

FINDING STRONG PSEUDOPRIMES TO SEVERAL BASES. II

ZHENXIANG ZHANG AND MIN TANG

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 efficient primality testing algorithm which is easy to implement. Thanks to Pomerance et al. and Jaeschke, the ψ_m are known for $1 \leq m \leq 8$. Upper bounds for ψ_9, ψ_{10} and ψ_{11} were first given by Jaeschke, and those for ψ_{10} and ψ_{11} were then sharpened by the first author in his previous paper (Math. Comp. **70** (2001), 863–872).

In this paper, we first follow the first author's previous work to use bi-quadratic residue characters and cubic residue characters as main tools to tabulate all strong pseudoprimes (spsp's) $n < 10^{24}$ to the first five or six prime bases, which have the form $n = pq$ with p, q odd primes and $q - 1 = k(p - 1)$, $k = 4/3, 5/2, 3/2, 6$; then we tabulate all Carmichael numbers $< 10^{20}$, to the first six prime bases up to 13, which have the form $n = q_1 q_2 q_3$ with each prime factor $q_i \equiv 3 \pmod{4}$. There are in total 36 such Carmichael numbers, 12 numbers of which are also spsp's to base 17; 5 numbers are spsp's to bases 17 and 19; one number is an spsp to the first 11 prime bases up to 31. As a result the upper bounds for ψ_9, ψ_{10} and ψ_{11} are lowered from 20- and 22-decimal-digit numbers to a 19-decimal-digit number:

$$\begin{aligned}\psi_9 \leq \psi_{10} \leq \psi_{11} \leq Q_{11} &= 3825\,12305\,65464\,13051 \quad (19 \text{ digits}) \\ &= 149491 \cdot 747451 \cdot 34233211.\end{aligned}$$

We conjecture that

$$\psi_9 = \psi_{10} = \psi_{11} = 3825\,12305\,65464\,13051,$$

and give reasons to support this conjecture. The main idea for finding these Carmichael numbers is that we loop on the largest prime factor q_3 and propose necessary conditions on n to be a strong pseudoprime to the first 5 prime bases. Comparisons of effectiveness with Arnault's, Bleichenbacher's, Jaeschke's, and Pinch's methods for finding (Carmichael) numbers with three prime factors, which are strong pseudoprimes to the first several prime bases, are given.

1. INTRODUCTION

Given a positive odd integer $n > 1$, write $n - 1 = 2^s d$ with d odd. If n is prime, then

$$(1.1) \quad \text{either } b^d \equiv 1 \pmod{n} \text{ or } b^{2^r d} \equiv -1 \pmod{n} \text{ for some } r = 0, 1, \dots, s - 1$$

Received by the editor July 9, 2001.

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

Key words and phrases. Strong pseudoprimes, Carmichael numbers, Rabin-Miller test, bi-quadratic residue characters, cubic residue characters, Chinese remainder theorem.

Supported by the NSF of China Grant 10071001, the SF of Anhui Province Grant 01046103, and the SF of the Education Department of Anhui Province Grant 2002KJ131.

holds for every b with $\gcd(n, b) = 1$. If (1.1) holds, then we say that n passes the Miller (strong pseudoprime) test [7] to base b ; if, in addition, n is composite, then we say that n is a strong pseudoprime to base b , or $\text{spsp}(b)$ for short. We say that n is an $\text{spsp}(b_1, b_2, \dots, b_t)$ if n is a strong pseudoprime to all the t bases b_i . Define

$$(1.2) \quad \text{SB}(n) = \#\{b \in \mathbb{Z} : 1 \leq b \leq n-1, n \text{ is an } \text{spsp}(b)\} \text{ and } P_R(n) = \frac{\text{SB}(n)}{\varphi(n)},$$

where φ is Euler's function. Monier [8] and Rabin [13] proved that if n is an odd composite positive integer, then $\text{SB}(n) \leq (n-1)/4$. In fact, as pointed by Damgård, Landrock and Pomerance [4], if $n \neq 9$ is odd and composite, then $\text{SB}(n) \leq \varphi(n)/4$, i.e., $P_R(n) \leq 1/4$. These facts lead to the Rabin-Miller test: given a positive integer n , pick k different positive integers less than n and perform the 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 existing deterministic primality testing algorithms. From Alford et al. [1] we know that, for any m , the function ψ_m exists.

From Pomerance et al. [12] and Jaeschke [6] we know the exact value of ψ_m for $1 \leq m \leq 8$ and the following facts:

$$\begin{aligned} \psi_9 &\leq M_9 = 41234\ 31613\ 57056\ 89041 \text{ (20 digits)} \\ &= 4540612081 \cdot 9081224161, \\ \psi_{10} &\leq M_{10} = 155\ 33605\ 66073\ 14320\ 55410\ 02401 \text{ (28 digits)} \\ &= 22754930352733 \cdot 68264791058197, \\ \psi_{11} &\leq M_{11} = 5689\ 71935\ 26942\ 02437\ 03269\ 72321 \text{ (29 digits)} \\ &= 137716125329053 \cdot 413148375987157. \end{aligned}$$

Jaeschke [6] 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 95 numbers n having the form

$$(1.3) \quad n = pq \quad \text{with } p, q \text{ odd primes and } q-1 = k(p-1),$$

with $k = 2, 3, 4, 5, 6, 7, 13, 4/3, 5/2$; the other six numbers are Carmichael numbers with three prime factors in the sense that:

$$(1.4) \quad n = q_1 q_2 q_3 \quad \text{with } q_1 < q_2 < q_3 \text{ odd primes and each } q_i - 1 \mid n - 1.$$

For short we call numbers (strong pseudoprimes) having the form (1.3) Kk -numbers (spsp 's), say, $K2$ - spsp 's if $k = 2$.

In his previous paper [14], the first author tabulated all $K2$ -, $K3$ -, $K4$ -strong pseudoprimes $< 10^{24}$ to the first nine or ten prime bases. As a result the upper bounds for ψ_{10} and ψ_{11} were 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} was obtained:

$$\begin{aligned}\psi_{12} &\leq N_{12} = 3186\,65857\,83403\,11511\,67461 \text{ (24 digits)} \\ &= 399165290221 \cdot 798330580441.\end{aligned}$$

In this paper, we first follow our previous work to use biquadratic residue characters and cubic residue characters as main tools for finding all K4/3-, K5/2-, K3/2-, K6-spsp's $< 10^{24}$ to the first several prime bases. No spsp's of such forms to the first 8 prime bases are found. Note that the three bounds N_{10}, N_{11} and N_{12} are all K2-spsp's with $P_R(n) = 3/16$. These facts give us a hint that to lower these upper bounds, we should find those numbers n with $P_R(n)$ equal to or close to $1/4$.

For short, we call a Carmichael number $n = q_1 q_2 q_3$ with each prime factor $q_i \equiv 3 \pmod{4}$ a C_3 -number. If n is a C_3 -number and an $\text{spsp}(b_1, b_2, \dots, b_t)$, we call n a C_3 -spsp($b_1, b_2, \dots, b_t$). We can prove that (see §5 below)

$$(1.5) \quad \begin{aligned} P_R(n) = 1/4 &\iff \\ \text{either } n = pq &\text{ is a K2-number with } p \equiv 3 \pmod{4} \text{ or } n \text{ is a } C_3\text{-number;} \end{aligned}$$

and

$$(1.6) \quad \text{if } n \text{ is an } \text{spsp}(2), \text{ then } P_R(n) = 1/4 \iff n \text{ is a } C_3\text{-number.}$$

We then focus our attention to develop a method for finding all C_3 -spsp($2, 3, 5, 7, 11$) $< 10^{20}$. There are in total 110 such numbers, 36 numbers of which are also $\text{spsp}(13)$; 12 numbers are spsp's to bases 13 and 17; 5 numbers are spsp's to bases 13, 17 and 19; one number is an spsp to the first 11 prime bases up to 31. As a result the upper bounds for ψ_9, ψ_{10} and ψ_{11} are considerably lowered:

$$\begin{aligned}\psi_9 \leq \psi_{10} \leq \psi_{11} &\leq Q_{11} = 3825\,12305\,65464\,13051 \text{ (19 digits)} \\ &= 149491 \cdot 747451 \cdot 34233211.\end{aligned}$$

The main idea of our method for finding these C_3 -numbers is as follows. We loop on the largest prime factor q_3 and propose necessary conditions on $q_1 q_2 - 1$ for n to be a strong pseudoprime to the first 5 prime bases. Thus we have a certain number of candidates n (determined by candidates $Q = q_1 \cdot q_2$) at hand. Then we subject these candidates n to Miller's tests and obtain the desired numbers.

Arnault [2] used a sufficient condition for constructing Carmichael numbers which are spsp's to several prime bases and successfully found a 397-digit Carmichael number which is an spsp to all the prime bases < 300 . Bleichenbacher [3] used a method similar to Arnault's for finding C_3 -numbers, which are spsp's to several prime bases and found several such numbers much smaller than Arnault's. But both Arnault's and Bleichenbacher's method could find only C_3 -numbers with additional special forms. They were not able to find all C_3 -numbers to a given limit. Our bound Q_{11} could not be found by their methods. Pinch [9] computed all Carmichael numbers up to 10^{15} , then extended the computations to 10^{16} , and computed all Carmichael numbers with three prime factors up to 10^{18} (see [10]). For finding all Carmichael numbers having three prime factors to a given limit, his method loops on q_1 and q_2 and checks candidates of q_3 to see if $n = q_1 q_2 q_3$ is a Carmichael number. Thus his method is much more expensive than ours for finding C_3 -spsp's. See Remarks 2.1, 4.5, 4.6, and 4.7 for comparisons in details.

All K4/3-, K5/2-, K3/2-, and K6-spsp's $< 10^{24}$ to the first 5 or 6 prime bases are tabulated in §§2–3. In §4 we tabulate all C_3 -spsp($2, 3, 5, 7, 11, 13$) $< 10^{20}$ and

describe the method for finding these numbers. In §5 we give reasons to support the following

Conjecture. $\psi_9 = \psi_{10} = \psi_{11} = 3825\ 12305\ 65464\ 13051$ (19 digits).

2. K4/3- AND K5/2-STRONG PSEUDOPRIMES

Let $n = pq$ be of the form (1.3) with $k = 4/3$ or $k = 5/2$. If $k = 4/3$, then $q = N(\pi) \equiv 1 \pmod{8}$ and $p = (3q + 1)/4 \equiv 1 \pmod{6}$; if $k = 5/2$, then $p = N(\pi) \equiv 1 \pmod{4}$ and $q = (5p - 3)/2 \equiv 1 \pmod{10}$; for some primary irreducible π of the ring $\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$ of Gaussian integers. Let b be a positive integer (not necessarily prime). With $\left(\frac{b}{\pi}\right)_4$ the biquadratic residue character symbol of b modulo π , it is easy to prove that

$$(2.1) \quad \text{if } n = pq \text{ is a K4/3-psp}(b), \text{ then } \left(\frac{b}{\pi}\right)_4 = 1$$

and

$$(2.2) \quad \text{if } n = pq \text{ is a K5/2-spsp}(b), \text{ then } \left(\frac{b}{\pi}\right)_4 = \left(\frac{b}{q}\right).$$

Using lemmas on biquadratic residue characters (cf. [14, §2]) and the Chinese Remainder Theorem, we subject those candidates n , with π satisfying (2.1) for $k = 4/3$, or satisfying (2.2) for $k = 5/2$, to Miller tests to decide whether they are spsp's or not. We find all K4/3- and K5/2- spsp's $< 10^{24}$ to the first 5 prime bases up to 11, listed in Tables 1 and 2 (on the following pages). There are in total 157 K4/3-numbers among which three numbers are spsp(13) and 30 K5/2-numbers among which only one is an spsp(13). The Pascal program (with multi-precision package partially written in Assembly language) ran on a PC Pentium III/800, about 8 hours for $k = 4/3$ and about 3 hours for $k = 5/2$.

Remark 2.1. As mentioned in Arnault [2, §4], the primality test of Maple V.2 consists of three stages. The first is a search for factors less than 1000. The second is an actual Rabin-Miller test. The bases used are 2, 3, 5, 7, 11 (however, more bases can be used, on request). The last stage consists in checking if n is not of the form

$$(u + 1) \left(k \frac{u}{2} + 1\right) \text{ with } 3 \leq k \leq 9 \quad \text{or} \quad (u + 1)(ku + 1) \text{ with } 5 \leq k \leq 20.$$

Arnault [2] constructed four Carmichael numbers which pass the Maple test, the smallest one of which has 29 decimal digits. All the 157 K4/3-numbers tabulated in Table 1 pass the Maple V.2 test, all of which have at most 24 decimal digits. See also Remark 4.5 below.

3. K3/2- AND K6-STRONG PSEUDOPRIMES

Let $n = pq$ be of the form (1.3) with $k = 3/2$ or $k = 6$. If $k = 3/2$, then $q = N(\pi) \equiv 1 \pmod{6}$ and $p = (2q + 1)/3 \equiv 1 \pmod{4}$; if $k = 6$, then $q = N(\pi) \equiv 1 \pmod{12}$ and $p = (q + 5)/6$; for some primary irreducible π of the ring $\mathbb{Z}[\omega] = \{x + y\omega : x, y \in \mathbb{Z}\}$, where $\omega = \frac{-1 + \sqrt{-3}}{2}$. Let b be a positive integer (not necessarily prime). With $\left(\frac{b}{\pi}\right)_3$ the cubic residue character symbol of b modulo π , it is easy to prove that

$$(3.1) \quad n = pq \text{ is a K3/2-psp}(b) \text{ iff } \left(\frac{b}{\pi}\right)_3 = \left(\frac{b}{p}\right) = 1;$$

TABLE 1. List of K4/3-spsp's $< 10^{24}$ to the first 5 prime bases

number	factorization	spsp-base		
		13	17	19
1 49568 04560 64411	33492691· 4465921	0	0	0
17230 39799 10558 66091	594829411· 793105881	0	0	0
1 44394 53855 26560 46311	10406531791· 13875375721	0	0	0
1 57953 52954 73172 33463	10884169567· 14512226089	0	0	0
3 47237 60535 21718 81213	16137788077· 21517050769	0	0	0
5 19178 48661 70603 97063	19732811887· 26310415849	0	0	0
6 72092 85020 39639 53381	22451495221· 29935326961	0	0	0
18 24108 82957 49574 49063	36987587407· 49316783209	0	0	0
23 72017 93228 38869 86651	42178352851· 56237803801	0	0	0
37 12490 81132 09994 00013	52767111997· 70356149329	0	0	0
38 47303 98366 89076 69151	53716645351· 71622193801	0	0	0
39 26637 79419 73965 22411	54267654691· 72356872921	0	0	0
42 83131 36636 74489 77131	56677583971· 75570111961	0	0	0
52 25944 70439 38115 54451	62605579051· 83474105401	0	0	0
55 21832 64147 38105 14201	64353511801· 85804682401	0	0	0
61 37744 03597 53686 48763	67847682547· 90463576729	0	0	0
68 34030 97541 89934 21671	71592759631· 95457012841	0	0	0
72 70126 71778 89490 45963	73841689027· 98455585369	0	0	0
79 34247 33531 16914 90181	77140686421· 102854248561	0	0	0
87 29093 18238 27647 00011	80912421091· 107883228121	0	0	0
90 23910 34055 95722 81991	82267446511· 109689928681	0	0	0
92 53777 77243 62478 67111	83308662991· 111078217321	0	0	0
92 89086 63147 01619 12563	83467448587· 111289931449	0	0	0
.....		...	...	...
1474 76320 91370 36599 12563	332576648587· 443435531449	1	0	0
.....		...	...	...
3155 19832 06199 08555 35013	486456446197· 648608594929	1	0	0
.....		...	...	...
5046 67554 29515 98288 77851	615224077651· 820298770201	1	0	1
.....		...	...	...
9041 82566 78973 64001 32063	823490695207· 1097987593609	0	0	0
9140 42705 14734 50826 76963	827968615867· 1103958154489	0	0	0
9270 56633 26015 99953 67711	833841996391· 1111789328521	0	0	0
9392 14060 81950 64434 88063	839291692807· 1119055590409	0	0	0
9487 04022 55897 35280 06963	843521201227· 1124694934969	0	0	0
9920 02228 28265 90865 57231	862555314871· 1150073753161	0	0	0
9924 00583 00644 97734 70063	862728484087· 1150304645449	0	0	1
9964 48545 46279 73239 62451	864486211051· 1152648281401	0	0	0

and

$$(3.2) \quad n = pq \text{ is a K6-psp}(b) \text{ iff } \left(\frac{b}{\pi}\right)_3 = \left(\frac{b}{q}\right) = 1.$$

Using the Cubic Reciprocity Law and its Supplement (cf. [14, §5]) and the Chinese Remainder Theorem, we subject those candidates n , with π satisfying (3.1) for $k = 3/2$, or satisfying (3.2) for $k = 6$, to Miller tests to decide whether they are spsp's or not. We find all K3/2- and K6-spsp's $< 10^{24}$ to the first 6 prime bases up to 13 listed in Tables 3 and 4 (on the following pages). There are in total 44 K3/2-numbers among which two numbers are spsp(17) and 94 K6-numbers among which seven numbers are spsp(17). The Pascal program ran on a PC Pentium III/800, about 15 minutes for $k = 3/2$ and about one hour for $k = 6$.

Remark 3.1. We may use biquadratic residue characters and thus work in the ring $\mathbb{Z}[i]$ for finding K3/2- and K6-spsp's as for finding K4/3- and K5/2-spsp's in §2.

TABLE 2. List of all K5/2-spsp's $< 10^{24}$ to the first 5 prime bases

number	factorization	spsp-base		
		13	17	19
3 97448 34525 17604 24469	12608700889· 31521752221	0	0	0
10 44928 25019 73114 68589	20444346409· 51110866021	0	0	0
16 83748 41900 90806 56261	25951866361· 64879665901	0	0	0
20 34747 90686 78179 33189	28528918009· 71322295021	0	0	0
23 77617 72823 75415 79901	30839051401· 77097628501	0	0	0
34 90196 54457 19998 75829	37364135449· 93410338621	0	0	0
37 91638 68715 09344 94909	38944261129· 97360652821	0	0	0
38 77389 72629 76435 76621	39382177321· 98455443301	0	0	0
43 86094 76204 35352 35729	41886010849· 104715027121	0	0	0
51 68882 85059 53573 16821	45470354521· 113675886301	0	0	0
107 51051 57579 63844 57541	65577592441· 163943981101	0	0	0
211 64776 21429 21790 14069	92010382489· 230025956221	0	0	0
309 59514 94792 82890 25701	111282550201· 278206375501	1	0	0
314 42425 97389 02539 54029	112147092649· 280367731621	0	0	0
632 32972 94454 68528 22409	159038326129· 397595815321	0	0	0
1173 49209 06142 08869 15581	216655679881· 541639199701	0	0	0
1217 52544 53044 07018 90949	220683070969· 551707677421	0	0	0
1519 05264 76597 63179 73021	246499707721· 616249269301	0	0	0
1526 51189 19732 58519 21489	247104179809· 617760449521	0	0	0
2040 89678 46723 77414 17009	285719917729· 714299794321	0	0	0
2518 21600 70833 07258 31541	317377756441· 793444391101	0	0	0
2603 73638 20616 16647 71621	322721947321· 806804868301	0	0	0
3205 92590 12584 88337 49909	358101991129· 895254977821	0	0	0
3292 43892 71589 46320 15541	362901580441· 907253951101	0	0	0
5568 29137 02350 61516 21109	471944546329· 1179861365821	0	0	0
6057 64297 36383 63371 62141	492245588041· 1230613970101	0	0	0
6891 91568 28621 61943 29549	525049166569· 1312622916421	0	0	0
7096 84414 48205 71434 63181	532798053481· 1331995133701	0	0	0
7919 78070 47845 60348 97989	562842098809· 1407105247021	0	0	0
9955 53769 19498 60966 08141	631047944041· 1577619860101	0	0	0

But then we would subject more candidates to the Miller test, and the program would run longer.

4. C_3 -STRONG PSEUDOPRIMES

For b prime and $\varepsilon \in \{1, -1\}$, let

$$R_{b,\varepsilon} = \left\{ u : 0 \leq u < 4b, u \equiv 3 \pmod{4}, \left(\frac{b}{u} \right) = \varepsilon \right\}.$$

It is easy to compute:

$$\begin{aligned} R_{2,1} &= \{7\}, & R_{2,-1} &= \{3\}, \\ R_{3,1} &= \{11\}, & R_{3,-1} &= \{7\}, \\ R_{5,1} &= \{11, 19\}, & R_{5,-1} &= \{3, 7\}, \\ R_{7,1} &= \{3, 19, 27\}, & R_{7,-1} &= \{11, 15, 23\}, \\ R_{11,1} &= \{7, 19, 35, 39, 43\}, & R_{11,-1} &= \{3, 15, 23, 27, 31\}. \end{aligned}$$

Let $b_1 = 2$, $b_2 = 3$, $b_3 = 5$, $b_4 = 7$, $b_5 = 11$, and $M = 4b_1b_2b_3b_4b_5 = 9240$. For $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \in \{1, -1\}$, let

$$S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5} = \{ u : 0 \leq u < M, u \equiv r_i \pmod{4b_i} \text{ for some } r_i \in R_{b_i, \varepsilon_i}, 1 \leq i \leq 5 \}.$$

TABLE 3. List of all K3/2-spsp's $< 10^{24}$ to the first 6 prime bases

number	factorization	spsp-base		
		17	19	23
69729 29305 61765 92357	6818078569· 10227117853	0	1	0
1 31708 27666 78964 24277	9370459849· 14055689773	0	0	0
37 70848 10529 01278 77797	50138794729· 75208192093	0	0	0
55 74059 87854 08679 27501	60959330041· 91438995061	0	0	0
58 66946 53607 85860 30437	62540368489· 93810552733	1	0	0
113 39832 10310 35752 05317	86947616809· 130421425213	0	0	0
153 09112 64864 31707 91397	101025121129· 151537681693	0	1	0
224 25909 43625 14399 06537	122272671889· 183409007833	0	0	0
241 64596 86739 74609 25837	126924116089· 190386174133	0	0	0
365 49077 42198 92882 14301	156096289561· 234144434341	0	0	0
366 52213 92522 27969 93517	156316375609· 234474563413	0	0	0
433 24496 37187 59891 21997	169949985529· 254924978293	0	0	0
655 73396 43371 91368 18077	209082753049· 313624129573	0	0	0
1041 72337 64172 59203 20997	263530311529· 395295467293	0	0	0
1047 17568 39570 32486 01397	264219061129· 396328591693	0	1	0
1131 40803 32952 81787 63417	274640132209· 411960198313	0	0	0
1208 80119 34821 96873 54757	283878048169· 425817072253	0	0	0
1239 41900 17602 02951 04517	287450749609· 431176124413	0	0	0
1335 05235 86757 98976 33457	298334527969· 447501791953	0	0	0
1348 26751 08732 19056 84217	299807439409· 449711159113	0	0	0
1568 21780 73799 57347 51997	323338605529· 485007908293	0	0	0
1845 13866 83686 47647 47297	350726737729· 526090106593	0	0	0
1846 08121 43189 64806 74357	350816306569· 526224459853	0	0	0
2182 61072 02101 96818 91277	381454297849· 572181446773	0	0	0
2322 19458 47286 62214 50017	393462796609· 590194194913	0	0	0
2757 35909 80549 32438 15997	428746941529· 643120412293	0	0	0
3518 56467 88718 49300 64501	484325281801· 726487922701	0	0	0
3735 89027 18557 23710 23957	499058464969· 748587697453	0	0	0
4191 37697 69352 58025 16901	528606783721· 792910175581	0	0	0
4391 24961 84215 27021 88997	541063743529· 811595615293	0	0	0
4400 28733 86021 53921 84437	541620244489· 812430366733	0	0	0
5050 32715 40234 07031 41901	580248633721· 870372950581	0	0	0
5270 50781 55294 57512 60017	592762336609· 889143504913	0	0	0
5953 02497 46236 09194 26301	629974865881· 944962298821	0	0	0
6142 41516 00488 37257 19097	639917450929· 959876176393	0	0	0
6654 24596 73719 74117 65757	666045342169· 999068013253	0	0	0
7971 40697 93590 86153 84877	728990488249· 1093485732373	0	0	0
8389 17981 83462 82319 48777	747849352849· 1121774029273	0	0	0
8478 51079 02835 40115 20197	751820492329· 1127730738493	0	0	1
8629 85893 61815 38949 45501	758501106841· 1137751660261	0	0	0
8821 76945 94144 99408 42397	766888495129· 1150332742693	0	0	0
9064 51656 30675 90243 75877	777368062249· 1166052093373	1	0	0
9627 65739 59813 94695 84737	801151562689· 1201727344033	0	1	0
9841 46981 76937 91111 74597	809998757929· 1214998136893	0	1	0

There are in total $2^5 = 32$ such sets which are pairwise disjoint. For $u \in S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5}$, let $d_u = \gcd(M, u - 1)$, $m_u = M/d_u$, $h_u = \frac{u-1}{d_u}$, and

$$K_u = \left\{ w : 0 \leq w < m_u, w \equiv \frac{v_1 v_2 - 1}{d_u} h_u^{-1} \pmod{m_u} \right. \\ \left. \text{for some } v_1, v_2 \in S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5} \text{ with } d_u \mid v_1 v_2 - 1 \right\}.$$

With the above notation, our algorithm for finding all C_3 -spsp(2, 3, 5, 7, 11) $< 10^{20}$ is based on the following theorem.

TABLE 4. List of K6-spsp's $< 10^{24}$ to the first 6 prime bases

number	factorization	spsp-base		
		17	19	23
16697 26713 79531 48781	1668195989· 10009175929	0	0	0
46472 55476 66167 31941	2783060509· 16698363049	0	0	0
2 28257 22811 28845 99061	6167890349· 37007342089	0	0	0
8 22341 91735 98586 42781	11707133989· 70242803929	0	0	0
30 79791 78424 06521 53861	22656094781· 135936568681	0	0	0
30 93133 39050 14172 96221	22705114661· 136230687961	0	0	0
61 54123 57614 21995 06701	32026352629· 192158115769	0	0	0
105 35741 97069 25554 25661	41904140549· 251424843289	0	1	0
132 96130 37580 92088 82261	47074639981· 282447839881	0	0	0
136 46493 03217 04932 47941	47690832509· 286144995049	0	0	0
151 59151 96412 24655 44981	50264553389· 301587320329	0	0	0
209 42779 80166 71830 53901	59080143029· 354480858169	0	0	0
238 39015 33359 04772 29061	63033080381· 378198482281	0	0	0
250 17184 57808 79868 81141	64571903821· 387431422921	0	0	0
265 35875 44426 92637 71161	66502976681· 399017860081	0	0	0
316 50760 47487 27752 44861	72630067781· 435780406681	0	0	0
398 98138 34741 63323 99541	81545629709· 489273778249	1	0	0
.....		...	...	...
1858 96617 66977 41464 55601	176019230801· 1056115384801	1	0	0
.....		...	...	...
3714 58482 28899 38246 21021	248816693669· 1492900162009	1	0	1
.....		...	...	...
5199 40297 84796 97734 29661	294375128549· 1766250771289	1	0	0
.....		...	...	...
5958 43301 53200 92092 72901	315130476029· 1890782856169	1	0	0
.....		...	...	...
6409 57407 41045 49309 89381	326842828541· 1961056971241	1	0	1
.....		...	...	...
7482 14416 74656 98771 30181	353132273789· 2118793642729	1	0	0
7553 85557 16534 41305 79861	354820507949· 2128923047689	0	0	0
7685 24206 81853 31868 96181	357892955789· 2147357734729	0	0	0
7736 38028 07515 46718 97021	359081705669· 2154490234009	0	0	1
7880 99864 74475 07868 67981	362422374389· 2174534246329	0	0	0
8015 66065 42238 21849 19301	365505600829· 2193033604969	0	0	0
8136 86262 53554 57424 70161	368258573681· 2209551442081	0	0	0
8477 25020 45173 59201 21181	375882299941· 2255293799641	0	0	0
8635 76456 05512 05932 64821	379380296461· 2276281778761	0	0	0
9219 57200 51224 53075 57181	391994302789· 2351965816729	0	0	0
9395 82992 80107 49342 62341	395723597309· 2374341583849	0	0	0
9847 48407 03660 34769 01341	405123110309· 2430738661849	0	0	0
9943 95005 72454 05436 36701	407102568101· 2442615408601	0	0	0

Theorem 4.1. *If $n = q_1 q_2 q_3$ is a C_3 -spsp(2, 3, 5, 7, 11), then $q_1 q_2 - 1 = k(q_3 - 1)$ for some $k \in \mathbb{Z}$ with $k \equiv w \pmod{m_u}$ for some $w \in K_u$ where $u \equiv q_3 \pmod{M}$.*

To prove the Theorem we need two lemmas.

Lemma 4.1. *If p is a prime > 11 with $p \equiv 3 \pmod{4}$ and $\varepsilon = \left(\frac{b}{p}\right)$ with $b \in \{2, 3, 5, 7, 11\}$, then $p \equiv u \pmod{4b}$ for some $u \in R_{b, \varepsilon}$.*

Proof. Let u be such that $0 \leq u < 4b$ with $u \equiv p \pmod{4b}$. Since $p \equiv 3 \pmod{4}$, $u \equiv 3 \pmod{4}$.

If $b = 2$, then $\left(\frac{2}{u}\right) = (-1)^{(u^2-1)/8} = (-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right) = \varepsilon$. If b is odd, then $\left(\frac{b}{u}\right) = \left(\frac{u}{b}\right)(-1)^{\frac{u-1}{2} \cdot \frac{b-1}{2}} = \left(\frac{p}{b}\right)(-1)^{\frac{p-1}{2} \cdot \frac{b-1}{2}} = \left(\frac{b}{p}\right) = \varepsilon$. Thus $u \in R_{b, \varepsilon}$ for either $b = 2$ or b odd. $\square$

Lemma 4.2. [3, Theorem 3.17] *Let $n = q_1 q_2 q_3$ be a C_3 -number. Then*

$$n \text{ is an spsp}(b) \iff \left(\frac{b}{q_1}\right) = \left(\frac{b}{q_2}\right) = \left(\frac{b}{q_3}\right) \neq 0.$$

Proof of Theorem 4.1. Since each $q_i \equiv 3 \pmod{4}$ and n is an spsp(b_j), we have by Lemma 4.2,

$$\left(\frac{b_j}{q_1}\right) = \left(\frac{b_j}{q_2}\right) = \left(\frac{b_j}{q_3}\right) = \varepsilon_j \in \{1, -1\}$$

for $1 \leq j \leq 5$. Let v_i be such that $0 \leq v_i < M$ and $v_i \equiv q_i \pmod{M}$. Then $v_i \equiv q_i \pmod{4b_j}$. Thus $v_i \equiv r_{ij} \pmod{4b_j}$ for some $r_{ij} \in R_{b_j, \varepsilon_j}$ for $1 \leq j \leq 5$. Therefore $v_i \in S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5}$ for $1 \leq i \leq 3$.

Let $u = v_3$, $d_u = \gcd(M, u - 1)$, $h_u = (u - 1)/d_u$ and $m_u = M/d_u$. Since n is a Carmichael number,

$$q_1 q_2 - 1 = k(q_3 - 1)$$

for some $k \in \mathbb{Z}$. Then

$$v_1 v_2 - 1 \equiv k(u - 1) \pmod{M}.$$

Thus

$$d_u \mid v_1 v_2 - 1 \quad \text{and} \quad \frac{v_1 v_2 - 1}{d_u} \equiv k \frac{u - 1}{d_u} \pmod{m_u}.$$

Therefore

$$k \equiv \frac{v_1 v_2 - 1}{d_u} h_u^{-1} \pmod{m_u}.$$

This means that $k \equiv w \pmod{m_u}$ for some $w \in K_u$. □

Now we are ready to describe a procedure to compute all C_3 -numbers n with $19 \cdot 23 \cdot 31 = 13547 < n < L$, say, $L = 10^{20}$, which are spsp's to the first h (≥ 5) prime bases.

PROCEDURE Finding- C_3 -spsp's;

BEGIN

 For each 5-tuples $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5) \in \{1, -1\}^5$ Do

 begin compute the set $S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5}$;

 For each $u \in S_{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5}$ Do compute the set K_u

 end;

 For each prime $q \in [43, L^{1/2}/2 + 1]$ with $q \equiv 3 \pmod{4}$ Do

 begin $u \leftarrow q \pmod{M}$; $d \leftarrow \gcd(M, u - 1)$; $m \leftarrow M/d$;

 For each $k \in K_u$ Do

 Begin If $k = 0$ Then $k \leftarrow m$;

 Repeat $Q \leftarrow k(q - 1) + 1$; $n \leftarrow Q \cdot q$;

 If $2^n \equiv 2 \pmod{Q}$ Then

 begin If n is an spsp to the first h prime bases

 Then output(n, Q, q)

 end;

$k \leftarrow k + m$

 Until $(k > q)$ Or $(n > L)$

 End

end

END.

TABLE 5. List of all C_3 -spsp's $< 10^{20}$ to the first 6 prime bases

number	factorization			spsp-base		
				17	19	23
347 47496 60383	1303·	16927·	157543	0	0	0
4 49841 46825 39051	46411·	232051·	417691	1	0	0
159 93361 86255 83251	25771·	2293531·	2705851	0	0	0
228 68838 23203 21951	13831·	69151·	239106871	0	1	0
230 24566 07261 88031	214831·	787711·	1360591	1	1	0
355 28741 01713 90971	59011·	767131·	7848331	0	1	1
361 73823 06759 85351	15511·	77551·	300723391	0	0	1
897 17429 13752 20951	204439·	1022191·	4293199	0	0	0
2677 38006 75969 84751	390391·	1951951·	3513511	0	0	0
3183 45585 71620 65031	565111·	1017199·	5538079	0	0	1
3688 59773 78487 08851	12739·	522259·	554421451	0	1	1
3825 12305 65464 13051	149491·	747451·	34233211	1	1	1
3948 83565 86219 75551	301159·	1021879·	12831391	0	0	0
4208 46784 29991 26631	789391·	1841911·	2894431	0	0	0
5474 09379 21300 26911	21319·	2238391·	114712159	1	1	0
6019 39692 56407 61251	185371·	926851·	35034931	1	0	1
7315 03791 10592 08331	225611·	2932931·	11054891	0	0	0
7361 23518 72960 10651	412339·	2061691·	8659099	1	1	0
8276 44253 41010 54431	209431·	3560311·	11099791	1	1	0
10450 55828 23978 80151	614671·	3073351·	5532031	0	0	0
16989 96203 93566 84951	478351·	1753951·	20250151	1	0	0
17045 84699 13766 54351	80071·	2322031·	91680151	1	0	0
17577 53263 86566 47651	300931·	1504651·	38819971	0	0	1
20315 15577 77886 49051	767131·	3835651·	6904171	0	0	0
27221 90634 37899 80731	72211·	2094091·	180019531	1	0	0
27519 77153 47898 22751	889351·	3430351·	9020551	0	0	0
46651 98748 96521 95311	534799·	2673991·	32622679	0	0	0
65459 93985 63261 19651	767131·	3835651·	22246771	0	0	0
66464 49530 07468 62551	1138831·	5694151·	10249471	1	0	1
71718 02966 94207 16051	296731·	2670571·	90502651	0	0	0
80427 01952 31043 49551	499591·	2497951·	64447111	0	0	0
84633 42198 19966 30471	204439·	1022191·	404991679	0	1	0
91486 51754 57119 58671	2203111·	5140591·	8078071	0	0	1
92574 08533 13640 99751	2011951·	5325751·	8639551	1	0	0
93229 14587 06421 08251	724651·	3623251·	35507851	0	0	0
94722 65669 78115 91307	64067·	7751987·	190724483	0	0	0

The Pascal program (with multi-precision package partially written in Assembly language) ran about 1600 hours on a PC Pentium III/800 (in fact we used 10 PCs, each running 160 hours) to get all C_3 -spsp($2, 3, 5, 7, 11$) $< 10^{20}$. There are in total 110 numbers, among which 36 numbers are spsp(13), listed in Table 5; 12 numbers are spsp's to bases 13 and 17; 5 numbers are spsp's to bases 13, 17 and 19; one number is an spsp to the first 11 prime bases up to 31.

Remark 4.1. In Theorem 4.1, q_3 is not necessarily the largest of the three prime factors of n . If we keep in mind that $q_1 < q_2 < q_3$, then q in the procedure would be either q_2 or q_3 . So, if n is a C_3 -spsp($2, 3, 5, 7, 11$) with $q_1 q_3 < q_2^2$, then n would be output twice.

Remark 4.2. It is easy to see that in Theorem 4.1, $k \equiv 0 \pmod{4}$, so, $k \geq 4$. Thus $L > n > k(q_3 - 1)q_3 > 4(q_3 - 1)^2$. Therefore $q_3 < L^{1/2}/2 + 1$.

Remark 4.3. From Pinch [10], we know that there are 35585 Carmichael numbers with three prime factors up to 10^{18} . It is easy to check that, among these numbers

there are 28 $\text{spsp}(2, 3, 5, 7, 11)$, all of which are C_3 -numbers, eight of which are also $\text{spsp}(13)$. These facts coincide with our computation.

Remark 4.4. If $n = Qq$ is an $\text{spsp}(2, 3, 5, 7, 11)$ and Q is composite, then use either our “Near Group Orders” method [15] or Pollard’s ρ -method [11] to factor Q . If n is a C_3 -number, then $Q = q_1q_2$ with $q_1 < q_2$ odd primes. Since most candidates are not $\text{spsp}(2, 3, 5, 7, 11)$, time used for factorization is negligible.

Remark 4.5. The smallest example $C_3\text{-spsp}(2, 3, 5, 7, 11)$ given in Arnault [2] has 29 decimal digits. Bleichenbacher [3] gave only five examples of $C_3\text{-spsp}(2, 3, 5, 7, 11) < 10^{20}$. Besides the 157 $K4/3\text{-spsp}(2, 3, 5, 7, 11) < 10^{24}$, all our 110 $C_3\text{-spsp}(2, 3, 5, 7, 11) < 10^{20}$ pass the Maple V.2 test. See also Remark 2.1.

Remark 4.6. $\psi_5 = 215\,23028\,98747 = q_1q_2q_3$ is the smallest $\text{spsp}(2, 3, 5, 7, 11)$, found by Jaeschke [6], where $q_1 = 6763$, $q_2 = 10627$, and $q_3 = 29947$. Jaeschke considered 42233 feasible pairs (p_1, p_2) where $p_1 \leq 15139$, $p_2 \leq 516991$. For each pair (p_1, p_2) , do as follows: compute $\eta = \text{lcm}(\text{ord}_2(p_1), \text{ord}_2(p_2))$; if $\gcd(\eta, p_1p_2) = 1$, compute $c = (p_1p_2)^{-1} \bmod \eta$, and for each prime $p_3 \leq 3474749660383/(p_1p_2)$ with $y \equiv c \bmod \eta$ test whether $n = p_1p_2p_3$ is an $\text{spsp}(2, 3, 5, 7, 11)$ or not. Note that ψ_5 is a C_3 -number. Given $q_1 = 6273$, using the method of Pinch [9] for finding ψ_5 , about $\sum_{x=2}^{2400} \frac{q_1^2}{x} \left(\frac{q_1+3}{q_1+1} - 1 \right) \approx 95890$ candidates would be tested. With our method, given q_3 , to find $n = \psi_5$, less than $(\lfloor \frac{2400}{220} \rfloor + 1) \cdot 10 = 110$ candidates were tested, since $q_3 \equiv 2227 \bmod 9240$, and $m_{2227} = 220$ and $|K_{2227}| = 10$.

Remark 4.7. Bleichenbacher [3] used a method similar to Jaeschke’s for finding all $\text{spsp}(2, 3) < L = 10^{16}$; the running time of the algorithm under some assumption is $O(L^{9/11})$. It is easy to prove that, with our method to find all $C_3\text{-spsp}(2, 3, 5, 7, 11) < L$, only $O(L^{2/3})$ candidates would be tested and the running time would be $O(L^{2/3+\epsilon})$.

5. DISCUSSION

Let $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ be the prime decomposition of an odd integer $n > 0$. Write $n - 1 = 2^k q$ with q odd; and $p_i - 1 = 2^{k_i} q_i$ with q_i odd for $1 \leq i \leq s$, ordering the p_i ’s such that $k_1 \leq \cdots \leq k_s$. Monier [8] proved that

$$\text{SB}(n) = \left(1 + \frac{2^{k_1 s} - 1}{2^s - 1} \right) \prod_{i=1}^s \gcd(q, q_i).$$

Using this formula, it is easy to prove (1.5) and (1.6). (If n is a $K2$ -number but not an $\text{spsp}(2)$, we may have $P_R(n) = 1/4$, e.g., $P_R(91 = 7 \cdot 13) = 18/72 = 1/4$. But this fact does not help.)

For comparisons, Table 6 lists the maximum value of $P_R(n)$ and T_h —the number of $Kk\text{-spsp}$ ’s $< 10^{24}$ to the first h prime bases for $k = 2, 3, 4, 3/2, 6, 4/3$, and $5/2$. (The value of $\max P_R(n)$ needs the additional condition that n is an $\text{spsp}(2)$ for $k = 2, 5/2, 3/2, 6$.)

We see that there exist more spsp ’s (to a given limit) to more bases for larger $P_R(n)$. For finding all $K5\text{-spsp}$ ’s to a given limit to several bases efficiently, we should use 5th residue characters in $\mathbb{Z}[\zeta_5]$ —the ring of integers in the cyclotomic field $\mathbb{Q}[\zeta_5]$ of 5th roots of unity. Computations in this ring would be more complicated than that in either the ring $\mathbb{Z}[i]$ or the ring $\mathbb{Z}[\omega]$. We will discuss this issue in a future paper. Since $P_R(n) = 1/10$ for $K5$ -numbers, we may predicate that there

TABLE 6.

Type	K2-	K3-	K4-	K3/2-	K6-	K4/3-	K5/2-
$\max P_R(n)$	3/16	1/6	1/8	1/16	1/16	1/24	3/80
h	10	9	9	6	6	5	5
T_h	41	11	14	44	94	157	30
h	12	10	10	7	7	6	6
T_h	3	2	1	2	7	3	1

would not be many K5-spsp's to more bases. Combining these facts and (1.6), our conjecture stated in §1 would most likely be correct.

It might be possible that there exists a constant c such that no strong pseudoprime to the smallest $\lfloor c \cdot \log n \rfloor$ prime bases does exist. Davenport conjectured that for the choice $c = 1/\log 100$ no counterexample can be constructed. Bleichenbacher [3] constructed a 41-digit C_3 -number which is a strong pseudoprime to the smallest 21 prime bases and is a counterexample to Davenport's conjecture. Our 19-digit C_3 -number $Q_{11} = 3825123056546413051$ is a strong pseudoprime to the smallest 11 prime bases and is a better counterexample to Davenport's conjecture than that of Bleichenbacher in the sense that $\frac{11}{19} = 0.578\ldots > 0.512\ldots = \frac{21}{41}$. These examples show that it is not secure if one uses k bases for $2k$ -digit numbers as the 2.0 release of Axiom does (see [2]). Hopefully, the first author's one-parameter quadratic-base version of the Baillie-PSW probable prime test [16] has probability of error $< 1/n^{2/3}$ or $< 1/n^{2/7}$ for n a product of two or three different odd primes, and it seems much more difficult to break.

ACKNOWLEDGMENTS

We thank D. Bleichenbacher and C. Pomerance for sending us reprints of [3] and [1]; and we thank R. Pinch for informing us to access [10]. Special thanks go to the referee for kind and helpful comments that improved the paper.

REFERENCES

1. 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
2. F. Arnault, *Constructing Carmichael numbers which are strong pseudoprimes to several bases*, J. Symbolic Computation **20** (1995), 151-161. MR **96k**:11153
3. D. Bleichenbacher, *Efficiency and Security of Cryptosystems Based on Number Theory*, ETH Ph.D. dissertation 11404, Swiss Federal Institute of Technology, Zurich (1996).
4. I. Damgård, P. Landrock, and C. Pomerance, *Average case estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177-194. MR **94b**:11124
5. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982. MR **83g**:12001
6. G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915-926. MR **94d**:11004
7. G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. and System Sci. **13** (1976), 300-317. MR **58**:470a
8. Louis Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science **12** (1980), 97-108. MR **82a**:68078
9. R. G. E. Pinch, *The Carmichael numbers up to 10^{15}* , Math. Comp. **61** (1993), 381-389. MR **93m**:11137

10. ———, *All Carmichael numbers with three prime factors up to 10^{18}* , <http://www.-chalcedon.demon.co.uk/carpsp.html>.
11. J. M. Pollard, *A Monte-Carlo method for factorization*, BIT **15** (1975), 331–334. MR **52**:13611
12. 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
13. M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138. MR **81f**:10003
14. Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math. Comp. **70** (2001), 863–872. MR **2001g**:11009
15. ———, *Using Lucas Sequences to Factor Large Integers Near Group Orders*, The Fibonacci Quarterly **39** (2001), 228–237. MR **2002c**:11173
16. ———, *A one-parameter quadratic-base version of the Baillie-PSW probable prime test*, Math. Comp. **71** (2002), 1699–1734. MR **2003f**:11191

DEPARTMENT OF MATHEMATICS, ANHUI NORMAL UNIVERSITY, 241000 WUHU, ANHUI, PEOPLES
REPUBLIC OF CHINA

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

DEPARTMENT OF MATHEMATICS, ANHUI NORMAL UNIVERSITY, 241000 WUHU, ANHUI, PEOPLES
REPUBLIC OF CHINA