ON LEHMER SUPERPSEUDOPRIMES

LAWRENCE SOMER AND MICHAL KŘÍŽEK

Abstract. A Lehmer superpseudoprime is a Lehmer pseudoprime, all of whose divisors greater than 1 are either pseudoprimes with the same parameters or primes. Lehmer superpseudoprimes with exactly two distinct prime divisors are not very interesting, since their only proper divisors are primes. Phong and Joó have generated infinitely many Lehmer superpseudoprimes with exactly three distinct prime divisors for various parameters. In this paper, we generate infinitely many Lehmer superpseudoprimes with exactly four distinct prime divisors for Lehmer sequences having various parameters.

1. Introduction

We first present results on ordinary superpseudoprimes and then extend these results to Lehmer superpseudoprimes. 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 [9] have shown this is possible when $a = 2$. Fehér and Kiss [2] demonstrated that infinitely many such superpseudoprimes exist when $4 \nmid a$. Phong [7] proved that there exist infinitely many pseudoprimes to the base a which are products of exactly three distinct primes for any $a > 1$.

Somer [12] generalized these results in the following theorem. We let $k(m)$ denote the square-free kernel of any nonzero integer m, that is, m divided by its largest square factor.

Theorem 1.1. *Let $a > 1$ be an integer such that $k(a)$ is odd. Then there exist infinitely many superpseudoprimes to the base a which are products of exactly four distinct primes. Moreover,*

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

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

To continue, we will need some definitions and results concerning Lehmer sequences. Lehmer numbers are rational integers which are terms of the sequence

$$R_n(L, M) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & n \text{ odd}, \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & n \text{ even}, \end{cases} \tag{1.2}$$

where the characteristic roots α and β are roots of the characteristic polynomial

$$x^2 - \sqrt{L}x + M,$$

where $L = (\alpha + \beta)^2$ and $M = \alpha\beta$ are nonzero rational integers and the discriminant $K = L - 4M = (\alpha - \beta)^2 \neq 0$. We may assume without any essential loss of generality that $(L, M) = 1$ (see [15, p. 231]). We note also that $|R_n(L, M)| = |R_n(-L, -M)|$ (see [15, p. 231]). Accordingly, we will frequently assume without essential loss of generality that $L > 0$. Then

$$R_n(L,M) = \begin{cases} LR_{n-1} - MR_{n-2}, & n \text{ odd}, \\ R_{n-1} - MR_{n-2}, & n \text{ even}. \end{cases}$$

D. H. Lehmer [5, p. 423] proved that if N is an odd prime such that $(KLM, N) = 1$, then

$$R_{N-(KL/N)} \equiv 0 \pmod{N}, \tag{1.3}$$

where (KL/N) is the Legendre symbol. Rotkiewicz [10] defined a Lehmer pseudoprime with respect to $R(L, M)$ to be an odd composite integer N such that (1.3) holds, where $(KLM, N) = 1$ and (KL/N) is the Jacobi symbol. A *Lehmer superpseudoprime* N with respect to the Lehmer sequence $R(L, M)$ is a Lehmer pseudoprime with respect to $R(L, M)$ such that if $d|N$ and $d > 1$, then d is either a prime or d is a Lehmer pseudoprime with respect to $R(L, M)$, i.e.,

$$R_{d-(KL/d)} \equiv 0 \pmod{d}$$

for all $d > 1$ dividing N.

The Lehmer sequence $R(L, M)$ with characteristic roots α and β is *degenerate* if α/β is a root of unity. In particular, if the discriminant K of $R(L, M)$ is equal to zero, then $R(L, M)$ is degenerate. It follows from (1.2) that $R_n(L, M) = 0$ for some $n > 0$ only if $R(L, M)$ is degenerate.

Phong [8] proved that there exist infinitely many Lehmer superpseudoprimes with respect to an arbitrary nondegenerate Lehmer sequence $R(L, M)$ having exactly three distinct prime divisors. Phong [8] also showed that with respect to these same Lehmer sequences $R(L, M)$,

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

diverges, where $Q_i^{(3)}$ denotes the ith Lehmer superpseudoprime with respect to $R(L, M)$ having exactly three distinct prime divisors.

We will extend Phong's results in our main theorem given below.

Theorem 1.2. *Let $R(L, M)$ be a nondegenerate Lehmer sequence for which $(L, M) = 1$, $L > 0$, and $M \neq 0$. Suppose that $k(KL) \equiv 1 \pmod{4}$ and $k(M \cdot \max(K, L)) \equiv 1 \pmod{2}$. Then there exist infinitely many Lehmer superpseudoprimes with respect to $R(L, M)$ having exactly four distinct prime divisors. Moreover,*

$$\sum_{i=1}^{\infty} \frac{1}{\log Q_i^{(4)}}$$

diverges, where $Q_i^{(4)}$ denotes the ith Lehmer superpseudoprime with respect to $R(L, M)$ having exactly four distinct prime divisors.

The proof of Theorem 1.2 will be given in Section 3. Before presenting our next theorem, we will need the following definition.

Definition 1.3. *The prime p is a primitive prime divisor of $R_n(L, M)$ if $p|R_n$, but $p \nmid KLR_1R_2 \cdots R_{n-1}$.*

The following theorem shows that for special values of the parameters L and M, there exist infinitely many Lehmer superpseudoprimes with respect to $R(L,M)$, each having any prescribed number of distinct prime divisors. We let $\tau(n)$ denote the number of distinct positive divisors of the positive integer n. Note that if A is any positive integer greater than 1, then $\tau(p^{A-1}) = A$ when p is a prime. Since τ is a multiplicative function, it follows that if m is any positive integer, then there exists a positive integer n such that $\tau(n) = m$.

Theorem 1.4. *Let $M^* > 1$ be a fixed integer. Let k be an odd positive integer such that $\tau(k) = M^*$. Let $R(L', M')$ be a nondegenerate Lehmer sequence with characteristic roots α and β for which $(L', M') = 1$ and $L'M' \neq 0$. Let $L = (\alpha^k + \beta^k)^2$ and $M = \alpha^k\beta^k$. Then L and M are nonzero coprime rational integers and $R(L,M)$ is a nondegenerate Lehmer sequence. Let $p > 13$ be a prime such that $p \nmid k$. Let $d_i,\ i = 1, 2, \ldots, M^*$, be the distinct positive divisors of k. Then $R_{pd_i}(L', M')$ has an odd primitive prime divisor p_i which is also a primitive prime divisor of $R_p(L,M)$. Moreover, $p_1p_2\cdots p_{M^*}$ is a Lehmer superpseudoprime with respect to $R(L,M)$.*

2. Preliminaries

Before proceeding further, we will need the following definitions and results.

Definition 2.1. *Let m be a positive integer. The rank of appearance of m in $R(L,M)$, denoted by $\rho(m)$, is the least positive integer n such that $m|R_n$.*

Proposition 2.2. *Let $R(l,M)$ be a nondegenerate Lehmer sequence for which $(L,M) = 1$ and $LM \neq 0$. Then the following hold:*

(i) $(R_n, M) = 1$ *for all* $n > 0$,
(ii) $(R_m, R_n) = |R_{(m,n)}|$,
(iii) *If* $d|n$, *then* $R_d|R_n$,
(iv) $m|R_n$ *if and only if* $\rho(m)|n$,
(v) $\rho(mn) = [\rho(m), \rho(n)]$.

Proof. Parts (i) and (ii) are proved in Lemmas 1 and 3 of [13]. Part (iii) follows from part (ii). The necessity of part (iv) follows from part (iii). The sufficiency of part (iv) follows from part (ii) upon noting that R_n is not divisible by m if $n < \rho(m)$. Part (v) follows from part (iv). □

Remark 2.3. *It follows from Proposition 2.2 (i) that congruence (1.3) is satisfied by the odd composite integer N only if $(N,M) = 1$.*

Theorem 2.4. (Bilu, Hanrot, Voutier) *Let $R(L,M)$ be a nondegenerate Lehmer sequence for which $(L,M) = 1$ and $LM \neq 0$. Then R_n has no primitive divisor only if $1 \leq n \leq 10$, or $12 \leq n \leq 15$, or $n = 18,\ 24,\ 26$ or 30.*

Proof. This is proved in [1]. □

Theorem 2.5. (Schinzel) *Let $R(L,M)$ be a nondegenerate Lehmer sequence for which $(L,M) = 1,\ L > 0$, and $LM \neq 0$. Let $A_1 = k(M \cdot \max(K,L))$ and*

$$e = \begin{cases} 1 \text{ if } A_1 \equiv 1 \pmod 4, \\ 2 \text{ if } A_1 \equiv 2, 3 \pmod 4. \end{cases}$$

If $\frac{n}{eA_1}$ is an odd integer, then R_n has at least two primitive prime divisors provided that

(i) $n > \max(3eA_1, 20)$ *if* $K > 0$;
(ii) *for* $K < 0,\ n > C(L,M)$, *where* $C(L,M)$ *is an effectively computable constant.*

Proof. This is proved in [11]. □

Theorem 2.6. (Phong) *Let $R(L,M)$ be a Lehmer sequence for which $(L,M)=1$ and $LM \neq 0$. Let $p_1, p_2, \ldots, p_m$ be distinct odd primes such that $(p_1p_2\cdots p_m, KLM)=1$, where $m \geq 2$. Then $p_1p_2\cdots p_m$ is a Lehmer superpseudoprime with respect to $R(L,M)$ if and only if*

$$\rho(p_1p_2\cdots p_m) = [\rho(p_1), \rho(p_2), \ldots, \rho(p_m)] \mid (p_1 - (LK/p_1), p_2 - (LK/p_2), \cdots, p_m - (LK/p_m)).$$

Proof. This follows from the proof of Lemma 2 of [8]. □

3. Proofs of the Main Results

Proof of Theorem 1.2. We first prove that there exist infinitely many such Lehmer superpseudoprimes with respect to $R(L,M)$. Let $A_1 = k(M \cdot \max(K,L))$ and $A_2 = k(KL)$. Let e be defined as in Theorem 2.5. Let p be an odd prime such that $p > C_1(L,M)$, where $C_1(L,M) = \max(61, 3eA_1)$ if $K > 0$ and $C_1(L,M) = \max(61, C(L,M))$ if $K < 0$, where $C(L,M)$ is defined as in part (ii) of Theorem 2.5. Let $B = [A_1, A_2]$. Suppose further that

$$p \equiv 1 + 2B \pmod{4B}.$$

Then $p \equiv 1 + 2|A_2| \pmod{4|A_2|}$. Suppose also that $\rho(p) < \frac{p-1}{2}$. Since $p \equiv 1 \pmod{|A_2|}$ and $A_2 \equiv 1 \pmod 4$, we see by the law of quadratic reciprocity for the Jacobi symbol that

$$(LK/p) = (A_2/p) = (p/|A_2|) = (1/|A_2|) = 1.$$

Thus, $p | R_{p-1}$ by Proposition 2.2 (iv).

Suppose first that $A_1 \equiv 1 \pmod 4$. Then $e = 1$ and $\frac{p-1}{2}$ is an odd multiple of eA_1. Thus, there exist two primitive prime divisors q and r of $R_{\frac{p-1}{2}}$ by Theorem 2.5. Hence, $\rho(q) = \rho(r) = \frac{p-1}{2}$, and $\frac{p-1}{2}$ divides each of $(q - (LK/q))$ and $(r - (LK/r))$ by (1.3) and Proposition 2.2 (iv). Since $\frac{p-1}{2}$ is congruent to $|A_1| \pmod{2|A_1|}$, we see that $\frac{p-1}{2}$ is odd, and thus

$$p - 1 | q - (LK/q) \text{ and } p - 1 | r - (LK/r).$$

By Theorem 2.4, R_{p-1} has a primitive prime divisor s. Then $\rho(s) = p-1$, and $p-1 | s - (LK/s)$ by (1.3) and Proposition 2.2 (iv). Thus,

$$\rho(pqrs) = [\rho(p), \rho(q), \rho(r), \rho(s)] = p - 1,$$

and hence,

$$\rho(pqrs) | (p - (LK/p), q - (LK/q), r - (LK/r), s - (LK/s)).$$

Consequently, $pqrs$ is a Lehmer superpseudoprime with respect to $R(L,M)$ by Theorem 2.6.

Now suppose that $A_1 \equiv 3 \pmod 4$. Then $e = 2$. By Theorem 2.4, $R_{\frac{p-1}{2}}$ has a primitive prime divisor q. Since $\frac{p-1}{2}$ is odd, $p - 1 \mid q - (LK/q)$, as before. Moreover, $p-1$ is an odd multiple of $eA_1 = 2A_1$. Thus, R_{p-1} has two primitive prime divisors r and s by Theorem 2.5. Then $\rho(r) = \rho(s) = p-1$, and $p-1$ divides each of $(r - (L/K))$ and $(s - (L/K))$ by (1.3) and Proposition 2.2 (iv). Consequently, $\rho(pqrs) = p - 1$ and

$$\rho(pqrs) | (p - (LK/p), q - (LK/q), r - (LK/r), s - (LK/s)).$$

Therefore, $pqrs$ is a Lehmer superpseudoprime with respect to $R(L,M)$ in this case also.

We now show that there indeed exist infinitely many primes p such that $p \equiv 1 + 2B \pmod{4B}$ and $\rho(p) < \frac{p-1}{2}$. We find infinitely many such primes p for which $p | R_{\frac{p-1}{3}}$, which implies that $\rho(p) | \frac{p-1}{3} < \frac{p-1}{2}$.

Let ζ_n denote a primitive nth root of unity. Let $\mathcal{S}$ denote the set of primes p such that $p > C_1(L,M)$ and p splits completely in $\mathbb{Q}(\zeta_{2B})$, but p does not split in $\mathbb{Q}(\zeta_{4B})$. By the

Tchebotarev Density Theorem (see [3, Theorem 10.4, pp. 182–183]) 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 [3, Theorem 7.6, pp. 32–33] or [6, Theorem 27, pp. 79–82]), $\mathcal{S}$ consists of those p such that $p \equiv 1 + 2B \pmod{4B}$, and $\mathcal{S}$ has positive Dirichlet density in the set of primes. As shown earlier, if $p \in \mathcal{S}$, then $p | R_{p-1}$. Note that we can assume that $p > M = \alpha\beta$. Since

$$R_{p-1} = \frac{\alpha^{p-1} - \beta^{p-1}}{\alpha^2 - \beta^2} \equiv 0 \pmod{p},$$

we see that

$$\frac{R_{p-1}}{\beta^{p-1}} = \frac{(\frac{\alpha}{\beta})^{p-1} - 1}{\beta^{p-1}(\alpha^2 - \beta^2)} \equiv 0 \pmod{pR'},$$

which implies that

$$\left(\frac{\alpha}{\beta}\right)^{p-1} \equiv 1 \pmod{pR'},$$

where R' is the ring of integers of the algebraic number field $\mathbb{Q}(\sqrt{K})$. Thus, we can assume that $\frac{\alpha}{\beta} \in \mathbb{Z}/p$, the finite field with p elements.

Let $\mathcal{T}$ be the set of primes $p \in \mathcal{S}$ such that p also splits completely in $\mathbb{Q}(\zeta_3, (\frac{\alpha}{\beta})^{\frac{1}{3}})$. Then $p \equiv 1 \pmod 3$ and $\frac{\alpha}{\beta}$ is a cube in $\mathbb{Z}/p$. Hence, $\frac{\alpha}{\beta}^{\frac{p-1}{3}} \equiv 1 \pmod p$ and $p | R_{\frac{p-1}{3}}$. Thus, $\rho(p) | \frac{p-1}{3}$ and $\rho(p) < \frac{p-1}{2}$. By the Tchebotarev Density Theorem and Kummer's Theorem, $\mathcal{T}$ has positive Dirichlet density in the set of primes. Thus, there exist infinitely many Lehmer superpseudoprimes with respect to $R(L, M)$ having exactly four distinct prime divisors.

We now show that

$$\sum_{i=1}^{\infty} \frac{1}{\log \ Q_i^{(4)}}$$

diverges. Since $R(L, M)$ is nondegenerate, the larger characteristic root in absolute value satisfies $|\alpha| > 1$ (see [4, p. 123]). Furthermore,

$$|R_n| \leq 2|\alpha|^n \leq (2|\alpha|)^n.$$

Since

$$\rho(pqrs) = [\rho(p), \rho(q), \rho(r), \rho(s)] = p - 1$$

for the Lehmer superpseudoprimes we constructed, we see that

$$pqrs| \ |R_{p-1}| \leq (2|\alpha|)^{p-1}.$$

Thus,

$$\begin{aligned} \sum_{i=1}^{\infty} \frac{1}{\log Q_i^{(4)}} &\geq \sum_{p \in \mathcal{T}} \frac{1}{\log(2|\alpha|)^{p-1}} \\ &> \sum_{p \in \mathcal{T}} \frac{1}{\log(2|\alpha|)^{p}} \\ &= \frac{1}{\log 2|\alpha|} \sum_{p \in \mathcal{T}} \frac{1}{p}. \end{aligned} \tag{3.1}$$

Since the sum of reciprocals of primes diverges and the set $\mathcal{T}$ has positive Dirichlet density in the set of primes, it follows that the first sum in (3.1) diverges. □

Example 3.1. Consider the Fibonacci sequence $R(1,-1)$. Let $p = 151$. Then,

$$\rho(151) = 50 = \frac{p-1}{3} < \frac{p-1}{2}.$$

Since

$$k(M \cdot \max(K, L)) = k(-1 \cdot \max(5, 1)) = -5$$

and $-5 \equiv 3 \pmod 4$, we have $e = 2$. Then $e \cdot |A_1| = 2 \cdot 5 = 10$, and $R_{150} = R_{p-1}$ has two distinct primitive prime divisors by Theorem 2.5, namely, $r = 12301$ and $s = 18451$. Also $R_{75} = R_{\frac{p-1}{2}}$ has a primitive prime divisor $q = 230686501$ by Theorem 2.4. Thus,

$$pqrs = 151 \cdot 230686501 \cdot 12301 \cdot 18451$$

is a Lehmer superpseudoprime with respect to $R(1,-1)$ by Theorem 2.6.

Example 3.2. Consider the Lehmer sequence $R(9,1)$ with discriminant $K = 5$. Then

$$k(M \cdot \max(K, L)) = k(1 \cdot 9) = 1,$$

which implies that $e = 1$. Then $e \cdot |A_1| = 1$. Let $p = 139$. Then

$$\rho(139) = 23 = \frac{p-1}{6} \;\Big|\; \frac{p-1}{3} < \frac{p-1}{2}.$$

By Theorem 2.5, $R_{69} = R_{\frac{p-1}{2}}$ has two distinct primitive prime divisors, namely, $q = 137$ and $r = 829$. Moreover, by Theorem 2.4, $R_{138} = R_{p-1}$ has a primitive prime divisor $s = 16561$. Therefore,

$$pqrs = 139 \cdot 137 \cdot 829 \cdot 16561$$

is a Lehmer superpseudoprime with respect to $R(9,1)$ by Theorem 2.6.

Proof of Theorem 1.4. Since $L' = (\alpha+\beta)^2$ and $M' = \alpha\beta$ are rational integers, it is easily seen that $L = (\alpha^k + \beta^k)^2$, $M = \alpha^k\beta^k$, and $K = (\alpha^k - \beta^k)^2$ are rational integers. It follows from Lemma 1 of [13] that L and M are relatively prime. Since α/β is not a root of unity, α^k/β^k is not a root of unity, which implies that $R(L, M)$ is a nondegenerate Lehmer sequence and that both $L = (\alpha^k + \beta^k)^2$ and $K = (\alpha^k - \beta^k)^2$ are nonzero. Noting that $\alpha\beta \neq 0$, we see that $\alpha^k\beta^k \neq 0$.

By Theorem 2.4, $R_{pd_i}(L', M')$ has a primitive prime divisor p_i for $i = 1, 2, \dots, M^*$. By Proposition 2.2 (i), $(p_i, M) = 1$ for $1 \le i \le M^*$. From Proposition 2.2 (iii) we get

$$R_{pd_i}(L', M') \,|\, R_{pk}(L', M').$$

Thus, $p_1 p_2 \cdots p_{M^*} \mid R_{pk}(L', M')$. Notice that

$$R_p(L, M) = \frac{(\alpha^k)^p - (\beta^k)^p}{\alpha^k - \beta^k} = \frac{R_{pk}(L', M')}{R_k(L', M')}. \tag{3.2}$$

Since $R_1(L, M) = 1$ and $pd_i \nmid k$ for $1 \le i \le M^*$, it follows from (3.2) and Proposition 2.2 (iv) that p_i is a primitive prime divisor of $R_p(L, M)$ for $i = 1, 2, \dots, M^*$. By Theorem 2.6, $p_1 p_2 \cdots p_{M^*}$ is a Lehmer superpseudoprime with respect to $R(L, M)$. □

4. Acknowledgement

This paper was supported by Project RVO 67985840.

References

[1] Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers (With an appendix by M. Mignotte)*, J. Reine Angew. Math., **539** (2001), 75–122.

[2] J. Fehér and P. Kiss, *Note on super pseudoprime numbers*, Ann. Univ. Sci. Budapest. Eotvős Sect. Math., **26** (1983), 157–159.

[3] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.

[4] I. Joó and B. M. Phong, *On super Lehmer pseudoprimes*, Studia Sci. Math. Hungar, **25** (1990), 121–124.

[5] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., Second Series, **31** (1930), 419–448.

[6] D. Marcus, *Number Fields*, Springer-Verlag, Berlin, New York, 1977.

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

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

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

[10] A. Rotkiewicz, *On the pseudoprimes of the form* $ax + b$ *with respect to the sequence of Lehmer*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys., **20** (1972), 349–354.

[11] A. Schinzel, *On primitive factors of Lehmer numbers I*, Acta Arith., **8** (1962/63), 213–223.

[12] L. Somer, *On superpseudoprimes*, Math. Slovaca, **54** (2004), 443–451.

[13] C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc., Third Series, **35** (1977), 425–447.

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

[15] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math., Second Series, **62** (1955), 230–236.

MSC2010: 11A51, 11B39

Department of Mathematics, Catholic University of America, Washington, D.C. 20064
E-mail address: somer@cua.edu

Institute of Mathematics, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republic
E-mail address: krizek@math.cas.cz