MATHEMATICS OF COMPUTATION
Volume 74, Number 250, Pages 1009–1024
S 0025-5718(04)01693-X
Article electronically published on November 2, 2004

FINDING C_3-STRONG PSEUDOPRIMES

ZHENXIANG ZHANG

ABSTRACT. Let $q_1 < q_2 < q_3$ be odd primes and $N = q_1q_2q_3$. Put

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

Then we call d the *kernel*, the triple (h_1, h_2, h_3) the *signature*, and $H = h_1h_2h_3$ the *height* of N, respectively. We call N a C_3-number if it is a Carmichael number with each prime factor $q_i \equiv 3 \mod 4$. If N is a C_3-number and a strong pseudoprime to the t bases b_i for $1 \le i \le t$, we call N a C_3-spsp$(b_1, b_2, \ldots, b_t)$. Since C_3-numbers have probability of error 1/4 (the upper bound of that for the Rabin-Miller test), they often serve as the exact values or upper bounds of ψ_m (the smallest strong pseudoprime to all the first m prime bases). If we know the exact value of ψ_m, we will have, for integers $n < \psi_m$, a deterministic efficient primality testing algorithm which is easy to implement.

In this paper, we first describe an algorithm 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 $< 10^9$. We then give an overview of the 21978 C_3-spsp(2)'s and tabulate 54 of them, which are C_3-spsp's to the first 8 prime bases up to 19; three numbers 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. We conjecture that there exist no C_3-spsp's $< 10^{24}$ to the first 12 prime bases with heights $\ge 10^9$ and so that

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

which was found by the author in an earlier paper. We give reasons to support the conjecture. The main idea of our method for finding those 21978 C_3-spsp(2)'s is that we loop on candidates of signatures and kernels with heights bounded, subject those candidates $N = q_1q_2q_3$ of C_3-spsp(2)'s and their prime factors q_1, q_2, q_3 to Miller's tests, and obtain the desired numbers. At last we speed our algorithm for finding larger C_3-spsp's, say up to 10^{50}, with a given signature to more prime bases. Comparisons of effectiveness with Arnault's and our previous methods for finding C_3-strong pseudoprimes to the first several prime bases are given.

1. INTRODUCTION

A positive odd integer $n > 1$ is called a strong probable prime to base b, or sprp(b) for short, if it passes the Miller (strong pseudoprime) test [7] to base b, i.e.,

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

Received by the editor August 16, 2003 and, in revised form, January 8, 2004.
2000 *Mathematics Subject Classification.* Primary 11Y11, 11A15, 11A51.
Key words and phrases. Carmichael numbers, C_3-numbers, strong pseudoprimes, C_3-spsp's, Rabin-Miller test, Chinese Remainder Theorem.
Supported by the NSF of China Grant 10071001, the SF of Anhui Province Grant 01046103, and the SF of the Education Department of Anhui Province Grant 2002KJ131.

where $n-1=2^s q$ with q odd. If, in addition, n is composite, then we say that n is a strong pseudoprime to base b, or spsp(b) for short. We say that n is an spsp($b_1, b_2, \ldots, b_t$) if n is a strong pseudoprime to all the t bases b_i.

A Carmichael number is a positive composite integer which satisfies Fermat's Little Theorem

$$b^{n-1} \equiv 1 \mod n \tag{1.2}$$

for any b with $\gcd(n,b)=1$. It follows that a Carmichael number n must be square free with $p-1|n-1$ for each prime $p|n$ and must be a product of at least three odd prime factors. A Carmichael number $n=q_1q_2q_3$ with each prime factor $q_i \equiv 3 \mod 4$ is called a C_3-number. If n is a C_3-number and an spsp($b_1, b_2, \ldots, b_t$), we call n a C_3-spsp($b_1, b_2, \ldots, b_t$).

Define ψ_m to be the smallest strong pseudoprime to all the first m prime bases. If $n<\psi_m$, then only m Miller tests are needed to find out whether n is prime or not. This means that if we know the exact value of ψ_m, then for integers $n<\psi_m$ we will have a deterministic primality testing algorithm which is not only easier to implement but also faster than existing deterministic primality testing algorithms. From Pomerance et al. [9] and Jaeschke [6] we know the exact value of ψ_m for $1 \le m \le 8$ and upper bounds for ψ_9, ψ_{10} and ψ_{11}.

In [11], we tabulated all K2-, K3-, K4-strong pseudoprimes $< 10^{24}$ to the first nine or ten prime bases, where Kk-numbers are the numbers having the form

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

with $k=2,3,4$. As a result the upper bounds for ψ_{10} and ψ_{11} were considerably lowered:

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

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

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

In [12], we found all C_3-spsp$(2,3,5,7,11)$'s $< 10^{20}$. There are in total 110 such numbers. We tabulated 36 of them, which are C_3-spsp's to the first 6 prime bases; one number is an spsp to the first 11 prime bases up to 31. As a result the upper bounds for ψ_9, ψ_{10} and ψ_{11} are lowered from 20- and 22-decimal-digit numbers to a 19-decimal-digit number:

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

Define $\mathrm{SB}(n) = \#\{b \in \mathbb{Z} : 1 \le b \le n-1, n \text{ is an spsp}(b)\}$ and

$$P_R(n) = \frac{\mathrm{SB}(n)}{\varphi(n)}$$

where φ is the Euler's function. It is well known that [5], [10] if $n \ne 9$ is odd and composite, then $\mathrm{SB}(n) \le \varphi(n)/4$, i.e., $P_R(n) \le 1/4$. It is easy to prove that (see

[12, §5])

$$\begin{aligned}&P_R(n) = 1/4 \Longleftrightarrow \\ &\text{either } n = p\,q \text{ is a K2-number with } p \equiv 3 \bmod 4 \text{ or } n \text{ is a } C_3\text{-number};\end{aligned} \tag{1.4}$$

$$\text{if } n \text{ is a K2-spsp(2), then } P_R(n) = 3/16; \tag{1.5}$$

and

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

We see that the bounds N_{10}, N_{11}, N_{12} above are all K2-numbers and Q_{11} is a C_3-number. The reason for these facts is that these numbers n have $P_R(n)$ equal to or close to 1/4. So we [12] make the following conjecture.

Conjecture 1. $\psi_9 = \psi_{10} = \psi_{11} = 3825\ 12305\ 65464\ 13051$ (19 digits).

The main purpose of this paper is to give reasons and numerical evidence to support the following conjecture.

Conjecture 2.

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

Before stating the main results of this paper, we need the following definition.

Definition 1.1. Let $q_1 < q_2 < q_3$ be odd primes and $N = q_1 q_2 q_3$. Let

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

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. We also call H the *height* of the triple (h_1, h_2, h_3).

We describe in Section 2 an algorithm 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 $< 10^9$. In Section 3 we give an overview of the 21978 C_3-spsp(2)'s, among which 1434 numbers, including the 110 ones $< 10^{20}$ found in [12], are C_3-spsp's to the first 5 prime bases; and we tabulate 54 of them, which are C_3-spsp's to the first 8 prime bases up to 19; three numbers 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. In Section 4 we speed up the algorithm for finding larger C_3-spsp's, say up to 10^{50}, with a given signature, to more prime bases. We find 5851 C_3-spsp's $< 10^{50}$ to the first 13 prime bases up to 41 with signature $(1, 37, 41)$, which pass the Axiom release 1.1 test, and we tabulate 25 of them, which are C_3-spsp's to the first 17 prime bases up to 59. In Section 5 we show that C_3-numbers N with heights $> N^{1/3}$ are rare (such numbers are called *hard C_3-numbers*) and reasonably predict that there exist no C_3-spsp's $< 10^{24}$ to the first 12 prime bases with heights $\geq 10^9$. So, by the foregoing arguments, Conjecture 2 would be most likely correct.

The main idea of our method for finding those 21978 C_3-spsp(2)'s is that we loop on candidates of signatures and kernels with heights bounded, subject those candidates $N = q_1 q_2 q_3$ of C_3-spsp(2)'s and their prime factors q_1, q_2, q_3 to Miller's tests and obtain the desired numbers.

Arnault [2] used a sufficient condition for constructing Carmichael numbers which are spsp's to several prime bases and gave a 56 digit sample C_3-spsp, with signature $(1, 37, 41)$, to the first 11 prime bases up to 31, which pass the Axiom release 1.1 test. But his condition is too stringent for most C_3-spsp's to satisfy. The 5851 C_3-spsp's could not be found by his method. In our previous method [12], we loop on the largest prime factor q_3 and propose necessary conditions on $N = q_1q_2q_3$ to be a strong pseudoprime to the first 5 prime bases. Since the q_i are in general much larger than the component h_i of the signature, our previous method is much more expensive than our new one for finding all C_3-spsp(2)'s to a given limit with heights bounded. See Remarks 3.1 and 4.1 for comparisons in details.

2. The method

To state our algorithm more concisely we first need some definitions.

Definition 2.1. Let $h_1 < h_2 < h_3$ be three positive integers. The triple (h_1, h_2, h_3) is called *Carmichael acceptable* (or *C-acceptable*) if the h_i are pairwise relatively prime. A C-acceptable triple (h_1, h_2, h_3) is called C_3-*acceptable* if the h_i are all odd. A C_3-acceptable triple (h_1, h_2, h_3) is called C_3-spsp(2)-*acceptable* if $h_1 \equiv h_2 \equiv h_3 \mod 4$.

Definition 2.2. Let (h_1, h_2, h_3) be *C-acceptable* and

$$h_{i,j} = h_i^{-1} \mod h_j$$

for $1 \le i \ne j \le 3$. Then the system of linear congruences

$$\begin{cases} x \equiv -h_{2,1} - h_{3,1} \mod h_1, \\ x \equiv -h_{1,2} - h_{3,2} \mod h_2, \\ x \equiv -h_{1,3} - h_{2,3} \mod h_3 \end{cases} \tag{2.1}$$

has solutions $x \equiv x_0 \mod H = h_1h_2h_3$ where x_0 is the unique solution with $0 \le x_0 < H$, which is called the *seed* of the C-acceptable triple (h_1, h_2, h_3).

Definition 2.3. 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 $H = h_1h_2h_3$. If (h_1, h_2, h_3) is C-acceptable, let x_0 be the seed of the triple (h_1, h_2, h_3). The kernel d is called C-*acceptable* if (h_1, h_2, h_3) is C-acceptable and $d \equiv x_0 \mod H$. The kernel d is called C_3-*acceptable*, if (h_1, h_2, h_3) is C_3-acceptable and

$$d \equiv \overline{x_0} \mod 4H,$$

where

$$\overline{x_0} = x_0 + j_0H \equiv 2 \mod 4, \quad j_0 = (2 - x_0)H \mod 4, \quad 0 \le j_0 \le 3.$$

We call $\overline{x_0}$ the C_3-*seed* of the C_3-acceptable triple (h_1, h_2, h_3). The kernel d is called C_3-spsp(2)-*acceptable* if (h_1, h_2, h_3) is C_3–spsp(2)-acceptable and d is C_3-acceptable.

Our algorithm is based on the following theorem which needs a lemma.

Lemma 2.1 ([3, Theorem 3.17])**.** *Let $n = q_1q_2q_3$ be a C_3-number. Then*

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

Theorem 2.1. *Let $N = q_1q_2q_3$ be a product of three different odd primes. Then we have*

(1) *N is a Carmichael number if and only if its kernel d is C-acceptable;*
(2) *N is a C_3-number if and only if its kernel d is C_3-acceptable;*
(3) *N is a C_3-spsp(2) if and only if its kernel d is C_3-spsp(2)-acceptable.*

Proof. Let d be the kernel, (h_1, h_2, h_3) the signature, and $H = h_1h_2h_3$ the height of N, and let x_0 be the seed of the triple (h_1, h_2, h_3) when (h_1, h_2, h_3) is C-acceptable.

(1) N is a Carmichael number

$$\begin{aligned}
&\Longleftrightarrow q_i - 1 \mid N - 1 \text{ for } i = 1, 2, 3\\
&\Longleftrightarrow \begin{cases} q_1q_2 - 1 = d^2h_1h_2 + d(h_1 + h_2) \equiv 0 \mod q_3 - 1 = dh_3,\\ q_1q_3 - 1 = d^2h_1h_3 + d(h_1 + h_3) \equiv 0 \mod q_2 - 1 = dh_2,\\ q_2q_3 - 1 = d^2h_2h_3 + d(h_2 + h_3) \equiv 0 \mod q_1 - 1 = dh_1 \end{cases}\\
&\Longleftrightarrow (h_1, h_2, h_3) \text{ is } C\text{-acceptable and } d \equiv x_0 \mod H\\
&\Longleftrightarrow d \text{ is } C\text{-acceptable.}
\end{aligned}$$

(2) Suppose N is a Carmichael number and so d is C-acceptable. Then at least two of the h_i are odd and $d = x_0 + jH$ for some $j \geq 0$. We have

$$\begin{aligned}
&q_i = dh_i + 1 = (x_0 + jH)h_i + 1 \equiv 3 \mod 4 \text{ for } i = 1, 2, 3\\
&\Longleftrightarrow (x_0 + jH)h_i \equiv 2 \mod 4 \text{ for } i = 1, 2, 3\\
&\Longleftrightarrow x_0 + jH \text{ is even, each } h_i \text{ is odd and } j \equiv (2 - x_0)H \mod 4\\
&\Longleftrightarrow d \text{ is } C_3\text{-acceptable.}
\end{aligned}$$

(3) Suppose N is a C_3-number and so d is C_3-acceptable. Then the h_i are all odd and $d \equiv 2 \mod 4$. We have by Lemma 2.1

$$\begin{aligned}
&N \text{ is an spsp}(2) \Longleftrightarrow \left(\frac{2}{q_1}\right) = \left(\frac{2}{q_2}\right) = \left(\frac{2}{q_3}\right)\\
&\Longleftrightarrow q_1 \equiv q_2 \equiv q_3 \mod 8 \Longleftrightarrow dh_1 \equiv dh_2 \equiv dh_3 \mod 8\\
&\Longleftrightarrow h_1 \equiv h_2 \equiv h_3 \mod 4 \Longleftrightarrow d \text{ is } C_3\text{-spsp(2)-acceptable.} \quad \square
\end{aligned}$$

Before describing our algorithm, we need one more lemma.

Lemma 2.2. *Let $N = q_1q_2q_3$ be a Carmichael number with signature (h_1, h_2, h_3). Then*

$$h_3 < \frac{1}{2k}\left(h_1 + h_2 + \sqrt{(h_1 + h_2)^2 + 4h_1h_2\sqrt{kN}}\right),$$

where $k = 2$. If $N = q_1q_2q_3$ is a C_3-spsp(2), then we can take $k = 4$.

Proof. Let d be the kernel of N. Since

$$q_3 - 1 = dh_3 \mid q_1q_2 - 1 = d(dh_1h_2 + h_1 + h_2),$$

we have, $q_1q_2 - 1 = k_3(q_3 - 1)$ for some $k_3 \geq 2$. Thus

$$h_3 \leq \frac{1}{k}(dh_1h_2 + h_1 + h_2) \tag{2.2}$$

where $k = 2$. If $N = q_1q_2q_3$ is a C_3-spsp(2), then $q_1 \equiv q_2 \equiv q_3$ mod 8. Thus we can take $k = 4$, since in this case $q_1q_2 - 1 = k_3(q_3 - 1)$ for some $k_3 \geq 4$.

From (2.2) we have

$$d \geq \frac{kh_3 - h_1 - h_2}{h_1 h_2}.$$

Since $q_1 q_2 - 1 = k_3(q_3 - 1) \geq k(q_3 - 1)$, we have

$$\sqrt{N} > \sqrt{(q_1 q_2 - 1)(q_3 - 1)} \geq \sqrt{k}(q_3 - 1) = \sqrt{k} d h_3 \geq \sqrt{k} h_3 \frac{kh_3 - h_1 - h_2}{h_1 h_2}.$$

Then $k^{3/2} h_3^2 - k^{1/2}(h_1 + h_2)h_3 - h_1 h_2 \sqrt{N} < 0$. Thus

$$h_3 < \frac{1}{2k}\left(h_1 + h_2 + \sqrt{(h_1 + h_2)^2 + 4h_1 h_2 \sqrt{kN}}\right). \qquad \square$$

Now we are ready to describe a procedure to compute all C_3-spsp(2)'s $N = q_1 q_2 q_3 < L$, say, $L = 10^{24}$, with heights $H = h_1 h_2 h_3 < \mathcal{H}$, say, $\mathcal{H} = 10^9 > L^{1/3}$.
PROCEDURE. Finding C_3-spsp(2)'s looping on signatures with heights bounded;

BEGIN $h_1 \leftarrow 1$;
  Repeat $h_2 \leftarrow h_1$;
    repeat $h_2 \leftarrow h_2 + 4$; If $\gcd(h_2, h_1) = 1$ Then
      begin $h_3 \leftarrow h_2$; $\overline{h_3} \leftarrow \frac{1}{8}\left(h_1 + h_2 + \sqrt{(h_1 + h_2)^2 + 8h_1 h_2 \sqrt{L}}\right)$;
        If $\overline{h_3} > \mathcal{H}/(h_1 h_2)$ Then $\overline{h_3} \leftarrow \mathcal{H}/(h_1 h_2)$;
        Repeat $h_3 \leftarrow h_3 + 4$; If $(\gcd(h_3, h_1) = 1)$ And $(\gcd(h_3, h_2) = 1)$ Then
          Begin {Now the triple (h_1, h_2, h_3) is C_3-spsp(2)-acceptable}
            Using Euclidean Algorithm and the Chinese Remainder Theorem
            to compute the seed x_0 of the triple (h_1, h_2, h_3);
            $\overline{x_0} \leftarrow x_0$; $j_0 \leftarrow (6 - x_0 \mod 4)H \mod 4$;
            If $j_0 > 0$ Then $\overline{x_0} \leftarrow x_0 + j_0 H$;
            For $i := 1$ To 3 Do $q_i \leftarrow \overline{x_0} h_i + 1$;
            $q_1 q_2 \leftarrow q_1 \cdot q_2$; $N \leftarrow q_1 q_2 \cdot q_3$;
            If $N < L$ Then
              repeat If $2^N \equiv 2 \mod q_1 q_2$ Then
                begin If (q_1, q_2 and q_3 are all sprp's to the first several prime
                  bases) And (N is an spsp(2)) Then
                  output$(N, q_1, q_2, q_3, h_1, h_2, h_3, x_0, \dots)$
                end;
                For $i := 1$ To 3 Do $q_i \leftarrow q_i + 4h_i H$;
                $q_1 q_2 \leftarrow q_1 \cdot q_2$; $N \leftarrow q_1 q_2 \cdot q_3$
              until $N > L$
          End
        Until $h_3 > \overline{h_3}$
      end
    until $h_2 > (\mathcal{H}/h_1)^{1/2}$;
    $h_1 \leftarrow h_1 + 2$
  Until $h_1 > \mathcal{H}^{1/3}$
END.

Remark 2.1. One may easily modify the procedure a little for computing all Carmichael numbers $N = q_1 q_2 q_3 < L$, with heights $H = h_1 h_2 h_3 < \mathcal{H}$, instead of just only C_3-spsp's.

Remark 2.2. Alford, Granville and Pomerance [1] have proved that there are infinitely many Carmichael numbers, but no one has yet been able to show that there are infinitely many Carmichael numbers n with a fixed number of prime factors. Let (h_1, h_2, h_3) be a C-acceptable triple with height H and seed x_0. If the widely believed Prime k-Tuples Conjecture (see [4, Conjecture 1.2.1]) is true, then there would exist infinitely many integers

$$0 \le j_1 < j_2 < j_3 < \cdots$$

such that

$$q_{i,u} = q_{i,u}(h_1, h_2, h_3) = d_u h_i + 1 = x_0 h_i + 1 + j_u h_i H$$

are all primes for $1 \le i \le 3$ and $u = 1, 2, 3, \ldots,$ where $d_u = x_0 + j_u H$. Let $N_u = N_u(h_1, h_2, h_3) = q_{1,u} q_{2,u} q_{3,u}$, $u = 1, 2, 3, \ldots$. Then

$$N_1 < N_2 < N_3 < \cdots \tag{2.3}$$

would be infinitely many Carmichael numbers with three prime factors. We call (2.3) the chain of Carmichael numbers with signature (h_1, h_2, h_3). Since there exist infinitely many C-acceptable triples, there would exist infinitely many pairwise disjoint chains of Carmichael numbers with three prime factors. The same arguments can be applied to C_3-numbers and C_3-spsp(2)'s.

Example 2.1. The C-acceptable triple having the smallest height among all C-acceptable ones is $(1, 2, 3)$ with height $H = 6$ and seed $x_0 = 0$; the first (the smallest) element of the Carmichael number chain with signature $(1, 2, 3)$ is

$$1729 = 7 \cdot 13 \cdot 19$$

with kernel $d = 6 = 0 + 6 \cdot 1$. The C_3-acceptable triple having the smallest height among all C_3-acceptable ones is $(1, 3, 5)$ with height $H = 15$, seed $x_0 = 12$ and C_3-seed $\overline{x_0} = 42 = 12 + 15 \cdot 2$; the first (the smallest) element of the C_3-number chain with signature $(1, 3, 5)$ is

$$1152271 = 43 \cdot 127 \cdot 211$$

with kernel $d = 42 = 42 + (15 \cdot 4) \cdot 0$. The C_3-spsp(2)-acceptable triple having the smallest height among all C_3-spsp(2)-acceptable ones is $(1, 5, 9)$ with height $H = 45$, seed $x_0 = 15$, and C_3-seed $\overline{x_0} = 150 = 15 + 45 \cdot 3$; the first (the smallest) element of the C_3-spsp(2) chain with signature $(1, 5, 9)$ is

$$83828294551 = 1231 \cdot 6151 \cdot 11071$$

with kernel $d = 1230 = 150 + (45 \cdot 4) \cdot 6$.

3. Numerical results and statistics

The Pascal program (with multi-precision package partially written in Assembly language) ran about 50 hours on a PC Pentium III/800 to get all C_3-spsp(2)'s $< 10^{24}$ with heights $< 10^9$. There are in total 21978 numbers, among which 54 numbers are spsp's to the first 8 prime bases up to 19 (listed in Table 1), 21 numbers are spsp's to base 23, 8 numbers are spsp's to bases 23 and 29, 3 numbers are spsp's to the first 11 prime bases up to 31. No C_3-spsp's $< 10^{24}$ with heights $< 10^9$, to the first 12 prime bases, are found.

TABLE 1. List of all C_3-spsp's $< 10^{24}$, with heights $< 10^9$, to the first 8 prime bases

$N = q_1q_2q_3$	q_1	h_1	h_2	h_3	x_0	spsp-base		
						23	29	31
230245660726188031	214831	3	11	19	132	0	0	1
3825123056546413051	149491	1	5	229	640	1	1	1
5474093792130026911	21319	1	105	5381	21318	0	0	0
7361235187296010651	412339	1	5	21	3	0	0	0
8276442534101054431	209431	1	17	53	398	0	0	1
19506933590956650531 1	393031	1	17	189	1044	0	0	0
25469985015649185453 1	712219	1	5	141	168	1	0	0
40610917351557456703 9	307399	1	41	341	13797	1	0	0
112773764045349826965 1	1133731	3	7	995	1800	0	1	1
139779427151487584565 1	1336891	1	9	65	165	0	0	0
224292158717904151875 1	3993991	7	23	75	3045	1	0	0
319460742982089687825 1	526051	1	105	209	21315	0	1	0
441213088540587948585 1	1570339	11	91	1515	142758	0	0	0
570104655158443952547 1	2518231	1	17	21	309	0	0	0
595869509740552324095 1	2897311	1	5	49	185	1	0	0
911314525340775178935 1	976951	15	247	8903	65130	0	1	0
993972731979000137535 1	6778351	15	43	167	21030	0	1	1
1037055616416837046575 1	1395871	1	41	93	312	1	1	0
1176657172366284018837 1	12264211	21	29	97	52353	0	1	0
1313889853517903418603 1	1360591	11	347	1819	123690	1	0	1
1766159991152186496466 7	334643	1	13	36253	334642	0	0	1
2237787157962922024095 1	2281231	1	29	65	380	0	1	0
2380362741442179991305 1	4756771	5	57	97	11424	0	0	0
2464196018797992453975 1	2320399	51	451	11375	45498	1	0	0
3111409371765198556470 7	2248507	1	17	161	1429	1	0	1
3495719492846984063644 3	3436987	1	21	41	735	0	1	1
3631156270342606676853 1	574939	1	265	721	1743	0	0	0
4041589346619830405127 1	2327599	1	5	641	768	1	1	0
4555599196577337237483 1	7570399	1	5	21	3	0	0	0
4667208996813629921109 1	4983931	1	13	29	367	0	1	0
4885749362750954023161 1	2505859	1	5	621	123	1	0	0
5253413101542350063865 1	7002451	1	9	17	99	0	0	0
12617461148084254071225 1	4585051	1	17	77	932	1	1	0
13819973458347443930697 1	3157771	1	21	209	2079	0	0	0
17073808938169743162403 1	3926231	1	13	217	2219	1	0	1
20931227641082404344699 1	11881879	19	99	455	625362	0	0	1
21663766795648804414315 1	5003951	1	13	133	224	0	1	1
23353411629509907754809 1	784939	1	221	2185	302053	1	0	0
25551757030400281388565 1	9047611	1	5	69	330	1	0	1
28610231065329864173643 1	17614759	7	27	95	2694	1	0	1
33427721081950041218229 1	2771011	9	13	97889	307890	0	0	0
35173884248991928130145 1	3400531	1	5	1789	1430	1	1	0
36867647851609373432310 7	10507267	7	87	179	83895	0	1	1
42734391822939375637356 7	10617847	1	17	21	309	1	1	1
47091936544470035249358 7	36877387	29	53	149	126569	0	1	0
54451329379819377319041 1	5744131	1	17	169	1003	0	0	0
60486203039414891522745 1	4783819	1	25	221	4693	0	1	1
69437782666361849976423 1	11493871	31	99	4439	370770	1	1	0
73964292495163101143847 1	2960791	1	69	413	25599	1	0	0
76950674716263576321436 3	4035043	1	53	221	5770	0	0	0
79364433000345398723223 1	754111	1	393	4709	754110	0	0	0
85810426518262041380295 1	15186511	1	5	49	185	1	1	1
86743397258379346787445 1	35988811	13	17	185	29075	0	1	1
89609846055247280537775 1	5389231	1	25	229	2005	0	0	1

For the rest of this paper let b_i be the ith prime. Define sets

$$(3.1)\qquad \begin{cases} C_3(t,L) & = \{N : N \text{ is a } C_3\text{-spsp}(b_1, b_2, \ldots, b_t) < L\}, \\ C_3(t,L,\mathcal{H}) & = \{N : N \in C_3(t,L) \text{ with height} < \mathcal{H}\} \end{cases}$$

and functions

$$(3.2)\qquad f(t,L) = \#C_3(t,L) \quad \text{and} \quad f(t,L,\mathcal{H}) = \#C_3(t,L,\mathcal{H})$$

for $t \geq 1$. The sets and functions can be extended for $t = 0$, in which case $C_3(0,L)$ is the set of all C_3-numbers $< L$, etc. Then we have

$$C_3(0,L) \supseteq C_3(1,L) \supseteq C_3(2,L) \supseteq \cdots .$$

In Table 2 we give $f(t,L,10^9)$ for $t = 1, 2, \ldots, 11$ and $L = 10^{10}, 10^{12}, \ldots, 10^{24}$. In Table 3, we give $f(t, 10^{24}, \mathcal{H})$ for $1 \leq t \leq 11$ and $\mathcal{H} = 10^2, 10^3, \ldots, 10^9$.

Table 2. The function $f(t,L,10^9)$

L	10^{10}	10^{12}	10^{14}	10^{16}	10^{18}	10^{20}	10^{22}	10^{24}
$t = 1$	1	8	35	157	522	1790	6179	21978
$t = 2$	1	6	28	100	364	1277	4381	15575
$t = 3$	1	4	18	60	203	710	2446	8581
$t = 4$	1	1	7	19	89	337	1205	4205
$t = 5$	0	0	3	6	28	110	393	1434
$t = 6$	0	0	1	2	8	36	128	481
$t = 7$	0	0	0	1	2	12	48	165
$t = 8$	0	0	0	0	1	5	17	54
$t = 9$	0	0	0	0	0	1	5	21
$t = 10$	0	0	0	0	0	1	1	8
$t = 11$	0	0	0	0	0	1	1	3

Table 3. The function $f(t, 10^{24}, \mathcal{H})$

$\mathcal{H}$	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
$t = 1$	1883	7214	12290	16280	19040	20675	21562	21978
$t = 2$	1883	6009	9481	12106	13836	14851	15344	15575
$t = 3$	1341	3523	5336	6704	7646	8186	8464	8581
$t = 4$	321	1888	2728	3355	3800	4036	4167	4205
$t = 5$	81	568	886	1124	1285	1364	1419	1434
$t = 6$	29	170	283	366	428	456	476	481
$t = 7$	6	53	91	119	144	155	163	165
$t = 8$	0	14	29	39	47	50	53	54
$t = 9$	0	5	13	17	18	19	20	21
$t = 10$	0	2	7	7	7	7	8	8
$t = 11$	0	2	3	3	3	3	3	3

Remark 3.1. The smallest five numbers $< 10^{20}$ in Table 1 appeared earlier in [12, Table 5] where we used 1600 hours of CPU time on a PC Pentium III/800 to find all 110 C_3-spsp$(2,3,5,7,11)$'s $< 10^{20}$. Since all the 110 numbers have heights $< 10^9$, they were caught once again (see Table 2: $f(5, 10^{20}, 10^9) = 110$) and much more information than that was obtained by our new method, using only 50 hours of CPU time on the same machine. In our previous method, we loop on the largest prime factor q_3 and propose necessary conditions on $N = q_1q_2q_3$ to be a strong pseudoprime to the first 5 prime bases. In the new method we loop on C_3-spsp(2)-acceptable signatures (h_1, h_2, h_3) and kernels d. For a given C_3-spsp(2)-acceptable triple (h_1, h_2, h_3), the procedure loops at most $\lfloor (L/(4^3H^4))^{1/3} \rfloor$ times in the "repeat $\cdots$ until $N > L$" loop. So, when L is not too large, say, $L = 10^{24}$, it does not take much time on a modern PC (say, Pentium III/800) for a given triple (h_1, h_2, h_3) until $N > L$. Since the h_i are in general much smaller than the prime factors q_i of N, our new method is much faster than the previous one for finding all those $N < L$ with heights H to a given limit, say, $H < L^{1/3}$ or $H < L^{3/8}$.

Remark 3.2. From Table 3 we see the following facts:
(1) there is only one C_3-spsp$(b_1, b_2, \ldots, b_9) < 10^{24}$ with $10^8 < H < 10^9$;
(2) there is no C_3-spsp$(b_1, b_2, \ldots, b_{10}) < 10^{24}$ with $10^8 < H < 10^9$;
(3) there is no C_3-spsp$(b_1, b_2, \ldots, b_{11}) < 10^{24}$ with $10^4 < H < 10^9$.
Reasons for these facts will be discussed in Remark 5.2 below.

Remark 3.3. A difficult problem is the decision of a favorable upper bound $\mathcal{H}$ of heights of C_3-spsp(2)-acceptable triples (h_1, h_2, h_3) so that we can obtain all C_3-spsp's $< L$, say, $L = 10^{24}$, to the first t, say, $t \geq 11$, prime bases. We will explain in Section 5 why we choose $\mathcal{H} = 10^9$, i.e., why we did not run the procedure for $H = h_1h_2h_3 > 10^9$.

4. Larger C_3-spsp's to more bases

In this section we will speed up the method so that we can find all C_3-spsp's less than a larger limit L, say $L = 10^{50}$, with the same signature, say $(1, 37, 41)$, to $t \geq 9$ prime bases.

Definition 4.1. Let $N, q_1, q_2, q_3, h_1, h_2, h_3, x_0, \overline{x_0}, d$ be as in Definition 2.3. Let b be an odd prime, and suppose (h_1, h_2, h_3) is C_3-acceptable. Define the set

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

A C_3-acceptable triple (h_1, h_2, h_3) is called C_3-spsp(b)-*acceptable*, if the set

$$S_b^{(h_1,h_2,h_3)} \neq \emptyset \tag{4.1}$$

and if the system of linear congruences

$$\begin{cases} x \equiv x_0 \mod H, \\ x \equiv u \mod 4b \text{ for some } u \in S_b^{(h_1,h_2,h_3)} \end{cases} \tag{4.2}$$

has solutions. The kernel d is called C_3-spsp(b)-*acceptable* if (h_1, h_2, h_3) is C_3-spsp(b)-acceptable and $d = x_0 + jH \equiv u \mod 4b$ for some $u \in S_b^{(h_1,h_2,h_3)}$ with $j \equiv (2 - x_0)H \mod 4$, or in other words, if

$$\begin{cases} d \equiv \overline{x_0} \mod 4H, \\ d \equiv u \mod 4b \text{ for some } u \in S_b^{(h_1,h_2,h_3)}. \end{cases} \tag{4.3}$$

Definition 4.2. Let $N, q_1, q_2, q_3, h_1, h_2, h_3, x_0, \overline{x_0}, d$ be as in Definition 2.3. Let b_i be the ith prime, $t \geq 2$ and $M_t = 4b_2 \cdots b_t$; and suppose (h_1, h_2, h_3) is C_3-spsp(2)-acceptable. Define the set

$$R_t^{(h_1,h_2,h_3)} = \Big\{ r : 0 \leq r < M_t, r \equiv u_i \bmod 4b_i \text{ for some } u_i \in S_{b_i}^{(h_1,h_2,h_3)},\ 2 \leq i \leq t \Big\}.$$

The triple (h_1, h_2, h_3) is called C_3-spsp$(b_1, b_2, \ldots, b_t)$-*acceptable* if the system of linear congruences

$$\begin{cases} x \equiv \overline{x_0} \mod 4H, \\ x \equiv u_i \mod 4b_i \text{ for some } u_i \in S_{b_i}^{(h_1,h_2,h_3)},\ 2 \leq i \leq t, \end{cases} \tag{4.4}$$

has solutions, or in other words, the system

$$\begin{cases} x \equiv \overline{x_0} \mod 4H, \\ x \equiv r \mod M_t \text{ for some } r \in R_t^{(h_1,h_2,h_3)} \end{cases} \tag{4.5}$$

has solutions. The kernel d is called C_3-spsp$(b_1, b_2, \ldots, b_t)$-*acceptable* if (h_1, h_2, h_3) is C_3-spsp$(b_1, b_2, \ldots, b_t)$-acceptable and (4.5) holds with x replaced by d.

Example 4.1. The triple $(1, 5, 13)$ is C_3-spsp(b)-acceptable for $b = 2$ and 3, but it is not C_3-spsp(5)-acceptable. Clearly, if $\gcd(b, H) = 1$ with $H = h_1h_2h_3$, then a C_3-acceptable triple (h_1, h_2, h_3) must be C_3-spsp(b)-acceptable. But the converse is not true. For example, the triple $(1, 5, 9)$ is C_3-spsp(b)-acceptable for all primes b, including $b = 3$ and 5.

Theorem 4.1. *Let $N = q_1q_2q_3$ be a product of three different odd primes and let b be an odd prime. Then we have*

$$N \textit{ is a } C_3\textit{-spsp}(b) \iff \textit{its kernel } d \textit{ is } C_3\textit{-spsp}(b)\textit{-acceptable.}$$

Proof. Suppose N is a C_3-number and so d is C_3-acceptable. Then we have by Theorem 2.1 and Lemma 2.1

$$\begin{aligned} & N \text{ is an spsp}(b) \\ \iff & \Big(\frac{b}{dh_1+1}\Big) = \Big(\frac{b}{dh_2+1}\Big) = \Big(\frac{b}{dh_3+1}\Big) \\ \iff & d \equiv u \mod 4b \text{ for some } u \in S_b^{(h_1,h_2,h_3)} \\ \iff & d \text{ is } C_3\text{-spsp}(b)\text{-acceptable.} \end{aligned}$$

□

By the Chinese Remainder Theorem, we have the following corollary.

Corollary 4.1. *Let $N = q_1q_2q_3$ be a product of three different odd primes and let b_i be the ith 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.*

Example 4.2. The triple $(1, 37, 41)$ is C_3-spsp(b)-acceptable for all primes b, with seed $x_0 = 563$ and height $H = 1 \cdot 37 \cdot 41 = 1517$. Let $t = 9$ and $M_t = 4b_2 \cdots b_t = 446185740$. We have $\overline{x_0} = x_0 + 3H = 5114$ and $\#R_9^{(1,37,41)} = 2880$. In Table 4 we give $S_{b_i} = S_{b_i}^{(1,37,41)}$ and $\#R_i = \#R_i^{(1,37,41)}$ for $2 \leq i \leq 9$.

Table 4.

i	b_i	M_i	$\#S_{b_i}$	S_{b_i}	$\#R_i$
2	3	12	1	{6}	1
3	5	60	2	{6, 10}	2
4	7	420	2	{2, 14}	4
5	11	4620	3	{18, 22, 38}	12
6	13	60060	2	{10, 26}	24
7	17	1021020	4	{10, 18, 30, 34}	96
8	19	19399380	5	{26, 38, 50, 54, 74}	480
9	23	446185740	6	{38, 42, 46, 82, 86, 90}	2880

A procedure based on Corollary 4.1 ran about 5 hours on a PC Pentium III/800 to get all C_3-spsp$(b_1, b_2, \ldots, b_9)$'s $< 10^{50}$ with signature $(1, 37, 41)$. There are in total 86687 numbers, among which 5851 numbers are spsp's to the first 13 prime bases up to 41, 25 numbers are spsp's to the first 17 prime bases up to 59 (listed in Table 5), 7 numbers are spsp's to base 61, 3 numbers are spsp's to the first 19 prime bases up to 67.

Table 5. List of all C_3-spsp's $< 10^{50}$ with signature $(1, 37, 41)$ to the first 17 prime bases up to 59

		spsp-base		
$N = q_1q_2q_3$	q_1	61	67	71
664285341720894140846825851168090899459337851067	759375118130107	0	0	0
1801188787585914139564810592131100649232502090131	1058907159503971	0	0	0
2254188563707371059999034172489288735827395166967	1141129380182767	1	0	0
2295419709119519138624774107607428487397986227711	1148044815933991	1	0	0
4830615526563629640707213324003423570276032239067	1471201968695707	0	0	1
5606141065699774478327048822491526469151721036191	1546059297919111	0	0	0
6079037109932002285849522788586785893918822839651	1588362912440851	0	0	0
6177545012072454394180280121837534201011666749867	1596896537577547	0	0	0
6792469965351873320846123947106517207243763369651	1648215707510851	1	0	0
9231658871799183872380918591735012360063879509367	1825708296411247	0	1	0
9688312712744590973050578123260748216127001625571	1855328670525331	1	1	0
17077389050992177663907511962926227202811796430411	2241189765445291	1	1	0
20419468508849496652785114968040727226399506005367	2378772729204847	0	0	0
24989407894883186945549938905182259644632907446867	2544427779105187	0	0	1
26706083736620248445278451981338590391039943640367	2601406424985847	0	0	0
29976443610578528721850170580010674973747257453171	2703531964889731	0	0	1
37022269021333497793028821196322216146297759893567	2900630998141927	0	1	0
39397023402592750173016278148536552680399692486831	2961369573201271	1	0	1
49765723320580275663033246960798005905092493704271	3201215516700631	0	0	0
54137204419251617397822551921251265769160917390091	3292330421343211	1	1	0
60182972252640561414204431408975362441401651006367	3410588713549447	0	0	1
63627021553793884438571687827273322639293179452371	3474444171754531	0	1	0
68172488800119872312050407892588071592239057698791	3555285837408511	0	0	1
69102192250587765543843633166409535362271092418091	3571374676875211	0	0	0
95305641129861756749783024175271806664680889298311	3975371093655391	0	0	0

Remark 4.1. Arnault [2, Equation (4)] used a sufficient condition derived from the condition

$$\left(\frac{b}{q_1}\right) = \left(\frac{b}{q_2}\right) = \left(\frac{b}{q_3}\right) = -1 \tag{4.6}$$

for finding C_3-spsp's $n = q_1q_2q_3$ to all the first several prime bases b with C_3-spsp(2)-acceptable signature (h_1, h_2, h_3) satisfying additional conditions $h_1 = 1$ and $\gcd(b, h_2h_3) = 1$, whereas our method has no restrictions either on h_1 or on $\gcd(b, h_2h_3)$ (see Definition 4.1, Example 4.2, Theorem 4.1). Arnault found a 56-digit C_3-spsp to the first 11 prime bases (actually his 56-digit sample is an spsp to the first 13 prime bases up to 41), which passes the Axiom release 1.1 test. All our 5851 C_3-spsp$(b_1, b_2, \ldots, b_{13})$'s $< 10^{50}$ with signature $(1, 37, 41)$ also pass the Axiom release 1.1 test, but they are much smaller than his 56-digit sample. Arnault's Condition (4.6) is too stringent for most C_3-spsp's to satisfy. Our 5851 numbers could not be found by Arnault's condition.

5. Discussion

Let $N, q_1, q_2, q_3, h_1, h_2, h_3, H, x_0, \overline{x_0}, d$ be as in Definition 2.3. Define

$$\beta = \beta(N) = \log_H N = \frac{\log N}{\log H}, \tag{5.1}$$

which is called the *height index* of N. We call N a *hard Carmichael number* (resp. *hard C_3-number* or *hard* C_3-spsp$(b_1, \ldots, b_t)$) if $N = q_1q_2q_3$ is a Carmichael number (resp. C_3-number or C_3-spsp$(b_1, \ldots, b_t)$) with height index $\beta < 3$.

Proposition 5.1. *If N is a hard Carmichael number, then we have*

$$x_0 = d < H^{2/3}. \tag{5.2}$$

Proof. Put $\alpha = \log_H d = \frac{\log d}{\log H}$. Then

$$x_0 \le d = H^\alpha.$$

Since $d^3H < N$, we have

$$\alpha < \frac{1}{3}(\beta - 1)$$

where $\beta = \frac{\log N}{\log H}$ is the height index of N. If N is a hard Carmichael number, then $\beta < 3$. Thus $\alpha < 2/3$, and therefore equation (5.2) holds since $d \equiv x_0 \mod H$. □

Corollary 5.1. *If N is a hard C_3-number, then we have*

$$x_0 = \overline{x_0} = d < H^{2/3}; \tag{5.3}$$

moreover if N is a hard C_3-spsp$(b_1, \ldots, b_t)$ with $t \ge 2$, then we have

$$x_0 \equiv r \mod M_t \text{ for some } r \in R_t^{(h_1,h_2,h_3)} \tag{5.4}$$

where M_t and $R_t^{(h_1,h_2,h_3)}$ are as defined in Definition 4.2.

Example 5.1. We list in Table 6 hard C_3-spsp$(b_1, \ldots, b_t)$'s for $0 \le t \le 9$ with the smallest height indices among the three sets of C_3-numbers: the 2837 C_3-numbers $< 10^{18}$; the 110 C_3-spsp$(2, 3, 5, 7, 11)$'s $< 10^{20}$ and the 21978 C_3-spsp(2)'s $< 10^{24}$.

TABLE 6. Sample hard C_3-spsp$(b_1, \ldots, b_t)$

t	N	h_1	h_2	h_3	H	$x_0 = d$	β
0	67902031	7	45	971	305865	6	$1.427\cdots$
1	145936981694079451	115	903	1324151	137506460595	102	$1.541\cdots$
2	145936981694079451	115	903	1324151	137506460595	102	$1.541\cdots$
3	64770695384645251	67	147	92675	912756075	414	$1.876\cdots$
4	90022554326251	29	125	2681	9718625	210	$1.997\cdots$
5	3948835658621975551	117	397	4985	231548265	2574	$2.223\cdots$
6	3948835658621975551	117	397	4985	231548265	2574	$2.223\cdots$
7	24641960187979924539751	51	451	11375	261636375	45498	$2.660\cdots$
8	24641960187979924539751	51	451	11375	261636375	45498	$2.660\cdots$
9	24641960187979924539751	51	451	11375	261636375	45498	$2.660\cdots$

Define

$$C_3'(t, L, \overline{\beta}) = \{N : N \text{ is a } C_3\text{-spsp}(b_1, \ldots, b_t) < L \text{ with height index } < \overline{\beta}\} \tag{5.5}$$

and

$$C_3'(t, L, \overline{\beta}, \mathcal{H}) = \{N : N \in C_3'(t, L, \overline{\beta}) \text{ with height } < \mathcal{H}\} \tag{5.6}$$

for $t \geq 1$ and $C_3'(0, L, \overline{\beta})$ is the set of all C_3-numbers $< L$ with height index $< \overline{\beta}$. Thus $C_3'(0, L, 3)$ is the set of all hard C_3-numbers $< L$ and $C_3(t, L, 3)$ is the set of hard C_3-spsp$(b_1, \ldots, b_t)$'s $< L$ for $t \geq 1$. Define

$$g(t, L, \overline{\beta}) = \#C_3'(t, L, \overline{\beta}) \quad \text{and} \quad g(t, L, \overline{\beta}, \mathcal{H}) = \#C_3'(t, L, \overline{\beta}, \mathcal{H}). \tag{5.7}$$

Studying the 2837 C_3-numbers $< 10^{18}$ given by Pinch [8] and the 110 C_3-spsp(2, 3, 5, 7, 11)'s $< 10^{20}$ obtained in [12], we obtain values of $g(t, L, 3)$ and $f(t, L)$ (see equation (3.2) for the definition) tabulated in Table 7, where the numerator is $g(t, L, 3)$ and the denominator is $f(t, L)$. If both $g(t, L, 3)$ and $f(t, L)$ are 0, we write only 0 instead of $\frac{0}{0}$. The values of $g(t, 10^{20}, 3)$ and $f(t, 10^{20})$ for $0 \leq t \leq 4$ are unknown.

Remark 5.1. If $N < L$ with height $H > L^{1/\overline{\beta}}$, then $\beta(N) = \log_H N < \log_H L < \overline{\beta}$. So, we have

$$f(t, L) - f(t, L, L^{1/\overline{\beta}}) \leq g(t, L, \overline{\beta}). \tag{5.8}$$

The left side of inequality (5.8) is the number of C_3-spsp$(b_1, \ldots, c_t)$'s $< L$ with height $H > L^{1/\overline{\beta}}$. For example, $f(0, 10^{18}) - f(0, 10^{18}, 10^6) = 2837 - 2620 = 217 < 384 = g(0, 10^{18}, 3)$.

Remark 5.2. Since x_0 is a positive residue modulo H (see Definition 2.2), condition (5.2) (resp. condition (5.3)) is too stringent for most Carmichael numbers with three prime factors (resp. C_3-numbers) to satisfy. So, hard Carmichael numbers are rare, and hard C_3-numbers are even more rare. Because of the even more stringent condition (5.4), hard C_3-spsp$(b_1, \ldots, b_t)$'s are even more rare as t increases as can be seen in Table 7. This explains Remark 3.2.

Studying the 21978 C_3-spsp(2)'s $< 10^{24}$ with heights $< 10^9$, we obtain values of $g(t, L, 3, 10^9)$ (the number of hard C_3-spsp$(b_1, \ldots, b_t)$'s $< L$ with heights $< 10^9$ for $t \geq 1$) tabulated in Table 8, whereas $g(0, L, 3, 10^9)$ (the number of hard C_3-numbers $< L$ for $L \leq 10^{18}$ with heights $< 10^9$) are obtained from Pinch [8].

TABLE 7. The functions $g(t, L, 3)$ (numerator) and $f(t, L)$ (denominator)

L	10^4	10^6	10^8	10^{10}	10^{12}	10^{14}	10^{16}	10^{18}	10^{20}
$t = 0$	$\frac{1}{1}$	$\frac{1}{1}$	$\frac{4}{8}$	$\frac{13}{29}$	$\frac{27}{79}$	$\frac{70}{271}$	$\frac{163}{868}$	$\frac{384}{2837}$	
$t = 1$	0	0	0	$\frac{0}{1}$	$\frac{3}{8}$	$\frac{10}{35}$	$\frac{36}{157}$	$\frac{89}{527}$	
$t = 2$	0	0	0	$\frac{0}{1}$	$\frac{1}{6}$	$\frac{6}{28}$	$\frac{20}{100}$	$\frac{49}{366}$	
$t = 3$	0	0	0	$\frac{0}{1}$	$\frac{0}{4}$	$\frac{3}{18}$	$\frac{10}{60}$	$\frac{25}{203}$	
$t = 4$	0	0	0	$\frac{0}{1}$	$\frac{0}{1}$	$\frac{1}{7}$	$\frac{3}{19}$	$\frac{6}{89}$	
$t = 5$	0	0	0	0	0	$\frac{0}{3}$	$\frac{0}{6}$	$\frac{2}{28}$	$\frac{7}{110}$
$t = 6$	0	0	0	0	0	$\frac{0}{1}$	$\frac{0}{2}$	$\frac{0}{8}$	$\frac{2}{36}$
$t = 7$	0	0	0	0	0	0	$\frac{0}{1}$	$\frac{0}{2}$	$\frac{0}{12}$

TABLE 8. The function $g(t, L, 3, 10^9)$

$\log_{10} L$	12	14	16	18	20	22	24
$t = 0$	27	69	161	369			
$t = 1$	3	10	36	84	198	424	874
$t = 2$	1	6	20	47	105	237	480
$t = 3$	0	3	10	25	52	120	248
$t = 4$	0	1	3	6	20	44	95
$t = 5$	0	0	0	2	7	21	42
$t = 6$	0	0	0	0	2	6	12
$t = 7$	0	0	0	0	0	2	5
$t = 8$	0	0	0	0	0	1	2
$t = 9$	0	0	0	0	0	0	1
$t = 10$	0	0	0	0	0	0	0

From Tables 7 and 8 we find that

$$\begin{aligned} g(0, 10^{18}, 3) &= g(0, 10^{18}, 3, 10^9) + 15, \\ g(1, 10^{18}, 3) &= g(1, 10^{18}, 3, 10^9) + 5, \\ g(2, 10^{18}, 3) &= g(2, 10^{18}, 3, 10^9) + 2, \\ g(t, 10^{18}, 3) &= g(t, 10^{18}, 3, 10^9) \text{ for } t \geq 3, \\ g(t, 10^{20}, 3) &= g(t, 10^{20}, 3, 10^9) \text{ for } t \geq 5. \end{aligned}$$

So we may predict that

$$g(t, 10^{24}, 3) = g(t, 10^{24}, 3, 10^9) \text{ for } t \geq t_0$$

for some $t_0 \geq 9$. To be safe, we may take $t_0 = 12$. If so, i.e., if $g(t, 10^{24}, 3) = g(t, 10^{24}, 3, 10^9) = 0$ for $t \geq 12$, there would exist no hard C_3-spsp's to the first 12 prime bases. Then from (5.8) we would have

$$f(t, 10^{24}) - f(t, 10^{24}, 10^8) \leq g(t, 10^{24}, 3) = 0$$

for $t \geq 12$. This means that there would exist no C_3-spsp's $< 10^{24}$ to the first 12 prime bases, with heights $> 10^8$. These arguments explain Remark 3.3.

At last, we point out an argument which is perhaps unfavorable for our method. Given any small $\varepsilon > 0$, does there always exist a C-acceptable triple $(h_1, h_2, h_3) = (h_1, h_2, h_3)(\varepsilon)$ with height $H = h_1 h_2 h_3$ and positive seed $x_0 < H^{\varepsilon}$? If so, and if one wants to compute ALL! Carmichael numbers $< L$ with three prime factors, one should check as many as $O(L^{1+o(1)})$ C-acceptable triples. The algorithm would take time $O(L^{1+o(1)})$. The same argument can be used for finding ALL! C_3-numbers or ALL! C_3-spsp(2)'s with a smaller constant for the big O- and/or a smaller order for the small $o(1)$. To this end, a favorable estimate of $\mathcal{H}$ in Remark 3.3 as a function of L and t would be an interesting but difficult problem.

Acknowledgment

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

References

1. W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. **140** (1994), 703–722. MR95k:11114
2. F. Arnault, *Constructing Carmichael numbers which are strong pseudoprimes to several bases*, J. Symbolic Computation **20** (1995), 151–161. MR96k:11153
3. D. Bleichenbacher, *Efficiency and Security of Cryptosystems Based on Number Theory*, ETH Ph. D. dissertation 11404, Swiss Federal Institute of Technology, Zurich (1996).
4. R. Crandall and C. Pomerance, *Prime numbers, a computational perspective*, Springer-Verlag, New York, 2001. MR2002a:11007
5. I. Damgård, P. Landrock, and C. Pomerance, *Average case estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177–194. MR94b:11124
6. G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926. MR94d:11004
7. G. Miller, *Riemann's hypothesis and tests for primality*, J. Comput. and System Sci. **13** (1976), 300–317. MR58:470a
8. R. G. E. Pinch, *All Carmichael numbers with three prime factors up to* 10^{18}, http://www.chalcedon.demon.co.uk/carpsp.html.
9. C. Pomerance, J. L. Selfridge and Samuel S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026. MR82g:10030
10. M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138. MR81f:10003
11. Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math. Comp. **70** (2001), 863–872. `http://www.ams.org/journal-getitem?pii=S0025-5718-00-01215-1` MR2001g:11009
12. Zhenxiang Zhang and Min Tang, *Finding strong pseudoprimes to several bases.* II, Math. Comp. **72** (2003), 2085–2097. `http://www.ams.org/journal-getitem?pii=S0025-5718-03-01545-X` MR2004c:11008

Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, Peoples Republic of China

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