SOME NEW KINDS OF PSEUDOPRIMES

JERZY BROWKIN

ABSTRACT. We define some new kinds of pseudoprimes to several bases, which generalize strong pseudoprimes. We call them Sylow p-pseudoprimes and elementary Abelian p-pseudoprimes. It turns out that every $n < 10^{12}$, which is a strong pseudoprime to bases 2, 3 and 5, is not a Sylow p-pseudoprime to two of these bases for an appropriate prime $p | n - 1$.

We also give examples of strong pseudoprimes to many bases which are not Sylow p-pseudoprimes to two bases only, where $p = 2$ or 3.

1. INTRODUCTION

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. In the present paper we define more general pseudoprimes using a similar idea. In a finite field the equation $X^r = 1$ has at most r solutions, for every $r \geq 2$. Thus if for some n the congruence $X^r \equiv 1 \pmod{n}$ has more than r solutions, then n is composite. In our definition we consider several bases simultaneously to get many solutions of this congruence.

We give examples of strong pseudoprimes n to several bases $b_1, \ldots, b_k$ which are not pseudoprimes in the new sense. In other words, no number b_j $(1 \leq j \leq k)$ is a witness for n individually, but the set $\{b_1, \ldots, b_k\}$ is a witness for n; i.e., some properties of the set imply that n is composite.

2. DEFINITIONS

Let $n > 1$ be odd and let p be a prime divisor of $n - 1$. More precisely, let $n - 1 = p^r m$, where $r > 0$ and $p \nmid m$. Let $b_1, \ldots, b_k$ be some residues modulo n prime to n, and denote $a_j = b_j^m$, for $j = 1, \ldots, k$.

If n is a prime number, then $(\mathbb{Z}/n)^*$ is a cyclic group of order $n-1$. Consequently

(1) $b^{n-1} = 1$, for every $b \in (\mathbb{Z}/n)^*$.

(2) The Sylow p-subgroup of $(\mathbb{Z}/n)^*$ is cyclic of order p^r.

(3) The maximal elementary Abelian p-subgroup of $(\mathbb{Z}/n)^*$ is cyclic of order p. In particular, for $p = 2$, it is equal to $\{-1, 1\}$.

(4) If a is an element of $(\mathbb{Z}/n)^*$ of order $t > 1$, then $1 + a + a^2 + \cdots + a^{t-1} = 0$.

It follows that also the subgroup $G = \langle b_1, \ldots, b_k \rangle$ generated by the residues $b_1, \ldots, b_k$ is cyclic.

Hence

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

(2′) The Sylow p-subgroup of G is cyclic of order dividing p^r.
(3′) The maximal elementary Abelian p-subgroup of G is cyclic of order 1 or p.
    In particular, for $p = 2$, it is a subgroup of $\{-1, 1\}$.
(4′) For $1 \leq j \leq k$, if the order of a_j is $p^t > 1$, then

$$1 + a_j + a_j^2 + \cdots + a_j^{p^t - 1} = 0.$$

Since the Sylow p-subgroup of G is generated by $a_1, \ldots, a_k$, condition (2′) can be stated equivalently as

(2″) If, say, ord$(a_1) \geq$ ord(a_j), for $j = 1, \ldots, k$, then $a_2, \ldots, a_k$ belong to the group generated by a_1.

To reformulate (3′), we need the following notation. For $j = 1, \ldots, k$, let

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

Thus c_j is an element of order 1 or p.

Evidently the maximal elementary Abelian p-subgroup of G is generated by $c_1, \ldots, c_k$. Consequently (3′) can be stated equivalently as

(3″) If, say, ord$(c_1) \geq$ ord(c_j), for $j = 1, \ldots, k$, then $c_2, \ldots, c_k$ belong to the group generated by c_1. In particular, for $p = 2$, every c_j is equal to 1 or -1.

Finally, from (4′) if follows

(4″) If ord $c_j = p$, then $1 + c_j + c_j^2 + \cdots + c_j^{p-1} = 0$.

The above properties of an odd prime number n lead to the following definition.

Definition.

(i) We call a composite number n satisfying (1′) a p-pseudoprime to bases $b_1, \ldots, b_k$. We use the notation $n \in psp_p\,(b_1, \ldots, b_k)$.

(ii) We call a composite number n satisfying (1′), (2″) and (4′) a Sylow p-pseudoprime to bases $b_1, \ldots, b_k$, and we use the notation

$$n \in Syl_p\text{-}psp\,(b_1, \ldots, b_k).$$

(iii) We call a composite number n satisfying (1′), (3″) and (4″) an elementary Abelian p-pseudoprime to bases $b_1, \ldots, b_k$, and we use the notation

$$n \in Elem_p\text{-}psp\,(b_1, \ldots, b_k).$$

In particular, elementary Abelian 2-pseudoprimes to bases $b_1, \ldots, b_k$ are strong pseudoprimes to these bases. Therefore in place of $Elem_2\text{-}psp\,(b_1, \ldots, b_k)$ we use the notation $spsp\,(b_1, \ldots, b_k)$.

3. Remarks

1. Condition (2″) and condition (3″) for $p > 2$ are nontrivial only, if $k > 1$, i.e., if we consider at least two bases. Conditions (4), (4′) and (4″) give some information also if $k = 1$.

2. Every Sylow p-pseudoprime to bases $b_1, \ldots, b_k$ is a fortiori an elementary Abelian p-pseudoprime to the same bases; thus

$$Syl_p\text{-}psp\,(b_1, \ldots, b_k) \subset Elem_p\text{-}psp\,(b_1, \ldots, b_k) \subset psp_p(b_1, \ldots, b_k).$$

If moreover $p \| n - 1$, then the first two sets are equal.

3. If the set $\{c_1, \ldots, c_k\} \setminus \{1\}$ contains at least p elements, then $(3'')$ is not satisfied, since in a cyclic group of order p there are only $p-1$ elements of order p. Consequently n is composite.

4. If an odd integer n is Sylow p-pseudoprime or elementary Abelian p-pseudoprime, then $p \mid n-1$. Thus to prove that n is not such a pseudoprime, we should consider prime divisors of $n-1$. The examples given in Tables 1 and 2 show that usually very small prime divisors p of $n-1$ suffice, namely 2, 3 or 5 with only one exception.

5. Evidently, if a positive integer n satisfies (1) and does not satisfy at least one of the above conditions (2)–$(4'')$ for some prime divisor p of $n-1$, then n is composite. There are fast primality proving techniques available if $n-1$ is completely or even partially factored (see [KP] and [BLS]). Our examples suggest that the necessary information on prime divisors of $n-1$ can be further reduced.

4. Examples

We illustrate the above definitions by some known examples (see [J], [PSW]) of strong pseudoprimes n to several bases $b_1, \ldots, b_k$. For some small prime divisors p of $n-1$ and for bases $b_1, \ldots, b_k$ we write down the sequences

$$b_j \quad : \quad a_j, \ a_j^p, \ a_j^{p^2}, \ \ldots, \ a_j^{p^r}, \quad \text{for} \quad j = 1, \ldots, k.$$

If $a_j^{p^t} = 1$, for some t, we omit the next terms of the sequence since they are equal to 1.

Example 1. Let $n = 829 \cdot 1657 = 1373653$. Then $n - 1 = 2^2 \cdot 3^3 \cdot 7 \cdot 23 \cdot 79$.

$\underline{p = 2}$
$b_1 = 2 \ : \ a_1 = 890592, \ a_1^2 = -1, \ a_1^4 = 1.$
$b_2 = 3 \ : \ a_2 = 1.$

Therefore n is $spsp\,(2,3)$ and even $n \in Syl_2\text{-}psp\,(2,3)$.

$\underline{p = 3}$
$b_1 = 2 \quad : \quad a_1 = 339686, \ a_1^3 = 1168186, \ a_1^9 = 1.$
$b_2 = 3 \quad : \quad a_2 = 220519, \ a_2^3 = 1282588, \ a_2^9 = 1.$

Therefore $c_1 = a_1^3$, and $c_2 = a_2^3$ are elements of order 3. Since $c_1^2 = 1168186^2 \equiv 210440 \not\equiv c_2 \pmod{n}$, it follows that condition $(2')$ is not satisfied. Hence n is composite, and n is *not* $Elem_3\text{-}psp\,(2,3)$. A fortiori it is *not* $Syl_3\text{-}psp\,(2,3)$.

Example 2. Let $n = 4540612081 \cdot 9081224161 = 41234316135705689041$. Then $n - 1 = 2^4 \cdot 3^3 \cdot \ldots$.

$\underline{p = 2}$
$b_1 = 2 \quad : \quad a_1 = 401\ldots, \ a_1^2 = 406\ldots, \ a_1^4 = -1, \ a_1^8 = 1.$
$b_2 = 3 \quad : \quad a_2 = 261\ldots, \ a_2^2 = 639\ldots, \ a_2^4 = -1, \ a_2^8 = 1.$
$b_3 = 5 \quad : \quad a_3 = 256\ldots, \ a_3^2 = 551\ldots, \ a_3^4 = -1, \ a_3^8 = 1.$

We have replaced last digits of large numbers by dots since these digits are not important for our purposes.

For $b_j \in \{7, 11, 13, 17\}$ we have $a_j^8 = -1$, and for $b_9 = 19$ we have $a_9^4 = -1$.

Therefore n is $spsp\,(2, 3, 5, 7, 11, 13, 17, 19)$.

Since a_1^2, a_2^2, a_3^2 are distinct elements of order four, the group generated by b_1, b_2, b_3 is not cyclic. Hence n is composite and $n \notin Syl_2\text{-}psp\,(2, 3, 5)$.

Now, let G be the group generated by b_1 and b_2 only.

One can easily verify that $(a_1^2)^3 = a_3^2 \neq a_2^2$. Hence in G there are three distinct elements of order four: a_1^2, a_1^6, a_2^2. Consequently the group G is not cyclic. Therefore in view of $(2')$ n is composite and $n \notin Syl_2\text{-}psp\,(2,3)$.

We list the following numbers which are strong pseudoprimes to several bases (see [J]). The numbers n_1 and n_7 have been discussed in the above examples; we include them here for completeness.

$$n_1 = 829 \cdot 1657 = 1373653, \qquad n_1 - 1 = 2^2 \cdot 3^3 \dots.$$
$$n_2 = 2251 \cdot 11251 = 25326001, \qquad n_2 - 1 = 2^4 \cdot 3^3 \cdot 5^3 \dots.$$
$$n_3 = 151 \cdot 751 \cdot 28351 = 3215031751, \qquad n_3 - 1 = 2 \cdot 3^4 \cdot 5^3 \dots.$$
$$n_4 = 6763 \cdot 10627 \cdot 29947 = 2152302898747, \qquad n_4 - 1 = 2 \cdot 3 \cdot 7^2 \dots.$$
$$n_5 = 1303 \cdot 16927 \cdot 157543 = 3474749660383, \qquad n_5 - 1 = 2 \cdot 3^3 \cdot 7 \dots.$$
$$n_6 = 10670053 \cdot 32010157 = 341550071728321, \qquad n_6 - 1 = 2^6 \cdot 3 \cdot 5 \dots.$$
$$n_7 = 4540612081 \cdot 9081224161 = 41234316135705689041,$$
$$n_7 - 1 = 2^4 \cdot 3^3 \dots.$$
$$n_8 = 22754930352733 \cdot 68264791058197 = 1553360566073143205541002401,$$
$$n_8 - 1 = 2^5 \cdot 3^2 \cdot 5^2 \dots.$$
$$n_9 = 137716125329053 \cdot 413148375987157 = 56897193526942024370326972321,$$
$$n_9 - 1 = 2^5 \cdot 3^2 \cdot 5 \dots.$$

5. Tables

The above numbers n_j satisfy (1) but do not satisfy some conditions of $(2')$–$(4'')$. Hence they are composite and are not elementary Abelian (respectively, Sylow) p-pseudoprimes to some bases, as is shown in Table 1. Let us remark that every number n_j $(j = 1, \dots, 9)$ does not belong to some $Syl_p\text{-}psp\,(b_1, b_2)$, where $p = 2$ or 3 and $b_1, b_2 \in \{2, 3, 5\}$ are appropriate bases.

The computations have been done using the GP/PARI package, version 1.39.

We reproduce from [J] the list of all strong pseudoprimes $n < 10^{12}$ to bases 2, 3 and 5. We have verified that for every n in the list (with one exception) there exists a prime $p \in \{2, 3, 5\}$ and a basis $b_1, b_2 \in \{2, 3, 5\}$ such that some of the conditions $(2')$–$(4'')$ are not satisfied. In some cases it is sufficient to consider only the one-element basis, when we use condition $(4'')$. It follows that n is composite, and $n \notin Syl_p\text{-}psp\,(b_1, b_2)$. The results are given in Table 2.

The exceptional number n (No. 73 in Table 2) satisfies $n - 1 = 2^2 \cdot 5 \cdot 13 \cdot \dots$. Moreover, $n \in Syl_p\text{-}psp\,(2, 3, 5)$ for $p = 2$ and 5, but $n \notin psp_2(13) \cup psp_5(13)$.

Table 1.

n	Is *spsp* to bases	Is $Syl_p\text{-}psp$?			Is $Elem_p\text{-}psp$?		
		p	bases		p	bases	
n_1	$2, 3$	2	2,3	YES	3	2,3	NO
n_2	$2, 3, 5$	2	2,3,5	YES	3	2,3	NO
n_3	$2, 3, 5, 7$	2	2,3,5,7	YES	3	2,3	NO
n_4	$2, 3, 5, 7, 11$	2	2,3,5,7,11	YES	3	2,5	NO
n_5	$2, 3, 5, 7, 11, 13$	2	2,3,5,7,11,13	YES	3	2,3	NO
n_6	$2, 3, 5, 7, 11, 13, 17$	2	2,17	NO	3	3,5	NO
n_7	$2, 3, 5, 7, 11, 13, 17, 19$				2	2,3	NO
n_8	$2, 3, 5, 7, 11, 13, 17, 19, 23$	2	2,11	NO	3	2	NO
n_9	$2, 3, 5, 7, 11, 13, 17, 19, 23, 29$	2	2,7	NO	3	2,5	NO

TABLE 2.

No.	n	factorization of $n-1$	p	b_1, b_2
1.	25326001	$2^4 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 67$	3	2,3
2.	161304001	$2^6 \cdot 3 \cdot 5^3 \cdot 11 \cdot 13 \cdot 47$	3	3,5
3.	960946321	$2^4 \cdot 3 \cdot 5 \cdot 29 \cdot 101 \cdot 1367$	2	2,5
4.	1157839381	$2^2 \cdot 3^3 \cdot 5 \cdot 401 \cdot 5347$	3	3,5
5.	3215031751	$2 \cdot 3^4 \cdot 5^3 \cdot 7 \cdot 37 \cdot 613$	3	2,3
6.	3697278427	$2 \cdot 3^3 \cdot 31 \cdot 563 \cdot 3923$	3	2,3
7.	5764643587	$2 \cdot 3^3 \cdot 13 \cdot 19 \cdot 37 \cdot 11681$	3	2
8.	6770862367	$2 \cdot 3 \cdot 199 \cdot 827 \cdot 6857$	3	2,5
9.	14386156093	$2^2 \cdot 3^3 \cdot 7 \cdot 11^3 \cdot 17 \cdot 29^2$	2	2,5
10.	15579919981	$2^2 \cdot 3^2 \cdot 5 \cdot 29 \cdot 1471 \cdot 2029$	3	2,3
11.	18459366157	$2^2 \cdot 3^3 \cdot 7 \cdot 11 \cdot 17 \cdot 37 \cdot 3529$	3	2,3
12.	19887974881	$2^5 \cdot 3 \cdot 5 \cdot 19 \cdot 23 \cdot 59 \cdot 1607$	3	2
13.	21276028621	$2^2 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 47 \cdot 191$	3	2,3
14.	27716349961	$2^3 \cdot 3^4 \cdot 5 \cdot 13 \cdot 109 \cdot 6037$	2	3,5
15.	29118033181	$2^2 \cdot 3^2 \cdot 5 \cdot 257 \cdot 313 \cdot 2011$	3	2,3
16.	37131467521	$2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 73 \cdot 127 \cdot 149$	2	2,5
17.	41752650241	$2^9 \cdot 3^2 \cdot 5 \cdot 7 \cdot 29 \cdot 79 \cdot 113$	2	2,5
18.	42550716781	$2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 97241$	3	2,3
19.	43536545821	$2^2 \cdot 3^5 \cdot 5 \cdot 2459 \cdot 3643$	3	3,5
20.	44732778751	$2 \cdot 3^2 \cdot 5^4 \cdot 11 \cdot 47 \cdot 7691$	3	2
21.	44778481441	$2^5 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 17 \cdot 10181$	3	2,5
22.	48354810571	$2 \cdot 3^7 \cdot 5 \cdot 11 \cdot 19 \cdot 71 \cdot 149$	3	2,3
23.	52139147581	$2^2 \cdot 3^4 \cdot 5 \cdot 13 \cdot 23 \cdot 107641$	3	2,3
24.	53700690781	$2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 2731 \cdot 9931$	3	2,3
25.	56209415767	$2 \cdot 3 \cdot 7^2 \cdot 23 \cdot 859 \cdot 9677$	3	2,5
26.	57698562127	$2 \cdot 3 \cdot 37 \cdot 73 \cdot 541 \cdot 6581$	3	2,3
27.	67403434561	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 73 \cdot 12491$	2	2,5
28.	73796984161	$2^5 \cdot 3 \cdot 5 \cdot 79 \cdot 1307 \cdot 1489$	3	2,5
29.	74190097801	$2^3 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 83{\cdot}107$	3	2,3
30.	75285070351	$2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 269 \cdot 15679$	3	2,5
31.	75350936251	$2 \cdot 3^2 \cdot 5^4 \cdot 19 \cdot 61 \cdot 5779$	3	2,3
32.	77475820141	$2^2 \cdot 3^3 \cdot 5 \cdot 163 \cdot 541 \cdot 1627$	3	2,3
33.	79696887661	$2^2 \cdot 3^3 \cdot 5 \cdot 13 \cdot 29 \cdot 353 \cdot 1109$	3	2,5
34.	83828294551	$2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 41 \cdot 89$	3	2
35.	88473676747	$2 \cdot 3 \cdot 7 \cdot 13 \cdot 67 \cdot 683 \cdot 3541$	3	2,3
36.	88974090367	$2 \cdot 3 \cdot 7 \cdot 53 \cdot 67 \cdot 596573$	3	2
37.	98515393021	$2^2 \cdot 3^5 \cdot 5 \cdot 11 \cdot 137 \cdot 13451$	3	2
38.	111737197441	$2^7 \cdot 3^3 \cdot 5 \cdot 11 \cdot 17 \cdot 151 \cdot 229$	3	2
39.	114247549027	$2 \cdot 3^2 \cdot 13 \cdot 41 \cdot 149 \cdot 229 \cdot 349$	3	2,3
40.	118670087467	$2 \cdot 3^2 \cdot 7 \cdot 47 \cdot 107 \cdot 137 \cdot 1367$	3	2
41.	126223730461	$2^2 \cdot 3^5 \cdot 5 \cdot 53 \cdot 79 \cdot 6203$	5	2,3
42.	134670080641	$2^7 \cdot 3 \cdot 5 \cdot 61 \cdot 521 \cdot 2207$	2	2,3
43.	135586888951	$2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 19^2 \cdot 147289$	3	2,3
44.	136136947201	$2^9 \cdot 3 \cdot 5^2 \cdot 1627 \cdot 2179$	2	2,3
45.	148600530541	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 59 \cdot 181721$	3	3,5
46.	150401047441	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 349 \cdot 256517$	3	2,3

Table 2 (continued)

No.	n	factorization of $n-1$	p	b_1, b_2
47.	156677923729	$2^4 \cdot 3^3 \cdot 19 \cdot 163 \cdot 181 \cdot 647$	3	2,3
48.	157615339681	$2^5 \cdot 3^2 \cdot 5 \cdot 6367 \cdot 17191$	2	2,5
49.	167259489409	$2^7 \cdot 3^5 \cdot 11 \cdot 433 \cdot 1129$	3	2,3
50.	174460968067	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 571 \cdot 34807$	3	2
51.	183413388211	$2 \cdot 3 \cdot 5 \cdot 13 \cdot 31 \cdot 317 \cdot 47857$	3	2
52.	187403492251	$2 \cdot 3^2 \cdot 5^3 \cdot 13 \cdot 37 \cdot 43 \cdot 4027$	3	2,3
53.	216291665041	$2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 47 \cdot 102539$	5	2,3
54.	218215348801	$2^6 \cdot 3 \cdot 5^2 \cdot 29 \cdot 31 \cdot 61 \cdot 829$	3	3,5
55.	218673063181	$2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 31 \cdot 167 \cdot 547$	3	2
56.	234311749201	$2^4 \cdot 3^2 \cdot 5^2 \cdot 53 \cdot 863 \cdot 1423$	2	2,3
57.	240438464197	$2^2 \cdot 3 \cdot 7 \cdot 29 \cdot 4831 \cdot 20431$	2	2,5
58.	244970876021	$2^2 \cdot 5 \cdot 13 \cdot 179 \cdot 521 \cdot 10103$	5	2,3
59.	245291853691	$2 \cdot 3^4 \cdot 5 \cdot 13 \cdot 17 \cdot 1370269$	3	2
60.	247945488451	$2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 19 \cdot 43 \cdot 193 \cdot 953$	3	2
61.	252505670761	$2^3 \cdot 3^4 \cdot 5 \cdot 7 \cdot 47 \cdot 236881$	2	2,5
62.	272447722207	$2 \cdot 3^6 \cdot 11 \cdot 179 \cdot 94903$	3	2
63.	291879706861	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 6367 \cdot 36383$	3	2
64.	295545735181	$2^2 \cdot 3^4 \cdot 5 \cdot 137 \cdot 1331647$	3	2,3
65.	307768373641	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 467 \cdot 20117$	2	2,5
66.	315962312077	$2^2 \cdot 3^2 \cdot 37 \cdot 211 \cdot 479 \cdot 2347$	2	2,5
67.	331630652449	$2^5 \cdot 3^2 \cdot 139 \cdot 193 \cdot 42923$	3	2,3
68.	342221459329	$2^7 \cdot 3^4 \cdot 7 \cdot 757 \cdot 6229$	3	2,3
69.	353193975751	$2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 11 \cdot 283 \cdot 21611$	3	2
70.	354864744877	$2^2 \cdot 3 \cdot 199 \cdot 5987 \cdot 24821$	3	2
71.	362742704101	$2^2 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 239 \cdot 240913$	3	2
72.	398214876001	$2^5 \cdot 3 \cdot 5^3 \cdot 97 \cdot 313 \cdot 1093$	2	2,5
73.	405439595861	$2^2 \cdot 5 \cdot 13 \cdot 47 \cdot 4999 \cdot 6637$	-	-
74.	407979839041	$2^6 \cdot 3 \cdot 5 \cdot 79 \cdot 389 \cdot 13829$	3	3,5
75.	431229929521	$2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 19 \cdot 37 \cdot 421 \cdot 467$	3	2,3
76.	457453568161	$2^5 \cdot 3^2 \cdot 5 \cdot 10847 \cdot 29287$	2	2,5
77.	490883439061	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 23 \cdot 29 \cdot 359 \cdot 1627$	5	2,3
78.	503691743521	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 271 \cdot 61463$	3	2,3
79.	505130380987	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 8461 \cdot 129223$	3	2,3
80.	528929554561	$2^7 \cdot 3 \cdot 5 \cdot 11 \cdot 3181 \cdot 7873$	2	2,5
81.	546348519181	$2^2 \cdot 3^3 \cdot 5 \cdot 19 \cdot 31 \cdot 281 \cdot 6113$	3	2
82.	549866444221	$2^2 \cdot 3^4 \cdot 5 \cdot 101 \cdot 971 \cdot 3461$	3	2
83.	591090138721	$2^5 \cdot 3^4 \cdot 5 \cdot 17 \cdot 137 \cdot 19583$	3	2
84.	641498618881	$2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 367 \cdot 5419$	3	2,3
85.	602248359169	$2^8 \cdot 3^4 \cdot 4519 \cdot 6427$	3	2,3
86.	659937299407	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 509 \cdot 147703$	3	2,5
87.	688529415421	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \cdot 127 \cdot 5669$	3	2
88.	712614969307	$2 \cdot 3^2 \cdot 67 \cdot 113 \cdot 131 \cdot 179 \cdot 223$	3	2,3
89.	729421133761	$2^6 \cdot 3^2 \cdot 5 \cdot 11 \cdot 41^2 \cdot 13697$	3	2
90.	733224429367	$2 \cdot 3 \cdot 11 \cdot 13 \cdot 251 \cdot 499 \cdot 6823$	3	3,5
91.	736775510329	$2^3 \cdot 3^3 \cdot 11 \cdot 13 \cdot 2237 \cdot 10663$	3	2

Table 2 (continued)

No.	n	factorization of $n-1$	p	b_1, b_2
92.	741881186287	$2 \cdot 3 \cdot 71777 \cdot 1722653$	3	2
93.	744049848481	$2^5 \cdot 3 \cdot 5 \cdot 41 \cdot 47 \cdot 883 \cdot 911$	3	2,3
94.	774840343681	$2^7 \cdot 3^2 \cdot 5 \cdot 13 \cdot 19 \cdot 733 \cdot 743$	3	2
95.	842638521121	$2^5 \cdot 3 \cdot 5 \cdot 11^2 \cdot 23 \cdot 73 \cdot 8641$	3	2
96.	851402588401	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 131 \cdot 389$	3	2
97.	853196213761	$2^9 \cdot 3 \cdot 5 \cdot 11 \cdot 1091 \cdot 9257$	2	2,3
98.	863370140641	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 991 \cdot 8941$	3	2
99.	908201935681	$2^6 \cdot 3 \cdot 5 \cdot 13 \cdot 47 \cdot 439 \cdot 3527$	3	2
100.	966299321527	$2 \cdot 3 \cdot 7 \cdot 11^2 \cdot 677 \cdot 280859$	3	2,5
101.	997031384161	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 6863 \cdot 43237$	2	2,5

Note added in March 2002. In a recent paper by Zhang [ZZ] there are given tables of all strong pseudoprimes $< 10^{24}$ (of some special kinds) to at least the first nine prime bases. We have verified that all these pseudoprimes are not elementary Abelian p-pseudoprimes for some bases $b_1, b_2 \in \{2, 3, 5\}$ and some prime $p \in \{2, 3, 5\}$ with one exception. The number n (No. 36 in Table 1 in [ZZ]) is not $Elem_2\text{-}psp\,(2, 7)$.

Note added in October 2002. M. Agrawal, N. Kayal and N. Saxena [AKS] on August 6, 2002, presented a deterministic polynomial time algorithm that determines if a positive integer is prime or composite. In view of this result the importance of pseudoprimes of different kinds, including those defined in the present paper, has been drastically reduced.

References

[AKS] M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, http://www.cse.iitk.ac.in.

[BLS] J. Brillhart, D.H. Lehmer, J.L. Selfridge, *New primality criteria and factorizations of $2^m \pm 1$*, Math. Comp. **29** (1975), 620–647. MR **52:**5546

[J] G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926. MR **94d:**11004

[KP] S. Konyagin, C. Pomerance, *On primes recognizable in deterministic polynomial time*, The mathematics of Paul Erdős (R.L. Graham, J. Nesetril, eds.), vol. I, Springer, Berlin, 1997, pp. 176–198. MR **98a:**11184

[PSW] C. Pomerance, J.L. Selfridge, S.S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$*, Math. Comp. **35** (1980), 1003–1026. MR **82g:**10030

[ZZ] Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math. Comp. **70** (2001), 863–872. MR **2001g:**11009

Institute of Mathematics, University of Warsaw, ul. Banacha 2, PL–02–097 Warsaw, Poland

E-mail address: bro@mimuw.edu.pl