N$ in the sequence. We define a *Carmichael number* to be a composite N for which $a^{N-1} \equiv 1 \mod N$ for any a prime to N.

It is clear that if N is an Euler pseudoprime or a strong pseudoprime then it is also a pesudoprime in the sense we have been using. (It is in fact also true that if N is a strong pseudoprime then it is also an Euler pseudoprime.) Since every Carmichael number is odd, it is again also a pseudoprime.

We can therefore tabulate the Euler pseudoprimes and strong pseudoprimes by extracting them from the tables of pseudoprimes. The Carmichael numbers in this range have already been tabulated in [?]. In Table 9 we give the numbers $EP(x)$, $SP(x)$ and $C(x)$ of Euler pseudoprimes, strong pseudoprimes and Carmichael numbers up to x for various values of x up to 10^{12}.

11. Even pseudoprimes.

The condition $2^{N-1} \equiv 1 \mod N$ implies that N is odd. If we replace this condition by the closely related $2^N \equiv 2 \mod N$ then it is possible for N to be even: for example, $N = 161038 = 2 \cdot 73 \cdot 1103$. Let us call such a number an *even pseudoprime*. It is easy to see that such an N satisfies $N = 2R$ with R odd and the condition becomes $2^{2R-1} \equiv 1 \mod R$. It is then necessary that $f(R) \mid 2R-1$, so $f(R)$ must be odd. Of the 145270 primes in $\mathcal{B}\left[10^{12}\right]$, 51607 have an odd value of f and so are candidates for being an odd prime factor of an even pseudoprime.

We adapted the methods of the previous sections to use this restricted set of possible prime factors and modified condition on N. There are only 40 even pseudoprimes up to 10^{10}: they are listed in Table 7.

12. Acknowledgements.

The author is grateful to Prof. S.S. Wagstaff jr for providing files containing the tables described in [1] and [5]; to Dr R. Heath-Brown for discussions on Proposition 3; and to Prof. H. te Riele for discussions on even pseudoprimes.

References

1. J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckermann and S.S. Wagstaff jr, *Factorizations of* $b^n \pm 1$ *(2nd ed)*, American Mathematical Society, Providence, R.I., 1988.
2. N. Koblitz, *A course in number theory and cryptography*, Springer, New York, 1987.
3. D.H. Lehmer, *On Fermat's quotient, base two*, Math. Comp. **36** (1981), 289–290.
4. R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Preprint (1992).
5. C. Pomerance, J.L. Selfridge and S.S. Wagstaff jr, *The pseudoprimes to* 25.10^9, Math. Comp. **35** (1980), 1003–1026.
6. C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
7. C. Pomerance, *A new lower bound for the pseudoprime counting function*, Illinois J. Maths **26** (1982), 4–9.
8. C. Pomerance, *Two methods in elementary analytic number theory*, Number theory and its applications (ed R.A. Mollin), Kluwer, Dordrecht, 1989.
9. P. Ribenboim, *The book of prime number records*, Springer, New York, 1988.
10. ______, *The little book of big primes*, Springer, New York, 1991.
11. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhauser, Boston, Mass., 1985.

	d								
X	1	2	3	4	5	6	7	8	$P(X)$
10^3	0	1	2	0	0	0	0	0	3
10^4	0	11	11	0	0	0	0	0	22
10^5	0	34	34	10	0	0	0	0	78
10^6	0	107	89	48	1	0	0	0	245
10^7	1	311	229	189	20	0	0	0	750
10^8	2	880	485	563	124	3	0	0	2057
10^9	2	2455	1105	1417	563	54	1	0	5597
10^{10}	2	6501	2391	3435	2133	405	13	0	14884
25.10^9	2	9581	3146	4842	3454	786	42	0	21853
10^{11}	2	17207	4886	7909	6845	1966	156	4	38975
10^{12}	2	46080	9949	17087	19132	8196	1146	37	101629

TABLE 1. THE NUMBER OF PSEUDOPRIMES WITH d DISTINCT PRIME FACTORS UP TO 10^{12}

d		N / factors
2		341 $11 \cdot 31$
3	**C**	561 $3 \cdot 11 \cdot 17$
4		11305 $5 \cdot 7 \cdot 17 \cdot 19$
5	**C**	825265 $5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$
6		45593065 $5 \cdot 7 \cdot 17 \cdot 19 \cdot 37 \cdot 109$
7		370851481 $7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37$
8		38504389105 $5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73 \cdot 97$
9		7550611589521 $7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 41 \cdot 59 \cdot 61 \cdot 97$
10		277960972890601 $7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 101 \cdot 181$
11		32918038719446881 $7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 47 \cdot 73 \cdot 631$
12		1730865304568301265 $5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 37 \cdot 59 \cdot 67 \cdot 73 \cdot 199 \cdot 241$
13		606395069520916762801 $11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 41 \cdot 43 \cdot 61 \cdot 73 \cdot 97 \cdot 127 \cdot 151$
14		59989606772480422038001 $7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 97 \cdot 151 \cdot 241 \cdot 251$
15		6149883077429715389052001 $11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 73 \cdot 97 \cdot 113 \cdot 181 \cdot 257$
16		540513705778955131306570201 $11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 71 \cdot 73 \cdot 109 \cdot 113 \cdot 127 \cdot 151 \cdot 163$
17	**C**	35237869211718889547310642241 $13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71 \cdot 73 \cdot 97 \cdot 113 \cdot 127 \cdot 211$

TABLE 2. THE SMALLEST PSEUDOPRIMES WITH d PRIME FACTORS, $2 \le d \le 17$. **C** DENOTES A CARMICHAEL NUMBER.

N	factors
1194649	1093^2
12327121	3511^2
3914864773	$29 \cdot 113 \cdot 1093^2$
5654273717	$1093^2 \cdot 4733$
6523978189	$43 \cdot 127 \cdot 1093^2$
22178658685	$5 \cdot 47 \cdot 79 \cdot 1093^2$
26092328809	$1093^2 \cdot 21841$
31310555641	$1093^2 \cdot 26209$
41747009305	$5 \cdot 29 \cdot 241 \cdot 1093^2$
53053167441	$3 \cdot 113 \cdot 131 \cdot 1093^2$
58706246509	$157 \cdot 313 \cdot 1093^2$
74795779241	$137 \cdot 457 \cdot 1093^2$
85667085141	$3 \cdot 11 \cdot 41 \cdot 53 \cdot 1093^2$
129816911251	$3511^2 \cdot 10531$
237865367741	$1093^2 \cdot 199109$
259621495381	$3511^2 \cdot 21061$
333967711897	$1093^2 \cdot 279553$
346157884801	$3511^2 \cdot 28081$
467032496113	$313 \cdot 1093^2 \cdot 1249$
575310702877	$337 \cdot 1093^2 \cdot 1429$
601401837037	$1093^2 \cdot 503413$
605767053061	$157 \cdot 313 \cdot 3511^2$
962329192917	$3 \cdot 29 \cdot 47 \cdot 197 \cdot 1093^2$

TABLE 3A. THE 23 PSEUDOPRIMES WITH REPEATED FACTOR UP TO 10^{12}.

N	factors
1087566636885	$3 \cdot 5 \cdot 137 \cdot 443 \cdot 1093^2$
1101047056201	$29 \cdot 61 \cdot 521 \cdot 1093^2$
1122789668001	$3 \cdot 23 \cdot 53 \cdot 257 \cdot 1093^2$
1492414068601	$73 \cdot 109 \cdot 157 \cdot 1093^2$
1629827375177	$53 \cdot 1093^2 \cdot 25741$
1784634771193	$547 \cdot 1093^2 \cdot 2731$
2046850669501	$11 \cdot 29 \cdot 41 \cdot 131 \cdot 1093^2$
2063809906705	$5 \cdot 73 \cdot 1093^2 \cdot 4733$
2179915453717	$911 \cdot 1093^2 \cdot 2003$
2327330361721	$1093^2 \cdot 1948129$
2854371271753	$1093^2 \cdot 2389297$
2897421643117	$53 \cdot 67 \cdot 683 \cdot 1093^2$
2972216227709	$911 \cdot 1093^2 \cdot 2731$
3427506518801	$53 \cdot 1093^2 \cdot 54133$
3950198906473	$157 \cdot 1093^2 \cdot 21061$
4026732900009	$3 \cdot 17 \cdot 29 \cdot 43 \cdot 53 \cdot 1093^2$
4081524281745	$3 \cdot 5 \cdot 239 \cdot 953 \cdot 1093^2$
4556817775693	$53 \cdot 79 \cdot 911 \cdot 1093^2$
4662486869041	$17 \cdot 19 \cdot 43 \cdot 281 \cdot 1093^2$
5072117675353	$79 \cdot 223 \cdot 241 \cdot 1093^2$
5352597367573	$547 \cdot 1093^2 \cdot 8191$
5993134711201	$11 \cdot 17 \cdot 139 \cdot 193 \cdot 1093^2$
5999657494741	$79 \cdot 151 \cdot 421 \cdot 1093^2$
6151420925105	$5 \cdot 137 \cdot 1093^2 \cdot 7517$
6317168754781	$31 \cdot 61 \cdot 271 \cdot 3511^2$
6537569710673	$911 \cdot 1093^2 \cdot 6007$
6922923480721	$433 \cdot 1297 \cdot 3511^2$
6984597809281	$31 \cdot 151 \cdot 1093^2 \cdot 1249$
7793422968241	$31 \cdot 127 \cdot 1093^2 \cdot 1657$
7816904988985	$5 \cdot 37 \cdot 113 \cdot 313 \cdot 1093^2$
8914472032649	$911 \cdot 1093^2 \cdot 8191$

Table 3b. The 31 pseudoprimes with repeated factor between 10^{12} and 10^{13}.

m	c	25.10^9	10^{11}	10^{12}
3	0	628	1042	2251
	1	18413	33001	86672
	2	2812	4932	12706
4	1	19269	34556	90317
	3	2584	4419	11312
5	0	1474	2485	5695
	1	12721	22936	61119
	2	2743	4824	12643
	3	2685	4768	12198
	4	2230	3962	9974
7	0	2025	3476	8546
	1	8730	15868	42605
	2	2049	3605	9407
	3	2491	4387	11111
	4	2039	3567	9178
	5	2258	4030	10315
	6	2261	4042	10467
8	1	12654	22911	60415
	3	1295	2180	5646
	5	6615	11645	29902
	7	1289	2239	5666
9	1	11395	20644	54852
	2	935	1649	4287
	3	318	526	1117
	4	3513	6148	15833
	5	937	1634	4197
	6	310	516	1134
	7	3505	6209	15987
	8	940	1649	4222
11	0	1690	2930	7610
	1	5314	9763	26416
	2	1572	2773	7186
	3	1554	2740	7090
	4	1603	2739	7084
	5	1776	3125	7806
	6	1593	2886	7530
	7	1709	3004	7667
	8	1774	3114	8049
	9	1428	2600	6727
	10	1840	3301	8464
12	1	16281	29360	77269
	3	29	48	90
	5	2389	4202	10887
	7	2132	3641	9403
	9	599	994	2161
	11	423	730	1819

TABLE 4. THE NUMBER OF PSEUDOPRIMES CONGRUENT TO c MODULO m

p	25.10^9	10^{11}	10^{12}
3	628	1042	2251
5	1474	2485	5695
7	2025	3476	8546
11	1690	2930	7610
13	2270	3997	9974
17	1756	3018	7708
19	1530	2725	7129
23	671	1189	3137
29	954	1717	4492
31	1575	2783	7138
37	1267	2286	5972
41	1269	2238	5931
43	930	1641	4296
47	254	429	1091
53	400	707	1878
59	145	246	631
61	1007	1824	4897
67	486	830	2156
71	501	907	2502
73	1104	1990	5069
79	307	558	1432
83	82	143	355
89	434	783	2098
97	653	1147	2988

Table 5. The number of times a prime $p \leq 97$ occurs in a pseudoprime

p	25.10^9	10^{11}	10^{12}
3	628	1042	2251
5	1340	2278	5278
7	1763	3044	7586
11	1260	2203	5850
13	1149	2147	5624
17	654	1152	3100
19	619	1099	2929
23	272	475	1277
29	345	628	1638
31	551	966	2406
37	301	531	1354
41	237	444	1224
43	257	446	1081
47	61	94	235
53	102	181	434
59	46	75	156
61	162	282	770
67	103	171	433
71	119	191	506
73	135	246	614
79	76	131	304
83	34	50	94
89	68	130	282
97	105	179	389

Table 6. The number of times a prime $p \leq 97$ occurs as the least prime factor of a pseudoprime

N	factors
161038	$2 \cdot 73 \cdot 1103$
215326	$2 \cdot 23 \cdot 31 \cdot 151$
2568226	$2 \cdot 23 \cdot 31 \cdot 1801$
3020626	$2 \cdot 7 \cdot 359 \cdot 601$
7866046	$2 \cdot 23 \cdot 271 \cdot 631$
9115426	$2 \cdot 31 \cdot 233 \cdot 631$
49699666	$2 \cdot 311 \cdot 79903$
143742226	$2 \cdot 23 \cdot 31 \cdot 100801$
161292286	$2 \cdot 127 \cdot 199 \cdot 3191$
196116194	$2 \cdot 127 \cdot 599 \cdot 1289$
209665666	$2 \cdot 7 \cdot 89 \cdot 191 \cdot 881$
213388066	$2 \cdot 23 \cdot 31 \cdot 151 \cdot 991$
293974066	$2 \cdot 73 \cdot 631 \cdot 3191$
336408382	$2 \cdot 73 \cdot 1103 \cdot 2089$
377994926	$2 \cdot 23 \cdot 89 \cdot 127 \cdot 727$
410857426	$2 \cdot 7 \cdot 191 \cdot 153649$
665387746	$2 \cdot 23 \cdot 3463 \cdot 4177$
667363522	$2 \cdot 7 \cdot 5471 \cdot 8713$
672655726	$2 \cdot 73 \cdot 1103 \cdot 4177$
760569694	$2 \cdot 1319 \cdot 288313$
1066079026	$2 \cdot 23 \cdot 31 \cdot 151 \cdot 4951$
1105826338	$2 \cdot 23 \cdot 73 \cdot 127 \cdot 2593$
1423998226	$2 \cdot 7 \cdot 79 \cdot 271 \cdot 4751$
1451887438	$2 \cdot 79 \cdot 89 \cdot 223 \cdot 463$
1610063326	$2 \cdot 73 \cdot 2089 \cdot 5279$
2001038066	$2 \cdot 47 \cdot 311 \cdot 68449$
2138882626	$2 \cdot 73 \cdot 3191 \cdot 4591$
2952654706	$2 \cdot 31 \cdot 71 \cdot 631 \cdot 1063$
3220041826	$2 \cdot 73 \cdot 103 \cdot 233 \cdot 919$
3434672242	$2 \cdot 727 \cdot 911 \cdot 2593$
4338249646	$2 \cdot 4721 \cdot 459463$
4783964626	$2 \cdot 7 \cdot 23 \cdot 73 \cdot 271 \cdot 751$
5269424734	$2 \cdot 7 \cdot 1433 \cdot 262657$
5820708466	$2 \cdot 79 \cdot 3257 \cdot 11311$
6182224786	$2 \cdot 23 \cdot 31 \cdot 151 \cdot 28711$
6381449614	$2 \cdot 73 \cdot 199 \cdot 239 \cdot 919$
8356926046	$2 \cdot 7 \cdot 79 \cdot 7555991$
8419609486	$2 \cdot 31 \cdot 2441 \cdot 55633$
9548385826	$2 \cdot 7 \cdot 31 \cdot 89 \cdot 247201$
9895191538	$2 \cdot 127 \cdot 1289 \cdot 30223$

Table 7. The 40 even pseudoprimes up to 10^{10}.

X	$\alpha(X)$	$\beta(X)$
10^3	0.048663	2.466690
10^4	0.508262	1.849388
10^5	0.602306	1.700002
10^6	0.649319	1.636881
10^7	0.679908	1.602218
10^8	0.697435	1.596159
10^9	0.711006	1.595093
10^{10}	0.721350	1.598918
25.10^9	0.724828	1.601292
10^{11}	0.729621	1.605264
10^{12}	0.736643	1.612232

Table 8. The functions α and β of section 10

X	$P(X)$	$EP(X)$	$SP(X)$	$C(X)$
10^4	22	12	5	7
10^5	78	36	16	16
10^6	245	114	46	43
10^7	750	375	162	105
10^8	2057	1071	488	255
10^9	5597	2939	1282	646
10^{10}	14884	7706	3291	1547
25.10^9	21853	11347	4842	2163
10^{11}	38975	20417	8607	3605
10^{12}	101629	53332	22407	8241

Table 9. The numbers of pseudoprimes, Euler pseudoprimes, strong pseudoprimes and Carmichael numbers up to X

University of Cambridge, Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge CB2 1SB, U.K.

E-mail address: RGEP @ PHX.CAM.AC.UK