FINDING STRONG PSEUDOPRIMES TO SEVERAL BASES

ZHENXIANG ZHANG

Dedicated to the memory of P. Erdős (1913–1996)

Abstract. Define \( m \) to be the smallest strong pseudoprime to all the first \( m \) prime bases. If we know the exact value of \( m \), we will have, for integers \( n < m \), a deterministic primality testing algorithm which is not only easier to implement but also faster than either the Jacobi sum test or the elliptic curve test. Thanks to Pomerance et al. and Jaeschke, \( m \) are known for \( 1 \leq m \leq 8 \). Upper bounds for \( m \) were given by Jaeschke.

In this paper we tabulate all strong pseudoprimes (spsp’s) \( n < 10^{24} \) to the first ten prime bases 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29, which have the form \( n = pq \) with \( p, q \) odd primes and \( q = 1 = k(p - 1), k = 2, 3, 4 \). There are in total 44 such numbers, six of which are also spsp(31), and three numbers are spsp’s to both bases 31 and 29. As a result the upper bounds for \( \psi_{10} \) and \( \psi_{11} \) are lowered from 28- and 29-decimal-digit numbers to 22-decimal-digit numbers, and a 24-decimal-digit upper bound for \( \psi_{12} \) is obtained. The main tools used in our methods are the biquadratic residue characters and cubic residue characters. We propose necessary conditions for \( n \) to be a strong pseudoprime to one or to several prime bases. Comparisons of effectiveness with both Jaeschke’s and Arnault’s methods are given.

1. Introduction

If \( n \) is prime, then (as Fermat knew) the congruence

\[ b^{n-1} \equiv 1 \mod n \]

holds for every \( b \) with \( \gcd(n, b) = 1 \). In general, if (1.1) holds, then we say that \( n \) passes the Fermat (pseudoprime) test to base \( b \); if, in addition, \( n \) is composite, then we call \( n \) a pseudoprime to base \( b \) (or sps(b) for short). It is well-known that for each base \( b \), there are infinitely many sps(b)’s. There are odd composites \( n \), called Carmichael numbers, which are pseudoprimes to every base relatively prime to \( n \). Alford, Granville and Pomerance [2] proved that there are infinitely many Carmichael numbers.

For these reasons, in some cases it will be difficult to find proofs of compositeness using the Fermat test (1.1). A stronger form of the test does much better. Write
n - 1 = 2^s d with d odd. If n is prime, then

\[ (1.2) \quad \text{either } b^d \equiv 1 \pmod{n} \text{ or } b^{2^r d} \equiv -1 \pmod{n} \text{ for some } r = 0, 1, \ldots, s - 1 \]

holds for every b with gcd(n, b) = 1. If (1.2) holds then we say that n passes the Miller (strong pseudoprime) test \[12\] to base b; if, in addition, n is composite, then we say n is a strong pseudoprime to base b, or spsp(b) for short. Monier \[13\] and Rabin \[15\] proved that if n is an odd composite positive integer, then n passes the Miller test for at most \((n - 1)/4\) bases \(b\) with \(1 \leq b \leq n - 1\). Thus the Rabin-Miller test appeared: given a positive integer n, pick k different positive integers less than n and perform Miller test on n for each of these bases; if n is composite the probability that n passes all k tests is less than \(1/4^k\).

Define \(\psi_m\) to be the smallest strong pseudoprime to all the first m prime bases. If \(n < \psi_m\), then only m Miller tests are needed to find out whether n is prime or not. This means that if we know the exact value of \(\psi_m\), then for integers \(n < \psi_m\) we will have a deterministic primality testing algorithm which is not only easier to implement but also faster than either the Jacobi sum test \[1, 6, 7, 8\] or the elliptic curve test \[5\]. From Alford et al. \[3\] we know that, for any \(m\), the function \(m\) exists.

From Pomerance et al. \[14\] and Jaeschke \[11\] we know the exact value of \(\psi_m\) for \(1 \leq m \leq 8\) and the following facts:

\[
\begin{align*}
\psi_9 & \leq M_9 = 41234 \; 31613 \; 57056 \; 89041 = 4540612081 \cdot 9081224161, \\
\psi_{10} & \leq M_{10} = 155 \; 33605 \; 66073 \; 14320 \; 55410 \; 02401 \; (28 \text{ digits}) \\
& = 22754930352733 \; 22754930352733 \; \cdot \; 68264791058197, \\
\psi_{11} & \leq M_{11} = 5689 \; 71935 \; 26942 \; 02437 \; 03269 \; 72321 \; (29 \text{ digits}) \\
& = 137716125329053 \; 413148375987157.
\end{align*}
\]

Jaeschke \[11\] tabulated all strong pseudoprimes \(< 10^{12}\) to the bases 2, 3, and 5. There are in total 101 of them. Among these 101 numbers there are 75 numbers \(n\) having the form

\[ n = pq \text{ with } p, q \text{ odd primes and } q - 1 = k(p - 1), k = 2, 3, 4. \]

For short we call strong pseudoprimes having the form (1.3) K2-, K3- or K4-spsp’s according as \(k = 2, 3, \text{ or } 4\).

In this paper we tabulate all strong pseudoprimes \(n < 10^{24}\) to the first ten prime bases 2, 3, \ldots, 29 which have the form (1.3). There are in total 44 such numbers, among which six numbers are also spsp(31)’s, and three numbers are spsp’s to both bases 31 and 37. As a result the upper bounds for \(\psi_{10}\) and \(\psi_{11}\) are considerably lowered:

\[
\begin{align*}
\psi_{10} & \leq N_{10} = 19 \; 55097 \; 53037 \; 45565 \; 03981 \; (22 \text{ digits}) \\
& = 31265776261 \; \cdot \; 62531552521, \\
\psi_{11} & \leq N_{11} = 73 \; 95010 \; 24079 \; 41207 \; 09381 \; (22 \text{ digits}) \\
& = 60807114061 \; \cdot \; 121614228121,
\end{align*}
\]

and a 24-digit upper bound for \(\psi_{12}\) is obtained:

\[
\begin{align*}
\psi_{12} & \leq N_{12} = 3186 \; 65857 \; 83403 \; 11511 \; 67461 \; (24 \text{ digits}) \\
& = 399165290211 \cdot \; 798330580441.
\end{align*}
\]

The three integers \(N_{10}, N_{11}, \text{ and } N_{12}\) should have the same style as integers \(M_9, M_{10}, \text{ and } M_{11}\) (above), i.e., insert a small space for each 5 digits. The main
tools used in finding these numbers are biquadratic residue characters and cubic residue characters defined in certain Euclidean domains which are larger than the integer ring \( \mathbb{Z} \). Let \( D \) be such a domain and \( \alpha, \beta, \pi \in D \). If \( \pi \) is a nonunit and such that if \( \pi \mid \alpha \beta \) then either \( \pi \mid \alpha \) or \( \pi \mid \beta \), then \( \pi \) is called irreducible. By a prime we will always mean a positive prime of \( \mathbb{Z} \). Note that a number \( n \) having the form (1.3) is determined by a prime \( q \), and the prime \( q \) is determined by an irreducible \( \pi \). We propose necessary conditions on \( \pi \) for \( n \) to be a strong pseudoprime to one prime base or to the first several prime bases. Thus we have a certain number of candidates \( n \) (determined by candidates for irreducibles) strong pseudoprimes at hand. Then we subject these candidates \( n \) to Miller’s tests, and obtain the desired numbers.

Arnault \[4\] used a sufficient condition for finding K2-spss’s and successfully found a 337-digit K2-spss to all the prime bases < 200. But his condition is too stringent for most K2-spss’s to satisfy. Examples found by the condition are usually much larger than the corresponding \( \psi_m \). Our bounds \( N_{10}, N_{11} \) and \( N_{12} \) could not be found by Arnault’s condition. Jaeschke \[11\] used Jacobi symbols (quadratic residue characters) as his main tools for finding large K2- and K3-spss’s; thus his methods are less effective than ours. See Remarks 3.1 and 3.2 for comparisons in details.

**Notation.** Let \( r \) be a prime and \( b \) a positive integer with \( r \mid b \). Denote by \( \text{ord}_r(b) \) the order of \( b \) in the group \( \mathbb{Z}_r^\ast \). We write \( v_2(x) = s \) iff \( 2^s \mid x \) and \( 2^{s+1} \not\mid x \) for \( x \) a positive integer.

With the above notation we state a lemma which is fundamental for our methods.

**Lemma 1.1** (a part of \[11\] Proposition 1)). Let \( n, p, q, k \) be as in (1.3), and let \( b \) be a positive integer. If \( n \) is an spsp(b), then \( v_2(\text{ord}_r(b)) = v_2(\text{ord}_q(b)) \).

In §2 we recall and state some basic facts concerning biquadratic residue characters, which are necessary in §§3 and 4, where we describe methods for finding K2- and K4-spss’s. Note that the three bounds \( N_{10}, N_{11} \) and \( N_{12} \) are all K2-spss’s which are found in §3. In §5 we recall and state some basic facts concerning cubic residue characters and describe a method for finding K3-spss’s. All K2-, K3- and K4-spss’s < \( 10^{25} \) to the first 10 or 9 prime bases are tabulated.

## 2. Biquadratic residue characters

Throughout this section and the following two sections \( D \) denotes the ring \( \mathbb{Z}[i] \) of Gaussian integers. It is well-known that \( D \) is a Euclidean domain. Let \( \alpha, \beta, \pi \in D \). The norm of \( \alpha, N(\alpha) = \alpha \bar{\alpha} = 1 \) if \( \alpha \) is a unit. The units of \( D \) are \( \pm 1, \pm i \). The irreducibles of \( D \) are \( \pm 1 \pm i \) with norm 2, primes \( \equiv 3 \mod 4 \) and their associates, and non-real elements with prime norms \( \equiv 1 \mod 4 \). A prime \( \equiv 1 \mod 4 \) must be the norm of an irreducible of \( D \). A nonunit \( \alpha \) is called primary if \( \alpha \equiv 1 \) or \( 3 + 2i \mod 4 \). Among four associates of a nonunit \( \alpha \) satisfying \((1 + i) \nmid \alpha \) there is (only) one which is primary.

If \( \pi \) is an irreducible with \( N(\pi) \neq 2, \) then there exists a unique integer \( m, 0 \leq m \leq 3, \) such that \( \alpha^{(N(\pi) - 1)/4} \equiv i^m \mod \pi \). The biquadratic residue character of \( \alpha \), for \( \pi \nmid \alpha \), is defined and denoted by \( \left( \frac{\alpha}{\pi} \right)_4 = i^m \), which is 1, \(-1, i \) or \(-i \). If \( \pi \nmid \alpha \), then \( \left( \frac{\alpha}{\pi} \right)_4 = 0 \). If \( b \) is an odd prime \( \equiv 3 \mod 4 \), then

\[
(2.1) \quad \left( \frac{\alpha}{\pi} \right)_4 \equiv \alpha^{(b^2 - 1)/4} \mod b.
\]
Let \( \pi = a + bi \) and \( \beta = c + di \) be relatively prime primary irreducibles. Then (the general law of biquadratic reciprocity \[10, \text{Theorem 9.2}\])

\[
\left( \frac{\beta}{\pi} \right)_4 = \left( \frac{\pi}{\beta} \right)_4 (-1)^{\frac{N(\beta)-1}{4} \frac{N(\pi)-1}{4}} = \left( \frac{\pi}{\beta} \right)_4 (-1)^{\frac{a-1}{2} \frac{c-1}{2}}.
\]

**Lemma 2.1.** Let \( \pi \) be primary irreducible with prime \( q = N(\pi) \equiv 1 \mod 4 \). Let \( b \in \mathbb{Z} \) with \( q \nmid b \). Then we have

(I) \[10\] Lemma 9.10.1. \( \left( \frac{b}{\pi} \right)_4 = 1 \) iff \( x^4 \equiv b \mod q \) has a solution with \( x \in \mathbb{Z} \) (\( b \) is a fourth power modulo \( q \));

(II) \[10\] Lemma 9.10.2. \( \left( \frac{b}{\pi} \right)_4 = -1 \) iff \( b \) is a square but not a fourth power modulo \( q \).

**Lemma 2.2.** Let \( \pi = r + si \) be primary irreducible. Then we have

(I) \( \left( \frac{1}{\pi} \right)_4 = (-1)^{\frac{-1}{2}} \) \[10\] Proposition 9.8.3(d)];

(II) \( \left( \frac{2}{\pi} \right)_4 = i \) \[9\] Theorem 4.23]; \[10\] Exercise 5.27).

We also need the following three lemmas, the proofs of which are easy.

**Lemma 2.3.** Let \( b \) be prime \( \equiv 3 \mod 4 \) and \( \pi = r + si \) be primary irreducible. Then we have

\[
\left( \frac{b}{\pi} \right)_4 = (-1)^{\frac{p-1}{2}} \left( \frac{\pi}{b} \right)_4.
\]

**Lemma 2.4.** Let \( \beta \) and \( \pi \) be primary irreducible with different prime norms \( \equiv 1 \mod 4 \). If \( b = N(\beta) \), then we have

\[
\left( \frac{b}{\pi} \right)_4 = \left( \frac{\pi \pi^{-1}}{\beta} \right)_4,
\]

where \( \pi^{-1} \) denotes the inverse of \( \pi \) modulo \( b \).

**Lemma 2.5.** Let \( \beta = u + vi \) be primary irreducible with prime \( b = N(\beta) \equiv 1 \mod 4 \) and \( \alpha = c + di \). Then we have

\[
\left( \frac{\alpha}{\beta} \right)_4 \equiv (c - duv^{-1})(b-1)/4 \mod b.
\]

3. K2-Strong Pseudoprimes

Throughout this section let \( \pi \) be a primary irreducible of \( D \) such that \( q = N(\pi) \equiv 1 \mod 4 \) and \( p = (q+1)/2 \) are two primes determined by \( \pi \). We are going to describe a method to compute all composite numbers \( n = pq \), below a given limit (say \( 10^{24} \)), which are strong pseudoprimes to the first several (say \( 10 \)) prime bases. For this purpose we are looking for necessary conditions on \( \pi \) for \( n = pq \) to be a strong pseudoprime, first to a prime base \( b \), then to several prime bases.

**Proposition 3.1.** If \( n = pq \) is a strong pseudoprime to a (not necessarily prime) base \( b \), then

\[
\left( \frac{b}{\pi} \right)_4 = \left( \frac{b}{p} \right).
\]

**Proof.** If \( n = pq \) is an spsp(b) then, by Lemma 1.1,

\[
v_2(\text{ord}_p(b)) = v_2(\text{ord}_q(b)).
\]
If \((\frac{b}{\pi}) = 1\), then \(v_2(\text{ord}_q(b)) = v_2(\text{ord}_p(b)) \leq v_2(p - 1) - 1 = v_2(q - 1) - 2\); thus \(b\) is a fourth power modulo \(q\), and so, by Lemma 2.1(I),
\[
\left(\frac{b}{\pi}\right)_4 = 1 = \left(\frac{b}{p}\right).
\]
If \((\frac{b}{\pi}) = -1\), then \(v_2(\text{ord}_q(b)) = v_2(\text{ord}_p(b)) = v_2(p - 1) = v_2(q - 1) - 1\); thus \(b\) is a square but not a fourth power modulo \(q\), and so
\[
\left(\frac{b}{\pi}\right)_4 = -1 = \left(\frac{b}{p}\right)
\]
by Lemma 2.1(II).

For the rest of this section, let \(p_\alpha = (N(\alpha)+1)/2\) be a positive integer determined by a primary (but not necessarily irreducible) element \(\alpha\) of \(D\). If a prime \(b \equiv 1 \mod 4\), then \(b = \beta\beta\) for some primary irreducible \(\beta\). If \(\gcd(b,N(\alpha)) = 1\), then \(\alpha^{-1}\) denotes the inverse of \(\alpha\) modulo \(b\).

Let
\[
R_2 = \left\{\text{primary } \alpha = x + yi : 0 \leq x, y < 8, \frac{\alpha^2}{b} = (-1)^{\frac{p_\alpha - 1}{2}}\right\} = \{1, 5 + 4i\}.
\]

By Lemma 2.2(II) and Proposition 3.1 we have

**Lemma 3.1.** If \(n = pq\) is an spsp(2), then there exists \(\alpha \in R_2\) such that \(\pi \equiv \alpha \mod 8\).

For a prime \(b \equiv 3 \mod 4\), let
\[
R_b = \left\{\alpha = x + yi : 0 \leq x, y < 4b, \alpha \equiv 1 \mod 4, \left(\frac{\alpha}{b}\right)_4 = \left(\frac{p_\alpha}{b}\right)\right\};
\]
and for a prime \(b \equiv 1 \mod 4\), let
\[
R_b = \left\{\alpha = x + yi : 0 \leq x, y < 4b, \alpha \equiv 1 \mod 4, \left(\frac{\alpha\alpha^{-1}}{b}\right)_4 = \left(\frac{p_\alpha}{b}\right)\right\}.
\]

Using (2.3) for \(b \equiv 3 \mod 4\) and Lemma 2.5 for \(b \equiv 1 \mod 4\), it is easy to compute the sets:

\[
R_3 = \{1, 5\}; \quad R_5 = \{1, 9\};
\]

\[
R_7 = \{1, 13, 21, 8i, 21 + 20i, 1 + 8i, 1 + 20i, 13 + 8i, 13 + 20i,
17 + 4i, 17 + 24i, 25 + 4i, 25 + 24i\};
\]

\[
R_{11} = \{1, 5 + 8i, 5 + 36i, 9 + 12i, 9 + 32i, 13 + 12i, 13 + 32i, 17 + 8i,
17 + 36i, 21, 25, 29, 29 + 20i, 29 + 24i, 37, 37 + 20i,
37 + 24i, 41, 5 + 12i, 5 + 32i, 17 + 12i, 17 + 32i, 29 + 8i,
29 + 36i, 33 + 16i, 33 + 20i, 33 + 24i, 33 + 28i, 37 + 8i, 37 + 36i\};
\]

and

\[
R_{13} = \{1, 1 + 4i, 1 + 48i, 25, 25 + 4i, 25 + 48i, 29 + 12i, 29 + 40i,
33, 33 + 24i, 33 + 28i, 37, 41, 45, 45 + 24i, 45 + 28i,
49 + 12i, 49 + 40i, 5 + 24i, 5 + 28i, 13 + 4i, 13 + 16i, 13 + 36i, 13 + 48i,
21 + 24i, 21 + 28i, 33 + 8i, 33 + 44i, 45 + 8i, 45 + 44i\}.
\]

By Lemmas 2.3 and 2.4 and Proposition 3.1 we have
Lemma 3.2. Let $b$ be an odd prime. If $n = pq$ is an spsp($b$) and $\pi \equiv 1 \mod 4$, then there exists $\alpha \in R_b$ such that $\pi \equiv \alpha \mod 4b$.

Let $m = 4 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 120120$. Applying the Chinese Remainder Theorem, it is easy to compute the set

$$R = \{x + yi : 0 \leq x, y < m, x + yi \equiv 0 \mod 4b\},$$

which has cardinality $\#R = 2 \cdot 2 \cdot 2 \cdot 12 \cdot 30 \cdot 30 = 86400$. By Lemmas 3.1 and 3.2 and the Chinese Remainder Theorem we have

Proposition 3.2. If $n = pq$ is an spsp to the bases 2, 3, 5, 7, 11 and 13, then there exists $\alpha \in R$ such that $\pi \equiv \alpha \mod m$.

Now we are ready to describe a procedure to compute all K2-spsp’s $< L$, to the first $h(\geq 6)$ prime bases.

PROCEDURE Finding-K2-spsp;
BEGIN
For every $x + yi \in R, u \geq 0, v \geq 0, u + v \leq \frac{\sqrt{m} \pi}{m} + 1$ Do
begin
$q \leftarrow (x + um)^2 + (y + vm)^2; p \leftarrow (q + 1)/2; n \leftarrow p \cdot q$;
If $n$ is an spsp to the first $h$ prime bases then output $n, p$ and $q$;
$q \leftarrow (x - um)^2 + (y + vm)^2; p \leftarrow (q + 1)/2; n \leftarrow p \cdot q$;
If $n$ is an spsp to the first $h$ prime bases then output $n, p$ and $q$;
end
END.

The Pascal program (with multi-precision package partially written in Assembly language) ran about 33 hours on my PC486/66 to get all K2-spsp’s $< 10^{24}$ to the bases 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29, listed in Table 1. There are in total 41 numbers, among which six numbers are spsp(31), and three numbers are spsp’s to both bases 31 and 37.

Example 3.1.

$$n = N_{10} = 1955097530374556503981 = 31265776261 \cdot 62531552521$$

is the smallest K2-spsp to the first 10 prime bases.

$q = 225739^2 + 107580^2, \quad \pi = -225739 + 107580i \equiv 14501 + 107580i \mod m,$

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{b}{\pi}\right)_4 = \begin{cases} -1, & \text{for } b = 2, 7, 13, 19 \text{ and } 29; \\ 1, & \text{for } b = 3, 5, 11, 17 \text{ and } 23. \end{cases} \quad \square$$

Remark 3.1. The 22–digit number $N_{10}$ in Example 3.1 yields the lowered upper bound for $\psi_{10}$. The old bound $M_{10}$ in §1 has 28 decimal digits, which is a K3-spsp found by Jaeschke [11], where about $2275493052733 \cdot 400 \approx 1.02 \cdot 10^7$ candidates were tested. If the method of Jaeschke [11] for finding large K2-spsp’s had been used for finding the number $N_{10}$, about $31265776261 \cdot 15 \approx 1.015 \cdot 10^8$ candidates would have subjected to the Miller tests. With our method less than 86400 · 6 ≈ 5.184 · 10^5 candidates were tested, and the whole calculation took about 40 minutes on my PC486/66.

Remark 3.2. The only example spsp to the first 10 prime bases given in Arnault [4] has 46 decimal digits.
Table 1. List of all K2-spsp’s < $10^{24}$ to the first 10 prime bases

<table>
<thead>
<tr>
<th>number</th>
<th>factorization</th>
<th>spsp-base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>31 37 41</td>
</tr>
<tr>
<td>1955097</td>
<td>5303714556503981</td>
<td>0 0 0</td>
</tr>
<tr>
<td>2690332</td>
<td>9682556326725221</td>
<td>0 0 0</td>
</tr>
<tr>
<td>3080476</td>
<td>16946586653821</td>
<td>0 0 1</td>
</tr>
<tr>
<td>7395010</td>
<td>24079420708231</td>
<td>1 0 0</td>
</tr>
<tr>
<td>8322676</td>
<td>92468418807061</td>
<td>0 0 0</td>
</tr>
<tr>
<td>9363077</td>
<td>444494472257261</td>
<td>0 0 0</td>
</tr>
<tr>
<td>14677609</td>
<td>160350838689301</td>
<td>0 0 0</td>
</tr>
<tr>
<td>20403862</td>
<td>733296847400661</td>
<td>0 0 1</td>
</tr>
<tr>
<td>4382302</td>
<td>471716234754141</td>
<td>0 0 0</td>
</tr>
<tr>
<td>53174906</td>
<td>711723993213881</td>
<td>0 1 0</td>
</tr>
<tr>
<td>55571792</td>
<td>871197983341781</td>
<td>0 0 0</td>
</tr>
<tr>
<td>63251216</td>
<td>292423798286901</td>
<td>0 0 1</td>
</tr>
<tr>
<td>66990115</td>
<td>045864781688781</td>
<td>0 0 1</td>
</tr>
<tr>
<td>74900868</td>
<td>097492114932621</td>
<td>0 0 0</td>
</tr>
<tr>
<td>81867072</td>
<td>311110130740741</td>
<td>0 1 0</td>
</tr>
<tr>
<td>85985927</td>
<td>737923413798461</td>
<td>0 1 1</td>
</tr>
<tr>
<td>9445517</td>
<td>51190637525501</td>
<td>0 0 0</td>
</tr>
<tr>
<td>134155760</td>
<td>348927603751301</td>
<td>0 0 0</td>
</tr>
<tr>
<td>164280218</td>
<td>643672633986221</td>
<td>1 0 0</td>
</tr>
<tr>
<td>168232033</td>
<td>789138283986261</td>
<td>0 0 1</td>
</tr>
<tr>
<td>16899564</td>
<td>08374452545381</td>
<td>0 0 0</td>
</tr>
<tr>
<td>24795573</td>
<td>307378767707901</td>
<td>0 0 0</td>
</tr>
<tr>
<td>31356651</td>
<td>41534839556661</td>
<td>0 0 0</td>
</tr>
<tr>
<td>31868558</td>
<td>834031151167461</td>
<td>1 1 0</td>
</tr>
<tr>
<td>360681321</td>
<td>802296952566181</td>
<td>1 0 0</td>
</tr>
<tr>
<td>37197464</td>
<td>578582748133501</td>
<td>0 0 0</td>
</tr>
<tr>
<td>37972084</td>
<td>842671685653341</td>
<td>0 0 0</td>
</tr>
<tr>
<td>398206323</td>
<td>4055039262661</td>
<td>0 0 0</td>
</tr>
<tr>
<td>44957957</td>
<td>324649310270021</td>
<td>1 0 0</td>
</tr>
<tr>
<td>50081683</td>
<td>57545360593041</td>
<td>0 0 0</td>
</tr>
<tr>
<td>552727800</td>
<td>697763694556181</td>
<td>1 0 0</td>
</tr>
<tr>
<td>592245699</td>
<td>799679504737021</td>
<td>1 0 0</td>
</tr>
<tr>
<td>667636712</td>
<td>015520329618581</td>
<td>1 0 1</td>
</tr>
<tr>
<td>767218076</td>
<td>27153771976431</td>
<td>0 1 0</td>
</tr>
<tr>
<td>787275625</td>
<td>773786753842101</td>
<td>0 0 0</td>
</tr>
<tr>
<td>804312078</td>
<td>555704182158061</td>
<td>0 0 0</td>
</tr>
<tr>
<td>885194158</td>
<td>945172723165341</td>
<td>0 0 0</td>
</tr>
<tr>
<td>919429103</td>
<td>53163178344061</td>
<td>0 0 0</td>
</tr>
<tr>
<td>959800605</td>
<td>00761974191261</td>
<td>0 0 0</td>
</tr>
<tr>
<td>959872525</td>
<td>439982764342041</td>
<td>0 0 0</td>
</tr>
<tr>
<td>995879862</td>
<td>373955074887861</td>
<td>0 0 1</td>
</tr>
</tbody>
</table>
### Table 2. List of all K4-spsp’s \( < 10^{24} \) to the first 9 prime bases

<table>
<thead>
<tr>
<th>number</th>
<th>factorization</th>
<th>spsp-base</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>37</td>
</tr>
<tr>
<td>1638219926987824973501</td>
<td>20513525581 · 82054102321</td>
<td>0</td>
</tr>
<tr>
<td>22816011932095901892127</td>
<td>75524850103 · 302099400409</td>
<td>0</td>
</tr>
<tr>
<td>5305015467573141089751</td>
<td>115163095951 · 460652383801</td>
<td>0</td>
</tr>
<tr>
<td>62226037292690827434451</td>
<td>124725736411 · 498902945641</td>
<td>0</td>
</tr>
<tr>
<td>746160999219444440751</td>
<td>136579290151 · 546317160601</td>
<td>0</td>
</tr>
<tr>
<td>1366758997811482107</td>
<td>137502006883 · 550008027529</td>
<td>0</td>
</tr>
<tr>
<td>88390841560813963877707</td>
<td>148652986483 · 594611945929</td>
<td>0</td>
</tr>
<tr>
<td>180539110735640469792951</td>
<td>212508300271 · 85003201081</td>
<td>0</td>
</tr>
<tr>
<td>190724964865903509771451</td>
<td>218360347171 · 873441388681</td>
<td>0</td>
</tr>
<tr>
<td>20072678585547132616207</td>
<td>224012714983 · 896050859929</td>
<td>0</td>
</tr>
<tr>
<td>287772220009667093616451</td>
<td>268222025611 · 1072888102441</td>
<td>0</td>
</tr>
<tr>
<td>372098606182110248554387</td>
<td>304999428763 · 1219997715049</td>
<td>0</td>
</tr>
<tr>
<td>79137550532200984077727</td>
<td>444796443703 · 1779185774809</td>
<td>0</td>
</tr>
<tr>
<td>93910965114428487866451</td>
<td>484538350171 · 1938153400681</td>
<td>1</td>
</tr>
</tbody>
</table>

### 4. K4-strong pseudoprimes

To compute all composite numbers \( n = pq \) below a given limit, of the form (1.3), with \( k = 4 \) and \( q = N(\pi) \) for some primary irreducible \( \pi \) of \( D \), which are strong pseudoprimes to the first several prime bases, the procedure is a little different from the case \( k = 2 \). We give equivalent conditions on \( \pi \) for \( n \) to be a psp (instead of an spsp) to one or several prime bases. We subject those candidates \( n \), with \( \pi \) satisfying the conditions, to Miller tests to decide whether they are spsp’s or not.

Let \( b \) be a positive integer (not necessarily prime). It is easy to prove that

\[
(4.1) \quad n = pq \text{ is a psp}(b) \iff \left( \frac{b}{\pi} \right)_4 = 1.
\]

A procedure based on (4.1), lemmas in §2 and the Chinese Remainder Theorem ran about 61 hours on my PC486/66 to get all K4-spsp’s \( < 10^{24} \) to the first 9 prime bases up to 23, listed in Table 2. There are in total 14 numbers, among which only one is spsp(29).

### 5. Cubic residue characters and K3-strong pseudoprimes

In this section \( D \) denotes the ring

\[
\mathbb{Z}[\omega] = \{x + y\omega : x, y \in \mathbb{Z}\},
\]

where \( \omega = \frac{-1 + \sqrt{-3}}{2} \). It is well-known that \( D \) is a Euclidean domain. Let \( \alpha, \beta, \pi \in D \). The norm of \( \alpha = x + y\omega \) is \( N(\alpha) = \alpha\overline{\alpha} = x^2 - xy + y^2 \). The units in \( D \) are the only six elements with norm 1 : \( \pm 1, \pm \omega, \pm \omega^2 \). The irreducibles of \( D \) are \( \pm(1 - \omega), \pm(1 + 2\omega), \pm(2 + \omega) \) with norm 3; primes \( \equiv 2 \) (mod 3) and their associates; and non-real elements with prime norm \( \equiv 1 \) (mod 3). A prime \( \equiv 1 \) (mod 3) must be the norm of an irreducible of \( D \); and the prime 3 is \( -\omega^2(1 - \omega)^2 \).
Table 3. List of all K3-spsp’s < 10^{24} to the first 9 prime bases

<table>
<thead>
<tr>
<th>number</th>
<th>factorization</th>
<th>spsp-base</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 12984 16254 13806 73761</td>
<td>25251958093 · 75755874277</td>
<td>0 0 1</td>
</tr>
<tr>
<td>340 96886 96900 51855 04481</td>
<td>106609704013 · 319829112037</td>
<td>0 0 0</td>
</tr>
<tr>
<td>559 80401 34753 42797 35681</td>
<td>136602100213 · 409806300637</td>
<td>0 0 0</td>
</tr>
<tr>
<td>1976 49490 97737 83580 89281</td>
<td>256706662021 · 770119986061</td>
<td>0 0 0</td>
</tr>
<tr>
<td>2361 94333 86845 27087 65441</td>
<td>280591241173 · 841773723517</td>
<td>0 0 0</td>
</tr>
<tr>
<td>3590 07177 34550 26409 08801</td>
<td>345932159701 · 1037796479101</td>
<td>0 0 1</td>
</tr>
<tr>
<td>4759 46318 31244 21564 84321</td>
<td>398307384781 · 1194922154341</td>
<td>0 0 0</td>
</tr>
<tr>
<td>5848 91146 05935 09248 24801</td>
<td>441546957133 · 132460871397</td>
<td>0 0 0</td>
</tr>
<tr>
<td>5979 58575 96757 02751 62721</td>
<td>446452153453 · 1339356460357</td>
<td>1 0 0</td>
</tr>
<tr>
<td>6091 09964 84997 37599 17761</td>
<td>450595888741 · 1351787666221</td>
<td>1 0 1</td>
</tr>
<tr>
<td>6929 26578 71186 76488 99521</td>
<td>480599132581 · 1441797397741</td>
<td>0 0 0</td>
</tr>
</tbody>
</table>

A nonunit α is called primary if α ≡ 2 (mod 3). Among six associates of a nonunit α satisfying \( 1 - \omega \) \( \not\mid \alpha \), there is (only) one which is primary. If \( \pi \) is an irreducible with \( N(\alpha) \neq 3 \) and \( \pi \not\mid \alpha \), there is a unique integer \( m = 0, 1, \) or \( 2 \) such that \( \alpha^{(N(\alpha)-1)/3} \equiv \omega^m \mod \pi \). The cubic residue character of \( \alpha \) modulo \( \pi \), with \( N(\alpha) \neq 3 \) and \( \pi \not\mid \alpha \), is defined and denoted by \( (\frac{\omega}{\pi})_3 = \omega^m \), which is \( 1, \omega \) or \( \omega^2 = -1 - \omega \). If \( \pi \mid \alpha \), then \( (\frac{\omega}{\pi})_3 = 0 \). We have \( (\frac{\omega}{\pi})_3 = 1 \iff \pi \equiv 1 \mod 2 \) [10, Proposition 9.1].

Let \( \pi \) be primary irreducible with prime \( q = N(\pi) \equiv 1 \mod 3 \). Let \( b \in \mathbb{Z} \) with \( q \not\mid b \). Then we have \( (\frac{b}{\pi})_3 = 1 \iff x^3 \equiv b \mod q \) has a solution with \( x \in \mathbb{Z} \), i.e., \( \equiv b \) is a cubic residue modulo \( q \) [10, Proposition 9.3.3(a)].

Let \( \pi \) and \( \beta \) be primary irreducibles with \( N(\pi) \neq 3, N(\beta) \neq 3, \) and \( N(\pi) \neq N(\beta) \). Then \( (\frac{\beta}{\pi})_3 = (\frac{\pi}{\beta})_3 \) (The law of cubic reciprocity [10, Theorem 9.1]).

Suppose that \( N(\pi) \neq 3 \). If \( \pi = q \) is rational, write \( q = 3m - 1 \); if \( \pi = u + \sqrt{-3} \omega \) is a primary complex irreducible, write \( u = 3m - 1 \). Then we have \( (\frac{1+\omega}{\pi})_3 = \omega^{2m} \) (Supplement to the Cubic Reciprocity Law [10, Theorem 9.1]).

Let \( \pi \) be a primary irreducible of \( D \), and \( q = N(\pi) \equiv 1 \mod 3 \) and \( p = (q + 2)/3 \) two primes determined by \( \pi \). It is easy to prove that if \( n = pq \) is a strong pseudoprime to the (not necessarily primary) base \( b \), then

\[
(\frac{b}{\pi})_3 = 1 \quad \text{and} \quad (\frac{b}{p})_3 = (\frac{b}{q})_3.
\]

A procedure based on (5.1), the Cubic Reciprocity Law and its Supplement, and the Chinese Remainder Theorem ran about 8 hours on my PC486/66 to get all K3-spsp’s < 10^{24} to the first 9 prime bases up to 23, listed in Table 3. There are in total 11 numbers, among which only two are spsp(29)’s.

Acknowledgments

I thank Professors F. Arnault, W. Bosma, A. K. Lenstra, H. W. Lenstra, Jr., C. Pomerance, G. Robin, and S. S. Wagstaff, Jr. for their sending me reprints or preprints concerning this subject or other topics in computational number theory. Special thanks go to the referee for helpful comments that improved the paper.
REFERENCES


Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, P. R. China

State Key Laboratory of Information Security, Graduate School USTC, 100039 Beijing, P. R. China

E-mail address: zhangzix@mail.ahwhptt.net.cn