TWO KINDS OF STRONG PSEUDOPRIMES UP TO $10^{36}$

ZHENXIANG ZHANG

Dedicated to the memory of Kencheng Zeng (1927–2004)

Abstract. Let $n > 1$ be an odd composite integer. Write $n - 1 = 2^s d$ with $d$ odd. If either $b^d \equiv 1 \pmod{n}$ or $b^{2^r d} \equiv -1 \pmod{n}$ for some $r = 0, 1, \ldots, s - 1$, then we say that $n$ is a strong pseudoprime to base $b$, or spsp($b$) for short. Define $\psi_t$ to be the smallest strong pseudoprime to all the first $t$ prime bases. If we know the exact value of $\psi_t$, we will have, for integers $n < \psi_t$, a deterministic efficient primality testing algorithm which is easy to implement. Thanks to Pomerance et al. and Jaeschke, the $\psi_t$ are known for $1 \leq t \leq 8$. Conjectured values of $\psi_9, \ldots, \psi_{12}$ were given by us in our previous papers (Math. Comp. 72 (2003), 2085–2097; 74 (2005), 1009–1024).

The main purpose of this paper is to give exact values of $\psi'_t$ for $13 \leq t \leq 19$; to give a lower bound of $\psi'_20$; $\psi'_20 > 10^{36}$; and to give reasons and numerical evidence of K2- and $C_3$-spsp’s $< 10^{36}$ to support the following conjecture: $\psi_t = \psi'_t < \psi''_t$ for any $t \geq 12$, where $\psi'_t$ (resp. $\psi''_t$) is the smallest K2- (resp. $C_3$-) strong pseudoprime to all the first $t$ prime bases. For this purpose we describe procedures for computing and enumerating the two kinds of spsp’s $< 10^{36}$ to the first 9 prime bases. The entire calculation took about 4000 hours on a PC Pentium IV/1.8GHz. (Recall that a K2-spsp is an spsp of the form: $n = pq$ with $p, q$ primes and $q - 1 = 2(p - 1)$; and that a $C_3$-spsp is an spsp and a Carmichael number of the form: $n = q_1 q_2 q_3$ with each prime factor $q_i \equiv 3 \pmod{4}$.)

1. Introduction

Let $n > 1$ be an odd integer. Write $n - 1 = 2^s d$ with $d$ odd. We say that $n$ passes the Miller (strong probable prime) test [5] to base $b$, or that $n$ is an sprp($b$) for short, if

\begin{equation}
\text{either } b^d \equiv 1 \pmod{n} \text{ or } b^{2^r d} \equiv -1 \pmod{n} \text{ for some } r = 0, 1, \ldots, s - 1.
\end{equation}

(The original test of Miller [5] was somewhat more complicated and was a deterministic, ERH-based test; see [1, Section 3.4].) If $n$ is composite and (1.1) holds, then we say that $n$ is a strong pseudoprime to base $b$, or spsp($b$) for short. An spsp($b_1, \ldots, b_l$) is an spsp to all the $t$ bases. Define

\begin{equation}
SB(n) = \#\{b \in \mathbb{Z} : 1 \leq b \leq n - 1, n \text{ is an spsp}(b)\} \quad \text{and} \quad P_R(n) = \frac{SB(n)}{\phi(n)},
\end{equation}

Received by the editor March 8, 2006 and, in revised form, July 8, 2006.

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

Key words and phrases. K2-strong pseudoprimes, $C_3$-strong pseudoprimes, the least strong pseudoprime to the first $t$ prime bases, Rabin-Miller test, biquadratic residue characters, Chinese remainder theorem.

The author was supported by the NSF of China Grant 10071001.

©2007 American Mathematical Society
Reverts to public domain 28 years from publication

2095
where \( \varphi \) is Euler’s function. Monier [6] and Rabin [8] proved that if \( n \) is an odd composite positive integer, then \( SB(n) \leq (n-1)/4 \). In fact, as pointed out by Damg˚ard, Landrock and Pomerance [2], if \( n \neq 9 \) is odd and composite, then \( SB(n) \leq \varphi(n)/4 \), i.e., \( P_9(n) \leq 1/4 \). 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 \( \psi_t \) to be the smallest strong pseudoprime to all the first \( t \) prime bases. If \( n < \psi_t \), then only \( t \) Miller tests are needed to find out whether \( n \) is prime or not. This means that if we know the exact value of \( \psi_t \), then for integers \( n < \psi_t \), 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 Pomerance et al. [7] and Jaeschke [4] we know the exact values of \( \psi_t \) for \( 1 \leq t \leq 8 \) and upper bounds for \( \psi_{10} \) and \( \psi_{11} \):

\[
\psi_9 \leq 41234316135705689041 \quad (20 \text{ digits})
= 4540612081 \cdot 9081224161,
\psi_{10} \leq 1553360566073143205541002401 \quad (28 \text{ digits})
= 2275493035273368264791058197,
\psi_{11} \leq 568971935269420326972321 \quad (29 \text{ digits})
= 137716125329053413148375987157.
\]

Jaeschke [4] 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 \( k \in \{2, 3, 4, 5, 6, 7, 13, 4/3, 5/2\} \); 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 [9], we used biquadratic residue characters and cubic residue characters as main tools to find all \( K2 \)-, \( K3 \)-, \( K4 \)-strong pseudoprimes \(< 10^{24} \) to the first nine or ten prime bases. As a result the upper bounds for \( \psi_{10} \) and \( \psi_{11} \) were considerably lowered:

\[
\psi_{10} \leq N_{10} = 1955097530374556503981 \quad (22 \text{ digits})
= 31265776261 \cdot 62531552521,
\psi_{11} \leq N_{11} = 7395010240794120709381 \quad (22 \text{ digits})
= 60807114061 \cdot 121614228121,
\]

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

\[
\psi_{12} \leq N_{12} = 3186665857834031151167461 \quad (24 \text{ digits})
= 399165290221 \cdot 798330580441.
\]

In [11], we first followed our previous work [9] to find 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 \( n = q_1 q_2 q_3 \) each prime factor \( q_i \equiv 3 \mod 4 \) a \( K_2 \)-number. If \( n \) is a \( K_2 \)-number and an spsp\((b_1, b_2, \ldots, b_t)\), we call \( n \) a \( C_3 \)-spsp\((b_1, b_2, \ldots, b_t)\). It is easy to prove that (see [11, §5])

\[
P_R(n) = 1/4 \iff \text{either } n = pq \text{ is a } K_2\text{-number with } p \equiv 3 \mod 4 \text{ or } n \text{ is a } C_3\text{-number;}
\]

and that

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

We [11] then focused our attention to develop a method for finding all \( C_3 \)-spsp\((2, 3, 5, 7, 11)'s < 10^{20} \). As a result the upper bounds for \( \psi_9, \psi_{10}, \psi_{11} \) are lowered from 20- and 22-decimal-digit numbers to a 19-decimal-digit number:

\[
\psi_9 \leq \psi_{10} \leq \psi_{11} \leq Q_{11} = 3825\,12305\,65464\,13051 \quad (19 \text{ digits})
\]

\[
= 149491 \cdot 747451 \cdot 34233211.
\]

We [11] at last gave reasons to support the following Conjecture 1 (see also [3, Problem A12]).

**Conjecture 1.** We have

\[
\psi_9 = \psi_{10} = \psi_{11} = 3825\,12305\,65464\,13051 \quad (19 \text{ digits}).
\]

Let \( q_1 < q_2 < q_3 \) be odd primes and \( N = q_1 q_2 q_3 \). Put

\[
d = \gcd(q_1 - 1, q_2 - 1, q_3 - 1) \text{ and } h_i = \frac{q_i - 1}{d}, \quad i = 1, 2, 3.
\]

Then we call \( d \) the kernel, the triple \((h_1, h_2, h_3)\) the signature, and \( H = h_1 h_2 h_3 \) the height of \( N \), respectively. In [10, Section 2], we described a procedure for finding \( C_3 \)-spsp\((2)'s \), to a given limit, with heights bounded. There are in total 21978 \( C_3 \)-spsp\((2)'s < 10^{24} \) with heights < \( 10^9 \), only three of which are spsp’s to the first 11 prime bases up to 31. No \( C_3 \)-spsp’s < \( 10^{24} \) to the first 12 prime bases with heights < \( 10^9 \) were found.

Denote by \( \psi'_t \) (resp. \( \psi''_t \)) the smallest \( K_2 \)- (resp. \( C_3 \)-) spsp to all the first \( t \) prime bases. In [10, §5], we gave reasons to support the following Conjecture 2.

**Conjecture 2.** We have

\[
\psi_{12} = \psi'_{12} < 10^{24} < \psi''_{12},
\]

where

\[
\psi'_{12} = N_{12} = 3186\,65857\,83403\,11511\,67461 \quad (24 \text{ digits})
\]

\[
= 399165290221 \cdot 798330580441
\]

was found in [9] (see (1.5)).

The main purpose of this paper is to give reasons and numerical evidence of \( K_2 \)- and \( C_3 \)- strong pseudoprimes < \( 10^{36} \) to support the following Conjecture 3, where the exact values of \( \psi'_t \) for \( 13 \leq t \leq 19 \) and an upper bound of \( \psi''_{20} \) are given in the following Proposition 1.1.

**Conjecture 3.** We have

\[
\psi_t = \psi'_t < \psi''_t
\]

for any \( t \geq 12 \).
Remark 1.1. Conjecture 3 covers Conjecture 2, which is the case \( t = 12 \).

Proposition 1.1. We have

\[
\psi'_1 = 33170 44064 67988 73859 61981 \quad \text{(25 digits)}
\]
\[
= 1287836182261 \cdot 2575672364521;
\]
\[
\psi'_3 = 33170 44064 67988 73859 61981 \quad \text{(25 digits)}
\]
\[
= 1287836182261 \cdot 2575672364521;
\]
\[
\psi'_5 = 5927 63610 75595 57326 34463 30101 \quad \text{(29 digits)}
\]
\[
= 172157429516701 \cdot 344314859033401;
\]
\[
\psi'_7 = 600 30942 89670 10580 03125 96501 \quad \text{(28 digits)}
\]
\[
= 54786377365501 \cdot 109572754731001;
\]
\[
\psi'_9 = 1543 26786 44434 20616 87767 76407 51301 \quad \text{(34 digits)}
\]
\[
= 27778299663977101 \cdot 55556599327954201;
\]
\[
\psi'_{11} > 10^{36}.
\]

In Section 2 we describe a procedure for finding all \( K_2 \)-spsp’s \(< L = 10^{36} \) to the first \( t = 9 \) prime bases. There are in total 90002828 numbers, 100920 of which are spsp’s to the first 13 prime bases. We tabulate 24 of them, which are spsp’s to the first 18 prime bases up to 61, 4 of which are spsp’s to the first 19 prime bases up to 67. No \( K_2 \)-spsp’s \(< 10^{36} \) to the first 20 prime bases are found. Thus the 100920 numbers prove Proposition 1.1. In Section 3 we describe procedures for finding all \( C_3 \)-spsp’s \(< 10^{36} \), to the first \( t = 9 \) prime bases, with heights \(< 10^{10} \). There are in total 43278 numbers. We tabulate 20 of them, which are spsp’s to the first 15 prime bases up to 47, 2 numbers are spsp’s to the first 16 prime bases up to 53. No \( C_3 \)-spsp’s \(< 10^{36} \) to the first 17 prime bases with heights \(< 10^{12} \) are found. Moreover, no \( C_3 \)-spsp’s \(< \psi'_t \) to the first \( t \) prime bases with heights \(< 10^{12} \) are found for \( t \geq 12 \). In Section 4 we reasonably predict that \( \psi'_t < \psi''_t \) for any \( t \geq 12 \). Since \( K_2 \)-spsp’s and \( C_3 \)-spsp’s have \( P_R(n) \) close to or equal to 1/4 (the upper bound of the probability of error for the Rabin-Miller test), Conjecture 3 would be most likely correct. The entire calculation for computing the two kinds of spsp’s \(< 10^{36} \) took about 4000 hours on a PC Pentium IV/1.8GHz.

2. \( K_2 \)-strong pseudoprimes up to \( 10^{36} \)

Let \( \pi \) be a primary irreducible of the ring \( \mathbb{Z}[i] \) of Gaussian integers such that \( q = \pi \overline{\pi} \equiv 1 \mod 4 \) and \( p = (q + 1)/2 \) are two primes determined by \( \pi \). Denote by \( \left( \frac{b}{\pi} \right)_4 \) the biquadratic residue character symbol of \( b \) modulo \( \pi \). Put \( p_\alpha = (\alpha \overline{\alpha} + 1)/2 \) for \( \alpha \in \mathbb{Z}[i] \). Let

\[
R_2 = \{ \text{primary } \alpha = x + yi : 0 \leq x, y < 8, \overline{x} = (-1)^{(x^2-1)/8} \} = \{ 1, 5 + 4i \}.
\]

For a prime \( b \equiv 3 \mod 4 \), let

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

\[
R_b = \{ \alpha = x + yi : 0 \leq x, y < 4b, \alpha \equiv 1 \mod 4, \left( \frac{\alpha \overline{\alpha} - 1}{\beta} \right)_4 = \left( \frac{p_\alpha}{b} \right)_4 \}.
\]
where \( (\cdot) \) is the Jacobi symbol. Let \( M^{(t)} = 4 \prod_{j=1}^{t} b_j \), where \( b_j \) is the \( j \)th prime. Applying the Chinese Remainder Theorem, it is easy to compute the set

\[
R^{(t)} = \{ x + yi : 0 \leq x, y < M^{(t)}, \\
x + yi \pmod{4b} \in R_b \text{ for all the first } t \text{ prime bases } b \}.
\]

In [9], we described a procedure to compute all K2-numbers \( n = pq \), below a given limit \( L \) (say \( 10^{24} \)), which are strong pseudoprimes to the first \( t \geq 6 \) prime bases. The procedure is based on the following proposition.

**Proposition 2.1 ([9] Proposition 3.2).** If \( n = pq \) is an spsp to the first \( t \) prime bases, then there exists \( \alpha \in R^{(t)} \) such that \( \pi \equiv \alpha \pmod{M^{(t)}} \).

Since \( M^{(6)} = 4 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 120120 \) and \( \#R^{(6)} = 2 \cdot 2 \cdot 12 \cdot 30 \cdot 30 = 86400 \) are of suitable size for programming on a PC486 with Turbo pascal 6.0, we [9] successfully found all K2-strong pseudoprimes < \( 10^{24} \) to the first six prime bases.

Now our objective is to compute all K2-numbers \( n = pq < 10^{36} \) on a PC Pentium IV/1.8 GHz with Delphi 6.0, which are strong pseudoprimes to the first 9 prime bases. To speed things up, we should use a larger database \( R^{(t)} \). However, since

\[
\#R^{(9)} = \#R^{(6)} \cdot 56 \cdot 90 \cdot 132 = 4838400 \cdot 11880 = 57480192000,
\]

the set \( R^{(9)} \) is too large to fit in either memory or in a disk file. Considering the storage requirements and the efficiency of the algorithm, we pre-compute the set \( R^{(7)} \) and the set

\[
S = \{ x + yi : 0 \leq x, y < 4 \cdot 19 \cdot 23, x + yi \pmod{4b} \in R_b \text{ for } b = 19 \text{ and } 23 \}
\]

with

\[
M^{(7)} = M^{(6)} \cdot 17 = 2042040, \quad \#R^{(7)} = \#R^{(6)} \cdot 56 = 4838400
\]

and \( \#S = 90 \cdot 132 = 11880 \).

Now we are ready to describe a procedure to compute all K2-spssp’s < \( L = 10^{36} \), to the first \( t \geq 9 \) prime bases, with \( M^{(9)} = M^{(7)} \cdot 19 \cdot 23 = 892371480 \).

**PROCEDURE 2.1.** Finding K2-spssp to the first \( t \geq 9 \) prime bases;

**BEGIN**

For every \( x_1 + y_1i \in R^{(7)} \) Do For every \( x_2 + y_2i \in S \) Do

begin Using the CRT, compute \( x \) and \( y \) such that

\[
0 \leq x, y < M^{(9)}, \quad x + yi \pmod{M^{(7)}} \in R^{(7)}
\]

and \( x + yi \pmod{4 \cdot 19 \cdot 23} \in S \);

For \( u \geq 0, v \geq 0, u + v \leq \frac{\sqrt{\pi}}{\pi - (q + 1)/2}; u \neq p \cdot q; \)

Begin

\[
q \leftarrow (x + uM^{(9)})^2 + (y + vM^{(9)})^2; p \leftarrow (q + 1)/2; n \leftarrow p \cdot q;
\]

If \( n \) is an spsp to the first \( t \) prime bases Then output \( n, p \) and \( q \);

\[
q \leftarrow (x - uM^{(9)})^2 + (y + vM^{(9)})^2; p \leftarrow (q + 1)/2; n \leftarrow p \cdot q;
\]

If \( n \) is an spsp to the first \( t \) prime bases Then output \( n, p \) and \( q \)

End

end

**END.**

The Delphi-Pascal program (with multi-precision package partially written in Assembly language) ran about 2400 hours on a PC Pentium IV/1.8GHz (in fact we
used 10 PCs with each running 10 days) to get all \( K2\)-spsp’s in the first prime bases to the first nine prime bases: 2, 3, 5, 7, 11, 13, 17, 19, and 23. There are in total 90002828 numbers, 100920 of which are spsp’s to the first 13 prime bases, 24 numbers are spsp’s to the first 18 prime bases up to 61 (listed in Table 1), 4 numbers are spsp’s to the first 19 prime bases up to 67. No \( K2\)-spsp’s to the first 20 prime bases are found. Thus, the 100920 numbers prove Proposition 1.1.

Thus, the \( 100920 \) numbers prove Proposition 1.1.

### Table 1. List of all \( K2\)-spsp’s \( n = p(2p - 1) < 10^{36} \) to the first 18 prime bases

<table>
<thead>
<tr>
<th>( n = p(2p - 1) )</th>
<th>( p )</th>
<th>spsp-base</th>
</tr>
</thead>
<tbody>
<tr>
<td>1543 26786 44434 20616 87767 76407 51301</td>
<td>27778290663977101</td>
<td>67 71 73</td>
</tr>
<tr>
<td>3573 96616 43156 88081 50098 90376 80081</td>
<td>422722672638961</td>
<td>0 0 1</td>
</tr>
<tr>
<td>3957 57039 03519 44096 54580 63660 50221</td>
<td>448337968286341</td>
<td>0 0 0</td>
</tr>
<tr>
<td>7434 11233 75303 11731 29413 76567 93141</td>
<td>6096766494438781</td>
<td>0 0 0</td>
</tr>
<tr>
<td>11068 90507 54608 90469 45172 83403 23501</td>
<td>7439390123274501</td>
<td>0 0 1</td>
</tr>
<tr>
<td>15837 76949 08094 27362 08053 96976 19981</td>
<td>88988115753988261</td>
<td>0 0 0</td>
</tr>
<tr>
<td>28474 73466 99486 58439 94849 77173 56181</td>
<td>1193204362881661</td>
<td>0 0 0</td>
</tr>
<tr>
<td>40367 25471 42188 26380 27978 16596 56101</td>
<td>14206909360275701</td>
<td>0 1 0</td>
</tr>
<tr>
<td>71361 96942 79138 04551 29896 91981 34381</td>
<td>188894109791589061</td>
<td>0 1 0</td>
</tr>
<tr>
<td>82824 36407 51608 91096 44501 71525 30181</td>
<td>20349983016099661</td>
<td>1 0 0</td>
</tr>
<tr>
<td>88957 81514 98055 54548 98662 46790 89781</td>
<td>21090023132965861</td>
<td>0 0 1</td>
</tr>
<tr>
<td>1 55559 41557 60759 71544 44226 02410 85421</td>
<td>278890135695676741</td>
<td>0 0 0</td>
</tr>
<tr>
<td>1 79574 77202 19886 65981 89846 22792 23261</td>
<td>29964543204572821</td>
<td>0 1 0</td>
</tr>
<tr>
<td>1 94375 57764 65156 30021 54227 05343 35741</td>
<td>311749561058644981</td>
<td>0 1 0</td>
</tr>
<tr>
<td>2 19337 01033 96078 99098 19416 68785 91181</td>
<td>33162354699026661</td>
<td>0 0 0</td>
</tr>
<tr>
<td>2 52100 58000 17252 74015 37676 90691 76741</td>
<td>35503617932711981</td>
<td>0 0 0</td>
</tr>
<tr>
<td>2 55173 55898 34500 77412 12085 09551 48501</td>
<td>35719291635154901</td>
<td>1 0 0</td>
</tr>
<tr>
<td>4 07387 35132 62980 70201 48352 55040 09841</td>
<td>451324357489321681</td>
<td>0 0 0</td>
</tr>
<tr>
<td>5 27946 43421 43471 71361 92967 10213 53301</td>
<td>513783294183111101</td>
<td>0 0 0</td>
</tr>
<tr>
<td>5 34925 55849 14817 98612 70909 62290 28021</td>
<td>5171680377263666941</td>
<td>0 0 0</td>
</tr>
<tr>
<td>8 08460 12435 54390 22735 02512 76681 37421</td>
<td>637590895010080741</td>
<td>1 0 0</td>
</tr>
<tr>
<td>8 12968 03943 72552 74477 32866 69713 53901</td>
<td>63756099239991301</td>
<td>0 0 0</td>
</tr>
<tr>
<td>8 16345 93783 72388 10402 16654 72644 26261</td>
<td>63884159232813821</td>
<td>0 1 0</td>
</tr>
<tr>
<td>9 64006 87022 43616 26772 79703 83092 14301</td>
<td>694264672233998101</td>
<td>0 0 0</td>
</tr>
</tbody>
</table>

Define the function

\[ F(t, L) = \# \{ N : N \text{ is a } K2\text{-spsp < } L \text{ to the first } t \text{ prime bases} \}. \]

In Table 2 we give \( F(t, L) \) for \( 9 \leq t \leq 19 \) and \( L = 10^{24}, \ldots, 10^{36} \).

### Table 2. The function \( F(t, L) \)

| \( L = 10^{24} \) | 214 | 41 | 6 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| \( L = 10^{28} \) | 15099 | 2680 | 551 | 105 | 12 | 1 | 0 | 0 | 0 | 0 | 0 |
| \( L = 10^{32} \) | 1146700 | 199736 | 38915 | 6913 | 1290 | 224 | 49 | 11 | 2 | 0 | 0 |
| \( L = 10^{36} \) | 90902828 | 15644487 | 3087051 | 546925 | 100920 | 18921 | 3778 | 664 | 128 | 24 | 4 |

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
3. C₃-STRONG PSEUDOPRIMES < 10^{36} WITH HEIGHTS < 10^{12}

The triple \((h_1, h_2, h_3)\) is called \(C₃\)-spsp(2)-acceptable if the \(h_i\) are all odd positive integers, pairwise relatively prime, and \(h_1 \equiv h_2 \equiv h_3 \mod 4\). Let \(q_1 < q_2 < q_3\) be odd primes and \(N = q_1q_2q_3\) with kernel \(d\), signature \((h_1, h_2, h_3)\), and height \(H = h_1h_2h_3\). The kernel \(d\) is called \(C₃\)-spsp(2)-acceptable if \((h_1, h_2, h_3)\) is \(C₃\)-spsp(2)-acceptable and

\[
d \equiv x_0 \mod 4H,
\]

where \(x_0 = x_0 + j_0H \equiv 2 \mod 4\), \(j_0 = (2 - x_0)H \mod 4\), \(0 \leq j_0 \leq 3\), \(x_0\) is the unique integer with \(0 \leq x_0 < H\) such that

\[
x_0 \equiv \begin{cases} 
-h_{2,1} - h_{3,1} \mod h_1, \\
-h_{1,2} - h_{3,2} \mod h_2, \\
-h_{1,3} - h_{2,3} \mod h_3,
\end{cases}
\]

and \(h_{i,j} = h_i^{-1} \mod h_j\) for \(1 \leq i \neq j \leq 3\).

In [10] Section 2, we described a procedure for finding \(C₃\)-spsp(2)’s, to a given limit, with heights bounded. The method is based on the following Lemma 3.1.

**Lemma 3.1 ([10] Theorem 2.1).** Let \(N = q_1q_2q_3\) be a product of three different odd primes. Then we have

\(N\) is a \(C₃\)-spsp(2) \(\iff\) its kernel \(d\) is \(C₃\)-spsp(2)-acceptable.

Let \(b_i\) be the \(i\)th prime, \(t \geq 2\) and \(M_t = 4b_2 \cdots b_t\), and suppose that \((h_1, h_2, h_3)\) is \(C₃\)-spsp(2)-acceptable. For an odd prime \(b\), define the set

\[S_b^{(h_1, h_2, h_3)} = \left\{ u : u = 2 + 4k, 0 \leq k < b, \left( \frac{b}{uh_1+1} \right) = \left( \frac{b}{uh_2+1} \right) = \left( \frac{b}{uh_3+1} \right) \right\},\]

Suppose

\[S_b^{(h_1, h_2, h_3)} \neq \emptyset\]

for \(2 \leq i \leq t\). Define the set

\[R_i^{(h_1, h_2, h_3)} = \left\{ r : 0 \leq r < M_i, r \equiv u_i \mod 4b_i \text{ for some } u_i \in S_{b_i}^{(h_1, h_2, h_3)}, 2 \leq i \leq t \right\}.
\]

The triple \((h_1, h_2, h_3)\) is called \(C₃\)-spsp \((b_1, b_2, \ldots, b_t)\)-acceptable if the system of linear congruences

\[
\begin{align*}
&x \equiv x_0 \mod 4H, \\
&x \equiv u_i \mod 4b_i \text{ for some } u_i \in S_{b_i}^{(h_1, h_2, h_3)}, 2 \leq i \leq t,
\end{align*}
\]

has solutions, or in other words, the system

\[
\begin{align*}
&x \equiv x_0 \mod 4H, \\
&x \equiv r \mod M_i \text{ for some } r \in R_i^{(h_1, h_2, h_3)}
\end{align*}
\]

has solutions. The kernel \(d\) is called \(C₃\)-spsp \((b_1, b_2, \ldots, b_t)\)-acceptable if \((h_1, h_2, h_3)\) is \(C₃\)-spsp \((b_1, b_2, \ldots, b_t)\)-acceptable and (3.3) holds with \(x\) replaced by \(d\).

In [10] Section 4, we speeded up the procedure described in [10] Section 2 so that we can find all \(C₃\)-spsp’s less than a larger limit \(L = 10^{50}\), with the same signature \((1, 37, 41)\), to the first \(t \geq 9\) prime bases. The accelerated procedure is based on the following Lemma 3.2.
Lemma 3.2 ([10 Corollary 4.1]). Let $N = q_1q_2q_3$ be a product of three different odd primes and let $b_i$ be the $i$th prime and $t \geq 2$; and suppose $(h_1, h_2, h_3)$ is $C_3$-$spsp(2)$-acceptable. Then $N$ is a $C_3$-$spsp(b_1, b_2, \ldots, b_t)$ if and only if its kernel $d$ is $C_3$-$spsp(b_1, b_2, \ldots, b_t)$-acceptable.

Now our objective is to find all $N = q_1q_2q_3 < L = 10^{36}$ which are $C_3$-spsp’s to the first $t = 9$ prime bases with heights $H < 10^{12}$. For this purpose, we use Procedure 3.1 (based on Lemma 3.1) for finding all $N$ with heights $10^9 < H < 10^{12}$; and use Procedure 3.2 (based on Lemma 3.2) for finding all $N$ with heights $H < 10^9$.

**PROCEDURE 3.1.** Finding $C_3$-$spsp(b_1, \ldots, b_t)$’s $< L$ with $10^9 < H < 10^{12}$;

**BEGIN** For each $C_3$-$spsp(2)$-acceptable triple $(h_1, h_2, h_3)$ with $10^9 < H = h_1h_2h_3 < 10^{12}$ **Do**

**begin** Using the Euclidean Algorithm and the Chinese Remainder Theorem, compute the seed $x_0$ of the triple $(h_1, h_2, h_3)$: $x_0 \leftarrow x_0; j_0 \leftarrow (6 - x_0 \mod 4)H \mod 4$; If $j_0 > 0$ Then $x_0 \leftarrow x_0 + j_0H$; For $i := 1$ To 3 Do $q_i \leftarrow x_0 h_i + 1; q_1q_2 \leftarrow q_1 \cdot q_2; N \leftarrow q_1q_2 \cdot q_3$; If $N < L$ Then

**begin** If $2^N \equiv 2 \mod q_1q_2$ Then

**begin** If $(q_1, q_2$ and $q_3$ are all spsr’s to the first several prime bases) And ($N$ is an spsp($b_1, \ldots, b_t$)) Then

**end**;

**end**;

**end**;

**END.**

Remark 3.1. Procedure 3.1 is in fact the same but simpler than the original procedure described in [10 Section 2] for finding all $C_3$-$spsp(2)$’s, but we save only those $C_3$-$spsp$’s to the first nine prime bases. Note that, “simpler” means that in the sentence “If $N < L$ Then Begin ... End” there is no loop “repeat ... until $N > L$”, since $H > 10^9$ and $N < 10^{36}$.

Remark 3.2. Using Procedure 3.1 for finding all $N$ with heights $10^9 < H < 10^{12}$, we use 10 PCs. We divide the computations into ten parts with each on one PC: $10^9 < H < 10^{11}$, $j \cdot 10^{11} < H < (j + 1) \cdot 10^{11}, 1 \leq j < 9$. For each part $H_0 \leq H = h_1h_2h_3 \leq H_1$, we loop on $C_3$-$spsp(2)$-acceptable triples $(h_1, h_2, h_3)$ with $1 \leq h_1 \leq \left\lfloor e^{\frac{\ln H_1}{H_1}} \right\rfloor$, $h_1 + 4 \leq h_2 \leq \left\lfloor \sqrt{\frac{H_1}{h_1}} \right\rfloor$, and

$$\max \left\{ h_2, \frac{H_0}{h_1h_2} \right\} < h_3 \leq \min \left\{ \frac{H_1}{h_1h_2}, \frac{1}{8} \left( h_1 + h_2 + \sqrt{(h_1 + h_2)^2 + 8h_1h_2\sqrt{L}} \right) \right\}.$$  

Remark 3.3. Procedure 3.2 is an extended version of the accelerated procedure which was mentioned (but not explicitly written) and which ran only for the triple $(1, 37, 41)$ in [10 Section 4], whereas Procedure 3.2 loops on all $C_3$-acceptable triples $(h_1, h_2, h_3)$ with $h_1h_2h_3 < 10^9$.

**PROCEDURE 3.2.** Finding $C_3$-$spsp(b_1, \ldots, b_t)$’s $< L$ with heights $H < 10^9$;

**BEGIN** For each $C_3$-$spsp(2)$-acceptable triple $(h_1, h_2, h_3)$
with \( H = h_1 h_2 h_3 < 10^9 \)

**Do**

**begin** Using the Euclidean Algorithm and the Chinese Remainder Theorem, compute the seed \( x_0 \) of the triple \((h_1, h_2, h_3)\):

\[
\overline{x_0} \leftarrow x_0; \quad j_0 \leftarrow (6 - x_0 \mod 4) H \mod 4; \quad \text{If } j_0 > 0 \text{ Then } \overline{x_0} \leftarrow x_0 + j_0 H;
\]

Compute the sets \( S_b^{(h_1, h_2, h_3)} \) for \( 2 \leq i \leq t \);

Using the Chinese Remainder Theorem, compute the set \( R_{t_1}^{(h_1, h_2, h_3)} \);

**For** each element \( r \) of the set \( R_{t_1}^{(h_1, h_2, h_3)} \)

**Do**

**Begin** Using the Chinese Remainder Theorem, find a solution

\[
x < L = \text{lcm}[4H, M_t]\]

to the system of congruence

\[
\begin{align*}
x & \equiv \overline{x_0} \mod 4H, \\
x & \equiv r \mod M_t;
\end{align*}
\]

**For** \( i := 1 \) **To** 3 **Do**

\( q_i \leftarrow x h_i + 1; \quad q_1 q_2 \leftarrow q_1 \cdot q_2; \quad N \leftarrow q_1 q_2 \cdot q_3; \)

**If** \( N < L \) **Then**

**repeat**

If \( 2^N \equiv 2 \mod q_1 q_2 \) **Then**

**begin**

If \( (q_1, q_2, q_3) \) are spsp’s to the first several prime bases **And** (\( N \) is an spsp\((b_1, \ldots, b_t)\)) **Then**

output\((N, q_1, q_2, q_3, h_1, h_2, h_3, \ldots)\)

**end**;

**For** \( i := 1 \) **To** 3 **Do**

\( q_i \leftarrow q_1 + h_i L; \quad q_1 q_2 \leftarrow q_1 \cdot q_2; \quad N \leftarrow q_1 q_2 \cdot q_3 \)

**until** \( N > L \)

**End**

**END.**

The two Delphi-Pascal programs with multi-precision package partially written in Assembly language ran about 1600 hours in total on a PC Pentium IV/1.8GHz to get all \( C_3\)-spsp’s \(< 10^{36} \) to the first nine prime bases \( 2, 3, 5, 7, 11, 13, 17, 19, \) and 23, with heights \( H < 10^{12} \). There are in total 43278 numbers, among which 20 numbers are spsp’s to the first 15 prime bases up to 47 (listed in Table 3), 2 numbers are spsp’s to the first 16 prime bases up to 53. No \( C_3\)-spsp’s \(< 10^{36} \) to the first 17 prime bases with heights \(< 10^{12} \) are found. Define the function

\[
(3.4) \quad f(t, L, H) = \# \{ N : N \text{ is a } C_3\text{-spsp}(b_1, b_2, \ldots, b_t) < L \text{ with height } H \}.
\]

In Table 4 we give \( f(t, L, 10^{12}) \) for \( 9 \leq t \leq 16 \) and \( L = 10^{24}, \ldots, 10^{36} \). In Table 5 we give \( f(t, 10^{36}, H) \) for \( 9 \leq t \leq 16 \) and \( H = 10^2, 10^3, \ldots, 10^{12} \). Note that \( f(t, 10^{36}, 10^{12}) = 0 \) for \( t > 16 \).

**Remark** 3.4. Procedure 3.2 ran only 11 hours on a PC Pentium IV/1.8GHz for computing all \( C_3\)-spsp\((b_1, b_2, \ldots, b_9)\)'s \(< 10^{36} \) with heights \( H < 10^9 \). Note that, since

\[
\max \left\{ \# R_{9}^{(h_1, h_2, h_3)} : (h_1, h_2, h_3) \text{ is } C_3\text{-spsp}(b_1, b_2, \ldots, b_9)\text{-acceptable} \right\} = 129600,
\]

each \( R_{9}^{(h_1, h_2, h_3)} \) is of suitable size to fit in the memory of a PC Pentium IV/1.8GHz.
Table 3. List of all $C_3$-spsp's $n = q_1q_2q_3 < 10^{36}$ to the first 15 prime bases with signature $(h_1, h_2, h_3)$ and height $H = h_1h_2h_3 < 10^{12}$

<table>
<thead>
<tr>
<th>$n = q_1q_2q_3$</th>
<th>$q_1$</th>
<th>$h_1$</th>
<th>$h_2$</th>
<th>$h_3$</th>
<th>spsp-base</th>
</tr>
</thead>
<tbody>
<tr>
<td>168779087752367691118001924541713451</td>
<td>46743484851</td>
<td>1</td>
<td>29</td>
<td>57</td>
<td>0 1 0</td>
</tr>
<tr>
<td>4049006419196517352340186981763431</td>
<td>84567440411</td>
<td>17</td>
<td>21</td>
<td>913</td>
<td>0 0 1</td>
</tr>
<tr>
<td>63848482945542749898128326408678791</td>
<td>8854488831</td>
<td>1</td>
<td>29</td>
<td>31713</td>
<td>0 0 1</td>
</tr>
<tr>
<td>73864919593228969777412581863267131</td>
<td>63367821291</td>
<td>1</td>
<td>13</td>
<td>2233</td>
<td>1 0 0</td>
</tr>
<tr>
<td>149872666152476389521373597949057667</td>
<td>34754907427</td>
<td>1</td>
<td>17</td>
<td>21</td>
<td>0 0 0</td>
</tr>
<tr>
<td>22072884304282812126783178906582551</td>
<td>533845618991</td>
<td>1</td>
<td>5</td>
<td>29</td>
<td>0 0 1</td>
</tr>
<tr>
<td>2223715167187667632587593731458561</td>
<td>90866269051</td>
<td>5</td>
<td>13</td>
<td>57</td>
<td>0 1 0</td>
</tr>
<tr>
<td>225351375851571582993575508559015391</td>
<td>243280729991</td>
<td>1</td>
<td>341</td>
<td>4641</td>
<td>1 0 0</td>
</tr>
<tr>
<td>3319780568916064028097700673029575</td>
<td>42096868351</td>
<td>1</td>
<td>5</td>
<td>89</td>
<td>0 0 0</td>
</tr>
<tr>
<td>73956318488637456060742721079709511</td>
<td>4862373591</td>
<td>5</td>
<td>261</td>
<td>61621</td>
<td>0 0 1</td>
</tr>
<tr>
<td>846999408653768764613613557947572971</td>
<td>51195714571</td>
<td>3</td>
<td>23</td>
<td>247</td>
<td>0 1 0</td>
</tr>
<tr>
<td>8611494622243439192567305723901132651</td>
<td>243674295091</td>
<td>41</td>
<td>69</td>
<td>145</td>
<td>0 1 1</td>
</tr>
<tr>
<td>157909679365259951550191589707564171</td>
<td>150454839791</td>
<td>1</td>
<td>165</td>
<td>281</td>
<td>0 0 0</td>
</tr>
<tr>
<td>164290818022112438861652311253450671</td>
<td>191971388071</td>
<td>3</td>
<td>11</td>
<td>19</td>
<td>0 0 1</td>
</tr>
<tr>
<td>32968882238374477242050277300667051</td>
<td>51877805111</td>
<td>1</td>
<td>5</td>
<td>472269</td>
<td>0 0 1</td>
</tr>
<tr>
<td>38129537619606348492758138463105491</td>
<td>12299803975391</td>
<td>1</td>
<td>5</td>
<td>41</td>
<td>0 0 0</td>
</tr>
<tr>
<td>488694766114162789165236319667944651</td>
<td>112309637411</td>
<td>1</td>
<td>5</td>
<td>69</td>
<td>0 1 1</td>
</tr>
<tr>
<td>615953281715442032393107126795144451</td>
<td>326850934411</td>
<td>5</td>
<td>9</td>
<td>49</td>
<td>0 0 0</td>
</tr>
<tr>
<td>66387152401351448198475760839039183</td>
<td>187835202127</td>
<td>11</td>
<td>31</td>
<td>391</td>
<td>0 0 0</td>
</tr>
<tr>
<td>678033047702587416969292603094722251</td>
<td>114879489139</td>
<td>3</td>
<td>23</td>
<td>175</td>
<td>0 0 1</td>
</tr>
</tbody>
</table>

Table 4. The function $f(t, L, 10^{12})$

<table>
<thead>
<tr>
<th>$t$</th>
<th>$L = 10^{24}$</th>
<th>$L = 10^{28}$</th>
<th>$L = 10^{32}$</th>
<th>$L = 10^{36}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>21</td>
<td>217</td>
<td>2808</td>
<td>43278</td>
</tr>
<tr>
<td>10</td>
<td>8</td>
<td>70</td>
<td>821</td>
<td>12623</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>6</td>
<td>249</td>
<td>3655</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>6</td>
<td>70</td>
<td>1019</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>6</td>
<td>17</td>
<td>271</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>80</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 5. The function $f(t, 10^{36}, \mathcal{H})$

<table>
<thead>
<tr>
<th>$\mathcal{H}$</th>
<th>$t = 10^4$</th>
<th>$t = 10^3$</th>
<th>$t = 10^2$</th>
<th>$t = 10^1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H = 10^4$</td>
<td>894</td>
<td>51</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>$H = 10^3$</td>
<td>11592</td>
<td>814</td>
<td>221</td>
<td>56</td>
</tr>
<tr>
<td>$H = 10^2$</td>
<td>22249</td>
<td>1717</td>
<td>482</td>
<td>125</td>
</tr>
<tr>
<td>$H = 10^1$</td>
<td>30385</td>
<td>2531</td>
<td>710</td>
<td>176</td>
</tr>
<tr>
<td>$H = 10^0$</td>
<td>35526</td>
<td>2995</td>
<td>846</td>
<td>216</td>
</tr>
<tr>
<td>$H = 10^{-1}$</td>
<td>38811</td>
<td>3287</td>
<td>922</td>
<td>238</td>
</tr>
<tr>
<td>$H = 10^{-2}$</td>
<td>40872</td>
<td>3454</td>
<td>966</td>
<td>253</td>
</tr>
<tr>
<td>$H = 10^{-3}$</td>
<td>42070</td>
<td>3548</td>
<td>989</td>
<td>264</td>
</tr>
<tr>
<td>$H = 10^{-4}$</td>
<td>42731</td>
<td>3609</td>
<td>1003</td>
<td>268</td>
</tr>
<tr>
<td>$H = 10^{-5}$</td>
<td>43087</td>
<td>3637</td>
<td>1011</td>
<td>270</td>
</tr>
<tr>
<td>$H = 10^{-6}$</td>
<td>43278</td>
<td>3655</td>
<td>1019</td>
<td>271</td>
</tr>
</tbody>
</table>

4. DISCUSSION

In Tables 6, 7, 8, 9, and 10 we give $f(t, \psi^*_u, \mathcal{H})$ for $u = 13, 14, 15, 16$ and 18; and for $t \geq 9$, $\mathcal{H} \leq 10^{12}$. In these tables, if $f(t, \psi^*_u, \mathcal{H}) = 0$ for $\mathcal{H} = 10^{12}$ and for $t \geq t_0$, then the columns for $t \geq t_0$ are all deleted since all entries are 0.
Table 6. The function $f(t, \psi'_{13}, \mathcal{H})$

<table>
<thead>
<tr>
<th>$t$</th>
<th>$\mathcal{H} = 10^1$</th>
<th>$\mathcal{H} = 10^2$</th>
<th>$\mathcal{H} = 10^3$</th>
<th>$\mathcal{H} = 10^4$</th>
<th>$\mathcal{H} = 10^5$</th>
<th>$\mathcal{H} = 10^6$</th>
<th>$\mathcal{H} = 10^7$</th>
<th>$\mathcal{H} = 10^8$</th>
<th>$\mathcal{H} = 10^9$</th>
<th>$\mathcal{H} = 10^{10}$</th>
<th>$\mathcal{H} = 10^{11}$</th>
<th>$\mathcal{H} = 10^{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^1$</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^2$</td>
<td>19</td>
<td>11</td>
<td>4</td>
<td>24</td>
<td>12</td>
<td>5</td>
<td>26</td>
<td>12</td>
<td>5</td>
<td>27</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^3$</td>
<td>25</td>
<td>12</td>
<td>5</td>
<td>26</td>
<td>12</td>
<td>5</td>
<td>27</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^4$</td>
<td>26</td>
<td>12</td>
<td>5</td>
<td>27</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^5$</td>
<td>27</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^6$</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^7$</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
<td>28</td>
<td>13</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 7. The function $f(t, \psi'_{14}, \mathcal{H})$

<table>
<thead>
<tr>
<th>$t$</th>
<th>$\mathcal{H} = 10^2$</th>
<th>$\mathcal{H} = 10^3$</th>
<th>$\mathcal{H} = 10^4$</th>
<th>$\mathcal{H} = 10^5$</th>
<th>$\mathcal{H} = 10^6$</th>
<th>$\mathcal{H} = 10^7$</th>
<th>$\mathcal{H} = 10^8$</th>
<th>$\mathcal{H} = 10^9$</th>
<th>$\mathcal{H} = 10^{10}$</th>
<th>$\mathcal{H} = 10^{11}$</th>
<th>$\mathcal{H} = 10^{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^2$</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^3$</td>
<td>49</td>
<td>15</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^4$</td>
<td>95</td>
<td>37</td>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^5$</td>
<td>129</td>
<td>44</td>
<td>12</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^6$</td>
<td>150</td>
<td>52</td>
<td>13</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^7$</td>
<td>161</td>
<td>56</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^8$</td>
<td>172</td>
<td>58</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^9$</td>
<td>179</td>
<td>60</td>
<td>15</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{10}$</td>
<td>180</td>
<td>60</td>
<td>15</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{11}$</td>
<td>180</td>
<td>60</td>
<td>15</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{12}$</td>
<td>182</td>
<td>61</td>
<td>15</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 8. The function $f(t, \psi'_{15}, \mathcal{H})$

<table>
<thead>
<tr>
<th>$t$</th>
<th>$\mathcal{H} = 10^2$</th>
<th>$\mathcal{H} = 10^3$</th>
<th>$\mathcal{H} = 10^4$</th>
<th>$\mathcal{H} = 10^5$</th>
<th>$\mathcal{H} = 10^6$</th>
<th>$\mathcal{H} = 10^7$</th>
<th>$\mathcal{H} = 10^8$</th>
<th>$\mathcal{H} = 10^9$</th>
<th>$\mathcal{H} = 10^{10}$</th>
<th>$\mathcal{H} = 10^{11}$</th>
<th>$\mathcal{H} = 10^{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^2$</td>
<td>9</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^3$</td>
<td>91</td>
<td>26</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^4$</td>
<td>180</td>
<td>60</td>
<td>15</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^5$</td>
<td>245</td>
<td>71</td>
<td>21</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^6$</td>
<td>283</td>
<td>83</td>
<td>25</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^7$</td>
<td>311</td>
<td>93</td>
<td>26</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^8$</td>
<td>336</td>
<td>97</td>
<td>27</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^9$</td>
<td>344</td>
<td>99</td>
<td>28</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{10}$</td>
<td>348</td>
<td>101</td>
<td>28</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{11}$</td>
<td>348</td>
<td>101</td>
<td>28</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\mathcal{H} = 10^{12}$</td>
<td>350</td>
<td>102</td>
<td>28</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
From Table 6 we may predict that \( f(13, \psi'_{13}, \mathcal{H}) = 0 \) for \( \mathcal{H} > 10^{12} \) and so that 

(4.1) \[ \psi'_{13} < \psi''_{13}. \]

From Table 7 we may predict that \( f(14, \psi'_{14}, \mathcal{H}) = 0 \) for \( \mathcal{H} > 10^{12} \) and so that 

(4.2) \[ \psi'_{14} < \psi''_{14}. \]

From Table 8 we may predict that \( f(15, \psi'_{15}, \mathcal{H}) = 0 \) for \( \mathcal{H} > 10^{12} \) and so that 

(4.3) \[ \psi'_{15} < \psi''_{15}. \]

From Table 9 we may predict that \( f(16, \psi'_{16}, \mathcal{H}) = 0 \) for \( \mathcal{H} > 10^{12} \) and so that 

(4.4) \[ \psi'_{16} = \psi'_{17} < \psi''_{16} \leq \psi''_{17}. \]

From Table 10 we may predict that \( f(18, \psi'_{18}, \mathcal{H}) = 0 \) for \( \mathcal{H} > 10^{12} \) and so that 

(4.5) \[ \psi'_{18} = \psi'_{19} < \psi''_{18} \leq \psi''_{19}. \]

Table 9. The function \( f(t, \psi'_{16}, \mathcal{H}) \)

<table>
<thead>
<tr>
<th>( t )</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{H} = 10^2 )</td>
<td>11</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^3 )</td>
<td>165</td>
<td>50</td>
<td>13</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^4 )</td>
<td>332</td>
<td>106</td>
<td>30</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^5 )</td>
<td>452</td>
<td>128</td>
<td>42</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^6 )</td>
<td>519</td>
<td>146</td>
<td>46</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^7 )</td>
<td>570</td>
<td>164</td>
<td>50</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^8 )</td>
<td>605</td>
<td>169</td>
<td>51</td>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^9 )</td>
<td>618</td>
<td>175</td>
<td>52</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{10} )</td>
<td>622</td>
<td>177</td>
<td>52</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{11} )</td>
<td>625</td>
<td>177</td>
<td>52</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{12} )</td>
<td>630</td>
<td>179</td>
<td>53</td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 10. The function \( f(t, \psi'_{18}, \mathcal{H}) \)

<table>
<thead>
<tr>
<th>( t )</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{H} = 10^2 )</td>
<td>133</td>
<td>31</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^3 )</td>
<td>1641</td>
<td>438</td>
<td>104</td>
<td>29</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^4 )</td>
<td>3212</td>
<td>900</td>
<td>251</td>
<td>75</td>
<td>19</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^5 )</td>
<td>4424</td>
<td>1242</td>
<td>370</td>
<td>110</td>
<td>26</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^6 )</td>
<td>5207</td>
<td>1505</td>
<td>449</td>
<td>133</td>
<td>30</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^7 )</td>
<td>5714</td>
<td>1658</td>
<td>491</td>
<td>142</td>
<td>33</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^8 )</td>
<td>6036</td>
<td>1745</td>
<td>519</td>
<td>150</td>
<td>35</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^9 )</td>
<td>6211</td>
<td>1797</td>
<td>527</td>
<td>153</td>
<td>38</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{10} )</td>
<td>6309</td>
<td>1832</td>
<td>544</td>
<td>157</td>
<td>39</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{11} )</td>
<td>6352</td>
<td>1842</td>
<td>547</td>
<td>158</td>
<td>39</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>( \mathcal{H} = 10^{12} )</td>
<td>6384</td>
<td>1853</td>
<td>549</td>
<td>159</td>
<td>39</td>
<td>15</td>
<td>3</td>
</tr>
</tbody>
</table>
Since the conditions for a number to be a $C_3$-spsp are more stringent than those for it to be a K2-spsp, K2-spsp’s are much more numerous than $C_3$-spsp’s as can be seen from Tables 2 and 4. Thus, combining (4.1)-(4.5) and (1.8), it is reasonable to predict that

$$
\psi'_t < \psi''_t
$$

for any $t \geq 12$.

ACKNOWLEDGMENT

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

REFERENCES


Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, People’s Republic of China
E-mail address: zhangzhx@mail.ah.cn
E-mail address: ahnu_zzx@sina.com
URL: http://www.ahnu.edu.cn/~math/jiaoshou/zzx.htm
URL: http://my.hn8868.com/zhangzhx/