Lawrence Somer
On superpseudoprimes

Mathematica Slovaca, Vol. 54 (2004), No. 5, 443--451

Persistent URL: http://dml.cz/dmlcz/130094

Mathematica Slovaca
© 2004
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **54** (2004), No. 5, 443–451

ON SUPERPSEUDOPRIMES

LAWRENCE SOMER

(*Communicated by Stanislav Jakubec*)

ABSTRACT. A superpseudoprime to the base a is a pseudoprime to the base a, all of whose divisors greater than 1 are either pseudoprimes or primes. Superpseudoprimes with exactly two distinct prime divisors are not very interesting, since their only proper divisors are primes. Several authors have generated infinitely many superpseudoprimes with exactly three distinct prime divisors for various bases a. In this paper, given any integer $a > 1$, we generate infinitely many superpseudoprimes to the base a with exactly four distinct prime divisors when the square-free kernel of a is congruent to 1 or 3 modulo 4.

1. Introduction

Let $a > 1$ be an integer. The positive odd composite integer N is called a *pseudoprime to the base* a if

$$a^{N-1} \equiv 1 \pmod{N}. \tag{1.1}$$

A composite odd integer N satisfying (1.1) is called a *superpseudoprime to the base* a if each divisor of N greater than 1 is either a pseudoprime to the base a or a prime.

Superpseudoprimes with exactly two distinct prime divisors are not very interesting, since their only proper divisors are primes. Several authors have generated infinitely many superpseudoprimes with exactly three distinct prime divisors. Szymiczek [14] and Rotkiewicz [12] have shown this is possible when $a = 2$. Fehér and Kiss [3] demonstrated that infinitely many such superpseudoprimes exist when $4 \nmid a$. Phong [9] proved that there exist infinitely

2000 Mathematics Subject Classification: Primary 11A51.
Keywords: pseudoprime, superpseudoprime, Euler pseudoprime, strong pseudoprime, primitive prime divisor.

This paper was written while the author visited the Mathematical Institute of the Academy of Sciences in Prague. His stay was supported by grant A 1019201 of the Grant Agency of the Academy of Sciences of the Czech Republic.

many pseudoprimes to the base a which are products of exactly three distinct primes for any $a > 1$.

We generalize these results in the following theorem. We let $\overline{a}$ denote the square-free kernel of a, that is, a divided by its largest square factor.

THEOREM 1.1. *Let $a > 1$ be an integer such that $\overline{a} \equiv 1 \pmod 2$. Then there exist infinitely many superpseudoprimes to the base a which are products of exactly four distinct primes. Moreover,*

$$\sum_{i=1}^{\infty} \frac{1}{\log P_i^{(4)}} \tag{1.2}$$

diverges, where $P_i^{(4)}$ denotes the ith superpseudoprime to the base a which is a product of exactly four distinct primes.

The proof of Theorem 1.1 will be given in Section 3.

Remark 1.2. Let $a > 1$ and $\overline{a} \equiv 1 \pmod 2$. Let $\mathcal{P}_a^{(3)}(x)$ denote the number of superpseudoprimes to the base a which are products of exactly three distinct primes and which are less than or equal to x. It follows from [5] that for all large x,

$$\mathcal{P}_a^{(3)}(x) > \frac{\log x}{4\overline{a} \log a}.$$

It was also proved in [9] that

$$\sum_{i=1}^{\infty} \frac{1}{\log P_i^{(3)}}$$

diverges, where $P_i^{(3)}$ denotes the ith superpseudoprime to the base a which is a product of exactly three distinct primes.

It was earlier proved by Szymiczek [15] that

$$\sum_{i=1}^{\infty} \frac{1}{Q_i(2)}$$

converges and by Mąkowski [7] that

$$\sum_{i=1}^{\infty} \frac{1}{\log Q_i(a)}$$

diverges, where $Q_i(a)$ stands for the ith pseudoprime to the base $a > 1$.

The proof of Theorem 1.1 depends on the criterion presented below in Theorem 1.3 for an integer to be a superpseudoprime. Recall that a prime p is a *primitive prime divisor* of $a^t - 1$ if $a(p) = t$, where $a(n)$ denotes the least positive integer t such that $n \mid a^t - 1$. Clearly $a(n)$ is the order of a modulo n. Moreover, $a(mn) = \operatorname{lcm}(m, n)$.

THEOREM 1.3. *Let $p_1, p_2, \ldots, p_r$ be distinct odd primes and let $a \geq 2$ be such that $\gcd(a, p_i) = 1$ for every $i = 1, \ldots, r$. Suppose that p_i is a primitive prime divisor of $a^{t_i} - 1$ with multiplicity m_i for $1 \leq i \leq r$. We allow the possibility that $t_i = t_j$ for $1 \leq i < j \leq r$. Let*

$$h = \operatorname{lcm}(t_1, t_2, \ldots, t_r) .$$

Let N be a composite integer such that

$$N = \prod_{i=1}^{r} p_i^{\ell_i} ,$$

where $1 \leq \ell_i \leq m_i$.

Then N is a superpseudoprime to the base a if and only if for each $i = 1, \ldots, r$,

$$p_i \equiv 1 \pmod{h} .$$

The proof of Theorem 1.3 is given in [6; pp. 141–142]. P h o n g [9] proves Theorem 1.3 in the case in which $N = pqr$, where p, q, and r are distinct odd primes.

In order to present the next result, we need to review the definition of additional types of pseudoprimes called Euler pseudoprimes and strong pseudoprimes.

DEFINITION 1.4. The composite odd integer N is called an *Euler pseudoprime to the base a* if $\gcd(a, N) = 1$ and

$$\left(\frac{a}{N}\right) \equiv a^{(N-1)/2} \pmod{N} ,$$

where $a \geq 1$ and $\left(\frac{a}{N}\right)$ denotes the Jacobi symbol.

DEFINITION 1.5. Let N be a composite odd integer and write $N - 1 = 2^s t$, where t is odd. Let $a \geq 1$ be coprime to N. Then N is a *strong pseudoprime to the base a* if

$$a^t \equiv 1 \pmod{N}$$

or

$$a^{2^r t} \equiv -1 \pmod{N} \qquad \text{for some} \quad r , \ 0 \leq r < s .$$

It follows easily from Definition 1.5 that the odd composite integer N is a strong pseudoprime to the base a if and only if N is a pseudoprime to the base a and there exists an integer k such that $2^k \parallel \operatorname{ord}_p a$ for each prime factor p of N, where $\operatorname{ord}_p a$ denotes the order of a modulo p (see [11; p. 1008]). It was

proved in [11; p. 1009] that if N is a strong pseudoprime to the base a, then N is an Euler pseudoprime to the base a.

In the proof of [11; Theorem 1], the authors generated infinitely many strong pseudoprimes to the base a by examining products of primitive prime divisors of $a^t - 1$, where $a^t - 1$ has at least two primitive prime divisors. We think it is of interest to point out that such strong pseudoprimes are also superpseudoprimes. This leads to the following proposition which we will prove in Section 3.

PROPOSITION 1.6. *Let $a > 1$ be an integer. Then there exist infinitely many composite odd integers N, each of which is simultaneously an Euler pseudoprime, a strong pseudoprime, and a superpseudoprime, all to the base a. Let S denote this set of integers N. Let P_i denote the ith member of this set arranged in order of magnitude. Let $\mathcal{P}'_a(x)$ denote the number of elements of S which are less than or equal to x. Then*

$$\mathcal{P}'_a(x) > \frac{\log x}{4a \log a} \qquad \text{for} \quad x \geq a^{15a} + 1 \tag{1.3}$$

and

$$\sum_{i=1}^{\infty} \frac{1}{\log P_i}$$

diverges.

The following theorem shows that for special values of a, there exist infinitely many superpseudoprimes to the base a, each having an arbitrarily large number of distinct prime divisors. We let $\tau(n)$ denote the number of distinct divisors of the positive integer n.

THEOREM 1.7. *Let M be a fixed positive integer. Let $a = b^k$, where $b \geq 2$ and $\tau(k) = M$. Let $p \geq 5$ be a prime such that $p \nmid k$. Let d_i, $i = 1, \ldots, M$, be the distinct divisors of k. Then $b^{pd_i} - 1$ has an odd primitive prime divisor p_i which is also a primitive divisor of $a^p - 1$. Moreover, $p_1 p_2 \cdots p_M$ is a superpseudoprime to the base a.*

We give the proof in Section 3.

2. Preliminaries

Before proceeding further, we will need the following results.

LEMMA 2.1. *If the odd prime p is a primitive prime divisor of $a^n - 1$, then*

(i) $p \equiv 1 \pmod{n}$,

(ii) $p \equiv 1 \pmod{2n}$ *if n is odd.*

P r o o f . Part (i) is a consequence of Fermat's little theorem. Part (ii) follows from the fact that p is odd. □

THEOREM 2.2 (BANG). *Let $a > 1$ be an integer. Then $a^n - 1$ has a primitive prime divisor except in the following cases:*

$$\begin{aligned} &n = 1, && a = 2, \\ &n = 2, && a = 2^k - 1 \quad (k \geq 2), \\ &n = 6, && a = 2. \end{aligned}$$

This theorem is proved in [1], [2], and [16].

THEOREM 2.3 (SCHINZEL). *Let $a > 1$ be an integer. Let*

$$\begin{aligned} &e = 1 && \text{if } \overline{a} \equiv 1 \pmod 4, \\ &e = 2 && \text{if } \overline{a} \equiv 2 \text{ or } 3 \pmod 4. \end{aligned}$$

If $n/(e\overline{a})$ is an odd integer, then $a^n - 1$ has at least two primitive prime divisors except in the following cases:

$$\begin{aligned} &n = 1, && a = 4 \text{ or } a = 9, \\ &n = 3, && a = 4, \\ &n = 4, && a = 2, \\ &n = 6, && a = 3, \\ &n = 12, && a = 2, \\ &n = 20, && a = 2. \end{aligned}$$

This theorem is proved in [13].

Remark 2.4. It is easily seen that if p is a primitive prime divisor of $a^t - 1$ for $t \geq 2$, then p is odd.

3. Proofs of the main results

P r o o f o f T h e o r e m 1.1 . We first prove that there exist infinitely many such superpseudoprimes to the base a. Let p be an odd prime such that $p > 7$, $p \equiv 1 + 2\overline{a} \pmod{4\overline{a}}$, and $a(p) < (p-1)/2$. We will show below that there exist infinitely many primes p satisfying the above conditions when $\overline{a} \equiv 1 \pmod 2$.

Suppose that $\overline{a} \equiv 1 \pmod 4$. Then $(p-1)/2$ is an odd multiple of $\overline{a}$ and by Lemma 2.1, Theorem 2.3 , and Remark 2.4, $a^{(p-1)/2} - 1$ has two odd primitive prime divisors q and r such that $q \equiv r \equiv 1 \pmod{(p-1)/2}$. Since $(p-1)/2$

is odd, we have $q \equiv r \equiv 1 \pmod{p-1}$. By Lemma 2.1 and Theorem 2.2, $a^{p-1}-1$ has an odd primitive prime divisor s such that $s \equiv 1 \pmod{p-1}$. Clearly, $p \equiv 1 \pmod{p-1}$. Moreover, p, q, r, and s are all distinct, since $a(p) < (p-1)/2$. By Theorem 1.3, $pqrs$ is a superpseudoprime to the base a.

Now assume that $\overline{a} \equiv 3 \pmod 4$. By Lemma 2.1 and Theorem 2.3, $a^{(p-1)/2}-1$ has an odd primitive prime divisor q such that $q \equiv 1 \pmod{(p-1)/2}$. Since $(p-1)/2$ is odd, $q \equiv 1 \pmod{p-1}$. By Lemma 2.1 and Theorem 2.3, $a^{p-1}-1$ has distinct primitive prime divisors r and s such that $r \equiv s \equiv 1 \pmod{p-1}$. Since $a(p) < (p-1)/2$, p, q, r, and s are again all distinct, and thus, by Theorem 1.3, $pqrs$ is a superpseudoprime to the base a.

We now show that there indeed exist infinitely many primes p such that $p \equiv 1 + 2\overline{a} \pmod{4\overline{a}}$ and $\overline{a} \equiv 1 \pmod 2$. Let ζ_n denote a primitive nth root of unity. Let $\mathcal{S}$ be the set of rational primes that split completely in $Q(\zeta_{2\overline{a}})$ but do not split completely in $Q(\zeta_{4\overline{a}})$. By the Čebotarev density theorem and Kummer's theorem relating the decomposition of a prime p into prime ideals in an algebraic number field and the factorization of a particular polynomial modulo p (see [4; Chap. V, Theorem 10.4] and [8; Theorem 27]), $\mathcal{S}$ consists of those primes which are congruent to $1 + 2\overline{a} \pmod{4\overline{a}}$ and $\mathcal{S}$ has a positive Dirichlet density

$$d_{\mathcal{S}} = \frac{1}{\phi(4\overline{a})} \tag{3.1}$$

in the set of primes.

We now further suppose that $\overline{a} = 1$. Let T be the set of those primes p in $\mathcal{S}$ such that $p > 7$ and p also splits completely in $Q(\zeta_3, a^{1/3})$. By the Čebotarev density theorem, Kummer's theorem, and Euler's criterion for the kth powers modulo a prime p, T has a positive Dirichlet density

$$d_T \geq \frac{1}{6} \tag{3.2}$$

in the set of primes. Moreover, the primes p in T satisfy the following conditions:

$$p \equiv 3 \pmod 4, \tag{3.3}$$

$$p \equiv 1 \pmod 3, \tag{3.4}$$

and

$$a^{(p-1)/3} \equiv 1 \pmod p. \tag{3.5}$$

Note that (3.5) implies that

$$a(p) \leq (p-1)/3 < (p-1)/2. \tag{3.6}$$

Thus, each prime p in T satisfies the required conditions.

Next suppose that $\overline{a} \equiv 1 \pmod 2$ and $\overline{a} > 1$. Let $\mathcal{T}$ be the set of those primes p in $\mathcal{S}$ such that $p > 7$ and p also splits completely in $Q(\zeta_{2\overline{a}}, a^{1/(2\overline{a}}))$.

By the Čebotarev density theorem, Kummer's theorem, and Euler's criterion, $\mathcal{T}$ has a positive Dirichlet density

$$d_{\mathcal{T}} \geq \frac{1}{2\overline{a}\phi(4\overline{a})} \tag{3.7}$$

in the set of primes. Furthermore, the following conditions hold for each prime p in $\mathcal{T}$:

$$p \equiv 1 + 2\overline{a} \pmod{4\overline{a}} \tag{3.8}$$

and

$$a^{(p-1)/(2\overline{a})} \equiv 1 \pmod{p}. \tag{3.9}$$

As before, each prime $p \in \mathcal{T}$ fulfills the required conditions.

We now show that the sum given in (1.2) diverges. Let p be an element of the set $\mathcal{T}$ which we constructed above under the supposition that either $\overline{a} = 1$ or $\overline{a} > 1$ and $\overline{a} \equiv 1 \pmod 2$. We found that there exist distinct odd primes q, r, and s, all different from p such that $pqrs$ is a superpseudoprime to the base a, q and r are primitive divisors of $a^{(p-1)/2} - 1$ or $a^{p-1} - 1$, and s is a primitive divisor of $a^{p-1} - 1$. Since $a(p) \mid p - 1$ by Lemma 2.1, we see that

$$a(pqrs) = \operatorname{lcm}\big(a(p), a(q), a(r), a(s)\big) = p - 1.$$

Thus, $pqrs \mid a^{p-1} - 1$. Therefore,

$$\begin{aligned} \sum_{i=1}^{\infty} \frac{1}{\log P_i^{(4)}} &\geq \sum_{p \in \mathcal{T}} \frac{1}{\log a^{p-1} - 1} \\ &> \sum_{p \in \mathcal{T}} \frac{1}{\log a^p} = \frac{1}{\log a} \sum_{p \in \mathcal{T}} \frac{1}{p}. \end{aligned} \tag{3.10}$$

Since the set $\mathcal{T}$ has a positive Dirichlet density $d_{\mathcal{T}}$ in the set of primes by (3.2) and (3.7), it follows that the first sum in (3.10) diverges. □

Proof of Proposition 1.6. By Theorem 2.3, $a^{ge\overline{a}} - 1$ has at least two odd primitive prime divisors, where $g > 5$ is an odd integer and e is defined as in Theorem 2.3. Let T consist of products of prime powers of the form

$$\prod_{i=1}^{k} p_i^{\ell_i}, \tag{3.11}$$

where $a(p_i) = ge\overline{a}$ for some odd integer $g > 5$ and all $i = 1, \ldots, k$, $p_i^{m_i} \parallel a^{ge\overline{a}} - 1$, $1 \leq \ell_i \leq m_i$, and $k \geq 2$. We note that g and k can vary for distinct products in T. By Theorem 1.3 and the discussion following Definition 1.5, each member of the set T is a superpseudoprime, a strong pseudoprime, and thus an Euler pseudoprime, all to the base a.

Let $T_a(x)$ denote the number of elements of T not exceeding x. Then $\mathcal{P}'_a(x) \geq T_a(x)$. By the proof of [11; Theorem 1], if $x \geq a^{15a} + 1$, then

$$\mathcal{P}'_a(x) \geq T_a(x) > \frac{\log x}{4a \log a}. \tag{3.12}$$

Letting $x = P_i$ in (3.12), where P_i is the ith element of the set S in terms of magnitude, it is easily seen that

$$\sum_{i=1}^{\infty} \frac{1}{\log P_i}$$

diverges. □

Proof of Theorem 1.7. By Theorem 2.2, $b^{pd_i} - 1$ has a primitive prime divisor p_i for $i = 1, \ldots, M$. Since $p \nmid k$, we have $p_i \nmid b^k - 1 = a - 1$ for $1 \leq i \leq M$. As $b^{pd_i} - 1 \mid b^{pk} - 1 = a^p - 1$, it follows that p_i is a primitive prime divisor of $a^p - 1$ for $i = 1, \ldots, M$. Thus, by Theorem 1.3, $p_1 p_2 \cdots p_M$ is a superpseudoprime to the base a. □

4. Concluding remarks

In a future paper, we will generalize the results of this paper and the papers [10] and [5] by finding infinitely many Lucas and Lehmer superpseudoprimes which are products of exactly four distinct primes for various classes of Lucas and Lehmer sequences.

Acknowledgement

The author is indebted to Michal Křížek for fruitful discussions.

REFERENCES

[1] BANG, A. S.: *Taltheoretiske undersøgelser*, Tidsskrift Math. **5** (1886), 70 80, 130 137.
[2] BIRKHOFF, G. D.—VANDIVER, H. S.: *On the integral divisors of* $a^n - b^n$, Ann. of Math. (2) **5** (1904), 173–180.
[3] FEHÉR, J.—KISS, P.: *Note on super pseudoprime numbers*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **26** (1983), 157–159.
[4] JANUSZ, G.: *Algebraic Number Fields*, Academic Press, New York, 1973.
[5] JOO, I.—PHONG, B. M.: *On super Lehmer pseudoprimes*, Studia Sci. Math. Hungar. **25** (1990), 121–124.

[6] KŘÍŽEK, M.—LUCA, F.—SOMER, L.: *17 Lectures on Fermat Numbers: From Number Theory to Geometry.* CMS Books Math./Ouvrages Math. SMC 9, Springer-Verlag, New York, 2001.

[7] MĄKOWSKI, A.: *On a problem of Rotkiewicz on pseudoprime numbers*, Elem. Math. **29** (1974), 13.

[8] MARCUS, D.: *Number Fields*, Springer-Verlag, Berlin-New York, 1977.

[9] PHONG, B. M.: *On super pseudoprimes which are products of three primes*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **30** (1987), 125–129.

[10] PHONG, B. M.: *On super Lucas and super Lehmer pseudoprimes*, Studia Sci. Math. Hungar. **23** (1988), 435–442.

[11] POMERANCE, C.—SELFRIDGE, J. L.—WAGSTAFF, S. S.: *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.

[12] ROTKIEWICZ, A.: *On the prime factors of the numbers* $2^{p-1} - 1$, Glasgow Math. J. **9** (1968), 83–86.

[13] SCHINZEL, A.: *On primitive prime factors of* $a^n - b^n$, Math. Proc. Cambridge Philos. Soc. **58** (1962), 555–562.

[14] SZYMICZEK, K.: *On prime numbers p, q, and r such that pq, pr, and qr are pseudoprimes*, Colloq. Math. **13** (1965), 259–263.

[15] SZYMICZEK, K.: *On pseudoprimes which are products of distinct primes*, Amer. Math. Monthly **74** (1967), 35–37.

[16] ZSIGMONDY, K.: *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265 284.

Received July 7, 2003

Department of Mathematics
Catholic University of America
Washington, D.C. 20064
U.S.A.

E-mail: somer@cua.edu