MATHEMATICS OF COMPUTATION
Volume 83, Number 290, November 2014, Pages 2915–2924
S 0025-5718(2014)02830-5
Article electronically published on May 5, 2014

STRONG PSEUDOPRIMES TO THE FIRST EIGHT PRIME BASES

YUPENG JIANG AND YINGPU DENG

ABSTRACT. Define ψ_m to be the smallest strong pseudoprime to the first m prime bases. The exact value of ψ_m is known for $1 \le m \le 8$. Z. Zhang has found a 19-decimal-digit number $Q_{11} = 3825\,12305\,65464\,13051$ which is a strong pseudoprime to the first 11 prime bases and he conjectured that $\psi_9 = \psi_{10} = \psi_{11} = Q_{11}$. We tabulate all the strong pseudoprimes $n \le Q_{11}$ to the first eight prime bases, and prove Zhang's conjecture.

1. INTRODUCTION

If n is prime, in view of Fermat's Little Theorem, the congruence

$$a^{n-1} \equiv 1 \mod n$$

holds for every a with $n \nmid a$. There are composite numbers also satisfying this congruence. Such an odd composite number n is called a *pseudoprime* to base a (psp(a) for short). Moreover, for an odd prime n, letting $n - 1 = 2^s d$ with d odd, we have

$$a^d \equiv 1 \mod n$$

or

$$a^{2^k d} \equiv -1 \mod n$$

for an integer k with $0 \le k < s$. If a psp(a) n satisfies one of these two equations, we call n a *strong pseudoprime* to base a (spsp(a) for short). This is the basis of the Miller-Rabin test [5].

Define ψ_m to be the smallest strong pseudoprime to each of the first m prime bases. If $n < \psi_m$, then only m strong pseudoprime tests are needed to determine whether n is prime or not. If we know the exact value of ψ_m, then for integers $n < \psi_m$, there is a deterministic primality testing algorithm which is easier to understand and also faster than other known tests. The exact value of ψ_m for $1 \le m \le 8$ is known [2, 4]: $\psi_1 = 2047$, $\psi_2 = 1373653$, $\psi_3 = 25326001$, $\psi_4 = 3215031751$, $\psi_5 = 215\,23028\,98747$, $\psi_6 = 347\,47496\,60383$, $\psi_7 = \psi_8 = 34155\,00717\,28321$.

Received by the editor August 23, 2012 and in revised form, January 26, 2013 and April 5, 2013.

2010 *Mathematics Subject Classification.* Primary 11Y11, 11A51.

Key words and phrases. Strong pseudoprimes, Chinese Remainder Theorem.

This research was supported by the NNSF of China (Grant Nos. 11071285, 61121062), 973 Project (2011CB302401) and the National Center for Mathematics and Interdisciplinary Sciences, CAS.

In [2], Jaeschke also gave upper bounds for ψ_9, ψ_{10} and ψ_{11}. These bounds were improved by Z. Zhang several times and Zhang conjectured that

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

Zhang also determined upper bounds and stated conjectures for ψ_m, with $12 \le m \le 20$ (see [6,8,9]).

In this paper, we calculate all the strong pseudoprimes $n \le Q_{11}$ to the first eight prime bases and obtain the following conclusion.

Theorem 1.1. $\psi_9 = \psi_{10} = \psi_{11} = 3825\,12305\,65464\,13051$.

This article is organized in the following way. In Section 2 we give notations and basic facts needed for our algorithm. Just as in [2], we consider the number of prime divisors of the testing number. Let $n = p_1 p_2 \cdots p_t$. In Section 3 we consider $t \ge 4$, in Section 4, the case $t = 3$, and Section 5, the case $t = 2$. In Section 6 we obtain our conclusion, and report the total time required for our algorithm.

2. Foundations of the algorithm

In this section, we give the foundations for our algorithm. Let p be a prime and a an integer with $p \nmid a$. Denote the smallest positive integer e such that $a^e \equiv 1 \mod p$ by $\mathrm{ord}_p(a)$. Moreover, for any integer n, if $n = p^e n'$ with $p \nmid n'$ and $e \ge 0$, we denote e by $v_p(n)$. In this article, we only use $v_p(n)$ for $p = 2$, so we write $v(n)$ for this case. For $\nu \in \mathbb{Z}^m$, $\nu = (a_1, \ldots, a_m)$ with $p \nmid a_i$ for each i, we define σ_p^ν by

$$\sigma_p^\nu = (v(\mathrm{ord}_p(a_1)), \ldots, v(\mathrm{ord}_p(a_m))).$$

If n is a pseudoprime (or strong pseudoprime) for all the a_i's, we denote it by $\mathrm{psp}(\nu)$ (or $\mathrm{spsp}(\nu)$).

We need to check all odd integers less than Q_{11} to see if there are strong pseudoprimes to the first eight prime bases. First, we exclude the integers having square divisors. If n is a $\mathrm{psp}(a)$ and $p^2 \mid n$ for some prime p, then we have

$$a^{n-1} \equiv 1 \mod p^2.$$

Also,

$$a^{p(p-1)} \equiv 1 \mod p^2,$$

and since $\gcd(p, n-1) = 1$, we have

$$a^{p-1} \equiv 1 \mod p^2.$$

If $a = 2$ and 3, then

$$2^{p-1} \equiv 1 \mod p^2, \qquad 3^{p-1} \equiv 1 \mod p^2.$$

These two equations do not hold simultaneously for any prime p less than $3 \cdot 10^9$[4], which is greater than $\sqrt{Q_{11}} \approx 1.9 \cdot 10^9$, so we only need to consider squarefree integers. In fact, by a search of Knauer and Richstein[3], the smallest prime which satisfies these two equations must be greater than $1.25 \cdot 10^{15}$. This bound is improved to $6.7 \cdot 10^{15}$ by Dorais and Klyve[1]. Thus all psp(2, 3)'s less than $4.4 \cdot 10^{31}$ are squarefree.

Now we give the following important proposition (Proposition 1 in [2]).

Proposition 2.1. *Let $n = p_1 \cdots p_t$ with different primes $p_1, \ldots, p_t$, and $\nu = (a_1, \ldots, a_m)$ with different integers such that $p_j \nmid a_i$ for all $i = 1, \ldots, m$ and $j = 1, \ldots, t$. Then n is an spsp(ν) if and only if n is a psp(ν) and $\sigma^\nu_{p_1} = \cdots = \sigma^\nu_{p_t}$.*

Example 2.2. Consider $\psi_3 = 25326001 = p_1 p_2 = 2251 \cdot 11251$ and $\nu = (2, 3, 5)$. Then ψ_3 is an spsp(ν). We have

$$\operatorname{ord}_{p_1}(2) = 750, \qquad \operatorname{ord}_{p_1}(3) = 250, \qquad \operatorname{ord}_{p_1}(5) = 1125$$

and

$$\operatorname{ord}_{p_2}(2) = 2250, \qquad \operatorname{ord}_{p_2}(3) = 2250, \qquad \operatorname{ord}_{p_2}(5) = 1125.$$

Thus, $\sigma^\nu_{p_1} = \sigma^\nu_{p_2} = (1, 1, 0)$.

This is the main necessary condition that we use to find strong pseudoprimes. In our algorithm, $\nu = (2, 3, 5, 7, 11, 13, 17, 19)$. For a given prime p, we find primes q satisfying $\sigma^\nu_p = \sigma^\nu_q$. Moreover, we use the following two propositions to reduce the number of candidates. Let $(\frac{a}{p})$ denote the Legendre symbol.

Proposition 2.3. *For primes p and q, if $v(p-1) = v(q-1)$ and $\sigma^{(a)}_p = \sigma^{(a)}_q$, then $(\frac{a}{p}) = (\frac{a}{q})$.*

Proposition 2.4. *For primes p and q, if $v(p-1) < v(q-1)$ and $\sigma^{(a)}_p = \sigma^{(a)}_q$, then $(\frac{a}{q}) = 1$.*

The proofs of these two propositions are similar, and Proposition 2.3 is Proposition 3 in [2]. We omit both proofs. The following example explains how we can reduce the number of candidates.

Example 2.5. Assume $p = 23$, and we need to find a prime q with $\sigma^\nu_p = \sigma^\nu_q$ for $\nu = (2, 3)$. First, if $q \equiv 3 \bmod 4$, then by Proposition 2.3 we have $(\frac{2}{23}) = (\frac{2}{q})$ and $(\frac{3}{23}) = (\frac{3}{q})$. Therefore, $q \equiv 7 \bmod 8$ and $q \equiv 2 \bmod 3$. By the Chinese Remainder Theorem, we obtain $q \equiv 23 \bmod 24$. If $q \equiv 1 \bmod 4$, then $(\frac{2}{q}) = (\frac{3}{q}) = 1$ by Proposition 2.4, so $q \equiv 1 \bmod 8$ and $q \equiv 1 \bmod 3$. By the Chinese Remainder Theorem, $q \equiv 1 \bmod 24$. Thus, $q \equiv \pm 1 \bmod 24$. We only need to check two of the total $\phi(24) = 8$ residue classes modulo 24. In fact, we only check $q \equiv -1 \bmod 24$ in our algorithm. We define binary primes to deal with the $q \equiv 1 \bmod 24$ case. See the details in Section 4.

3. $t \geq 5$ AND $t = 4$

From now on, we fix $\nu = (2, 3, 5, 7, 11, 13, 17, 19)$. If n is a psp(ν) and prime $p \mid n$, as $a^{n-1} \equiv 1 \bmod p$, then $\operatorname{ord}_p(a) \mid (n-1)$, for all $a = 2, 3, 5, 7, 11, 13, 17, 19$. Define λ_p to be the least common multiple of the eight orders, i.e.,

$$\lambda_p = \operatorname{lcm}\{\operatorname{ord}_p(a) : a = 2, 3, 5, 7, 11, 13, 17, 19\}.$$

Then we have $\lambda_p \mid (n-1)$. Since we only need to consider squarefree integers, we always denote $n = p_1 \cdots p_t$ with $p_1 < \cdots < p_t$. In this section, we consider two cases: first, $t \geq 5$, and second, $t = 4$.

3.1. $t \geq 5$. For each $p \leq [\sqrt[5]{Q_{11}}] = 5206$, let S_p be the set of all primes q with $\sigma_q^\nu = \sigma_p^\nu$, and denote the kth largest element in S_p by $s_{p,k}$. Our algorithm outputs the first l elements of S_p with $l \geq 5$ and

$$\prod_{i=1}^{5} s_{p,i} \leq Q_{11}, \qquad \left(\prod_{i=1}^{4} s_{p,i}\right) s_{p,l} \leq Q_{11}, \qquad \left(\prod_{i=1}^{4} s_{p,i}\right) s_{p,l+1} > Q_{11}.$$

There are 60 such sequences for all $p \leq 5206$ and the algorithm takes less than one minute to find them. We tabulate some sequences in the following table. The sequences are numbered according to the size of their first primes. l is the total number of primes in each sequence. The last column is the number of integers $n = p_1p_2p_3p_4p_5 \leq Q_{11}$ with each p_i in this sequence.

TABLE 1. Sequences with equal σ_p^ν

No.	Primes	σ_p^ν	l	Num
1	23, 3767, 13127, 16223, 18503, 22247, 38567, 39887, 48647, 54167, $\cdots$, 184727, 197807, 204143, 204983, 205703.	(0,0,1,1,1,0,1,1)	38	198
...	.....	...	...	...
23	479, 1151, 4919, 5519, 6599, 7559, 29399, 51719, 53591, 67751, 68879, 69431, 72551, 76919, 103319, 108191, 117431, 122471, 123791, 138071, 147311, 161999, 188999, 195359, 203279, 206351, 211151, 212999, 217271, 230999, 247799, 251831.	(0,0,0,0,0,1,1,1)	32	120
...	.....	...	...	...
47	1151, 4919, 5519, 6599, 7559.	(0,0,0,0,0,1,1,1)	5	1
...	.....	...	...	...
60	2503, 2767, 5167, 5623, 8887, 11887, 16447.	(0,1,1,1,0,1,0,0)	7	4

If we have $\prod_{i=1}^{6} s_{p,i} \leq Q_{11}$ in a sequence, then $p_2,\ p_3,\ p_4,\ p_5,\ p_6$ must be the first five primes of another sequence. There are in total three pairs of such sequences. In addition to the pair (23, 47) shown in Table 1, the other pairs are (24, 56) and (49, 57). Therefore, we only need to check sequence 23, 24 and 49 for $t > 5$. Each one has $\prod_{i=1}^{6} s_{p,i} > Q_{11}$, so $t > 5$ is impossible. For $t = 5$, our algorithm runs in less than 0.1 second and finds no strong pseudoprime.

3.2. $t = 4$. For $t = 4$, we first define (p_1, p_2, p_3) to be a feasible triple if it satisfies

$$p_1 < p_2 < p_3, \quad \sigma_{p_1}^\nu = \sigma_{p_2}^\nu = \sigma_{p_3}^\nu, \quad p_1p_2p_3^2 < Q_{11}.$$

Our algorithm proceeds as follows: for each $p_1 \leq [\sqrt[4]{Q_{11}}] = 44224$, find feasible triples (p_1, p_2, p_3). We have $\lambda_{p_i} \mid (n-1)$, for $i = 1, 2, 3$. Let $\lambda = \operatorname{lcm}\{\lambda_{p_1}, \lambda_{p_2}, \lambda_{p_3}\}$ and $b = p_1p_2p_3$. Then we have

$$n = bp_4 \equiv 1 \mod \lambda.$$

If $\gcd(b, \lambda) \neq 1$, it is impossible to have such n. If $\gcd(b, \lambda) = 1$, we need to check all p_4 with

$$p_3 < p_4 \leq Q_{11}/b, \qquad p_4 \equiv b^{-1} \mod \lambda.$$

Our algorithm takes less than 6 hours, finding 402273 feasible triples and no spsp(ν) with $t = 4$.

4. $t = 3$

In this section, we consider the case $t = 3$. As above, we define a feasible pair (p_1, p_2) by

$$p_1 < p_2, \quad \sigma^{\nu}_{p_1} = \sigma^{\nu}_{p_2}, \quad p_1 p_2^2 < Q_{11}.$$

Our algorithm is just as in the $t = 4$ case: for each $p_1 \le [\sqrt[3]{Q_{11}}] = 1563922$, find feasible pairs (p_1, p_2). Let $b = p_1 p_2$ and $\lambda = \operatorname{lcm}(\lambda_{p_1}, \lambda_{p_2})$, then $\lambda \mid (n-1)$. If $\gcd(b, \lambda) = 1$, we check all p_3 with

$$p_2 < p_3 \le Q_{11}/b, \qquad p_3 \equiv b^{-1} \mod \lambda.$$

We divide our algorithm into three parts according to $p_1 \equiv 3 \bmod 4$, $p_1 \equiv 5 \bmod 8$ and $p_1 \equiv 1 \bmod 8$.

4.1. $p_1 \equiv 3 \bmod 4$. For $p_1 \equiv 3 \bmod 4$, we first assume $p_2 \equiv 3 \bmod 4$. In this case, $\sigma^{\nu}_{p_1} = \sigma^{\nu}_{p_2}$ implies $(\frac{a}{p_1}) = (\frac{a}{p_2})$ for all $a = 2, 3, 5, 7, 11, 13, 17, 19$ by Proposition 2.3. Moreover, in this situation, the inverse is also true. We calculate the Legendre symbol $(\frac{a}{p_i})$ instead of $v(\operatorname{ord}_{p_i}(a))$. When searching p_2, we use the first five primes and then

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right), \qquad a = 2, 3, 5, 7, 11,$$

reducing to 30 residue classes modulo $9240 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$.

Example 4.1. For $p_1 = 31$, a feasible pair $(31, p_2)$ must satisfy

$$p_2 \le [\sqrt{Q_{11}/31}] = 351270645.$$

If we search p_2 the same way as in the $t \le 5$ and $t = 4$ cases, we need to check all odd numbers greater than 31; there are about $1.7 \cdot 10^8$ candidates. For our method, there are only $30 \cdot \frac{351270645}{9240} \approx 1.1 \cdot 10^6$ candidates.

We use another trick. If $b = p_1 p_2$ is less than $4 \cdot 10^6$, the corresponding λ may be too small. We do not find p_3 as described above. In fact, since

$$n = bp_3 \equiv b \mod p_3 - 1$$

and

$$a^{n-1} \equiv a^{b-1} \equiv 1 \mod p_3, \qquad a = 2,\ 3,$$

we calculate $\gcd(2^{b-1} - 1, 3^{b-1} - 1)$, and then factor it to get the prime divisors which are greater than p_2 and less than Q_{11}/b.

The following example explains why we need to factor the greatest common divisor instead of the usual search.

Example 4.2. Notice that for some b, the corresponding λ is small. For $b = p_1 p_2 = 43 \cdot 9283 = 399169$, $\sigma^{\nu}_{p_1} = \sigma^{\nu}_{p_2} = (1, 1, 1, 1, 0, 0, 0, 1)$, $\lambda = 9282$, we need to check all p_3 with

$$9283 < p_3 \le Q_{11}/b \approx 9.6 \cdot 10^{12}, \qquad p_3 \equiv 7771 \mod 9282,$$

and for $b = p_1 p_2 = 571 \cdot 2851 = 1627921$, $\sigma^{\nu}_{p_1} = \sigma^{\nu}_{p_2} = (1, 1, 0, 1, 0, 0, 1, 1)$, $\lambda = 2850$, all p_3 with

$$2851 < p_3 \le Q_{11}/b \approx 2.3 \cdot 10^{12}, \qquad p_3 \equiv 2281 \mod 2850.$$

There are 295 feasible pairs (p_1, p_2) with $p_1 p_2 < 4 \cdot 10^6$ no matter whether $p_1 \equiv 1 \bmod 4$ or $p_1 \equiv 3 \bmod 4$. Our algorithm takes less than 8 hours, finding 21110549 feasible pairs and two spsp(ν)'s:

$$3825\,12305\,65464\,13051 = 149491 \cdot 747451 \cdot 34233211,$$
$$230\,24566\,07261\,88031 = 214831 \cdot 787711 \cdot 1360591.$$

The first one is Q_{11}. Zhang has found these two numbers in [7] and [9].

For the case $p_2 \equiv 1 \bmod 4$, we have $\sigma^\nu_{p_2} = \sigma^\nu_{p_1} \in \{0,1\}^8$. We call a prime $p \equiv 1 \bmod 4$ with $\sigma^\nu_p \in \{0,1\}^8$ a *binary prime*. For a prime $p \equiv 5 \bmod 8$, $v(\mathrm{ord}_p(2)) = 2$, so binary primes must satisfy $p \equiv 1 \bmod 8$. We need to check binary primes p_2 with

$$p_1 p_2^2 < Q_{11}, \qquad p_1 \geq 23.$$

Then $p_2 \leq [\sqrt{Q_{11}/23}] = 407810860$. It takes 7 minutes to find a total of 51 binary primes in the range. Let p_2 be a binary prime. We check all $p_1 \equiv 3 \bmod 4$ and $p_1 < p_2$, and find 24 more feasible pairs (p_1, p_2) and no spsp(ν). By considering binary primes, we reduce half of the candidates at the cost of 7 minutes.

4.2. $p_1 \equiv 5 \bmod 8$**.** If $p_1 \equiv 5 \bmod 8$, we have $(\frac{2}{p_1}) = -1$, and then $v(\mathrm{ord}_{p_1}(2)) = 2$. Thus for each p_2 with $\sigma^\nu_{p_2} = \sigma^\nu_{p_1}$, we must have $p_2 \equiv 1 \bmod 4$. If $p_2 \equiv 5 \bmod 8$, by Proposition 2.3, we use the first five primes, then

$$\left(\frac{a}{p_2}\right) = \left(\frac{a}{p_1}\right), \qquad a = 2, 3, 5, 7, 11.$$

There are 30 residue classes module 9240. If $p_2 \equiv 1 \bmod 8$, by Proposition 2.4, we must have

$$\left(\frac{a}{p_2}\right) = 1, \qquad a = 2, 3, 5, 7, 11.$$

There are also 30 residue classes module 9240. As in the $p_1 \equiv 3 \bmod 4$ case, if $p_1 p_2 < 4 \cdot 10^6$, we factor $\gcd(2^{b-1} - 1, 3^{b-1} - 1)$ to get a possible p_3. The total time for checking all p_1 up to 1563922 is about 11 hours and we find 1401941 feasible pairs with no spsp(ν).

We give an example with $p_1 \equiv 5 \bmod 8$ and $b < 4 \cdot 10^6$.

Example 4.3. For $b = p_1 p_2 = 29 \cdot 7589 = 220081$, $\sigma^\nu_{p_1} = \sigma^\nu_{p_2} = (2, 2, 1, 0, 2, 1, 2, 2)$, $\lambda = 7588$, we need to check all p_3 with

$$7589 < p_3 \leq Q_{11}/b \approx 1.7 \cdot 10^{13}, \qquad p_3 \equiv 785 \mod 7588.$$

4.3. $p_1 \equiv 1 \bmod 8$**.** For $p_1 \equiv 1 \bmod 8$, denote $e = v(p_1 - 1)$ and $f = v(\lambda_{p_1})$. Then $f \leq e$ and $p_1 \equiv 1 + 2^e \bmod 2^{e+1}$. For p_2 with $\sigma^\nu_{p_2} = \sigma^\nu_{p_1}$, we have

$$p_2 \equiv 1 \mod 2^f.$$

If $f = e$, we consider two cases. For $p_2 \equiv 1 + 2^e \bmod 2^{e+1}$, by Proposition 2.3 we have

$$\left(\frac{a}{p_2}\right) = \left(\frac{a}{p_1}\right), \qquad a = 2, 3, 5, 7, 11.$$

There are 30 residue classes module $2^{e+1} \cdot 1155$. For $p_2 \equiv 1 \bmod 2^{e+1}$, by Proposition 2.4, we have

$$\left(\frac{a}{p_2}\right) = 1, \qquad a = 2, 3, 5, 7, 11.$$

There are also 30 residue classes module $2^{e+1} \cdot 1155$. If $f < e$, we only use the condition $p_2 \equiv 1 \bmod 2^f$. Our algorithm takes about 2 hours, finding 93957 feasible pairs and no spsp(ν).

Until now, we finish the $t = 3$ case, and find two spsp(ν)'s with $p_1 \equiv 3 \bmod 4$. The total time is about 21 hours.

5. $t = 2$

For $t = 2$, there is no need to define feasible integers. If $n = p_1 p_2$ is an spsp(ν), as $\lambda_{p_1} \mid (n-1)$ and $\lambda_{p_1} \mid (p_1 - 1)$, we have

$$p_1 < p_2 \le Q_{11}/p_1, \qquad p_2 \equiv 1 \mod \lambda_{p_1}.$$

Since λ_{p_1} is close to $p_1 - 1$, there are about $Q_{11}/(p_1)^2$ candidates for each p_1. When p_1 is small, there are too many. According to the size of p_1, we divide our algorithm into three parts.

5.1. **Small and large p_1.** If $p_1 < 10^6$, we use the same method as for $t = 3$ with $p_1 p_2 < 4 \cdot 10^6$. We have

$$a^{p_1-1} \equiv a^{n-1} \equiv 1 \mod p_2, \qquad a = 2, 3.$$

We calculate $\gcd(2^{p_1-1} - 1, 3^{p_1-1} - 1)$ and factor it to get prime divisors p_2 with

$$p_1 < p_2 \le Q_{11}/p_1.$$

Our algorithm takes about 9 hours and finds no spsp(ν).

For $p_1 > 10^8$, almost all p_1 with $\lambda_{p_1} = p_1 - 1$. There are less than $Q_{11}/10^{16} \approx 380$ candidates. We just run the algorithm as described at the beginning of this section. It takes about 19 hours and finds five spsp(ν)'s:

$$\begin{aligned}
84\,98355\,74122\,37221 &= 206135341 \cdot 412270681,\\
1134\,93190\,66344\,89281 &= 753303361 \cdot 1506606721,\\
1144\,33608\,11500\,73701 &= 756417901 \cdot 1512835801,\\
1167\,74805\,34368\,49501 &= 764116501 \cdot 1528233001,\\
1646\,69761\,98511\,37101 &= 907385701 \cdot 1814771401.
\end{aligned}$$

5.2. **$10^6 < p_1 < 10^8$.** When p_1 is in this interval, p_1 is too large and calculating $2^{p_1-1} - 1$ and $3^{p_1-1} - 1$ takes too much time. It is also too small and there are too many candidates for p_2 with

$$p_1 < p_2 \le Q_{11}/p_1, \qquad p_2 \equiv 1 \mod \lambda_{p_1}.$$

We need to use the Chinese Remainder Theorem to reduce the number of candidates. Just as in the $t = 3$ case, we divide the algorithm into three parts according to $p_1 \equiv 3 \bmod 4$, $p_1 \equiv 5 \bmod 8$ and $p_1 \equiv 1 \bmod 8$. The difference is that we use the first six primes in these cases.

For $p_1 \equiv 3 \bmod 4$, we find p_2 with $\sigma^{\nu}_{p_2} = \sigma^{\nu}_{p_1}$. If $p_2 \equiv 3 \bmod 4$, then by Proposition 2.3

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right), \qquad a = 2, 3, 5, 7, 11, 13.$$

If $p_2 \equiv 1 \bmod 4$, then by Proposition 2.4

$$\left(\frac{a}{p_2}\right) = 1, \qquad a = 2, 3, 5, 7, 11, 13.$$

Since $8\cdot3\cdot5\cdot7\cdot11\cdot13 = 120120$, together with $p_2 \equiv 1 \bmod \lambda_{p_1}$, in each case there are at most 180 residue classes modulo $\operatorname{lcm}(\lambda_{p_1}, 120120)$. Our algorithm takes about 16 hours and finds no spsp(ν).

If $p_1 \equiv 5 \bmod 8$, then $p_2 \equiv 1 \bmod 4$. If $p_2 \equiv 5 \bmod 8$, then we have $p_2 \equiv 1 \bmod \lambda_{p_1}$ and

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right), \qquad a = 2, 3, 5, 7, 11, 13.$$

If $p_2 \equiv 1 \bmod 8$, then we have $p_2 \equiv 1 \bmod \lambda_{p_1}$ and

$$\left(\frac{a}{p_2}\right) = 1, \qquad a = 2, 3, 5, 7, 11, 13.$$

Our algorithm takes about 15 hours and finds only one spsp(ν):

$$34155\,00717\,28321 = 10670053 \cdot 32010157,$$

which is ψ_8.

For $p_1 \equiv 1 \bmod 8$, denote $e = v(p_1 - 1)$ and $f = v(\lambda_{p_1})$. Then $f \le e$. If $f = e$, there are two cases. For $p_2 \equiv 1 + 2^e \bmod 2^{e+1}$, then $p_2 \equiv 1 \bmod \lambda_{p_1}$ and

$$\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right), \qquad a = 2, 3, 5, 7, 11, 13.$$

If $p_2 \equiv 1 \bmod 2^{e+1}$, then $p_2 \equiv 1 \bmod \lambda_{p_1}$ and

$$\left(\frac{a}{p_2}\right) = 1, \qquad a = 2, 3, 5, 7, 11, 13.$$

If $f < e$, we only use the condition $p_2 \equiv 1 \bmod \lambda_{p_1}$, Our algorithm takes about 18 hours and finds no spsp(ν).

Then we finish the $t = 2$ case and find six strong pseudoprimes to the first eight prime bases. It takes 77 hours.

6. Conclusion

Until now, we have checked all the odd composite numbers up to Q_{11}, and find eight strong pseudoprimes to the first eight prime bases. See Table 2.

Table 2. Spsp's $n \le Q_{11}$ to the first eight prime bases

	Number	Factorization
$t = 3$	3825 12305 65464 13051	149491·747451·34233211
	230 24566 07261 88031	214831·787711·1360591
$t = 2$	84 98355 74122 37221	206135341·412270681
	1134 93190 66344 89281	753303361·1506606721
	1144 33608 11500 73701	756417901·1512835801
	1167 74805 34368 49501	764116501·1528233001
	1646 69761 98511 37101	907385701·1814771401
	34155 00717 28321	10670053·32010157

The first row is Q_{11} and the last row is ψ_8. It is easy to check that Q_{11} is also a strong pseudoprime to the bases 23, 29 and 31. The other seven numbers are not pseudoprimes to the base 23. Therefore, we have Theorem 1.1:

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

Thus, for an integer less than Q_{11}, only nine strong pseudoprime tests are needed to judge its primality and compositeness. We use Magma and all algorithms are run on a PC (an Intel(R) Core(TM)2 Duo CPU E7500 at 2.93GHz with 2Gb of RAM). The total time is about 104 hours.

Our algorithm is similar to Jaeschke's [2], but there are some differences. In the $t = 3$ case, when feasible pairs (p_1, p_2) with $b = p_1p_2 < 4 \cdot 10^6$, we factor $\gcd(2^{b-1} - 1, 3^{b-1} - 1)$ to get p_3 instead of searching p_3 in the range

$$p_2 < p_3 \le Q_{11}/b, \qquad p_3 \equiv b^{-1} \mod \lambda.$$

In contrast, Jaeschke just searched p_3 directly. This is necessary in our case as we search p_3 for the first feasible pair given in Example 4.2, i.e., $p_1 = 43$, $p_2 = 9283$. It requires more than 4 hours, but factorization only needs seconds. In the $t = 2$ case, Jaeschke did not use the Chinese Remainder Theorem and searched p_2 in the range

$$p_1 < p_2 \le Q_{11}/p_1, \qquad p_2 \equiv 1 \mod \lambda_{p_1}.$$

Our first version algorithm did the same thing. As our upper bound Q_{11} is much greater than his ψ_8, it took more than 10 days. By Proposition 2.3 and Proposition 2.4, we can use the Chinese Remainder Theorem to find p_2 with $\sigma_{p_2} = \sigma_{p_1}$ except for the case

$$p_1 \equiv 1 \mod 8, \qquad v(\lambda_{p_1}) < v(p_1 - 1).$$

Such primes are rare.

For future work, Zhang has conjectured in [7] that

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

which is the smallest known strong pseudoprime to the first 12 prime bases. We need to check all odd integers up to this bound to determine the exact value of ψ_{12}. Only for the $t = 2$ case, do we have to search p_2 for all $p_1 \le \sqrt{N_{12}} \approx 5.6 \cdot 10^{11}$. It is beyond the capability of a personal computer even if we use the Chinese Remainder Theorem.

We should mention Charles Greathouse's computation. He also reached the conclusion that $\psi_9 = \psi_{10} = \psi_{11} = Q_{11}$ based on the output of Jan Feitsma, who computed all odd psp(2)'s up to 2^{64}. Feitsma's result is available at `http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html` and Greathouse's result is stated as A014233 in OEIS. Our calculation is independent of their results and it is more efficient.

Acknowledgments

The authors thank the anonymous referees for many suggestions on how to improve the presentation of this paper.

References

[1] François G. Dorais and Dominic Klyve, *A Wieferich prime search up to* 6.7×10^{15}, J. Integer Seq. **14** (2011), no. 9, Article 11.9.2, 14. MR2859986

[2] Gerhard Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), no. 204, 915–926, DOI 10.2307/2153262. MR1192971 (94d:11004)

[3] Joshua Knauer and Jörg Richstein, *The continuing search for Wieferich primes*, Math. Comp. **74** (2005), no. 251, 1559–1563 (electronic), DOI 10.1090/S0025-5718-05-01723-0. MR2137018 (2006a:11006)

[4] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), no. 151, 1003–1026, DOI 10.2307/2006210. MR572872 (82g:10030)
[5] Michael O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138, DOI 10.1016/0022-314X(80)90084-0. MR566880 (81f:10003)
[6] Zhenxiang Zhang, *Finding strong pseudoprimes to several bases*, Math. Comp. **70** (2001), no. 234, 863–872, DOI 10.1090/S0025-5718-00-01215-1. MR1697654 (2001g:11009)
[7] Zhenxiang Zhang, *Finding* C_3*-strong pseudoprimes*, Math. Comp. **74** (2005), no. 250, 1009–1024 (electronic), DOI 10.1090/S0025-5718-04-01693-X. MR2114662 (2005k:11243)
[8] Zhenxiang Zhang, *Two kinds of strong pseudoprimes up to* 10^{36}, Math. Comp. **76** (2007), no. 260, 2095–2107 (electronic), DOI 10.1090/S0025-5718-07-01977-1. MR2336285 (2008h:11114)
[9] Zhenxiang Zhang and Min Tang, *Finding strong pseudoprimes to several bases. II*, Math. Comp. **72** (2003), no. 244, 2085–2097 (electronic), DOI 10.1090/S0025-5718-03-01545-X. MR1986825 (2004c:11008)

Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, 100190
E-mail address: jiangyupeng@amss.ac.cn

Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, 100190
E-mail address: dengyp@amss.ac.cn