**On Strong Pseudoprimes to Several Bases**

Gerhard Jaeschke

*Mathematics of Computation*, Vol. 61, No. 204 (Oct., 1993), 915-926.

Stable URL:
http://links.jstor.org/sici?sici=0025-5718%28199310%2961%3A204%3C915%3AOSPTSB%3E2.0.CO%3B2-G

*Mathematics of Computation* is currently published by American Mathematical Society.

---

MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 204
OCTOBER 1993, PAGES 915–926

# ON STRONG PSEUDOPRIMES TO SEVERAL BASES

GERHARD JAESCHKE

ABSTRACT. With $\psi_k$ denoting the smallest strong pseudoprime to all of the first $k$ primes taken as bases we determine the exact values for $\psi_5$, $\psi_6$, $\psi_7$, $\psi_8$ and give upper bounds for $\psi_9$, $\psi_{10}$, $\psi_{11}$. We discuss the methods and underlying facts for obtaining these results.

## 1. PRIMALITY TESTS BY MEANS OF STRONG PSEUDOPRIMES

Computer algebra systems, as for instance AXIOM [2], use strong pseudoprimes for testing primality of integers. The advantage of such tests is that they are very efficient. The disadvantage is that they are only probabilistic tests when the integers are not restricted to certain intervals. To make such tests deterministic for integers in prescribed intervals, one has to know the exact number of necessary so-called "strong pseudoprimality tests". For this purpose we introduce the numbers $\psi_1, \psi_2, \ldots$ for which we compute lower and upper bounds. These numbers are defined and discussed in this section; in §2 we derive some facts which are the basis for finding bounds for the numbers $\psi_k$. In §3 we discuss the methods which led to our results.

In view of Fermat's "Little Theorem" we know that $n$ is *certainly* not a prime when we have $b^{n-1} \not\equiv 1 \mod n$ for an integer $b$ with $1 < b < n-1$. That is, if $n$ is prime, then

$$b^{n-1} \equiv 1 \mod n. \tag{1}$$

An odd composite number $n$ for which (1) holds is called a "pseudoprime to base $b$" (we write $\mathrm{psp}(b, n)$). Usually, for a composite $n$ there exist small bases $b$ such that (1) is violated, but there are numbers $n$ which are pseudoprimes to every base $b$ coprime with $n$. These are called "Carmichael numbers". Therefore, a stronger criterion than (1) is needed for testing primality which leads to the concept of "strong pseudoprime to base $b$". When $n = 1 + 2^h d$ with $d$ odd, $h > 0$, and when $n$ is a composite number, then $n$ is called a "strong pseudoprime to base $b$" if either

$$b^d \equiv 1 \mod n \tag{2a}$$

or

$$b^{2^k d} \equiv -1 \mod n \tag{2b}$$

Received by the editor May 23, 1990 and, in revised form, October 28, 1991 and August 14, 1992.
1991 *Mathematics Subject Classification.* Primary 11A15.


0025-5718/93 $1.00 + $.25 per page

for an integer $k$ satisfying $0 \le k < h$. We write $\mathrm{spsp}(b, n)$ if and only if $n$ is a strong pseudoprime to base $b$. From [3] we know that there are 4842 strong pseudoprimes to base 2 which are less than $25 \cdot 10^9$, but there does not exist any integer below this limit that is simultaneously a strong pseudoprime to all the bases $2, 3, 5, 7, 11$. The last fact can be used for a fast primality test for numbers $n < 25 \cdot 10^9$, as is easily seen.

Now we turn to the definition of the integers $\psi_k$ mentioned above. Let $q_1, \ldots, q_k$ be the first $k$ primes. Then $\psi_k$ is the smallest positive integer $n$ such that $n$ is a strong pseudoprime to all the bases $q_1, \ldots, q_k$. Thus, if $n < \psi_k$, then only $k$ strong primality tests are needed in order to find out whether $n$ is prime or not. This shows the importance of knowing strong pseudoprimes to several bases.

From the paper [3] we obtain the following facts:

$$\begin{aligned}
\psi_1 &= 2047, \\
\psi_2 &= 1373653, \\
\psi_3 &= 25326001, \\
\psi_4 &= 3215031751, \\
\psi_5 &> 25 \cdot 10^9.
\end{aligned}$$

In this note we state some additional results, namely:

$$\begin{aligned}
\psi_5 &= 2152302898747 = 6763 \cdot 10627 \cdot 29947, \\
\psi_6 &= 3474749660383 = 1303 \cdot 16927 \cdot 157543, \\
\psi_7 &= 341550071728321 = 10670053 \cdot 32010157, \\
\psi_8 &= 341550071728321 = 10670053 \cdot 32010157, \\
\psi_9 &\le 41234316135705689041 = 4540612081 \cdot 9081224161, \\
\psi_{10} &\le 155336056607314320554100 2401 \\
&= 22754930352733 \cdot 68264791058197, \\
\psi_{11} &\le 56897193526942024370326972321 \\
&= 137716125329053 \cdot 413148375987157.
\end{aligned}$$

In order to obtain a lower bound $l_k$ for $\psi_k$, one has to show the nonexistence of strong pseudoprimes to the bases $q_1, \ldots, q_k$ less than $l_k$. The upper bounds for the $\psi_k$ are obtained by constructing strong pseudoprimes to the bases $q_1, \ldots, q_k$. How this is performed will be discussed in §§3 and 4.

## 2. Foundations of the algorithm

In this section we formulate some statements which form the basis for the algorithm in §3, where bounds for the numbers $\psi_k$ have to be computed. The first statement requires the concept "signature of the prime $p$ to the bases $a_1, \ldots, a_w$". Let $l_a(p)$ denote the smallest positive exponent $x$ such that $a^x \equiv 1 \bmod p$, where $\gcd(a, p) = 1$. Such an integer always exists by Fermat's theorem. Obviously, one has $p \equiv 1 \bmod l_a(p)$. Let us further denote by $\Delta(g)$ the exponent of the greatest power of 2 that divides the integer $g$. Then $\Delta(l_a(p))$ is called the "signature of $p$ to base $a$". More generally, if

$$\nu = (a_1, \ldots, a_w), \quad \gcd(a_i, p) = 1 \quad \text{for } i = 1, \ldots, w,$$

we define

$$\sigma_p^\nu = (\Delta(l_{a_1}(p)), \dots, \Delta(l_{a_w}(p)))$$

and call this $w$-tuple the "signature of $p$ to the bases $a_1, \dots, a_w$". Finally, we write

$$\mathrm{psp}((a_1, \dots, a_w), n) \quad \text{or} \quad \mathrm{spsp}((a_1, \dots, a_w), n),$$

respectively, if and only if $n$ is a pseudoprime or strong pseudoprime, respectively, to all the bases $a_1, \dots, a_w$. By means of these notions we formulate the first fact concerning strong pseudoprimes.

**Proposition 1.** *Let $n = p_1 \cdots p_t$ with different primes $p_1, \dots, p_t$. Further let $\nu = (a_1, \dots, a_w)$ with different integers $a_1, \dots, a_w$ greater than 1 such that $\gcd(a_i, p_j) = 1$ for all $i = 1, \dots, w$; $j = 1, \dots, t$. Under these assumptions $\mathrm{spsp}(\nu, n)$ holds if and only if $\mathrm{psp}(\nu, n)$ is valid and all $p_j$, $j = 1, \dots, t$, have the same signature to all of the bases $a_1, \dots, a_w$, i.e., $\sigma_{p_1}^\nu = \cdots = \sigma_{p_t}^\nu$.*

*Proof.* This statement is an immediate consequence of the following equivalences:

$$a^{2^k d} \equiv -1 \bmod n \Leftrightarrow \Delta(l_a(p_i)) = k + 1 \quad \text{for all } p_i | n \text{ and } \mathrm{psp}(a, n)$$

and

$$a^d \equiv 1 \bmod n \Leftrightarrow \Delta(l_a(p_i)) = 0 \quad \text{for all } p_i | n \text{ and } \mathrm{psp}(a, n),$$

where $n = 1 + 2^h d$, $d$ odd, $0 \le k < h$, and $\gcd(a, n) = 1$. □

Proposition 1 serves on the one hand for constructing strong pseudoprimes to several bases by multiplying primes which have identical signatures, and on the other hand for proving the nonexistence of such strong pseudoprimes below some given limit.

**Example.** For $\nu = (11, 13, 17)$ we have

$$\sigma_{1531}^\nu = \sigma_{2551}^\nu = \sigma_{3571}^\nu = (0, 0, 0),$$

and since $\mathrm{psp}(\nu, n)$ holds for $n = 1531 \cdot 2551 \cdot 3571$, we also have $\mathrm{spsp}(\nu, n)$.

**Proposition 2.** *Let $a_1, \dots, a_w$ be different primes. Then for primes $p \equiv 3 \bmod 4$ with $p$ not dividing $a_1, \dots, a_w$ the signature $\sigma_p^{(a_1, \dots, a_w)}$ depends only on the residue class of $p \bmod 4a_1 \cdots a_w$.*

*Proof.* For $p \equiv 3 \bmod 4$ we evidently have $\Delta(l_a(p)) \in \{0, 1\}$, and if $\sigma_p^{(a_1, \dots, a_w)} = (b_1, \dots, b_w)$, then

$$b_i = 0 \quad \text{if} \left(\frac{a_i}{p}\right) = 1, \qquad b_i = 1 \quad \text{if} \left(\frac{a_i}{p}\right) = -1.$$

Thus, $\sigma_p^{(a_1, \dots, a_w)}$ depends only on the quadratic residue character of the $a_i \bmod p$. By the law of quadratic reciprocity it then follows

$$\Delta(l_{a_i}(p)) = \Delta(l_{a_i}(q)) \quad \text{for } p \equiv q \bmod 4a_i,$$

hence the assertion of the proposition. □

**Example.** Let $\nu = (2, 3, 5, 7, 11)$. We want to find all primes $p \equiv 3 \bmod 4$ which have the signature $\sigma_p^\nu = (0, 1, 0, 0, 1)$. So we have to solve the system

$$\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{7}{p}\right) = 1 \quad \text{and} \quad \left(\frac{3}{p}\right) = \left(\frac{11}{p}\right) = -1.$$

This is equivalent to solving the system of congruences

$$\begin{aligned} p &\equiv 7 \mod 8, \\ p &\equiv 7 \mod 12, \\ p &\equiv 11, 19 \mod 20, \\ p &\equiv 3, 19, 27 \mod 28, \\ p &\equiv 3, 15, 23, 27, 31 \mod 44, \end{aligned}$$

which yields 30 classes mod 9240:

$$p \equiv 31, 199, 559, 1039, \ldots, 8959 \mod 9240.$$

By means of Proposition 2 exactly the primes in each of these 30 classes are the desired primes.

For primes $p \equiv 1 \mod 4$ we have no corresponding statement. But here the following proposition can be useful.

**Proposition 3.** *For primes $p, q$ it is true that*

$$\Delta(p-1) = \Delta(q-1) \text{ and } \sigma_p^{(a)} = \sigma_q^{(a)} \quad \text{imply} \quad \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

*Proof.* This follows from

$$\sigma_p^{(a)} = \Delta(p-1) \Leftrightarrow \left(\frac{a}{p}\right) = -1. \quad \square$$

**Example.** By Proposition 3 it is easy to determine all primes $p \equiv 5 \mod 8$ which have the signature $\sigma_p^{(2,3,5)} = (2, 2, 2)$. These are exactly the primes $p \equiv 53, 77 \mod 120$. But each of the signatures $\sigma_p^{\nu} = (2, 2, 0)$ and $(2, 2, 1)$ for $\nu = (2, 3, 5)$ does not depend only on residue classes mod 120, as we shall se below. We find by Proposition 3 that

$$\sigma_p^{(2,3,5)} = (2, 2, \Delta) \quad \text{with } \Delta \in \{0, 1\} \text{ for } p \equiv 29, 101 \mod 120.$$

For these $p$ we have (using the 4th power residue character symbol)

$$\left(\frac{5}{p}\right)_4 \equiv 5^{(p-1)/4} \mod p;$$

hence, in view of $(\frac{5}{p}) = 1$,

$$\begin{aligned} \left(\frac{5}{p}\right)_4 &= 1 \quad \text{implies} \quad \sigma_p^{(2,3,5)} = (2, 2, 0), \\ \left(\frac{5}{p}\right)_4 &= -1 \quad \text{implies} \quad \sigma_p^{(2,3,5)} = (2, 2, 1). \end{aligned}$$

Both $p$-types occur in each of the residue classes $29, 101 \mod 120$:

$$\sigma_{29}^{(2,3,5)} = \sigma_{701}^{(2,3,5)} = (2, 2, 1), \qquad \sigma_{149}^{(2,3,5)} = \sigma_{101}^{(2,3,5)} = (2, 2, 0).$$

For an efficient determination of large strong pseudoprimes to several bases we use later on

**Proposition 4.** *If $p$ and $q = 2p - 1$ are primes, and if $b$ is an odd integer with* $\gcd(b, p) = \gcd(b, q) = 1$, *then we have*

$$\operatorname{psp}(b, pq) \text{ if and only if } \left(\frac{q}{b}\right) = 1.$$

*Proof.* Under the above assumptions we have

$$b^{pq-1} \equiv 1 \bmod pq \Leftrightarrow b^{p-1} \equiv 1 \bmod q.$$

But with $p - 1 = \frac{q-1}{2}$ and $q \equiv 1 \bmod 4$ we obtain the assertion by the law of quadratic reciprocity. □

*Remark.* For $b = 2$ we simply have

$$\operatorname{psp}(2, p(2p - 1)) \Leftrightarrow p \equiv 1 \bmod 4$$

under the assumption that $p$, $2p - 1$ are primes.

## 3. Algorithm

In this section we start by describing the general procedure for determining all strong pseudoprimes $n$ to given bases, where $n$ is bounded by a prescribed limit $g$ and has a given number $t$ of prime factors. We continue by applying this procedure to special cases, which yield the results presented in §1.

In all the following discussions we can restrict ourselves to squarefree integers, in view of Proposition 4 in [3] and the fact the congruences $2^{p-1} \equiv 1 \bmod p^2$ and $3^{p-1} \equiv 1 \bmod p^2$ do not hold simultaneously for any prime $p$ below $3 \cdot 10^9$ [3].

Let $q_i$ denote the $i$th prime, and let $\nu = (q_1, \ldots, q_w)$. If a large integer $g$ is given and $t$ is a small positive integer $\geq 2$, then we want to solve the following problem:

Find all strong pseudoprimes $\leq g$ to the bases $q_1, \ldots, q_w$ that have $t$ different prime factors.

*Case* 1. We start by assuming $t \geq 3$.

*Phase* 1. We determine all $(t-1)$-tuples $(p_1, \ldots, p_{t-1})$ with primes $p_1, \ldots, p_{t-1}$ such that

(A) $q_w < p_1 < \cdots < p_{t-1}$,

(B) $\sigma_{p_1}^{\nu} = \cdots = \sigma_{p_{t-1}}^{\nu}$,

(C) $p_1 \cdots p_{t-2} p_{t-1}^2 < g$.

We call the $(t-1)$-tuples satisfying (A), (B), (C) "feasible $(t-1)$-tuples".

*Phase* 2. For each feasible $(t-1)$-tuple $(p_1, \ldots, p_{t-1})$ we proceed as follows. We choose one of the primes $q_1, \ldots, q_w$ as $b$.

Step 1. We compute $\eta = \operatorname{lcm}(l_b(p_1), \ldots, l_b(p_{t-1}))$.

Step 2. If $\gcd(\eta, p_1 \cdots p_{t-1}) > 1$, then the $(t-1)$-tuple $(p_1, \ldots, p_{t-1})$ is ignored. Otherwise, compute the multiplicative inverse $c$ of $p_1 \cdots p_{t-1} \bmod \eta$, i.e., $c = (p_1 \cdots p_{t-1})^{-1} \bmod \eta$.

Step 3. For each prime $y \leq g/(p_1 \cdots p_{t-1})$ with $y \equiv c \bmod \eta$ we test whether $\operatorname{spsp}(\nu, p_1 \cdots p_{t-1} y)$ holds or not.

*Case* 2. We now assume that $t = 2$. For each prime $p < \sqrt{g}$ we first compute

$$\lambda_p = \operatorname{lcm}(2, l_{q_1}(p), \ldots, l_{q_w}(p)).$$

Then all products $P = p(1 + k\lambda_p)$ are computed for $k = 1 + (p-1)/\lambda_p, \ldots, [(g-p)/p\lambda_p]$, where $1 + k\lambda_p$ must be prime. For each product $P$ we test whether $\operatorname{spsp}(\nu, P)$ holds or not.

**Improvements of the algorithm.** A central problem of this algorithm is the following. Given $\nu = (q_1, \dots, q_w)$ and a prime $p$, find all primes $q$ smaller than a given limit with $q > p$ and $\sigma_q^\nu = \sigma_p^\nu$. In order to do this efficiently, we apply Propositions 2 and 3.

If, for example, $p \equiv 3 \bmod 4$, then $p$ has a binary signature

$$\sigma_p^\nu = (\Delta_1, \dots, \Delta_w) \quad \text{with } \Delta_i \in \{0, 1\} \text{ for } i = 1, \dots, w.$$

Then by Proposition 2 *all* primes $q \equiv 3 \bmod 4$ with $(q_i/p) = (q_i/q)$, $i = 1, \dots, w$, satisfy $\sigma_q^\nu = \sigma_p^\nu$. But there might be primes $q \equiv 1 \bmod 4$ which have a binary signature $\sigma_q^\nu$. In order to find these $q$, we observe that

$$\text{(QR)} \qquad \left(\frac{q_i}{q}\right) = 1 \quad \text{for } i = 1, \dots, w$$

must hold; since this condition is not sufficient (cf. example after Proposition 3), these $q$ are only *candidates* for $\sigma_q^\nu = \sigma_p^\nu$.

Altogether, this means that the desired $q$-values belong to

$$2^{2-w} \prod_{i=2}^{w} (q_i - 1) \text{ residue classes } \bmod 8 \cdot \prod_{i=2}^{w} q_i.$$

The residue classes defined by (QR) can be ignored in many cases, since we know in advance (i.e., independently of $p$) which primes $q$ below a given limit satisfy (QR). So we know that

(F1) there are only 9 primes $q < 10^6$, $q \equiv 1 \bmod 4$, with binary signature $\sigma_q^{(2,3,5,7,11)}$:

$$q = 148201, 170809, 196681, 238681, 735529,$$
$$737641, 921001, 924361, 988681$$

and

(F2) there exist only 4 primes $q < 10^7$, $q \equiv 1 \bmod 4$, with binary signature $\sigma_q^{(2,3,5,7,11,13,17)}$:

$$q = 4179289, 7140169, 7781929, 8971561.$$

If, for instance, we have to determine all primes $q < 1000000$ with $\sigma_q^{(2,\dots,11)} = \sigma_{31}^{(2,\dots,11)}$, then by (F1) only the primes $q < 1000000$ in the 30 classes mod 9240 in the example after Proposition 2 solve the problem.

Another example shall be discussed for a prime $p \not\equiv 3 \bmod 4$, where we make use of Proposition 3. Let $w = 7$, that is $\nu = (2, 3, 5, 7, 11, 13, 17)$ and $p = 97$. Determine all primes $q < 300000$ with $\sigma_q^\nu = \sigma_{97}^\nu$. The maximal element in $\sigma_{97}^\nu = (4, 4, 5, 5, 4, 5, 5)$ is 5. Thus, by Proposition 3 we determine all primes $q \equiv 33 \bmod 64$ that satisfy

$$\left(\frac{3}{q}\right) = \left(\frac{11}{q}\right) = 1 \quad \text{and} \quad \left(\frac{5}{q}\right) = \left(\frac{7}{q}\right) = \left(\frac{13}{q}\right) = \left(\frac{17}{q}\right) = -1,$$

which yields 1440 classes mod 16336320. We find 12 primes $q$ with $97 < q < 300000$ in these classes, only two of which satisfy $\sigma_q^\nu = \sigma_{97}^\nu$: $q = 257953, 271393$.

Further, we find 9 primes $q \equiv 1 \mod 64$, $q < 300000$, from the equation

$$\left(\frac{3}{q}\right) = \left(\frac{5}{q}\right) = \left(\frac{7}{q}\right) = \left(\frac{11}{q}\right) = \left(\frac{13}{q}\right) = \left(\frac{17}{q}\right) = 1,$$

but none of them satisfies $\sigma_q^\nu = \sigma_{97}^\nu$. Therefore, the above 2 primes solve the problem.

In step 3 of phase 2 we can achieve a great reduction of the number of primality tests by applying Propositions 2 and 3. Let $\nu = (2, 3, 5, 7, 11, 13, 17)$, $g = 341550071728321$, $p = 307$, $q = 1987$. Then step 3 of phase 2 consists in computing all

$$r \leq 559909889 \quad \text{with } r \equiv 5227 \mod 33762$$

and testing $r$ for primality and for $\sigma_r^\nu = \sigma_{307}^\nu$. Therefore, 16584 such tests have to performed. When we use Proposition 2 and solve the systems

$$\left(\frac{2}{r}\right) = \left(\frac{2}{307}\right), \ldots, \left(\frac{13}{r}\right) = \left(\frac{13}{307}\right), \qquad r \equiv 3 \mod 4$$

and

$$\left(\frac{2}{r}\right) = \left(\frac{3}{r}\right) = \cdots = \left(\frac{17}{r}\right) = q, \qquad r \equiv 1 \mod 4,$$

we only have 304 $r$-values as test-candidates.

**Applications.** We apply the algorithm to the following two special cases for $w$, $g$:

(SC1) $\quad w_1 = 5, \quad g_1 = 3474749660383,$

(SC2) $\quad w_2 = 7, \quad g_2 = 341550071728321.$

It will be shown that there exists only one strong pseudoprime $n < g_1$ to the bases $2, 3, 5, 7, 11$, and no strong pseudoprime $n < g_2$ to the bases $2, 3, 5, 7, 11, 13, 17$.

Further, we present all strong pseudoprimes $\leq 10^{12}$ to the bases $2, 3, 5$ in Table 1 on the next page (see also Table 7 in [3]). It should be noted that Table 1 contains (in contrast to the results in [3]) two numbers being not of the form $(n+1)(kn+1)$, namely $77475820141 = 176041 \cdot 440101$ and $183413388211 = 370891 \cdot 494521$.

(SC1). Let $\nu = (2, 3, 5, 7, 11)$.

(a) $t \geq 5$.

Define $N_p$ to be the set of all primes $q > p$ with $\sigma_q^\nu = \sigma_p^\nu$. If $f_{p,k}$ denotes the $k$th element of $N_p$ in ascending order, then we compute for each $p \leq 317$ the values $f_{p,1}, \ldots, f_{p,4}$ and obtain

$$\min p \cdot \prod_{k=1}^{4} f_{p,k} = 19 \cdot \prod_{k=1}^{4} f_{19,k} > g_1,$$

so that no spsp$(\nu, n)$ exists with $n \leq g_1$ and which has more than 4 factors.

(b) $t = 4$.

When $t = 4$, phase 1 of the algorithm yields 1557 feasible triplets $(p_1, p_2, p_3)$.

TABLE 1. List of all strong pseudoprimes $< 10^{12}$ to the bases 2, 3, 5

| | | spsp-base | | | |
|---|---|---|---|---|---|
| number | factorisation | 7 | 11 | 13 | 17 |
| 25326001 | 2251 • 11251 | 0 | 0 | 0 | 0 |
| 161304001 | 7333 • 21997 | 0 | 1 | 0 | 0 |
| 960946321 | 11717 • 82013 | 0 | 0 | 0 | 0 |
| 1157839381 | 24061 • 48121 | 0 | 0 | 0 | 0 |
| 3215031751 | 151 • 751 • 28351 | 1 | 0 | 0 | 0 |
| 3697278427 | 30403 • 121609 | 0 | 0 | 0 | 1 |
| 5764643587 | 37963 • 151849 | 0 | 0 | 1 | 0 |
| 6770862367 | 41143 • 164569 | 0 | 0 | 0 | 1 |
| 14386156093 | 397 • 4357 • 8317 | 0 | 0 | 0 | 0 |
| 15579919981 | 88261 • 176521 | 0 | 1 | 0 | 0 |
| 18459366157 | 67933 • 271729 | 0 | 0 | 0 | 0 |
| 19887974881 | 81421 • 244261 | 0 | 0 | 0 | 0 |
| 21276028621 | 103141 • 206281 | 0 | 0 | 1 | 0 |
| 27716349961 | 117721 • 235441 | 0 | 0 | 0 | 0 |
| 29118033181 | 120661 • 241321 | 0 | 1 | 0 | 0 |
| 37131467521 | 111253 • 333757 | 0 | 0 | 0 | 0 |
| 41752650241 | 117973 • 353917 | 0 | 1 | 1 | 0 |
| 42550716781 | 145861 • 291721 | 0 | 0 | 0 | 0 |
| 43536545821 | 147541 • 295081 | 0 | 0 | 0 | 0 |
| 44732778751 | 105751 • 423001 | 0 | 0 | 0 | 0 |
| 44778481441 | 122173 • 366517 | 0 | 0 | 0 | 1 |
| 48354810571 | 331 • 2971 • 49171 | 0 | 1 | 1 | 0 |
| 52139147581 | 161461 • 322921 | 0 | 0 | 0 | 0 |
| 53700690781 | 163861 • 327721 | 0 | 0 | 0 | 0 |
| 56209415767 | 118543 • 474169 | 0 | 0 | 0 | 0 |
| 57698562127 | 120103 • 480409 | 0 | 0 | 0 | 0 |
| 67403434561 | 149893 • 449677 | 0 | 1 | 0 | 0 |
| 73796984161 | 156841 • 470521 | 0 | 0 | 1 | 0 |
| 74190097801 | 151 • 2551 • 192601 | 0 | 0 | 0 | 0 |
| 75285070351 | 137191 • 548761 | 0 | 0 | 0 | 1 |
| 75350936251 | 137251 • 549001 | 0 | 0 | 0 | 0 |
| 77475820141 | 176041 • 404101 | 0 | 0 | 0 | 0 |
| 79696887661 | 199621 • 399241 | 0 | 0 | 0 | 0 |
| 83828294551 | 1231 • 6151 • 11071 | 0 | 0 | 0 | 0 |
| 88473676747 | 148723 • 594889 | 0 | 0 | 1 | 0 |
| 88974090367 | 149143 • 596569 | 0 | 0 | 0 | 0 |
| 98515393021 | 221941 • 443881 | 0 | 1 | 1 | 0 |
| 111737197441 | 149491 • 747451 | 0 | 0 | 0 | 0 |
| 114247549027 | 169003 • 676009 | 0 | 1 | 0 | 0 |
| 118670087467 | 172243 • 688969 | 1 | 0 | 0 | 0 |
| 126223730461 | 251221 • 502441 | 0 | 0 | 0 | 0 |
| 134670080641 | 211873 • 635617 | 0 | 0 | 0 | 0 |
| 135586888951 | 184111 • 736441 | 0 | 0 | 1 | 0 |
| 136136947201 | 139457 • 976193 | 0 | 0 | 0 | 0 |
| 148600530541 | 272581 • 545161 | 0 | 0 | 0 | 0 |
| 150401047441 | 146581 • 1026061 | 0 | 0 | 0 | 0 |
| 156677923729 | 177019 • 885091 | 0 | 0 | 0 | 0 |
| 157615339681 | 229213 • 687637 | 0 | 0 | 0 | 0 |
| 167259489409 | 182899 • 914491 | 0 | 0 | 0 | 0 |
| 174460968067 | 208843 • 835369 | 0 | 0 | 0 | 0 |
| 183413388211 | 370891 • 494521 | 0 | 0 | 0 | 0 |
| 187403492251 | 216451 • 865801 | 0 | 0 | 0 | 0 |
| 216291665041 | 175781 • 1230461 | 0 | 0 | 0 | 0 |
| 218215348801 | 269701 • 809101 | 0 | 0 | 0 | 0 |
| 218673063181 | 330661 • 661321 | 0 | 0 | 0 | 1 |
| 234311749201 | 182957 • 1280693 | 0 | 0 | 0 | 0 |

TABLE 1 (continued)

| | | spsp-base | | | |
|---|---|---|---|---|---|
| number | factorisation | 7 | 11 | 13 | 17 |
| 240438464197 | 245173 • 980689 | 0 | 0 | 0 | 0 |
| 244970876021 | 202061 • 1212361 | 0 | 0 | 0 | 0 |
| 245291853691 | 1171 • 10531 • 19891 | 0 | 1 | 1 | 1 |
| 247945488451 | 248971 • 995881 | 0 | 0 | 0 | 0 |
| 252505670761 | 355321 • 710641 | 0 | 0 | 1 | 0 |
| 272447722207 | 260983 • 1043929 | 0 | 0 | 0 | 0 |
| 291879706861 | 382021 • 764041 | 0 | 1 | 0 | 0 |
| 295545735181 | 221941 • 1331641 | 0 | 0 | 0 | 0 |
| 307768373641 | 392281 • 784561 | 1 | 0 | 0 | 0 |
| 315962312077 | 281053 • 1124209 | 1 | 0 | 0 | 0 |
| 331630652449 | 257539 • 1287691 | 0 | 0 | 0 | 0 |
| 342221459329 | 261619 • 1308091 | 0 | 0 | 0 | 0 |
| 353193975751 | 297151 • 1188601 | 0 | 0 | 0 | 0 |
| 354864744877 | 297853 • 1191409 | 1 | 0 | 0 | 0 |
| 362742704101 | 301141 • 1204561 | 0 | 0 | 0 | 0 |
| 398214876001 | 364333 • 1092997 | 0 | 0 | 0 | 0 |
| 405439595861 | 259949 • 1559689 | 0 | 0 | 0 | 0 |
| 407979839041 | 368773 • 1106317 | 0 | 0 | 0 | 0 |
| 431229929521 | 182131 • 2367691 | 0 | 0 | 0 | 0 |
| 457453568161 | 390493 • 1171477 | 1 | 0 | 0 | 1 |
| 490883439061 | 495421 • 990841 | 0 | 0 | 0 | 0 |
| 503691743521 | 409753 • 1229257 | 0 | 0 | 0 | 1 |
| 505130380987 | 355363 • 1421449 | 0 | 0 | 0 | 0 |
| 528929554561 | 419893 • 1259677 | 1 | 0 | 0 | 1 |
| 546348519181 | 522661 • 1045321 | 1 | 0 | 1 | 0 |
| 549866444221 | 524341 • 1048681 | 0 | 0 | 0 | 0 |
| 591090138721 | 443881 • 1331641 | 0 | 0 | 0 | 0 |
| 602248359169 | 347059 • 1735291 | 1 | 0 | 0 | 0 |
| 641498618881 | 462421 • 1387261 | 0 | 0 | 0 | 0 |
| 659937299407 | 406183 • 1624729 | 0 | 0 | 0 | 0 |
| 688529415421 | 586741 • 1173481 | 0 | 1 | 0 | 0 |
| 712614969307 | 422083 • 1688329 | 0 | 0 | 0 | 0 |
| 729421133761 | 493093 • 1479277 | 0 | 1 | 0 | 0 |
| 733224429367 | 428143 • 1712569 | 0 | 0 | 1 | 0 |
| 736775510329 | 383869 • 1919341 | 0 | 0 | 0 | 0 |
| 741881186287 | 430663 • 1722649 | 0 | 1 | 0 | 0 |
| 744049848481 | 498013 • 1494037 | 0 | 0 | 0 | 0 |
| 774840343681 | 508213 • 1524637 | 0 | 0 | 0 | 0 |
| 842638521121 | 529981 • 1589941 | 0 | 0 | 0 | 0 |
| 851402588401 | 412651 • 2063251 | 0 | 0 | 0 | 0 |
| 853196213761 | 349121 • 2443841 | 0 | 0 | 0 | 0 |
| 863370140641 | 536461 • 1609381 | 0 | 0 | 0 | 0 |
| 908201935681 | 550213 • 1650637 | 0 | 0 | 0 | 0 |
| 966299321527 | 491503 • 1966009 | 0 | 0 | 0 | 0 |
| 997031384161 | 576493 • 1729477 | 0 | 0 | 0 | 0 |

It is easy to see that we only need to consider triplets with $p_1 \leq 1361$, $p_2 \leq 6427$, $p_3 \leq 36269$. In phase 2 we took $b = 3$. So we obtained 178 quadruples $(p_1, p_2, p_3, p_4)$ which satisfy $3^{p_1p_2p_3p_4-1} \equiv 1 \bmod p_1p_2p_3$, but no spsp$(\nu, p_1p_2p_3p_4)$ was detected.

(c) $t = 3$.

Here, phase 1 yields 42233 feasible pairs $(p_1, p_2)$, where $p_1, p_2$ could be restricted to $p_1 \leq 15139$, $p_2 \leq 516991$. In phase 2 we took $b = 2$ and found 261

triplets $(p_1, p_2, p_3)$ with $2^{p_1p_2p_3-1} \equiv 1 \bmod p_1p_2$, only one spsp$(\nu, p_1p_2p_3)$ with $p_1p_2p_3 < g_1$ was detected. This integer is

$$\tilde{n} = 2152302898747 = 6763 \cdot 10627 \cdot 29947.$$

Now, it is easy to verify that

$$g_1 = 3474749660383 = 1303 \cdot 16927 \cdot 157543$$

is a strong pseudoprime to the bases $2, 3, 5, 7, 11, 13$, which means that $\psi_5 \leq \tilde{n}$ and $\psi_6 \leq g_1$.

(d) $t = 2$.

At first we compute for all primes $p < \sqrt{g_1}$ (that is $p < 1864068$) the value $\lambda_p$ as defined above. We further define $\mu_p = (p-1)/\lambda_p$ and $\tau_k$ to be the number of primes $p$ with $13 \leq p < 1864068$ and $\mu_p = k$. It turns out that

$$\tau_k = 0 \text{ for } k \geq 6, \quad \tau_5 = 7, \quad \tau_4 = 47, \quad \tau_3 = 242, \quad \tau_1 + \tau_2 = 139238.$$

This means that for nearly all $p$ our search for primes $q$ with spsp$(\nu, pq)$ is restricted to

$$q = 1 + k \cdot \frac{p-1}{2} \quad \text{with } 3 \leq k \leq \frac{2g_1}{p(p-1)}.$$

For small values of $p$ this search is very time-consuming (for instance if $p < 10000$ then the number of $k$-values to be checked is $> 69000$). Therefore, we used another procedure to perform this job when $p < 10000$. For each such $p$ we calculated

$$h = \gcd(2^{p-1} - 1, 3^{p-1} - 1, 5^{p-1} - 1)$$

and factored $h$ (this is easy, since $h$ usually has many small prime factors). When $h$ has a factor $q > p$, then we tested $pq$ for strong pseudoprimality to the bases $2, 3, 5, 7, 11$.

Since no pair $pq < g_1$ with spsp$(\nu, pq)$ was detected, we have the results $\psi_5 = 2152302898747$ and $\psi_6 = 3474749660383$.

(SC2). Let $\nu = (2, 3, 5, 7, 11, 13, 17)$.

(a) $t \geq 5$.

Analogous to the case (SC1) we compute for each $p \leq 797$ the values $f_{p,1}, \ldots, f_{p,4}$ and obtain

$$\min p \cdot \prod_{k=1}^{4} f_{p,k} = 131 \cdot \prod_{k=1}^{4} f_{131,k} > g_2,$$

so that no spsp$(\nu, n)$ exists with $n \leq g_2$ and which has more than 4 factors.

(b) $t = 4$.

When $t = 4$, phase 1 of the algorithm yields 1902 feasible triplets $(p_1, p_2, p_3)$. In phase 2 we took $b = 2$. So we obtained 231 quadruples $(p_1, p_2, p_3, p_4)$ which satisfy $2^{p_1p_2p_3p_4-1} \equiv 1 \bmod p_1p_2p_3$, but no spsp$(\nu, p_1p_2p_3p_4)$ was detected.

(c) $t = 3$.

Here, phase 1 yields 154953 feasible pairs $(p_1, p_2)$. In phase 2 we put $b = 2$ and found 265 triplets $(p_1, p_2, p_3)$ with $2^{p_1p_2p_3-1} \equiv 1 \bmod p_1p_2$, but no spsp$(\nu, p_1p_2p_3)$ with $p_1p_2p_3 < g_2$ was detected.

(d) $t = 2$.

We compute $\lambda_p = \operatorname{lcm}(2, l_2(p), \ldots, l_{17}(p))$ for each $p < 18481073$. We define

$\tau_k$ to be the number of primes $p$ with $19 \le p < 18481073$ and $\mu_p = k$. It turns out that

$$\tau_k = 0 \text{ for } k \ge 6, \quad \tau_5 = 1, \quad \tau_4 = 15, \quad \tau_3 = 207, \quad \tau_1 + \tau_2 = 1179824.$$

Again, for nearly all $p$ our search for primes $q$ with $\operatorname{spsp}(\nu, pq)$ is restricted to

$$q = 1 + k \cdot \frac{p-1}{2} \quad \text{with } 3 \le k \le \frac{2g_2}{p(p-1)}.$$

Here we factored

$$h = \gcd(2^{p-1} - 1, 3^{p-1} - 1, 5^{p-1} - 1)$$

for all $p < 120000$. It turned out that there is no $\operatorname{spsp}(\nu, pq)$ for $pq < g_2$, but $g_2 = 10670053 \cdot 32010157$ itself is a strong pseudoprime to the bases $2, 3, 5, 7, 11, 13, 17, 19$. This means that $\psi_7 = \psi_8 = g_2$.

## 4. Upper bounds for $\psi_9, \psi_{10}, \psi_{11}$

In order to find upper bounds for $\psi_9, \psi_{10}, \psi_{11}$, we started an extensive search for numbers of the forms

(H1) $\quad p(2p-1)$ with $p, 2p-1$ prime,

(H2) $\quad p(3p-2)$ with $p, 3p-2$ prime

which are strong pseudoprimes to the bases $2, 3, 5, 7, 11, 13, 17, 19, 23$. In the case of (H1) we used Proposition 4: $(\frac{2p-1}{b}) = 1$ for $b = 3, 5, 7, 11$ and $p \equiv 1 \mod 4$ yield together 15 residue classes mod 4620:

$$p \equiv 1, 181, 421, 481, 841, 1321, 1741, 1861, 2161, 2521, 3121, 3781, 3841, 3961, 4381 \mod 4620.$$

It turns out that for $p = 4540612081$ the number

$$n = p(2p-1) = 41234316135705689041$$

is an $\operatorname{spsp}(\nu, n)$ for $\nu = (2, 3, 5, 7, 11, 13, 17, 19, 23)$. This $n$ yields the upper bound for $\psi_9$ stated in §1.

In the case of (H2) we solve the system

$$p \equiv 13 \mod 24,$$

$$\left(\frac{b}{p}\right) = \left(\frac{b}{3p-2}\right) = -1 \quad \text{for } b = 5, 7, 11, 13, 17, 19, 23$$

and obtain 400 residue classes mod 892371480. For each $p$ in these classes we test strong pseudoprimality to the bases $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$. So we find

$$\operatorname{spsp}((2, \ldots, 29), p(3p-2)) \quad \text{for } p = 22754930352733,$$
$$\operatorname{spsp}((2, \ldots, 31), p(3p-2)) \quad \text{for } p = 137716125329053.$$

These two numbers yield the upper bounds for $\psi_{10}, \psi_{11}$ stated in §1.

## 5. Other bases than the first primes

If we use only the first $k$ primes as bases, then $\psi_k$ is the limit up to which primality tests are correct by performing $k$ strong primality tests. When we

take instead $k$ arbitrary primes as bases, it is evident that the above 'correctness limit' may be increased considerably. But generally these bases are very large and not easy to find. We give a short survey on the magnitude of the correctness limit for up to 3 bases, when these are chosen conveniently.

Let $\nu = (b_1, \ldots, b_w)$, $b_i$ prime for $i = 1, \ldots, w$, and define

$$\chi_\nu = \min\{n | \operatorname{spsp}(\nu, n)\}.$$

Then we find for $w = 1$

$$\max_{b<1000000} \chi_b = \chi_{377687} = 5329,$$

whereas $\chi_2 = 2047$. For $w = 2$ we find

$$\max_{b_1, b_2<100} \chi_{(b_1, b_2)} = \chi_{(31, 73)} = 9080191,$$

whereas $\chi_{(2,3)} = 1373653$. We further computed

$$\max_{b<300000} \chi_{(2,b)} = \chi_{(2,299417)} = 19471033.$$

For $w = 3$ we find

$$\max_{b_1, b_2, b_3<100} \chi_{(b_1, b_2, b_3)} = \chi_{(2,7,61)} = 4759123141,$$

whereas $\chi_{(2,3,5)} = 25326001$. For $w = 4$ we have

$$\max_{b<5000000} \chi_{(2,3,5,b)} = \chi_{(2,3,5,4086253)} = 736775510329.$$

Recently, I found $\chi_{(2,13,23,1662803)} > 10^{12}$, meaning that up to $10^{12}$ only four strong pseudoprimality tests are necessary for proving primality.

*Remark.* All computations have been performed on an IBM 3081 at Heidelberg Scientific Center.

## ACKNOWLEDGMENT

I thank the referee for his valuable suggestions in the improvement of this paper. With respect to Table 1, I should mention Richard Schroeppel's computing all strong pseudoprimes up to $10^{11}$ to the bases 2, 3, and 5, which was based on an output of Richard Pinch, who computed all odd base-2 pseudoprimes up to this limit.

## BIBLIOGRAPHY

1. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory, Academic Press, London, 1971, pp. 213–222.
2. R. D. Jenks and R. F. Sutor, *AXIOM*, The Scientific Computation System, Springer-Verlag, Berlin-Heidelberg-New York, 1992.
3. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.

IBM SCIENTIFIC CENTER HEIDELBERG, TIERGARTENSTR. 15, 6900 HEIDELBERG, GERMANY