MATHEMATICS OF COMPUTATION
Volume 70, Number 234, Pages 863–872
S 0025-5718(00)01215-1
Article electronically published on February 17, 2000

FINDING STRONG PSEUDOPRIMES TO SEVERAL BASES

ZHENXIANG ZHANG

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

Abstract. Define ψ_m to be the smallest strong pseudoprime to all the first m prime bases. If we know the exact value of ψ_m, we will have, for integers $n < \psi_m$, 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, ψ_m are known for $1 \leq m \leq 8$. Upper bounds for ψ_9, ψ_{10} and ψ_{11} were given by Jaeschke.

In this paper we tabulate all strong pseudoprimes (spsp's) $n < 10^{24}$ to the first ten prime bases $2, 3, \cdots, 29$, which have the form $n = p\,q$ 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 37. As a result the upper bounds for ψ_{10} and ψ_{11} are lowered from 28- and 29-decimal-digit numbers to 22-decimal-digit numbers, and a 24-decimal-digit upper bound for ψ_{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

$$b^{n-1} \equiv 1 \mod n \tag{1.1}$$

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 psp(b) for short). It is well-known that for each base b, there are infinitely many psp(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

Received by the editor August 1, 1997 and, in revised form, June 22, 1998 and May 24, 1999.

2000 *Mathematics Subject Classification.* Primary 11Y11, 11A15, 11A51.

Key words and phrases. Strong pseudoprimes, Rabin-Miller test, biquadratic residue characters, cubic residue characters, Chinese remainder theorem.

Supported by the China State Educational Commission Science Foundation and by NSF of China Grant 10071001.

$n-1 = 2^s d$ with d odd. If n is prime, then

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

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 compoite 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 ψ_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 ψ_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 ψ_m exists.

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

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

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

$$\text{(1.3)}\qquad n = p\,q \text{ with } p, q \text{ odd primes and } q-1 = k(p-1), k = 2, 3, 4.$$

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

In this paper we tabulate all strong pseudoprimes $n < 10^{24}$ to the first ten prime bases $2, 3, \cdots, 29$ 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 ψ_{10} and ψ_{11} are considerably lowered:

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

and a 24-digit upper bound for ψ_{12} is obtained:

$$\begin{aligned}
\psi_{12} \leq N_{12} &= 3186\,65857\,83403\,11511\,67461 \text{ (24 digits)} \\
&= 399165290211 \cdot 798330580441.
\end{aligned}$$

The three integers N_{10}, N_{11}, and N_{12}, should have the same style as integers M_9, M_{10}, 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 π is a nonunit and such that if $\pi \mid \alpha\beta$ then either $\pi \mid \alpha$ or $\pi \mid \beta$, then π 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 π. We propose necessary conditions on π 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-spsp's and successfully found a 337-digit K2-spsp to all the prime bases < 200. But his condition is too stringent for most K2-spsp's to satisfy. Examples found by the condition are usually much larger than the corresponding ψ_m. Our bounds N_{10}, N_{11} and N_{12} could not be found by Arnault's condition. Jaeschke [11] used Jacobi sysbols (quadratic residue characters) as his main tools for finding large K2- and K3-spsp'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 $r \nmid b$. Denote by $\mathrm{ord}_r(b)$ the order of b in the group $\mathbb{Z}_r^*$. We write $v_2(x) = s$ iff $2^s \mid x$ and $2^{s+1} \nmid x$ 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* $v_2(\mathrm{ord}_p(b)) = v_2(\mathrm{ord}_q(b))$.

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-spsp's. Note that the three bounds N_{10}, N_{11} and N_{12} are all K2-spsp'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-spsp's. All K2-, K3- and K4-spsp's $< 10^{24}$ 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 $\alpha, N(\alpha) = \alpha\bar{\alpha} = 1$ iff α 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 α is called primary if $\alpha \equiv 1$ or $3 + 2i \mod 4$. Among four associates of a nonunit α satisfying $(1 + i) \nmid \alpha$ there is (only) one which is primary.

If π 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 α, 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 $\pi \mid \alpha$, then $\left(\frac{\alpha}{\pi}\right)_4 = 0$. If b is an odd prime $\equiv 3 \mod 4$, then

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{(b^2-1)/4} \mod b. \tag{2.1}$$

Let $\pi = a + bi$ and $\beta = c + di$ be relatively prime primary irreducibles. Then (the general law of biquadratic reciprocity [10, 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 π 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) $\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{r-1}{2}}$ [10, Proposition 9.8.3(d)]*;*

(II) $\left(\frac{2}{\pi}\right)_4 = i^{\frac{rs}{2}}$ [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*

$$\left(\frac{b}{\pi}\right)_4 = (-1)^{\frac{r-1}{2}} \left(\frac{\pi}{b}\right)_4.$$

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

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

where π^{-1} denotes the inverse of π 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 π 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 π. 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 π 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,

$$v_2(\mathrm{ord}_p(b)) = v_2(\mathrm{ord}_q(b)).$$

If $\left(\frac{b}{p}\right) = 1$, then $v_2(\mathrm{ord}_q(b)) = v_2(\mathrm{ord}_p(b)) \leq v_2(p-1) - 1 = v_2(q-1) - 2$; 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 $\left(\frac{b}{p}\right) = -1$, then $v_2(\mathrm{ord}_q(b)) = v_2(\mathrm{ord}_p(b)) = v_2(p-1) = v_2(q-1) - 1$; 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 α of D. If a prime $b \equiv 1 \mod 4$, then $b = \beta\bar{\beta}$ for some primary irreducible β. If $\gcd(b, N(\alpha)) = 1$, then α^{-1} denotes the inverse of α modulo b.

Let

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

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

$$R_b = \left\{\alpha = x + yi : 0 \leq x, y < 4b, \alpha \equiv 1 \mod 4, \left(\frac{\alpha\overline{\alpha^{-1}}}{\beta}\right)_4 = \left(\frac{p_\alpha}{b}\right)\right\}.$$

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:

$$R_3 = \{1, 5\}; \qquad R_5 = \{1, 9\};$$

$$\begin{aligned} R_7 = \{&1, 13, 21 + 8i, 21 + 20i, 1 + 8i, 1 + 20i, 13 + 8i, 13 + 20i, \\ &17 + 4i, 17 + 24i, 25 + 4i, 25 + 24i\}; \end{aligned}$$

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

and

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

By Lemmas 2.3 and 2.4 and Proposition 3.1 we have

Lemma 3.2. *Let b be an odd prime. If $n = p\,q$ 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

$$R = \{x + yi : 0 \le x, y < m, x + yi (\text{mod } 4b) \in R_b \text{ for } b = 2, 3, 5, 7, 11 \text{ and } 13\},$$

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 $n = p\,q$ 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 $h (\ge 6)$ prime bases.

```
PROCEDURE Finding-K2-spsp;
BEGIN
   For every $x + yi \in R, u \ge 0, v \ge 0, u + v \le \frac{\sqrt[4]{8L}}{m} + 1$ 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.

$$n = N_{10} = 19\,55097\,53037\,45565\,03981 = 31265776261 \cdot 62531552521$$

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

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

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

Remark 3.1. The 22−digit number N_{10} in Example 3.1 yields the lowered upper bound for ψ_{10}. The old bound M_{10} in §1 has 28 decimal digits, which is a K3-spsp found by Jaeschke [11], where about $\frac{22754930352733}{892371480} \cdot 400 \approx 1.02 \cdot 10^7$ cadidates were tested. If the method of Jaeschke [11] for finding large K2-spsp's had been used for finding the number N_{10}, about $\frac{31265776261}{4620} \cdot 15 \approx 1.015 \cdot 10^8$ candidates would have subjected to the Miller tests. With our method less than $86400 \cdot 6 \approx 5.184 \cdot 10^5$ 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

		spsp-base		
number	factorization	31	37	41
19 55097 53037 45565 03981	31265776261 · 62531552521	0	0	0
26 90332 96825 63267 25221	36676511341 · 73353022681	0	0	0
30 08407 16946 58668 53821	38784063541 · 77568127081	0	0	1
73 95010 24079 41207 09381	60807114061 · 121614228121	1	0	0
83 22676 92468 41880 70621	64508437141 · 129016874281	0	0	0
93 63077 44449 44722 57261	68421770821 · 136843541641	0	0	0
146 77609 16035 03876 89301	85666823101 · 171333646201	0	0	0
204 03862 73329 86474 00661	101004610621 · 202009221241	0	0	1
438 32302 47171 62347 54141	148041045781 · 296082091561	0	0	0
531 74906 71172 39932 13881	163056595561 · 326113191121	0	1	0
555 71792 87119 79833 41781	166691020861 · 333382041721	0	0	0
632 51216 29424 37982 86901	177835902301 · 355671804601	0	0	1
669 90115 04586 47816 88781	183016549861 · 366033099721	0	0	1
749 00686 09749 21149 32621	193520911141 · 387041822281	0	0	0
818 67072 31111 01307 40741	202320379981 · 404640759961	0	1	0
859 85927 73792 34137 98461	207347447221 · 414694894441	0	1	1
944 65534 51190 61375 25501	217331008501 · 434662017001	0	0	0
1341 55760 34892 76307 51301	258993977101 · 517987954201	0	0	0
1642 80218 64367 26339 86221	286600958341 · 573201916681	1	0	0
1682 32033 78913 82839 62861	290027614021 · 580055228041	0	0	1
1689 95964 08374 44559 45381	290685366061 · 581370732121	0	0	0
2479 55734 30737 87677 07901	352104909301 · 704209818601	0	0	0
3135 65701 41534 83953 56661	395958142621 · 791916285241	0	0	0
3186 65857 83403 11511 67461	399165290221 · 798330580441	1	1	0
3606 81321 80229 69255 66181	424665351661 · 849330703321	1	0	0
3719 74764 57852 27481 33501	431262544501 · 862525089001	0	0	0
3797 20840 84267 16856 53341	435729756181 · 871459512361	0	0	0
3982 06433 02455 41305 92661	446209834621 · 892419669241	0	1	0
4495 97567 32464 93102 70021	474129500941 · 948259001881	0	0	0
5008 16683 57545 63605 90341	500408175181 · 1000816350361	0	1	0
5527 27880 69776 36945 56181	525703281661 · 1051406563321	1	1	0
5922 45699 79967 95047 37021	544171709941 · 1088343419881	0	0	1
6676 36712 01552 03296 18581	577770158461 · 1155540316921	1	1	0
7672 18076 27153 77191 64381	619361799061 · 1238723598121	0	1	0
7872 75625 77378 67538 42101	627405620701 · 1254811241401	0	0	0
8043 12708 55570 41821 58061	634157988421 · 1268315976841	0	0	0
8851 94158 94517 72231 65341	665279700181 · 1330559400361	0	0	0
9194 29103 51631 37183 44061	678022530421 · 1356045060841	0	0	1
9598 00605 00761 97414 91261	692748368821 · 1385496737641	0	0	0
9598 72525 43998 27643 42041	692774323081 · 1385548646161	0	0	0
9958 79862 37395 06748 87861	705648589021 · 1411297178041	0	0	1

TABLE 2. List of all K4-spsp's $< 10^{24}$ to the first 9 prime bases

		spsp-base		
number	factorization	29	31	37
16 83218 92698 78249 73501	20513525581 · 82054102321	0	0	0
228 16011 93209 59018 92127	75524850103 · 302099400409	0	0	0
530 50154 67573 14410 89751	115163095951 · 460652383801	0	0	0
622 26037 29269 08274 34451	124725736411 · 498902945641	0	0	1
746 15609 99219 44445 40751	136579290151 · 546317160601	0	0	0
756 27207 58699 78114 82107	137502006883 · 550008027529	0	0	0
883 90841 56081 39638 77707	148652986483 · 594611945929	0	0	0
1806 39110 73564 04697 92951	212508300271 · 850033201081	0	1	0
1907 24964 86590 35097 71451	218360347171 · 873441388681	0	1	0
2007 26785 89554 71326 16207	224012714983 · 896050859929	0	0	0
2877 72220 09066 70936 16451	268222025611 · 1072888102441	0	0	0
3720 98606 18211 02485 54387	304999428763 · 1219997715049	0	0	0
7913 75505 32200 98040 77727	444796443703 · 1779185774809	0	0	0
9391 09651 14428 48478 66451	484538350171 · 1938153400681	1	0	1

4. K4-STRONG PSEUDOPRIMES

To compute all composite numbers $n = p\,q$ below a given limit, of the form (1.3), with $k = 4$ and $q = N(\pi)$ for some primary irreducible π 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 π for n to be a psp (instead of an spsp) to one or several prime bases. We subject those candidates n, with π satifying 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

$$n = p\,q \text{ is a psp}(b) \text{ iff } \left(\frac{b}{\pi}\right)_4 = 1. \tag{4.1}$$

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 $N(\alpha) = \alpha\bar{\alpha} = x^2 - xy + y^2$. 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 $\equiv 2 \pmod 3$ and their associates; and non-real elements with prime norm $\equiv 1 \pmod 3$. A prime $\equiv 1 \pmod 3$ must be the norm of an irreducible of D; and the prime $3 = -\omega^2(1-\omega)^2$.

TABLE 3. List of all K3-spsp's $< 10^{24}$ to the first 9 prime bases

		spsp-base		
number	factorization	29	31	37
19 12984 16254 13806 73761	$25251958093 \cdot 75755874277$	0	0	1
340 96886 96900 51855 04481	$106609704013 \cdot 319829112037$	0	0	0
559 80401 34753 42797 35681	$136602100213 \cdot 409806300637$	0	0	0
1976 94930 97737 83580 89281	$256706662021 \cdot 770119986061$	0	0	0
2361 94333 86845 27687 65441	$280591241173 \cdot 841773723517$	0	0	0
3590 07177 34550 26409 08801	$345932159701 \cdot 1037796479101$	0	0	1
4759 46318 31244 21564 84321	$398307384781 \cdot 1194922154341$	0	0	0
5848 91146 05935 09248 24801	$441546957133 \cdot 1324640871397$	0	0	0
5979 58575 96757 02751 62721	$446452153453 \cdot 1339356460357$	1	0	0
6091 09964 84997 37599 17761	$450595888741 \cdot 1351787666221$	1	0	1
6929 26578 71186 76488 99521	$480599132581 \cdot 1441797397741$	0	0	0

A nonunit α is called primary if $\alpha \equiv 2 \pmod 3$. Among six associates of a nonunit α satisfying $(1-\omega) \nmid \alpha$, there is (only) one which is primary. If π is an irreducible with $N(\pi) \neq 3$ and $\pi \nmid \alpha$, there is a unique integer $m = 0, 1$, or 2 such that $\alpha^{(N(\pi)-1)/3} \equiv \omega^m \mod \pi$. The cubic residue character of α modulo π, with $N(\pi) \neq 3$ and $\pi \nmid \alpha$, is defined and denoted by $\left(\frac{\alpha}{\pi}\right)_3 = \omega^m$, which is $1, \omega$ or $\omega^2 = -1 - \omega$. If $\pi \mid \alpha$, then $\left(\frac{\alpha}{\pi}\right)_3 = 0$. We have $\left(\frac{2}{\pi}\right)_3 = 1$ iff $\pi \equiv 1 \mod 2$ [10, Proposition 9.1].

Let π be primary irreducible with prime $q = N(\pi) \equiv 1 \mod 3$. Let $b \in \mathbb{Z}$ with $q \nmid b$.Then we have $\left(\frac{b}{\pi}\right)_4 = 1$ iff $x^3 \equiv b \mod q$ has a solution with $x \in \mathbb{Z}$, i.e., iff b is a cubic residue modulo q [10, Proposition 9.3.3(a)].

Let π and β be primary irreducibles with $N(\pi) \neq 3, N(\beta) \neq 3$, and $N(\pi) \neq N(\beta)$. Then $\left(\frac{\beta}{\pi}\right)_3 = \left(\frac{\pi}{\beta}\right)_3$ (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 $\pi = u + v\omega$ is a primary complex irreducible, write $u = 3m - 1$. Then we have $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$ (Supplemment to the Cubic Reciprocity Law [10, Theorem 9.1′]).

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

$$\left(\frac{b}{\pi}\right)_3 = 1 \quad \text{and} \quad \left(\frac{b}{p}\right) = \left(\frac{b}{q}\right). \tag{5.1}$$

A procedure based on (5.1), the Cubic Reciprocity Law and its Supplemment, 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

1. L.M.Adleman, C.Pomerance and R.S.Rumely, *On distinguishing prime numbers from composite numbers.*, Annals of Math., **117** (1983), 173–206. MR **84e:**10008
2. W.R.Alford, A.Granville and C.Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math., **140** (1994), 703–722. MR **95k:**11114
3. W.R.Alford, A.Granville and C.Pomerance, *On the difficulty of finding reliable witnesses*, Algorithmic Number Theory, pp.1-16, Lecture Notes in Computer Science, vol. 877, Springer-Verlag, Berlin, 1994. MR **96d:**11136
4. F.Arnault, *Rabin-Miller primality test: Composite numbers which pass it*, Math. Comp., **64** (1995), 355–361. MR **95c:**11152
5. A.O.L.Atkin and F.Morain, *Elliptic curves and primality proving*, Math. Comp., **61** (1993), 29–68. MR **93m:**11136
6. W.Bosma and M.P. van der Hulst, *Primality proving with cyclotomy*, thesis, Univ. of Amsterdam, 1990.
7. H.Cohen and A.K.Lenstra, *Implementation of a new primality test*, Math. Comp., **48** (1987), 103-121. MR **88c:**11080
8. H.Cohen and H.W.Lenstra,Jr., *Primality testing and Jacobi sums*, Math. Comp., **42** (1984), 297–330. MR **86g:**11078
9. D.A.Cox, *Primes of the form* $x^2 + ny^2$, Interscience, New York, 1989. MR **90m:**11016
10. K.Ireland and M.Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982. MR **83g:**12001
11. G.Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp., **61** (1993),915-926. MR **94d:**11004
12. G.Miller, *Riemann's hypothesis and tests for primality*, J.Comput. and System Sc., **13** (1976),300-317. MR **58:**470a
13. Louis Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science, **12** (1980), 97-108. MR **82a:**68078
14. C.Pomerance, J.L.Selfridge and Samuel S.Wagstaff,Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp., **35** (1980), 1003-1026. MR **82g:**10030
15. M.O.Rabin, *Probabilistic algorithms for testing primality*, J.Number Theory, **12** (1980), 128-138. MR **81f:**10003

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: zhangzhx@mail.ahwhptt.net.cn