MATHEMATICS OF COMPUTATION
Volume 75, Number 253, Pages 451–460
S 0025-5718(05)01775-8
Article electronically published on September 15, 2005

NOTES ON SOME NEW KINDS OF PSEUDOPRIMES

ZHENXIANG ZHANG

Abstract. J. Browkin defined in his recent paper (Math. Comp. **73** (2004), pp. 1031–1037) some new kinds of pseudoprimes, called Sylow p-pseudoprimes and elementary Abelian p-pseudoprimes. He gave examples of strong pseudoprimes to many bases which are not Sylow p-pseudoprime to two bases only, where $p = 2$ or 3.

In this paper, in contrast to Browkin's examples, we give facts and examples which are unfavorable for Browkin's observation to detect compositeness of odd composite numbers. In Section 2, we tabulate and compare counts of numbers in several sets of pseudoprimes and find that most strong pseudoprimes are also Sylow 2-pseudoprimes to the same bases. In Section 3, we give examples of Sylow p-pseudoprimes to the first several prime bases for the first several primes p. We especially give an example of a strong pseudoprime to the first six prime bases, which is a Sylow p-pseudoprime to the same bases for all $p \in \{2, 3, 5, 7, 11, 13\}$. In Section 4, we define n to be a *k-fold Carmichael Sylow pseudoprime*, if it is a Sylow p-pseudoprime to all bases prime to n for all the first k smallest odd prime factors p of $n - 1$. We find and tabulate all three 3-fold Carmichael Sylow pseudoprimes $< 10^{16}$. In Section 5, we define a positive odd composite n to be a *Sylow uniform pseudoprime to bases* $b_1, \ldots, b_k$, or a Syl-upsp$(b_1, \ldots, b_k)$ for short, if it is a Syl$_p$-psp$(b_1, \ldots, b_k)$ for all the first $\omega(n-1) - 1$ small prime factors p of $n - 1$, where $\omega(n-1)$ is the number of distinct prime factors of $n - 1$. We find and tabulate all the 17 Syl-upsp$(2, 3, 5)$'s $< 10^{16}$ and some Syl-upsp$(2, 3, 5, 7, 11)$'s $< 10^{24}$. Comparisons of effectiveness of Browkin's observation with Miller tests to detect compositeness of odd composite numbers are given in Section 6.

1. Introduction

In August 2002, M. Agrawal, N. Kayal and N. Saxena [1] presented a deterministic polynomial time primality proof algorithm. This was a theoretical breakthrough, but was pointed out by Günter M. Ziegler [18] that, "it is not yet suitable for use in practice". A. Stiglic [13] pointed out that the Rabin-Miller test [8, 12] is probably the primality test the most used in practice.

Let $n > 1$ be an odd integer and let $b_1, \ldots, b_k$ be some reduced residues modulo n. If n is composite and the congruence

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

Received by the editor September 18, 2004.
2000 *Mathematics Subject Classification.* Primary 11A15; Secondary 11A51, 11Y11.
Key words and phrases. Strong pseudoprimes, Miller tests, Sylow p-pseudoprimes, elementary Abelian p-pseudoprimes, k-fold Carmichael Sylow pseudoprimes, Sylow uniform pseudoprimes.
This work was supported by the NSF of China Grant 10071001, and the SF of the Education Department of Anhui Province Grant 2002KJ131.

©2005 American Mathematical Society
Reverts to public domain 28 years from publication

holds for $1 \le j \le k$, then we say that n is a $\mathrm{psp}(b_1, \ldots, b_k)$ (a (Fermat) pseudoprime to bases $b_1, \ldots, b_k$), or write

$$n \in \mathrm{psp}(b_1, \ldots, b_k).$$

If n is composite with $n - 1 = 2^s d$ and d odd, and

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

holds for $1 \le j \le k$, then we say that n passes the Miller test to bases b_j and that n is an $\mathrm{spsp}(b_1, \ldots, b_k)$ (a strong pseudoprime to bases $b_1, \ldots, b_k$) [8], or write

$$n \in \mathrm{spsp}(b_1, \ldots, b_k).$$

(The original test of Miller [8] was somewhat more complicated and was a deterministic, ERH-based test; see [6, Section 3.4].)

The definition of strong pseudoprimes is based on the fact that in a finite field the equation $X^2 = 1$ has at most two solutions, 1 and -1. Browkin [5] defined more general pseudoprimes using the fact that, in a finite field, the equation $X^r = 1$ has at most r solutions for every $r \ge 2$. Let p be a prime such that $n - 1 = p^r m$ with $r > 0$ and $p \nmid m$, and let

$$a_j = b_j^m \tag{1.3}$$

for $1 \le j \le k$. Let

$$c_j = \begin{cases} 1, & \text{if } a_j = 1, \\ a_j^{\mathrm{ord}(a_j)/p}, & \text{if } p | \mathrm{ord}(a_j). \end{cases}$$

The following conditions hold if n is a prime.

(1′) $a_j^{p^r} = 1$ for $1 \le j \le k$.

(2″) If, say, $\mathrm{ord}(a_1) \ge \mathrm{ord}(a_j)$, for $1 \le j \le k$, then $a_2, \ldots, a_k$ belong to the group generated by a_1.

(3″) If, say, $\mathrm{ord}(c_1) \ge \mathrm{ord}(c_j)$, for $1 \le j \le k$, then $c_2, \ldots, c_k$ belong to the group generated by c_1.

(4″) For $1 \le j \le k$, if $\mathrm{ord}(c_j) = p$, then $1 + c_j + c_j^2 + \ldots + c_j^{p-1} = 0$.

Browkin [5, §2] defined a composite number n to be a *Sylow p-pseudoprime to bases* $b_1, \ldots, b_k$, denoted

$$n \in \mathrm{Syl}_p\text{-}\mathrm{psp}(b_1, \ldots, b_k), \tag{1.4}$$

if n satisfies (1′), (2″) and (4″); and to be an *elementary Abelian p-pseudoprime to bases* $b_1, \ldots, b_k$, denoted

$$n \in \mathrm{Elem}_p\text{-}\mathrm{psp}(b_1, \ldots, b_k),$$

if n satisfies (1′), (3″) and (4″). Note that

$$\text{(1.5)} \qquad \text{a composite number } n \text{ satisfies (1}') \iff n \in \mathrm{psp}(b_1, \ldots, b_k).$$

Browkin [5] gave examples of strong pseudoprimes to many bases which are not Sylow p-pseudoprime to two bases only, where $p = 2$ or 3. More precisely, in [5, §§4-5] he checked the numbers ψ_m for $2 \le m \le 8$ and upper bounds of ψ_9, ψ_{10} and ψ_{11} given in [7] and found that every number of which does not belong to some $\mathrm{Syl}_p\text{-}\mathrm{psp}(b_1, b_2)$ for $p = 2$ or 3 and $b_1, b_2 \in \{2, 3, 5\}$, where ψ_m is the smallest strong pseudoprime to all the first m prime bases [11]. In [5, §5] he then verified that for every number n (with one exception) in [7, Table 1: all strong pseudoprimes $n < 10^{12}$ to bases 2, 3 and 5] there exists a prime $p \in \{2, 3, 5\}$ and a

basis $b_1, b_2 \in \{2,3,5\}$ such that $n \notin \mathrm{Syl}_p\text{-psp}(b_1,b_2)$. The exceptional number (No. 73 in the list) $n \notin \mathrm{Syl}_{13}\text{-psp}(2,3)$, where 13 is the third smallest prime divisor of $n-1$.

In this paper, in contrast to Browkin's examples, we give facts and examples which are unfavorable for Browkin's observation to detect compositeness of odd composite numbers. In Section 2, we tabulate and compare counts of numbers in several sets of pseudoprimes and find that most strong pseudoprimes are also Sylow 2-pseudoprimes to the same bases. In Section 3, we give examples of Sylow p-pseudoprimes to the first several prime bases for the first several primes p. We especially give an example of strong pseudoprime to the first six prime bases, which is a Sylow p-pseudoprime to the same bases for all $p \in \{2,3,5,7,11,13\}$. In Section 4, we define n to be a *k-fold Carmichael Sylow pseudoprime*, if it is a Sylow p-pseudoprime to all bases prime to n for all the first k smallest odd prime factors p of $n-1$. We find and tabulate all three 3-fold Carmichael Sylow pseudoprimes $< 10^{16}$. In Section 5, we define a positive odd composite n to be a *Sylow uniform pseudoprime to bases* $b_1,\ldots,b_k$, or a Syl-upsp$(b_1,\ldots,b_k)$ for short, if it is a Syl_p-psp$(b_1,\ldots,b_k)$ for all the first $\omega(n-1)-1$ small prime factors p of $n-1$, where $\omega(n-1)$ is the number of distinct prime factors of $n-1$. We find and tabulate all the 17 Syl-upsp$(2,3,5)$'s $< 10^{16}$ and some Syl-upsp$(2,3,5,7,11)$'s $< 10^{24}$. Comparisons of effectiveness of Browkin's observation with Miller tests to detect compositeness of odd composite numbers are given in Section 6.

2. Sylow 2-pseudoprimes

Let $\mathcal{S}$ be a set of some odd composites and let b_j be the jth prime. Define

$$h_0(\mathcal{S},t) = \#\,\mathcal{S} \cap \ \mathrm{spsp}(b_1,\ldots,b_t),$$
$$h_1(\mathcal{S},t) = \#\,\mathcal{S} \cap \ \mathrm{Elem}_2\text{-psp}(b_1,\ldots,b_t),$$
$$h_2(\mathcal{S},t) = \#\,\mathcal{S} \cap \ \mathrm{Syl}_2\text{-psp}(b_1,\ldots,b_t).$$

Then we have

$$h_2(\mathcal{S},t) \le h_1(\mathcal{S},t) \le h_0(\mathcal{S},t).$$

Let $\mathcal{S}_1$ be the set of 264239 psp(2)'s $< 10^{13}$ [10], let $\mathcal{S}_2$ be the set of 246683 Carmichael numbers $< 10^{16}$ [9], and let $\mathcal{S}_3$ be the set of 52593 spsp$(2,3)$'s $< 10^{16}$

Table 1. The functions $h_i(\mathcal{S}_j,t)$

t	1	2	3	4	5	6	7	8
b_t	2	3	5	7	11	13	17	19
$h_0(\mathcal{S}_1,t)$	58892	2696	240	24	2	1	0	0
$h_1(\mathcal{S}_1,t)$	58892	2696	240	24	2	1	0	0
$h_2(\mathcal{S}_1,t)$	58892	2436	198	15	2	1	0	0
$h_0(\mathcal{S}_2,t)$	4185	435	99	25	9	3	1	0
$h_1(\mathcal{S}_2,t)$	4185	435	99	25	9	3	1	0
$h_2(\mathcal{S}_2,t)$	4185	375	88	25	9	3	1	0
$h_0(\mathcal{S}_3,t)$	52593	52593	4603	606	107	11	2	1
$h_1(\mathcal{S}_3,t)$	52593	52593	4603	606	107	11	2	1
$h_2(\mathcal{S}_3,t)$	52593	47614	3866	413	61	10	1	0

[3]. We list the values of the functions $h_i(\mathcal{S}_j, t)$ for $0 \le i \le 2$ and $1 \le j \le 3$ in Table 1.

Remark 2.1. From Table 1 we have $h_1(\mathcal{S}_j, t) = h_0(\mathcal{S}_j, t)$ for $1 \le j \le 3$. But there do exist strong pseudoprimes $> 10^{16}$ which are not elementary Abelian 2-pseudoprimes to the same bases. However such numbers are few.

Remark 2.2. From Table 1 we also see that most strong pseudoprimes are also Sylow 2-pseudoprimes to the same bases.

3. Sylow p-pseudoprimes to several bases for several p

We have checked all the 52593 spsp$(2,3)$'s $< 10^{16}$ given by Bleichenbacher [3] (also available in the package of [4]). In contrast to Browkin's observation [5, §5] on all the 101 strong pseudoprimes $n < 10^{12}$ to bases 2, 3 and 5, we find all 43 numbers $< 10^{16}$ which are Syl$_p$-psp$(2,3,5)$'s for all $p \in \{2,3,5\}$. Two of the 43 numbers are Syl$_p$-psp$(2,3,5,7)$'s for all $p \in \{2,3,5\}$ listed in Table 2, and another two of the 43 numbers are Syl$_p$-psp$(2,3,5)$'s for all $p \in \{2,3,5,7,11\}$ listed in Table 3.

We have also checked all the 44134 K3-spsp$(2,3,5,7,11)$'s $< 10^{24}$ obtained in our obvious paper [14] and all 330670 K3-spsp$(2,3,5,7,11,13)$'s $< 10^{28}$ computed recently by us. (We call $n = p \cdot q$ a Kk-number [14], if both p and q are primes with $q - 1 = k(p-1)$. A Kk-spsp is a Kk-number and an spsp.) We find a 24-digit number $N_1 \in$ Syl$_p$-psp$(2,3,5,7,11)$ for all $p \in \{2,3,5,7,11\}$, and a 27-digit number $N_2 \in$ Syl$_p$-psp$(2,3,5,7,11,13)$ for all $p \in \{2,3,5,7,11,13\}$; see Examples 3.1 and 3.2 below.

Example 3.1. Let

$$N_1 = 5387\ 86482\ 20306\ 86028\ 51041 = 423787085773 \cdot 1271361257317,$$

and let $B = \{b_1 < \ldots < b_5\} = \{2,3,5,7,11\}$. Then

$$N_1 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 8573 \cdot 4119397 \cdot 412779629$$

and $b_j^{N_1-1} \equiv 1 \mod N_1$ for $1 \le j \le 5$, i.e., $N_1 \in$ psp$(2,3,5,7,11)$. Next one can easily verify that, for all $p \in B$, Conditions $(2'')$ and $(4'')$ hold for $k = 5$. So, we have $N_1 \in$ Syl$_p$-psp$(2,3,5,7,11)$ for all $p \in B$.

Example 3.2. Let

$$N_2 = 54\ 33085\ 44680\ 44402\ 66202\ 96161 = 13457445828493 \cdot 40372337485477.$$

Table 2. List of all Syl$_p$-psp$(2,3,5,7)$'s $< 10^{16}$ for all $p \in \{2,3,5\}$

number n	$n-1$
$4251161764252561 = 24643637 \cdot 172505453$	$2^4 \cdot 3 \cdot 5 \cdot 17 \cdot 31 \cdot 53 \cdot 353 \cdot 563 \cdot 3191$
$7139051111621521 = 31935317 \cdot 223547213$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23 \cdot 83 \cdot 1151 \cdot 2917$

Table 3. List of all Syl$_p$-psp$(2,3,5)$'s $< 10^{16}$ for all $p \in \{2,3,5,7,11\}$

number n	$n-1$
$8724724360769341 = 66048181 \cdot 132096361$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 229 \cdot 6997$
$9048616783520161 = 54919993 \cdot 164759977$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 41 \cdot 83 \cdot 1289 \cdot 55813$

Then

$$N_2 - 1 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^3 \cdot 293 \cdot 6053 \cdot 632329 \cdot 5966273.$$

It is easy to verify that $N_2 \in \mathrm{Syl}_p\text{-psp}(2,3,5,7,11,13)$ for all $p \in \{2,3,5,7,11,13\}$.

Remark 3.1. The number N_1 in Example 3.1 is also an $\mathrm{spsp}(2,3,5,7,11)$ but not an $\mathrm{spsp}(13)$. So, only six Miller tests (1.2) would detect the compositeness of N_1. Since $N_1 \in \mathrm{Syl}_p\text{-psp}(2,3,5,7,11)$ for all $p \in \{2,3,5,7,11\}$, it would be much more expensive to use Browkin's observation to detect the compositeness of N_1 than to use only Miller tests. The same arguments can be used to N_2 in Example 3.2, noting that N_2 is an $\mathrm{spsp}(2,3,5,7,11,13)$ but not an $\mathrm{spsp}(17)$. Moreover, Tables 2 and 3, as well as Examples 3.1 and 3.2 suggest that, for any $k \geq 1$, there would exist Sylow p-pseudoprimes to the first k prime bases for all the first k primes p.

4. Carmichael Sylow p-pseudoprimes for odd p

There are positive odd numbers n such that some of the first several smallest odd primes $(3,5,7,\ldots)$ do not divide $n-1$. To make Browkin's observation applicable to these numbers, one may consider the first several smallest odd prime factors p of $n-1$. Unfortunately, there exist Sylow p-pseudoprimes n to all bases prime to n for all the first several smallest odd prime factors p of $n-1$.

Lemma 4.1. *Let $n = q_1 q_2 \ldots q_s$ be a Carmichael number, and let p be an odd prime such that $p|n-1$ but $p \nmid q_j - 1$ for $1 \leq j \leq s$. Write*

$$\big\{b : 1 \leq b \leq n-1, \gcd(b,n) = 1\big\} = \big\{1 = b_1 < b_2 < \ldots < b_k\big\}.$$

Then $n \in Syl_p\text{-}psp(b_1, b_2, \ldots, b_k)$, i.e., n is a Sylow p-pseudoprime to all bases prime to n.

Proof. Write $n - 1 = p^r m$. Since n is a Carmichael number, Condition $(1')$ holds for all b_j. Since $p \nmid q_j - 1$, we have $q_j - 1 \mid m$, thus $a_j = c_j = 1$ for $1 \leq j \leq k$, i.e., Conditions $(2'')$ and $(4'')$ hold trivially for the set of b_j. □

Definition 4.1. Let n be a Carmichael number, and let p be an odd prime such that $p\,|n-1$. We call n a *Carmichael Sylow p-pseudoprime* if it is a Sylow p-pseudoprime to all bases prime to n. We call n a *k-fold Carmichael Sylow pseudoprime* if it is a Carmichael Sylow p-pseudoprime for all the first k smallest odd prime factors p of $n-1$.

Example 4.1. Let $n = 278545 = 5 \cdot 17 \cdot 29 \cdot 113$. Then $n - 1 = 2^4 \cdot 3 \cdot 7 \cdot 829$. It is easy to check that n is the smallest Carmichael Sylow 3-pseudoprime. It is also a Carmichael Sylow 829-pseudoprime. But n is not a Carmichael Sylow 7-pseudoprime, since we have at least $n \notin \mathrm{Syl}_7\text{-spsp}(2)$. So, n is a 1-fold (but not a 2-fold) Carmichael Sylow pseudoprime.

Let p be an odd prime, and let p_j be the jth prime. Define

$$f_1(p) = \#\big\{n : n \text{ is a Carmichael number} < 10^{16} \text{ with } p|n-1\big\}$$

and

$$f_2(p) = \#\big\{n : n \text{ is a Carmichael Sylow } p\text{-pseudoprime} < 10^{16}\big\}.$$

TABLE 4. The functions $f_1(p_j)$ and $f_2(p_j)$

j	2	3	4	5	6	7	8	...	100
p_j	3	5	7	11	13	17	19	...	541
$f_1(p_j)$	245288	215713	168856	100071	77178	55109	36363	...	630
$f_2(p_j)$	504	6168	10145	12130	11217	10239	9755	...	464

TABLE 5. List of all 3-fold Carmichael Sylow pseudoprimes $< 10^{16}$

number n	factorization of n	factorization of $n-1$	the set $P(n)$
1592075340241	$23 \cdot 89 \cdot 12959 \cdot 60017$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 19 \cdot 31 \cdot 13297$	$\{3, 5, 7, 13297\}$
71370389440481	$1913 \cdot 7649 \cdot 4877513$	$2^5 \cdot 5 \cdot 13 \cdot 167 \cdot 239 \cdot 337 \cdot 2551$	$\{5, 13, 167, 337\}$
235549892165281	$353 \cdot 1013 \cdot 15137 \cdot 43517$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 23 \cdot 43 \cdot 479 \cdot 1223$	$\{3, 5, 7, 479, 1223\}$

After checking all the 246683 Carmichael numbers $< 10^{16}$ computed by Pinch [9], we obtain values of the functions $f_1(p_j)$ and $f_2(p_j)$ listed in Table 4.

We also find all 566 numbers which are 1-fold Carmichael Sylow pseudoprimes $< 10^{16}$. Twenty-three of the 566 numbers are 2-fold Carmichael Sylow pseudoprimes; three of the 23 numbers, listed in Table 5, are 3-fold Carmichael Sylow pseudoprimes, where the set

$$P(n) = \{\text{odd prime } p \mid n-1 : n \text{ is a Carmichael Sylow } p\text{-pseudoprime}\}.$$

Remark 4.1. It is clear that Browkin's observation with p odd is not suitable for detecting compositeness of k-fold Carmichael Sylow pseudoprimes. Alford, Granville and Pomerance [2] have proved that there are infinitely many Carmichael numbers. Table 5 suggests that, for any $k \geq 1$, there would exist (infinitely many) k-fold Carmichael Sylow pseudoprimes.

5. SYLOW UNIFORM PSEUDOPRIMES

In this section, we will exhibit examples n which are Sylow p-pseudoprimes to the first k prime bases for almost all prime divisors p of $n-1$.

Definition 5.1. A positive odd composite n is called a *Sylow uniform pseudoprime to bases* $b_1, \ldots, b_k$, or a Syl-upsp$(b_1, \ldots, b_k)$ for short, if it is a Syl$_p$-psp$(b_1, \ldots, b_k)$ for all the first $\omega(n-1)-1$ small prime factors p of $n-1$, where $\omega(n-1)$ is the number of distinct prime factors of $n-1$.

We have checked all the 52593 spsp$(2,3)$'s $< 10^{16}$ and found all the 17 Syl-upsp$(2,3,5)$'s $< 10^{16}$ listed in Table 6.

We have also checked all the 44134 K3-spsp$(2,3,5,7,11)$'s $< 10^{24}$ and found seven Syl-upsp$(2,3,5,7,11)$'s $n < 10^{24}$ listed in Table 7, where $d = \omega(n-1)-1$ and $n = q_1 \cdot q_2$ with $q_2 - 1 = 3(q_1 - 1)$.

Remark 5.1. Tables 6 and 7 suggest that, for any $k \geq 1$, there would exist (infinitely many) Sylow uniform pseudoprimes to the first k prime bases. However, it is not easy to check whether n is a Sylow uniform pseudoprime when n is large, since it is not an easy task to find the complete factorization of $n-1$ for large n.

TABLE 6. List of all Syl-upsp$(2,3,5)$'s $< 10^{16}$ with $d = \omega(n-1) - 1$

number n	factorization of n	factorization of $n-1$	d
1566655993781	$510989 \cdot 3065929$	$2^2 \cdot 5 \cdot 19 \cdot 59 \cdot 547 \cdot 127747$	5
106105595955049	$4606639 \cdot 23033191$	$2^3 \cdot 3^3 \cdot 47 \cdot 13613 \cdot 767773$	4
164780096725661	$5240549 \cdot 31443289$	$2^2 \cdot 5 \cdot 13^2 \cdot 127 \cdot 293 \cdot 1310137$	5
434625226948681	$5782103 \cdot 75167327$	$2^3 \cdot 3 \cdot 5 \cdot 103 \cdot 12163 \cdot 2891051$	5
436855364627767	$10450543 \cdot 41802169$	$2 \cdot 3 \cdot 7 \cdot 71 \cdot 241 \cdot 349 \cdot 1741757$	6
769527864203407	$13870183 \cdot 55480729$	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 307 \cdot 2347 \cdot 2311697$	6
1547043253687441	$14866277 \cdot 104063933$	$2^4 \cdot 3^4 \cdot 5 \cdot 64237 \cdot 3716569$	4
1650332552073367	$20312143 \cdot 81248569$	$2 \cdot 3 \cdot 7 \cdot 523 \cdot 22193 \cdot 3385357$	5
2149285447663661	$113559289 \cdot 18926549$	$2^2 \cdot 5 \cdot 19 \cdot 1195361 \cdot 4731637$	4
2442103514684021	$20174669 \cdot 121048009$	$2^2 \cdot 5 \cdot 11 \cdot 2200873 \cdot 5043667$	4
3338118916403521	$33357253 \cdot 100071757$	$2^6 \cdot 3 \cdot 5 \cdot 587 \cdot 2131 \cdot 2779771$	5
4334611601490721	$38011453 \cdot 114034357$	$2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 259169 \cdot 3167621$	5
5308450471467601	$27538157 \cdot 192767093$	$2^4 \cdot 3 \cdot 5^2 \cdot 642557 \cdot 6884539$	4
5837815430556961	$44112793 \cdot 132338377$	$2^5 \cdot 3 \cdot 5 \cdot 31 \cdot 213449 \cdot 1838033$	5
6384544705841317	$97861213 \cdot 65240809$	$2^2 \cdot 3 \cdot 7 \cdot 47 \cdot 97 \cdot 6133 \cdot 2718367$	6
6756944341866821	$33558269 \cdot 201349609$	$2^2 \cdot 5 \cdot 17 \cdot 113 \cdot 20963 \cdot 8389567$	5
7549337554356943	$30719167 \cdot 245753329$	$2 \cdot 3^2 \cdot 29 \cdot 31 \cdot 91121 \cdot 5119861$	5

TABLE 7. List of some Syl-upsp$(2,3,5,7,11)$'s $n = q_1 \cdot q_2 < 10^{24}$

number n	q_1	factorization of $n-1$	d
10430138148686413570561	58963655893	$2^9 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 71 \cdot 32713 \cdot 4913637991$	7
1528658307611119608312 01	225732755533	$2^5 \cdot 3 \cdot 5^2 \cdot 3385991333 \cdot 18811062961$	4
2356372504142592100435 21	280260147253	$2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 53^2 \cdot 179 \cdot 1493 \cdot 23355012271$	7
3586911782564145825182 41	345779880973	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 113 \cdot 32785703 \cdot 28814990081$	6
4870138209433562473742 41	402911826973	$2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 3697 \cdot 743069 \cdot 33575985581$	6
7783415838818715555499 21	509359592653	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 287232853 \cdot 42446632721$	6
8853338286835620287102 41	543241452973	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 47 \cdot 83 \cdot 87767 \cdot 45270121081$	8

6. COMPARISONS

Let n be an odd positive composite integer. Let b_k be the kth prime and let p_j be the jth smallest prime factor of $n-1$. If n is an spsp$(b_1, \ldots, b_t)$ but not an spsp(b_{t+1}), then we define

$$T_1(n) = t + 1,$$

i.e., $T_1(n)$ is the number of Miller tests (1.2) used for detecting the compositeness of n. Define

$$T_2(n) = \begin{cases} 3t+1, & \text{if } n \in \mathrm{Syl}_p(2,3,5) \text{ for all } p \in \{p_1, \ldots, p_t\} \text{but } n \notin \mathrm{Syl}_{p_{t+1}}(2); \\ 3t+2, & \text{if } n \in \mathrm{Syl}_p(2,3,5) \text{ for all } p \in \{p_1, \ldots, p_t\} \text{ and } n \in \mathrm{Syl}_{p_{t+1}}(2) \\ & \text{but } n \notin \mathrm{Syl}_{p_{t+1}}(2,3); \\ 3t+3, & \text{if } n \in \mathrm{Syl}_p(2,3,5) \text{ for all } p \in \{p_1, \ldots, p_t\} \text{ and } n \in \mathrm{Syl}_{p_{t+1}}(2,3) \\ & \text{but } n \notin \mathrm{Syl}_{p_{t+1}}(2,3,5). \end{cases}$$

Example 6.1. Let

$$N = 7\ 83218\ 67980\ 76961 = 51095293 \cdot 153285877.$$

Then

$$N - 1 = 2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 29 \cdot 41 \cdot 71 \cdot 293 \cdot 59971.$$

Since $N \in \mathrm{spsp}(2,3,5)$ but $N \notin \mathrm{spsp}(7)$, we have $T_1(N) = 4$. Since

$$N \in \mathrm{Syl}_p\text{-psp}(2,3,5) \text{ for all } p \in \{2,3,5,11,29,41\}$$

and $N \in \mathrm{Syl}_{41}$-psp(2), but $N \notin \mathrm{Syl}_{41}$-psp(2,3), we have $T_2(N) = 20$.

Now suppose Alice uses Miller tests (1.2) (Procedure A) and Bob uses Browkin's observation (Procedure B) to detect the compositeness of an odd positive composite number n, although Procedure B is not explicitly given in [5].

Procedure A; {Input an odd positive composite number n, output $T_1(n)$}
Begin $k \leftarrow 0$;
  Repeat $k \leftarrow k+1$ Until n is not an spsp(b_k) (i.e., (1.2) is not satisfied for b_k);
  $T_1(n) \leftarrow k$
End.

Procedure B; {Input an odd positive composite number n; output $T_2(n)$ and a message if it fails on detecting the compositeness of n}
Begin Using trial division to find all prime factors less than, say 1000, of $n-1$:
  $2 = p_1 < p_2 < \ldots < p_r < 1000$;
  $j \leftarrow 0$; $T_2(n) \leftarrow 0$;
  Repeat $j \leftarrow j+1$; $k \leftarrow 0$;
    repeat $k \leftarrow k+1$; $T_2(n) \leftarrow T_2(n)+1$;
      If (1.4) does not hold for $p = p_j$ Then
        begin Output $T_2(n), p_j$ and b_k; exit end
    until $k = 3$
  Until $j = r$;
  Output the message "The procedure fails on detecting the compositeness of n,"
  "since $n \in \mathrm{Syl}_p(2,3,5)$ for all prime factors $p < 1000$ of $n-1$,"
  "increase the number of bases and try once again"
End.

Remark 6.1. Then p is small, the arithmetic labor for checking (1.4) is almost the same as (in fact a little more than) that for doing k Miller tests, since it is dominated by the number of computations of (1.3). So, if $T_1(n) = T_2(n)$, then one may take into account that both Procedures A and B terminate at the same time.

Let $\mathcal{S}$ be a set of some odd composites, and let g be an integer. Define

$$\Delta(\mathcal{S}, g) = \#\{n \in \mathcal{S} : T_2(n) - T_1(n) = g\},$$

$$F(\mathcal{S}) = \#\{n \in \mathcal{S} : \text{ Procedure B fails on detecting the compositeness of } n\},$$

and for $i = 1$ and 2, define

$$\mathcal{T}_i(\mathcal{S}) = \sum_{n \in \mathcal{S}} T_i(n).$$

Let $\mathcal{S}_1$ be the set of all spsp(2,3,5)'s $< 10^{12}$, and let $\mathcal{S}_2$ be the set of all spsp(2,3,5)'s $< 10^{16}$. The values of $\mathcal{T}_i(\mathcal{S}_j)$, $F(\mathcal{S}_j)$ and $\Delta(\mathcal{S}_j, g)$ are listed in Table 8.

TABLE 8. List of $\mathcal{T}_i(\mathcal{S}_j)$, $F(\mathcal{S}_j)$ and $\Delta(\mathcal{S}_j, g)$

j	$\#\mathcal{S}_j$	$\mathcal{T}_1(\mathcal{S}_j)$	$\mathcal{T}_2(\mathcal{S}_j)$	$F(\mathcal{S}_j)$
1	101	413	443	0
2	4603	19139	20942	28

g	-4	-3	-2	-1	0	1	2	3	4	5 . . . 12	13	14	16
$\Delta(\mathcal{S}_1, g)$	0	0	8	15	38	26	10	1	3	0	0	0	0
$\Delta(\mathcal{S}_2, g)$	7	29	379	611	1673	1302	352	50	112	82	3	2	1

TABLE 9. Additional 11 spsp$(2, 3, 5)$'s $< 10^{16}$, the compositeness of which were not detected by Bob using Procedure B

number n	factorization of n	factorization of $n-1$
85755911820409	$4141399 \cdot 20706991$	$2^3 \cdot 3^2 \cdot 690233 \cdot 1725583$
523892725527121	$8651117 \cdot 60557813$	$2^4 \cdot 3 \cdot 5 \cdot 41 \cdot 103 \cdot 239 \cdot 1213 \cdot 1783$
674135799997687	$12982063 \cdot 51928249$	$2 \cdot 3 \cdot 13 \cdot 8642766666637$
707828998720421	$10861469 \cdot 65168809$	$2^2 \cdot 5 \cdot 35391449936021$
876990254595451	$14807011 \cdot 59228041$	$2 \cdot 3 \cdot 5^2 \cdot 493567 \cdot 11845609$
1085151991776847	$16470823 \cdot 65883289$	$2 \cdot 3 \cdot 7^2 \cdot 23 \cdot 53 \cdot 1103 \cdot 1361 \cdot 2017$
2193553913077421	$19120469 \cdot 114722809$	$2^2 \cdot 5 \cdot 109677695653871$
4253769090466087	$32610463 \cdot 130441849$	$2 \cdot 3 \cdot 708961515077681$
7365160150662949	$27138829 \cdot 271388281$	$2^2 \cdot 3 \cdot 31 \cdot 19798817609309$
7837087315919287	$44263663 \cdot 177054649$	$2 \cdot 3 \cdot 1306181219319881$
9988504355646277	$49971253 \cdot 199885009$	$2^2 \cdot 3 \cdot 832375362970523$

From Table 8 we see that $\mathcal{T}_2(\mathcal{S}_j) > \mathcal{T}_1(\mathcal{S}_j)$, which means that Procedure B runs slower in the average than Procedure A for detecting the compositeness of the 101 spsp$(2, 3, 5)$'s $< 10^{12}$ and of the 4603 spsp$(2, 3, 5)$'s $< 10^{16}$. Moreover, Procedure B fails on detecting the compositeness of 28 spsp$(2, 3, 5)$'s $< 10^{16}$, 17 of which are the Syl-upsp$(2, 3, 5)$'s listed in Table 6, and the other 11 numbers n of which are Syl$_p$-psp$(2, 3, 5)$'s for all prime divisors $p < 1000$ of $n-1$, listed in Table 9. Of course, the compositeness of these 28 spsp$(2, 3, 5)$'s could be detected by Bob using Procedure B, if he checked more than three bases for each prime p. But it is a difficult problem for Browkin's observation to decide how many bases should be checked for each prime p, due to the existence of a k-fold Carmichael Sylow pseudoprime and Sylow uniform pseudoprimes. However, using Miller tests (Procedure A), Alice may not only easily detect the compositeness of all odd composites, but also can give swift primality proofs for primes to given bounds [11, 7, 14, 17, 16, 15].

Remark 6.2. There are six numbers n in Table 9, for each of which $n-1$ has only two small prime divisors.

ACKNOWLEDGMENT

I thank the referee for helpful comments that improved the presentation of the paper.

References

1. M. Agrawal, N. Kayal and N. Saxena, *Primes is in P*, Annals of Mathematics, **160** (2004), 781–793; preprint, August 2002, http://www.cse.iitk.ac.in . MR2123939
2. W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. **140** (1994), 703–722. MR1283874 (95k:11114)
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. D. M. Bressoud and S. Wagon, *A course in computational number theory*, Key College Publishing, Springer-Verlag, New York, 2000. MR1756372 (2001f:11200)
5. Jerzy Browkin, *Some new kinds of pseudoprimes*, Math. Comp. **246** (2004), 1031–1037. MR2031424 (2004m:11006)
6. R. Crandall and C. Pomerance, *Numbers, a computational perspective*, Springer-Verlag, New York, 2001. MR1821158 (2002a:11007)
7. G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926. MR1192971 (94d:11004)
8. G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. and System Sci. **13** (1976), 300–317. MR0480295 (58:470a)
9. R. G. E. Pinch, *The Carmichael numbers up to* 10^{16}, preprint, 1998. http://www.chalcedon.demon.co.uk/carpsp.html.
10. ———, *The pseudoprimes up to* 10^{13}, Algorithmic number theory (Leiden, 2000), 459–473, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000. MR1850626 (2002g:11177) ftp://ftp.dpmms.cam.ac.uk/pub/PSP
11. C. Pomerance, J. L. Selfridge and Samuel S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026. MR0572872 (82g:10030)
12. M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138. MR0566880 (81f:10003)
13. Anton Stiglic, *The PRIMES is in P little FAQ*, http://crypto.cs.mcgill.ca/~stiglic/PRIMES_P_FAQ.html
14. Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math. Comp. **70** (2001), 863–872. MR1697654 (2001g:11009) http://www.ams.org/journal-getitem?pii=S0025-5718-00-01215-1
15. ———, *A one-parameter quadratic-base version of the Baillie-PSW probable prime test*, Math. Comp. **71** (2002), 1699–1734. MR1933051 (2003f:11191) http://www.ams.org/journal-getitem?pii=S0025-5718-02-01424-2
16. ———, *Finding C_3-strong pseudoprimes,* Math. Comp. **74** (2005), 1009–1024. MR2114662
17. Zhenxiang Zhang and Min Tang, *Finding strong pseudoprimes to several bases*. II, Math. Comp. **72** (2003), 2085–2097. MR1986825 (2004c:11008) http://www.ams.org/journal-getitem?pii=S0025-5718-03-01545-X
18. Günter M. Ziegler, *The great prime number record races*, Notices of the AMS **51**:4 (2004), 414–416. MR2039814 (2005a:11198)

Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, People's Republic of China

E-mail address: zhangzhx@mail.ahwhptt.net.cn, ahnu_zzx@sina.com