Bull. Aust. Math. Soc. **81** (2010), 165–176
doi:10.1017/S0004972709000744

SYLOW p-PSEUDOPRIMES TO SEVERAL BASES FOR SEVERAL PRIMES p

ZHENXIANG ZHANG ✉ and RUIRUI XIE

(Received 30 April 2009)

Abstract

Browkin ['Some new kinds of pseudoprimes', *Math. Comp.* **73** (2004), 1031–1037] gave examples of strong pseudoprimes to many bases which are not Sylow p-pseudoprimes to two bases only, where $p = 2$ or 3. In contrast to Browkin's examples, Zhang ['Notes on some new kinds of pseudoprimes', *Math. Comp.* **75** (2006), 451–460] gave facts and examples which are unfavorable for Browkin's observation on detecting compositeness of odd composite numbers. In particular, Zhang gave a Sylow p-pseudoprime (with 27 decimal digits) to the first 6 prime bases for all the first 6 primes p, and conjectured that for any $k \geq 1$, there would exist Sylow p-pseudoprimes to the first k prime bases for all the first k primes p. In this paper we tabulate 27 Sylow p-pseudoprimes less than 10^{36} to the first 7 prime bases for all the first 7 primes p (two of which are Sylow p-pseudoprimes to the first 7 prime bases for all the first 8 primes p). We describe the procedure for finding these numbers. The main tools used in our method are the cubic residue characters and the Chinese remainder theorem.

2000 *Mathematics subject classification*: primary 11A15; secondary 11A51, 11Y11.

Keywords and phrases: strong pseudoprimes, Miller tests, Sylow p-pseudoprimes, cubic residue characters, Chinese remainder theorem.

1. Introduction

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

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

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

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

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

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

Research supported by the NSF of China Grant 10071001.

holds for $1 \le j \le k$, then we say that n passes the Miller test to bases b_j and that n is an spsp$(b_1, \ldots, b_k)$ (a strong pseudoprime to bases $b_1, \ldots, b_k$) [7], or write

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

(The original test of Miller [7] was somewhat more complicated and was a deterministic, ERH-based test; see [4, Section 3.4].)

The definition of strong pseudoprimes is based on the fact that in a finite field the equation $X^2 = 1$ has at most two solutions, 1 and -1. Browkin [3] defined more general pseudoprimes using the fact that, in a finite field, the equation $X^r = 1$ has at most r solutions for every $r \ge 2$. Let p be a prime such that

$$n - 1 = p^r d$$

with $r > 0$ and $p \nmid d$, and let

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

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

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

where $\mathrm{ord}(x)$ is the order of x in the multiplicative group modulo n. The following conditions hold if n is a prime.

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

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

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

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

Browkin [3, Section 2] defined a composite number n to be a *Sylow p-pseudoprime to bases $b_1, \ldots, b_k$*, denoted

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

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

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

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

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

Browkin [3] gave examples of strong pseudoprimes to many bases which are not Sylow p-pseudoprimes to two bases only, where $p = 2$ or 3. More precisely, in

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

[3, Sections 4–5] he checked the numbers ψ_t for $2 \le t \le 8$ and upper bounds of ψ_9, ψ_{10} and ψ_{11} given in [6] and found that none of these numbers belong to some Syl_p-psp(b_1, b_2) for $p = 2$ or 3 and $b_1, b_2 \in \{2, 3, 5\}$, where ψ_t is the smallest strong pseudoprime to all the first t prime bases [6, 9–11, 13, 14].

In contrast to Browkin's examples, Zhang [12] gave facts and examples which are unfavorable for Browkin's observation of detecting compositeness of odd composite numbers. After checking all the 52 593 spsp(2, 3)s less than 10^{16} given by Bleichenbacher [1] (also available in the package of [2]), all the 246 683 Carmichael numbers less than 10^{16} [8], all the 193 961 K2-spsp(2, 3, 5, 7, 11)s less than 10^{24}, and all the 44 134 K3-spsp(2, 3, 5, 7, 11)s less than 10^{24}, Zhang [12] found that K3-strong pseudoprimes are most likely to be Sylow p-pseudoprimes to more prime bases for more primes p. Recall [10] that a Kk number is of the form

$$n = pq \quad \text{with } p, q \text{ primes and } q - 1 = k(p - 1). \tag{1.6}$$

In particular, Zhang [12, Examples 3.1] found a 24-digit K3-spsp(2, 3, 5, 7, 11) $N_1 \in \mathrm{Syl}_p$-psp(2, 3, 5, 7, 11) for all $p \in \{2, 3, 5, 7, 11\}$. Then Zhang calculated all 330 670 K3-spsp(2, 3, 5, 7, 11, 13)s less than 10^{28} and found [12, Examples 3.2] a 27-digit number $N_2 \in \mathrm{Syl}_p$-psp(2, 3, 5, 7, 11, 13) for all $p \in \{2, 3, 5, 7, 11, 13\}$. Zhang [12, Remark 3.1] made the following conjecture.

CONJECTURE 1.1. *For any $k \ge 1$, there exist Sylow p-pseudoprimes to the first k prime bases for all the first k primes p.*

In this paper we describe a procedure for finding all K3-Sylow p-pseudoprimes less than 10^{36} to the first 7 prime bases for all the first 7 primes p. There are in total 27 numbers, two of which are Sylow p-pseudoprimes to the first 7 prime bases for all the first 8 primes p. The main tools used in our method are the same as those used in finding all the 44 134 K3-spsp(2, 3, 5, 7, 11)s less than 10^{24} and all 330 670 K3-spsp(2, 3, 5, 7, 11, 13)s less than 10^{28}, namely, cubic residue characters and the Chinese remainder theorem. But we do not actually calculate all K3-strong pseudoprimes less than 10^{36} to the first 7 prime bases, which would be much more time-consuming (see Remark 3.10 below) as Zhang [13] calculated all K2-strong pseudoprimes less than 10^{36} to the first 9 prime bases. Instead, we propose necessary conditions for n to be a K3-strong pseudoprime to one or to several prime bases with

$$n \equiv 1 \bmod p$$

for one or for several small primes p. Thus we have a smaller number of candidate K3-strong pseudoprimes n at hand. Then we subject these candidates n to Sylow p-pseudoprime conditions, and obtain the desired numbers.

In Section 2 we recall and state some basic facts concerning cubic residue characters, which are necessary in Section 3, where we describe a method for finding K3-Sylow p-pseudoprimes. All K3-Sylow p-pseudoprimes less than 10^{36} to the first 7 prime bases for the first 7 primes p are tabulated. These numbers further support Conjecture 1.1.

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

2. Cubic residue characters

In this section and the next, D denotes the ring of Eisenstein integers

$$\mathbb{Z}[\omega] = \{x + y\omega \mid x, y \in \mathbb{Z}\},$$

where $\omega = (-1 + \sqrt{-3})/2$. It is well known that D is a Euclidean domain. Let $\alpha, \beta, \pi \in D$. The norm of $\alpha = x + y\omega$ is $N(\alpha) = \alpha\bar{\alpha} = x^2 - xy + y^2$. The units in D are the only six elements with norm 1: $\pm 1, \pm\omega, \pm\omega^2$. The irreducibles of D are $\pm(1-\omega), \pm(1+2\omega), \pm(2+\omega)$ with norm 3; primes $\equiv 2 \pmod 3$ and their associates; and nonreal elements with prime norm $\equiv 1 \pmod 3$. A prime $\equiv 1 \pmod 3$ must be the norm of an irreducible of D; and the prime $3 = -\omega^2(1-\omega)^2$. A nonunit α is called primary if $\alpha \equiv 2 \pmod 3$. Among six associates of a nonunit α satisfying $(1-\omega) \nmid \alpha$, there is (only) one which is primary.

If π is an irreducible with $N(\pi) \neq 3$ and $\pi \nmid \alpha$, then there is a unique integer $j = 0$, 1 or 2 such that

$$\alpha^{(N(\pi)-1)/3} \equiv \omega^j \bmod \pi. \tag{2.1}$$

Thus the cubic residue character of α modulo π, with $N(\pi) \neq 3$ and $\pi \nmid \alpha$, is defined and denoted by

$$\left(\frac{\alpha}{\pi}\right)_3 = \omega^j, \tag{2.2}$$

which is 1, ω or $\omega^2 = -1 - \omega$. If $\pi \mid \alpha$, then $(\alpha/\pi)_3 = 0$. If b is an odd prime $\equiv 2 \bmod 3$ then

$$\left(\frac{\alpha}{b}\right)_3 \equiv \alpha^{(b^2-1)/3} \bmod b \quad \text{and} \quad \left(\frac{x}{b}\right)_3 = 1 \text{ for } x \in \mathbb{Z} \text{ with } \gcd(b, x) = 1. \tag{2.3}$$

This character plays the same role in the theory of cubic residues as the Legendre symbol plays in the theory of quadratic residues. We need the following eight lemmas concerning cubic residue characters.

LEMMA 2.1 [5, Propositions 9.3.3 and 9.3.4].

(a) $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3(\beta/\pi)_3$.
(b) $(\bar{\alpha}/\bar{\pi})_3 = \overline{(\alpha/\pi)_3} = (\alpha^2/\pi)_3$.
(c) *If* $\alpha \equiv \beta \mod \pi$, *then* $(\alpha/\pi)_3 = (\beta/\pi)_3$.

LEMMA 2.2. *We have:*

(I) $(-1/\pi)_3 = 1$ [5, Remark (b) after Theorem 9.1];
(II) $(2/\pi)_3 = 1 \Longleftrightarrow \pi \equiv 1 \mod 2$ [5, Proposition 9.6.1].

LEMMA 2.3 (Law of cubic reciprocity [5, Theorem 9.1]). *Let π and β be primary irreducibles with $N(\pi) \neq 3$, $N(\beta) \neq 3$, $N(\pi) \neq N(\beta)$. Then*

$$\left(\frac{\beta}{\pi}\right)_3 = \left(\frac{\pi}{\beta}\right)_3.$$

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

LEMMA 2.4 (Supplement to the cubic reciprocity law [5, Theorem 9.1′]). *Suppose that $N(\pi) \neq 3$. If $\pi = q$ is rational, write $q = 3j - 1$; if $\pi = u + v\omega$ is a primary complex irreducible, write $u = 3j - 1$. Then*

$$\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2j}.$$

LEMMA 2.5. *Let β and π be primary irreducible with different prime norms $\equiv 1 \bmod 3$. Let $b = N(\beta)$ and $q = N(\pi)$. Then*

$$\left(\frac{b}{\pi}\right)_3 = \left(\frac{q\overline{\pi}}{\beta}\right)_3.$$

PROOF. By Lemmas 2.1(a) and 2.3,

$$\left(\frac{b}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3 \left(\frac{\overline{\beta}}{\pi}\right)_3 = \left(\frac{\pi}{\beta}\right)_3 \left(\frac{\pi}{\overline{\beta}}\right)_3.$$

By Lemma 2.1(b),

$$\left(\frac{\pi}{\overline{\beta}}\right)_3 = \overline{\left(\frac{\overline{\pi}}{\beta}\right)_3} = \left(\frac{\overline{\pi}^2}{\beta}\right)_3.$$

Thus

$$\left(\frac{b}{\pi}\right)_3 = \left(\frac{\pi}{\beta}\right)_3 = \left(\frac{\overline{\pi}^2}{\beta}\right)_3 = \left(\frac{q\overline{\pi}}{\beta}\right)_3$$

by Lemma 2.1(a). □

LEMMA 2.6. *Let $\beta = u + v\omega$ be primary irreducible with prime $b = N(\beta) \equiv 1 \bmod 3$. Let $\alpha = c + d\omega$ and $a = c - duv^{-1} \bmod b$. Then*

$$\alpha \equiv a \bmod \beta.$$

PROOF. $\alpha - a \equiv c + d\omega - c + duv^{-1} \equiv dv^{-1}(u + v\omega) \mod b$. The lemma follows. □

LEMMA 2.7. *Let β, b and α be as in Lemma 2.6. Then*

$$\left(\frac{\alpha}{\beta}\right)_3 = 1 \Longleftrightarrow (c - duv^{-1})^{(b-1)/3} \equiv 1 \bmod b.$$

PROOF. The lemma follows by Lemma 2.6, (2.1) and (2.2). □

LEMMA 2.8 [5, Proposition 9.3.3(a)]. *Let π be primary irreducible with prime $q = N(\pi) \equiv 1 \pmod 3$. Let $b \in \mathbb{Z}$ with $q \nmid b$. Then*

$$\left(\frac{b}{\pi}\right)_3 = 1 \quad \textit{if and only if} \quad x^3 \equiv b \bmod q \textit{ has a solution with } x \in \mathbb{Z},$$

that is, if and only if b is a cubic residue modulo q.

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

3. K3-Sylow b-pseudoprimes to several bases for several primes b

Throughout this section let π be a primary irreducible of D such that $q = N(\pi) \equiv 1 \mod 3$ and $p = (q+2)/3$ are two primes determined by π. We describe a method to compute all composite numbers $n = pq \equiv 1 \mod b$, below a given limit (say, 10^{36}), which are Sylow b-pseudoprimes to the first several (say, 7) prime bases for the first several primes b. For this purpose we look for necessary conditions on π for $n = pq$ to be a Sylow b-pseudoprime to several prime bases for several primes b.

Notation. Let r be a prime and a a positive integer with $r \nmid a$. Denote by $\mathrm{ord}_r(a)$ the order of a in the group $\mathbb{Z}_r^*$. We write $v_2(x) = s$ if and only if $2^s \mid x$ and $2^{s+1} \nmid x$ for x a positive integer.

LEMMA 3.1 (Part of [6, Proposition 1]). *Let n, p, q, k be as in (1.6), and let b be a positive integer. If n is an* spsp(b), *then* $v_2(\mathrm{ord}_p(b)) = v_2(\mathrm{ord}_q(b))$.

LEMMA 3.2. *Let b be a positive integer (not necessarily prime). Then*

$$n = pq \text{ is a } \mathrm{psp}(b) \Longleftrightarrow \left(\frac{b}{\pi}\right)_3 = 1.$$

PROOF. Since $n - 1 = (p-1)(q+3) = (q-1)p + (q-1)/3$, we have

$$\begin{aligned} &n = pq \text{ is a } \mathrm{psp}(b) \\ \Longleftrightarrow\ & b^{n-1} \equiv 1 \mod n \Longleftrightarrow b^{(q-1)/3} \equiv 1 \mod q \\ \Longleftrightarrow\ & b \text{ is a cubic residue modulo } q \Longleftrightarrow \left(\frac{b}{\pi}\right)_3 = 1 \end{aligned}$$

(the last equivalence follows by Lemma 2.8). □

PROPOSITION 3.3. *If $n = pq$ is a strong pseudoprime to a (not necessarily prime) base b, then*

$$\left(\frac{b}{\pi}\right)_3 = 1 \quad \text{and} \quad \left(\frac{b}{p}\right) = \left(\frac{b}{q}\right).$$

PROOF. Since $n = pq$ is an spsp(b), n is a psp(b). Thus

$$\left(\frac{b}{\pi}\right)_3 = 1$$

by Lemma 3.2. Also since n is an spsp(b),

$$v_2(\mathrm{ord}_p(b)) = v_2(\mathrm{ord}_q(b))$$

by Lemma 3.1. Since $v_2(p-1) = v_2(q-1)$,

$$\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right).$$

□

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

LEMMA 3.4. *If $n = pq$ is an* spsp(2), *then $\pi \equiv 5$ or $11 \bmod 12$.*

PROOF. Since $n = pq$ is an spsp(2),

$$\left(\frac{2}{\pi}\right)_3 = 1 \quad \text{and} \quad \left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$$

by Proposition 3.3. Since $(2/\pi)_3 = 1$ and π is primary,

$$\pi \equiv 5 \bmod 6 \tag{3.1}$$

by Lemma 2.2(II). Since $(2/p) = (2/q)$,

$$\frac{q^2-1}{8} \quad \text{and} \quad \frac{p^2-1}{8} = \frac{(q-1)(q+5)}{9 \cdot 8} \text{ have the same parity.}$$

Thus $q \equiv 1 \bmod 4$. On the other hand, $q \equiv 1 \bmod 3$, thus

$$q = N(\pi) \equiv 1 \bmod 12. \tag{3.2}$$

Combining (3.1) and (3.2), we have $\pi \equiv 5$ or $11 \bmod 12$. □

LEMMA 3.5. *If $n = pq$ is an* spsp(3), *then $\pi \equiv 8 \bmod 9$ and $n \equiv p \equiv q \equiv 1 \bmod 3$.*

PROOF. Since $n = pq$ is an spsp(3),

$$\left(\frac{3}{\pi}\right)_3 = 1 \quad \text{and} \quad \left(\frac{3}{p}\right) = \left(\frac{3}{q}\right)$$

by Proposition 3.3. Write $\pi = x + y\omega$. Since $3 = -(1-\omega)^2\omega^2$,

$$1 = \left(\frac{3}{\pi}\right)_3 = \left(\frac{-1}{\pi}\right)_3 \left(\frac{1-\omega}{\pi}\right)_3^2 \left(\frac{\omega}{\pi}\right)_3^2 = 1 \cdot \omega^{(x+1)/3} \cdot \omega^{2(q-1)/3}$$

by Lemmas 2.1(a), 2.2(I), 2.4, and (2.1) and (2.2). Thus

$$\frac{x+1}{3} + \frac{2(q-1)}{3} \equiv 0 \bmod 3,$$

therefore

$$\pi \equiv 2,\ 5,\ \text{or } 8 \bmod 9. \tag{3.3}$$

On the other hand, since

$$(-1)^{(q-1)/2} = \left(\frac{3}{q}\right) = \left(\frac{3}{p}\right) = (-1)^{(q-1)/6}\left(\frac{p}{3}\right),$$

then

$$\left(\frac{p}{3}\right) = 1, \text{ that is, } \frac{q+2}{3} = p \equiv 1 \bmod 3.$$

Thus

$$q = N(\pi) \equiv 1 \bmod 9. \tag{3.4}$$

Combining (3.3) and (3.4), we have $\pi \equiv 8 \bmod 9$ and $n \equiv p \equiv q \equiv 1 \bmod 3$. □

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

COROLLARY 3.6. *If $n = pq$ is an* spsp(3) *and $\pi \equiv 5 \mod 6$, then $\pi \equiv 17 \bmod 18$.*

In the rest of this section, let

$$p_\alpha = \frac{N(\alpha)+2}{3}$$

be a positive integer determined by a primary (but not necessarily irreducible) element α of D. Put

$$R_2 = R_2' = \{5, 11\} \quad \text{and} \quad R_3 = R_3' = \{17\};$$

for odd prime $b \equiv 2 \bmod 3$, put

$$R_b = \left\{\alpha = x + y\omega \mid 0 \le x,\ y < 6b,\ \alpha \equiv 5 \bmod 6,\ \left(\frac{\alpha}{b}\right)_3 = 1,\ \text{and}\ \left(\frac{N(\alpha)}{b}\right) = \left(\frac{p_\alpha}{b}\right)\right\};$$

and for prime $b \equiv 1 \bmod 3$ ($b = \beta\overline{\beta}$ for some primary irreducible β), put

$$R_b = \left\{\alpha = x + y\omega \mid 0 \le x,\ y < 6b,\ \alpha \equiv 5 \bmod 6,\ \left(\frac{N(\alpha)\overline{\alpha}}{\beta}\right)_3 = 1,\ \text{and}\ \left(\frac{N(\alpha)}{b}\right) = \left(\frac{p_\alpha}{b}\right)\right\}.$$

LEMMA 3.7. *Let prime $b > 3$. If $n = pq$ is an* spsp(b) *and $\pi \equiv 5 \bmod 6$, then there exists $\alpha \in R_b$ such that $\pi \equiv \alpha \bmod 6b$.*

PROOF. Let $\alpha = (\pi \bmod 6b)$. We prove that $\alpha \in R_b$.

Since $\alpha \equiv \pi \bmod 6b$ and $\pi \equiv 5 \bmod 6$, $\alpha \equiv 5 \bmod 6$. By Lemma 2.1(c),

$$\left(\frac{\alpha}{b}\right)_3 = \left(\frac{\pi}{b}\right)_3 \quad \text{for } b \equiv 2 \bmod 3;$$

and

$$\left(\frac{N(\alpha)\overline{\alpha}}{\beta}\right)_3 = \left(\frac{N(\pi)\overline{\pi}}{\beta}\right)_3 \quad \text{for } b \equiv 1 \bmod 3.$$

By Lemma 2.3,

$$\left(\frac{\pi}{b}\right)_3 = \left(\frac{b}{\pi}\right)_3 \quad \text{for } b \equiv 2 \bmod 3;$$

and by Lemma 2.5,

$$\left(\frac{N(\pi)\overline{\pi}}{\beta}\right)_3 = \left(\frac{b}{\pi}\right)_3 \quad \text{for } b \equiv 1 \bmod 3.$$

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

Since $n = pq$ is an spsp(b), then by Proposition 3.3,

$$\left(\frac{b}{\pi}\right)_3 = 1 \quad \text{and} \quad \left(\frac{b}{p}\right) = \left(\frac{b}{q}\right).$$

Thus

$$\left(\frac{\alpha}{b}\right)_3 = 1 \quad \text{for } b \equiv 2 \bmod 3;$$

and

$$\left(\frac{N(\alpha)\overline{\alpha}}{\beta}\right)_3 = 1 \quad \text{for } b \equiv 1 \bmod 3.$$

Since

$$\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right),$$

we have

$$\left(\frac{p}{b}\right) = (-1)^{\frac{p-1}{2}\frac{b-1}{2}}\left(\frac{b}{p}\right) = (-1)^{\frac{q-1}{2}\frac{b-1}{2}}\left(\frac{b}{q}\right) = \left(\frac{q}{b}\right).$$

Since $\pi \equiv \alpha \bmod 6b$, $q = N(\pi) \equiv N(\alpha) \bmod 6b$ and $p \equiv p_\alpha \bmod 2b$. Thus

$$\left(\frac{p}{b}\right) = \left(\frac{p_\alpha}{b}\right) \quad \text{and} \quad \left(\frac{q}{b}\right) = \left(\frac{N(\alpha)}{b}\right),$$

therefore

$$\left(\frac{p_\alpha}{b}\right) = \left(\frac{N(\alpha)}{b}\right).$$

This means that $\alpha \in R_b$ in both cases. □

COROLLARY 3.8. *Let prime $b > 3$. If $n = pq \equiv 1 \bmod b$ is an* spsp(b) *and $\pi \equiv 5 \bmod 6$, then there exists $\alpha \in R'_b$ such that $\pi \equiv \alpha \bmod 6b$, where*

$$R'_b = \{\alpha \in R_b : N(\alpha)p_\alpha \equiv 1 \bmod b\}.$$

Using (2.3) for $b \equiv 2 \bmod 3$ and Lemma 2.7 for $b \equiv 1 \bmod 3$, it is easy to compute the sets:

$$R'_5 = R_5 = \{11, 17 + 24\omega, 23 + 6\omega, 29\} \quad \text{with } |R'_5| = |R_5| = 4;$$
$$R'_7 = \{5, 23, 29, 41\} \quad \text{with } |R'_7| = 4 \text{ and } |R_7| = 6;$$
$$R'_{11} = \{5 + 36\omega, 17 + 30\omega, 23, 35 + 30\omega, 35 + 48\omega, 53 + 18\omega, 53 + 36\omega, 65\}$$

with $|R'_{11}| = 8$ and $|R_{11}| = 16$;

$$R'_{13} = \{5 + 36\omega, 23 + 72\omega, 29 + 6\omega, 47 + 42\omega, 53, 59, 71, 77\}$$

with $|R'_{13}| = 8$ and $|R_{13}| = 20$;

$$R'_{17} = \{17 + 18\omega, 17 + 84\omega, 35, 35 + 18\omega, 47 + 60\omega, 47 + 72\omega,$$
$$59 + 72\omega, 77 + 30\omega, 89 + 30\omega, 89 + 42\omega, 101, 101 + 84\omega\}$$

with $|R'_{17}| = 12$ and $|R_{17}| = 48$.

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

Using the Chinese remainder theorem we get the set

$$R' = \{x + y\omega : 0 \le x, y < m, x + y\omega \pmod{6b} \in R'_b \text{ for } b = 2, 3, 5, 7, 11, 13 \text{ and } 17\}$$

where

$$m = 6 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = 3\,063\,060 \tag{3.5}$$

and

$$|R'| = 2 \cdot 1 \cdot 4 \cdot 4 \cdot 8 \cdot 8 \cdot 12 = 24\,576. \tag{3.6}$$

By Lemma 3.4, Corollary 3.6, Lemma 3.7, and the Chinese remainder theorem we have the following proposition.

PROPOSITION 3.9. *If $n = pq$ is a strong pseudoprime to the bases* 2, 3, 5, 7, 11, 13 *and* 17 *with $n \equiv 1 \bmod b$ for every $b \in \{2, 3, 5, 7, 11, 13, 17\}$, then there exists $\alpha \in R'$ such that $\pi \equiv \alpha \bmod m$.*

Now we are ready to describe a procedure to compute all Sylow b-pseudoprimes less than L to the first h prime bases for the first h primes b with the form (1.6) (with $k = 3$) and $h \ge 7$.

PROCEDURE Finding-K3-Sylow b-pseudoprimes;
BEGIN
For every $x + y\omega \in R'$, $u \ge 0$, $v \ge 0$, $u + v \le 2\sqrt[4]{3L}/m + 1$ **Do**
begin
$q \leftarrow (x + um)^2 - (x + um)(y + vm) + (y + vm)^2$;
$p \leftarrow (q + 2)/3$; $n \leftarrow p \cdot q$;
If n is a Sylow b-pseudoprime to the first h prime bases for the first h primes b **Then** output n, p and q;
$q \leftarrow (x - um)^2 - (x - um)(y + vm) + (y + vm)^2$;
$p \leftarrow (q + 2)/3$; $n \leftarrow p \cdot q$;
If n is a Sylow b-pseudoprime to the first h prime bases for the first h primes b **Then** output n, p and q;
end
END.

The Delphi Pascal program with multi-precision package partially written in assembly language ran about 100 hours on a PC Pentium IV/1.8 GHz to get all K3-Syl$_b$-psp(2, 3, 5, 7, 11, 13, 17)s less than 10^{36} for all $b \in \{2, 3, 5, 7, 11, 13, 17\}$, listed in Table 1. There are in total 27 numbers, among which two numbers (the sixth and thirteenth) are Syl$_b$-psp(2, 3, 5, 7, 11, 13, 17)s for all $b \in \{2, 3, 5, 7, 11, 13, 17, 19\}$.

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

TABLE 1. List of all K3-Syl$_b$-psp(2, 3, 5, 7, 11, 13, 17)s less than 10^{36} for all $b \in \{2, 3, 5, 7, 11, 13, 17\}$.

Number $n = p(3p-2)$	p
3255 17827 22275 73465 86719 49264 64641	32940240194568373
33466 33475 94306 66263 63898 85517 11681	105619339705426213
34321 28590 82888 57089 81962 62261 67361	106959939398338693
48713 18970 16438 28071 46412 45454 14241	127427351461716973
60017 40243 22423 88826 28154 92527 72481	141441863713497013
89355 04851 01852 33181 84353 92607 18561	172583360061338893
94334 35296 71489 46803 71149 19685 16481	177326772717441013
98179 04432 48417 43511 75423 03439 79361	180904251216715693
1 04856 09580 68794 01567 53900 99146 60801	186954625338948133
1 12871 29226 59314 82708 83446 81805 61441	193968461582402173
1 26192 61529 27283 74198 55466 02203 86081	205095599898135613
1 26711 97581 08116 54632 87799 56034 36321	205517214048533053
2 19985 75905 09437 99374 12401 26723 63041	270792515314427773
2 56834 54509 92444 25550 34514 94742 32801	292594454891205133
2 76365 15704 35380 02159 47922 57112 04961	303515599293533293
2 92312 97147 05363 61635 70665 74413 60161	312150055513122493
4 25331 43489 83047 29003 61378 62460 24161	376533059592516493
5 22579 54718 56808 69563 05939 57404 85761	417364567728535093
5 38219 68806 12101 20549 34515 89207 23201	423564118743632533
5 38740 85469 88139 42679 53724 70656 91841	423769141042153573
5 69412 28819 97928 60780 89824 98295 20001	435665119175953333
5 77798 57433 03354 93608 87376 58622 96801	438861623722989133
6 12786 87162 58939 94274 66993 06985 12321	451953858863894053
7 21881 07313 53007 73925 69713 27672 21121	490537485191940853
7 83656 84165 70001 72473 19473 00249 58081	511095829780482613
8 30518 50508 75328 63726 24293 23951 81601	526155396908407933
9 93224 90312 41334 14784 52036 95543 35681	575391143230450213

REMARK 3.10. Let

$$R = \{x + y\omega : 0 \le x,\ y < m,\ x + y\omega \pmod{6b} \in R_b \text{ for } b = 2, 3, 5, 7, 11, 13 \text{ and } 17\}$$

where m is the same as given in (3.5). Then

$$|R| = 2 \cdot 1 \cdot 4 \cdot 6 \cdot 16 \cdot 20 \cdot 48 = 737\,280$$

and

$$\frac{|R|}{|R'|} = \frac{737\,280}{24\,576} = 30$$

where $|R'| = 24\,576$ is given in (3.6). If we had used the set R to actually calculate all K3-strong pseudoprimes less than 10^{36} to the first 7 prime bases and then to subject these K3-strong pseudoprimes to Sylow b-pseudoprime conditions, it would have taken about $100 \cdot 30 = 3000$ hours on a PC Pentium IV/1.8 GHz.

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press

References

[1] D. Bleichenbacher, 'Efficiency and security of cryptosystems based on number theory', ETH PhD Dissertation 11404, Swiss Federal Institute of Technology, Zurich, 1996.
[2] D. M. Bressoud and S. Wagon, *A Course in Computational Number Theory* (Key College Publishing, Emeryville, CA, 2000).
[3] J. Browkin, 'Some new kinds of pseudoprimes', *Math. Comp.* **73**(246) (2004), 1031–1037; Math. Comp. **74** (2005), 1573 (Erratum).
[4] R. Crandall and C. Pomerance, *Prime Numbers, a Computational Perspective*, 2nd edn (Springer, New York, 2005).
[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn Graduate Texts in Mathematics, 84 (Springer, New York, 1990).
[6] G. Jaeschke, 'On strong pseudoprimes to several bases', *Math. Comp.* **61** (1993), 915–926.
[7] G. Miller, 'Riemann's hypothesis and tests for primality', *J. Comput. System Sci.* **13** (1976), 300–317.
[8] R. G. E. Pinch, 'The Carmichael numbers up to 10^{16}', Preprint, 1998. http://www.chalcedon.demon.co.uk/carpsp.html.
[9] C. Pomerance, J. L. Selfridge and S. S. Wagstaff Jr, 'The pseudoprimes to $25 \cdot 10^9$', *Math. Comp.* **35** (1980), 1003–1026.
[10] Z. 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.
[11] Z. Zhang, 'Finding C_3-strong pseudoprimes', *Math. Comp.* **74** (2005), 1009–1024. http://www.ams.org/mcom/2005-74-250/S0025-5718-04-01693-X/home.html.
[12] Z. Zhang, 'Notes on some new kinds of pseudoprimes', *Math. Comp.* **75**(253) (2006), 451–460. http://www.ams.org/mcom/2006-75-253/S0025-5718-05-01775-8/home.html.
[13] Z. Zhang, 'Two kinds of strong pseudoprimes up to 10^{36}', *Math. Comp.* **76**(260) (2007), 2095–2107. http://www.ams.org/mcom/2007-76-260/S0025-5718-07-01977-1/home.html.
[14] Z. Zhang and M. 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.

ZHENXIANG ZHANG, Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, PR China
e-mail: zhangzhx@mail.wh.ah.cn, ahnu_zzx@sina.com

RUIRUI XIE, Department of Mathematics, Anhui Normal University, 241000 Wuhu, Anhui, PR China
e-mail: XieRR19860@163.com

https://doi.org/10.1017/S0004972709000744 Published online by Cambridge University Press