

## ON THE DISTRIBUTION OF LUCAS AND LEHMER PSEUDOPRIMES

Bui Minh Phong (Budapest, Hungary)

*Dedicated to Professor Karl-Heinz Indlekofer  
on the occasion of his fiftieth birthday*

**Abstract.** We prove that for any nondegenerate Lehmer sequence, the number of Lehmer pseudoprimes not exceeding  $x$  is greater than  $\exp\{(\log x)^{1/35}\}$  if  $x$  is sufficiently large. We also show that for a given positive integer  $d$  there is an absolute constant  $c$  such that the number of Lehmer pseudoprimes not exceeding  $x$  which are of the form  $dt + 1$  is greater than  $\exp\{(\log x)^c\}$  for all sufficiently large  $x$ .

### 1. Introduction and results

Let  $A$  and  $B$  be non-zero integers such that  $D = A^2 - 4B \neq 0$ . A Lucas sequence  $R = \{R_n\}_{n=0}^{\infty}$  is defined by the initial terms  $R_0 = 0, R_1 = 1$  and by the recursion

$$R_n = AR_{n-1} - BR_{n-2}$$

for all integers  $n > 1$ . We shall write  $R(A, B)$  for  $R$  when it is necessary to show the dependence on  $A$  and  $B$ . It is well-known that

$$(1) \quad R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

for any  $n \geq 0$ , where  $\alpha$  and  $\beta$  are the distinct roots of the equation  $x^2 - Ax + B = 0$ . In the following we say that  $R(A, B)$  is a non-degenerate sequence if  $(A, B) = 1$  and  $\alpha/\beta$  is not a root of unity.

For odd primes  $n$  with  $(n, BD) = 1$ , as it is well-known, we have

$$(2) \quad R_{n-(D/n)} \equiv 0 \pmod{n},$$

where  $(D/n)$  is the Jacobi symbol. If  $n$  is composite, but (2) still holds, then we say  $n$  is a Lucas pseudoprime with respect to the sequence  $R$ . It is a generalization of a pseudoprime to base an integer  $b > 1$ , namely a composite  $n$  is called a pseudoprime to base  $b$  if

$$b^{n-1} \equiv 1 \pmod{n}.$$

In 1930 D.H.Lehmer [13] generalized some results of Lucas on the divisibility properties of Lucas numbers to numbers  $U_n$  with  $n \geq 0$  satisfying

$$(3) \quad U_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{for } n \text{ odd} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{for } n \text{ even,} \end{cases}$$

where  $\alpha, \beta$  are the distinct roots of the equation  $z^2 - L^{1/2}z + M = 0$  and  $L, M$  are non-zero integers with the condition  $K = L - 4M \neq 0$ . The numbers defined above are known as Lehmer numbers. We also shall use the notation  $U(L, M)$  for the sequence  $U = \{U_n\}_{n=0}^{\infty}$  when it is necessary to show the dependence on  $L$  and  $M$ . We note that in the case  $L = A^2$  and  $M = B$  by (1) and (3) we have

$$(4) \quad R_n(A, B) = \begin{cases} U_n(A^2, B) & \text{for } n \text{ odd} \\ AU_n(A^2, B) & \text{for } n \text{ even,} \end{cases}$$

which is a connection between the Lucas and the Lehmer sequences. In the case of Lehmer sequence we can assume, without any essential loss of generality, that  $(L, M) = 1$  (see [13]). It is not true for Lucas sequences. In the following we also say that Lehmer sequence  $U(L, M)$  is a non-degenerate one if  $\alpha/\beta$  is not a root of unity.

A.Rotkiewicz [23] gave a proper generalization of pseudoprimes for Lehmer sequences. A composite number  $n$  is called a Lehmer pseudoprime with respect to the sequence  $U$  if  $(n, LMK) = 1$  and

$$U_{n-(LK/n)} \equiv 0 \pmod{n},$$

where  $(LK/n)$  is the Jacobi symbol and  $K = L - 4M$ . By (4) it is easily seen that the Lehmer pseudoprime is a generalization of the Lucas pseudoprime number.

Let  $P(b, x)$  denote the number of pseudoprimes to base  $b$  not exceeding  $x$ . It is known that there exist positive constants  $c_1$  and  $c_2$  such that for all large  $x$

$$c_1 \log x < P(2, x) < x \cdot \exp\left(-c_2(\log x \log_2 x)^{1/2}\right),$$

where the lower and the upper bound is due to D.H.Lehmer [14] and P.Erdős [2], respectively. Here, the notation  $\log_k$  denotes the  $k$ -fold iteration of the natural logarithm. C.Pomerance [19, 20] improved these results showing that for all large  $x$

$$\exp\left((\log x)^{5/14}\right) \leq P(b, x) \leq x \cdot (L(x))^{-1/2}$$

for any integer  $b \geq 2$ , where

$$L(x) := \exp(\log x \log_3 x / \log_2 x).$$

The exponent  $5/14$  has been improved to  $85/207$  in [21] by applying a recent result due to J.B.Freidlander [4].

Let  $P(R, x)$  denote the number of pseudoprimes with respect to sequence  $R$  not exceeding  $x$ . R.Baillie and S.S.Wagstaff, Jr. [1] proved that there exist positive constants  $c_3$  and  $c_4$  such that for all large  $x$

$$P(R, x) < x \cdot \exp\left(-c_3(\log x \log_2 x)^{1/2}\right)$$

holds for any non-degenerate Lucas sequence  $R$ , and

$$c_4 \log x < P(R, x)$$

for sequences  $R$  for which  $D > 0$  but  $D$  is not a perfect square. This lower bound was extended by P.Kiss [12] to all non-degenerate sequences  $R$ . In a recent paper [3] P.Erdős, P.Kiss and Sárközy improved the lower bound for  $P(R, x)$  extending Pomerance's result for Lucas pseudoprimes. They proved that there is a positive absolute constant  $c_5$  such that for all large  $x$

$$\exp((\log x)^{c_5}) < P(R, x)$$

for any non-degenerate Lucas sequence  $R$ . In the proof of this result Erdős-Kiss-Sárközy showed only the existence of  $c_5$  and they asked for the problem of finding the numerical estimate for the constant  $c_5$ .

Recently, D.M.Gordon and C.Pomerance [6] improved the upper bound for Lucas pseudoprimes, namely they showed that

$$P(R, x) < x \cdot (L(x))^{-1/2}.$$

For some results concerning Lehmer pseudoprimes we refer to [11], [15], [16], [17], [23] and [24]. For example, it follows from Theorem 4 of [16] that

the number of those Lehmer pseudoprimes with respect to the sequence  $U$  not exceeding  $x$  and which are products of exactly two distinct primes is  $\geq c_6 \log x$  for some positive absolute constant  $c_6$ .

Our purpose in this paper is to give the numerical value for the constant  $c_5$  and also to extend the results of Pomerance, Erdős-Kiss-Sárközy for Lehmer pseudoprimes. We shall prove the following

**Theorem 1.** *Let  $U = U(L, M)$  be a non-degenerate Lehmer sequence and let  $P(U, x)$  denote the number of Lehmer pseudoprimes with respect to the sequence  $U$  not exceeding  $x$ . Then for all large  $x$*

$$P(U, x) \geq \exp\left((\log x)^{1/35}\right).$$

**Theorem 2.** *Let  $U = U(L, M)$  be a non-degenerate Lehmer sequence and let  $d \geq 2$  be a given integer for which  $(d, M) = 1$ . Let  $P(U, x, d)$  denote the number of Lehmer pseudoprimes with respect to the sequence  $U$  of the form  $dt + 1$  not exceeding  $x$ . Then there is a positive absolute constant  $c$  such that for all large  $x$  we have*

$$P(U, x, d) \geq \exp((\log x)^c).$$

We note that for the ordinary pseudoprimes A. Rotkiewicz [22] proved that the number of pseudoprimes to base 2 of the form  $dt + 1$  not exceeding  $x$  is

$$\geq \log x / (2 \log 2) d.$$

**Remark.** To prove our theorems we shall use some ideas due to Pomerance [19,20] and Erdős-Kiss-Sárközy [3], furthermore some sieve results.

## 2. Preliminary results on Lehmer sequences

First we recall some results on Lehmer sequences and prove some lemmas which will be used at the proofs of our theorems.

Let  $U(L, M)$  be a non-degenerate Lehmer sequence defined by integers  $L$  and  $M$  for which  $LM \neq 0, (L, M) = 1, K = L - 4M \neq 0$  and  $\alpha/\beta$  is not a root of unity, where  $\alpha$  and  $\beta$  are roots of  $z^2 - L^{1/2}z + M = 0$ . It is known that for any non-zero integer  $n$  with  $(n, M) = 1$  there are terms in  $U(L, M)$  divisible by  $n$ . The least positive integer  $u$ , for which  $n|U_u$  is called the rank of apparation of  $n$  in the sequence  $U(L, M)$  and we shall denote it by  $u(n)$ . If a prime  $p$  is a divisor of  $U_n$  but  $(p, MLKU_1 \dots U_{n-1}) = 1$  then  $p$  is called a primitive prime divisor of  $U_n$ . It is well-known that there is an absolute constant  $n_0$  such that  $U_n$  has at least one primitive prime divisor for every  $n > n_0$  (see A.Schinzel [25] or C.L.Stewart [26]). The least positive integer  $\bar{u}$ , for which  $n|U_{\bar{u}}$  and  $U_{\bar{u}+1} \equiv 1 \pmod{n}$  is called the period of the sequence  $U(L, M)$  modulo  $n$  and we shall denote it by  $\bar{u}(n)$ . It is known that for any non-zero integer  $n$  with  $(n, M) = 1$  always exists  $\bar{u}(n)$ .

Let  $m$  and  $n$  be positive integers with  $(mn, MK) = 1$  and let  $p$  be a prime for which  $(p, 2LMK) = 1$ . Using the notations defined above, we have

- (i)  $n|U_m$  if and only if  $u(n)|m$ ,
- (ii)  $u(p)|(p - (LK/p))$ ,
- (iii)  $u(p^k) = p^{k-k(p)}u(p)$ , where  $k(p)$  is defined by  $p^{k(p)}||U_{u(p)}$ ,
- (iv)  $U_p \equiv (K/p) \pmod{p}$ ,
- (v)  $u(nm) = [u(n), u(m)]$ ,
- (vi)  $n|U_m$  and  $U_{m+1} \equiv 1 \pmod{n}$  if and only if  $\bar{u}(n)|m$ ,
- (vii)  $\bar{u}(nm) = [\bar{u}(n), \bar{u}(m)]$ ,

where  $[x, y]$  denotes the least common multiple of integers  $x, y$  and  $(K/p), (LK/p)$  are the Jacobi symbols. For these properties of Lehmer sequences we refer to D.H.Lehmer [13].

**Lemma 1.** *Let  $Q$  and  $k$  be positive integers for which  $(2, k) = 1$  and  $\bar{u}(Q)|k - 1$ . If a positive integer  $r$  satisfies the condition  $(Q, U_r) = 1$ , then*

$$\frac{U_{kr}}{U_r} \equiv 1 \pmod{Q}.$$

**Proof.** By using (3) it is easily seen that for positive integers  $t$  and  $s$ , we have

$$(5) \quad U_{st+1} = U_{(s-1)t+1}U_{t+1} - LMU_{(s-1)t}U_t \quad \text{if} \quad 2|t$$

and

$$(6) \quad U_{s(t+1)} = \begin{cases} U_s U_{st+1} - M U_{s-1} U_{st} & \text{if} \quad 2|s \\ U_s U_{st+1} - LM U_{s-1} U_{st} & \text{if} \quad (2, s) = 1. \end{cases}$$

By using (i), (5) and the induction on  $s$ , we have

$$U_{s,t+1} \equiv U_{t+1}^s \pmod{U_t^2} \quad \text{if } 2|t,$$

which with (6) implies

$$(7) \quad U_{s(t+1)} \equiv U_s U_{st+1} \equiv U_s U_{t+1}^s \pmod{U_t} \quad \text{if } 2|t.$$

Let  $Q$  and  $k$  be positive integers for which  $(2, k) = 1$ ,  $\bar{u}(Q) | k - 1$ . Then, by (vi), we have

$$(8) \quad U_k \equiv 1 \pmod{Q}.$$

Applying (7) with  $t = k - 1$  and  $s = r$  with  $(Q, U_r) = 1$ , we get by (8) that

$$U_{rk} \equiv U_r U_k^r \equiv U_r \pmod{Q},$$

which proves Lemma 1.

**Lemma 2.** *Let  $p$  be a prime for which  $(L/p) = (K/p) = 1$ , where  $K = L - 4M$ . If a positive integer  $r$  satisfies the condition  $(p, U_r) = 1$ , then*

$$T_p(r) := \frac{U_{pr}}{U_r} \equiv 1 \pmod{p}$$

and

$$(LK/T_p(r)) = 1.$$

**Proof.** Applying (7) with  $t = p - 1$  and  $r = s$ , we have

$$U_{pr} \equiv U_r U_p^r \pmod{U_{p-1}},$$

which using (ii), (iv) and the facts  $(p, U_r) = 1$ ,  $(L/p) = (K/p) = 1$ , shows that

$$(9) \quad T_p(r) = \frac{U_{pr}}{U_r} \equiv U_p^r \equiv (K/p)^r \equiv 1 \pmod{p}.$$

Let  $q > 2$  be a prime divisor of  $T_p(r)$ . Since

$$(T_p(r), U_r) = \left( \frac{U_{pr}}{U_r}, U_r \right) | p$$

(see Stewart [27]), it follows from  $(p, U_r) = 1$  and (9) that  $(q, U_r) = 1$ . On the other hand, by (i) and using the fact  $q|T_p(r)$ , we have  $u(q)|pr$ . Let  $u(q) = pr'$  for some positive integer  $r'$ ,  $r'|r$ . This with (i) and (ii) implies that

$$(10) \quad q \equiv (LK/q) \pmod{p} \quad \text{and} \quad T_p(r) \equiv (LK/T_p(r)) \pmod{p}.$$

Thus, by (9) and (10) the proof of Lemma 2 is finished.

In the following let

$$\Phi_n = \Phi_n(\alpha, \beta) = \prod_{i|n} (\alpha^i - \beta^i)^{\mu(\frac{n}{i})},$$

where  $\Phi_n(x, y)$  is the  $n$ -th cyclotomic polynomial,  $\mu$  is the Möbius function and  $\alpha, \beta$  are the distinct roots of  $z^2 - L^{1/2}z + M = 0$ . Let  $P(n)$  denote the greatest prime divisor of the positive integer  $n$  and  $n_0$  be the absolute constant of Schinzel [25] and Stewart [26] mentioned above.

We shall prove Theorem 1 and Theorem 2 from the following theorem.

**Theorem 3.** *Let  $U = U(L, M)$  be a non-degenerate Lehmer sequence and let  $Q > 1$  be an integer. If*

$$p = 4LK\bar{u}(Q)x + 1$$

*is a prime number satisfying  $p > \max(P(Q), |LMK|n_0)$  and if*

$$S = \{r \in \mathbb{N} : r|Q \quad \text{and} \quad (pQ, U_r) = 1\},$$

*then the number*

$$n = \prod_{r \in S'} \Phi_{pr}$$

*is a Lehmer pseudoprime with respect to the sequence  $U$  for any subset  $S'$  of  $S$  with cardinality at least 2. Furthermore, for these numbers  $n$ , we have*

$$n \equiv 1 \pmod{pQ}.$$

**Proof.** We first prove that for all  $r \in S$

$$(11) \quad \Phi_{pr} \equiv 1 \pmod{pQ}, \quad (LK/\Phi_{pr}) = 1$$

and

$$(12) \quad T_p(r) = \frac{U_{pr}}{U_r} \equiv 1 \pmod{pQ}, \quad (LK/T_p(r)) = 1.$$

Since  $p = 4LK\bar{u}(Q)x + 1$  is a prime, by (i), (ii), (iv) and (vi) we have  $\bar{u}(Q)|p-1$  and  $(L/p) = (K/p) = 1$ . Thus, (12) follows from Lemmas 1-2 and the facts  $(p, Q) = 1$  and  $(pQ, U_r) = 1$  for any  $r \in S$ .

Now we prove (11).

Let  $r \in S$  and let  $d_1 = 1, \dots, d_s$  be all square-free divisors of  $r$ . Since  $p > P(Q) \geq P(r)$  it follows that

$$d_1 = 1, \dots, d_s, \quad pd_1 = p, \dots, pd_s$$

are all square-free divisors of  $pr$ . It is well-known that for every positive integer  $v \geq 1$

$$\Phi_v = \prod_{d|v} (U_{\frac{v}{d}})^{\mu(d)},$$

and so by (12) we get

$$(13) \quad \begin{aligned} \Phi_{pr} &= \prod_{d|pr} \left( U_{\frac{pr}{d}} \right)^{\mu(d)} = \prod_{i=1}^s \left[ \left( U_{\frac{pr}{d_i}} \right)^{\mu(d_i)} \left( U_{\frac{pr}{pd_i}} \right)^{\mu(pd_i)} \right] = \\ &= \prod_{i=1}^s \left[ U_{\frac{pr}{d_i}} / U_{\frac{r}{d_i}} \right]^{\mu(d_i)} = \prod_{i=1}^s \left[ T_p \left( \frac{r}{d_i} \right) \right]^{\mu(d_i)} \equiv 1 \pmod{pQ}. \end{aligned}$$

In the last step we have used the fact  $r/d_i \in S$  for all  $d_i|r$  and for all  $r \in S$ .

On the other hand, by using the fact  $u(q) = n$  if  $q$  is a prime divisor of  $\Phi_n$  and  $q \neq P(n)$  (see [27]), it follows that for any  $r \in S$  and a prime divisor  $q$  of  $\Phi_{pr}$  we have  $u(q) = pr$ , because  $(p, U_r) = 1$  and  $p = P(pr)$ . Thus

$$q \equiv (LK/q) \pmod{p},$$

and

$$(14) \quad \Phi_{pr} \equiv (LK/\Phi_{pr}) \pmod{p}.$$

By (13) and (14) one can deduce that  $(LK/\Phi_{pr}) = 1$ , which proves (11).

Let  $S' \subset S$  with the cardinality of  $S'$  at least 2. Then the number of the form

$$n = \prod_{r \in S'} \Phi_{pr}$$



is composite and we get from (11) that

$$(LK/n) = 1 \quad \text{and} \quad pQ|n - 1 = \left( \prod_{r \in S'} \Phi_{pr} \right) - 1.$$

On the other hand, it follows from (v)

$$u(n) = u \left( \prod_{r \in S'} \Phi_{pr} \right) \mid pQ.$$

These imply  $u(n)|n - (LK/n)$ , i.e.  $n$  is a Lehmer pseudoprime with respect to the sequence  $U$ , furthermore  $n \equiv 1 \pmod{pQ}$ . This completes the proof of Theorem 3.

### 3. Distribution of primes satisfying suitable condition

In this section  $\mathcal{P}$  denotes the set of primes and for each set  $X$  we shall denote by  $|X|$  the cardinality of it.

For positive real numbers  $x > y$  let

$$T(x, y) := |\{p \in \mathcal{P} : y < p < x \text{ and } P[(p-1)(p+1)] \leq y\}|.$$

Let  $\pi(x)$  denote the number of primes not exceeding  $x$ . We shall prove the following

**Lemma 3.** *For each real number  $u$  with  $\frac{32}{33} < u < 1$  there exists  $x_0(u)$  such that*

$$T(x, x^u) \gg \pi(x)$$

for all  $x > x_0(u)$ .

**Proof.** Let  $u$  be a real number for which  $\frac{32}{33} < u < 1$ . We have

$$\begin{aligned} T(x, x^u) &= \\ &= |\{p \leq x : P[(p-1)(p+1)] \leq x^u\}| - |\{p \leq x^u : P[(p-1)(p+1)] \leq x^u\}| \geq \\ &\geq \pi(x) - \pi(x^u) - |\{p \leq x : P(p-1) > x^u\}| - |\{p \leq x : P(p+1) > x^u\}| = \\ &= \pi(x) - \pi(x^u) - M_1(x, u) - M_2(x, u), \end{aligned}$$

where

$$M_j(x, u) = |\{p \leq x : P(p+j) > x^u\}| \quad (j = -1, j = 1).$$

By using Corollary 5.8.4 of Halberstam and Richert [8], one can deduce that

$$\begin{aligned}
 M_1(x, u) &= \\
 &= \left| \left\{ p \leq x : P(p-1) = \frac{p-1}{a} > x^u \text{ for some even integer } a \right\} \right| \leq \\
 &\leq \sum_{2 \leq a < x^{1-u}} \left| \left\{ p \leq x : \frac{p-1}{a} \in \mathcal{P} \right\} \right| \leq 16 \prod_{p>2} \left( 1 - \frac{1}{(p-1)^2} \right) \times \\
 &\times \sum_{2 \leq a < x^{1-u}} \left( \prod_{p|a, p>2} \frac{p-1}{p-2} \frac{x}{a \log^2(x/a)} \left[ 1 + O\left( \frac{\log_2 3x}{\log(x/a)} \right) \right] \right) = \\
 &= 16Cx(1 + o(x)) \sum_{2 \leq a < x^{1-u}} \frac{\lambda(a)}{a \log^2(x/a)},
 \end{aligned}$$

where

$$C = \prod_{p>2} \left( 1 - \frac{1}{(p-1)^2} \right) \quad \text{and} \quad \lambda(a) = \prod_{p|a, p>2} \frac{p-1}{p-2}.$$

In the following let  $\lambda(1) = 1$ ,  $\lambda(2^\alpha) = 1$  for all  $\alpha \geq 1$  and we define the function  $h(n)$  by the relation

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \lambda(d).$$

It is obvious that  $\lambda(n)$  is a multiplicative function and the Möbius inversion formula shows that

$$\lambda(n) = \sum_{d|n} h(n),$$

consequently

$$\lambda(p^\alpha) = h(p^\alpha) + \lambda(p^{\alpha-1}) \quad \text{if } \alpha \geq 1,$$

$$\lambda(p^\alpha) = \lambda(p) \quad \text{if } \alpha \geq 1,$$

$$h(p^\alpha) = 0 \quad \text{if } \alpha > 1$$

and

$$h(p) = \lambda(p) - 1 = \frac{p-1}{p-2} - 1 = \frac{1}{p-2} \quad \text{if } p > 2.$$

Thus, we have

$$\begin{aligned} L(y) &:= \sum_{n \leq y} \lambda(n) = \sum_{n \leq y} \sum_{d|n} h(d) = \sum_{d \leq y} h(d) \left[ \frac{y}{d} \right] \leq y \cdot \sum_{d \leq y} \frac{h(d)}{d} \leq \\ &\leq y \prod_{p > 2} \left( 1 + \frac{h(p)}{p} \right) \leq y \prod_{p > 2} \left( 1 + \frac{1}{p(p-2)} \right) = y/C. \end{aligned}$$

By using the Abel's summation formula and the above result, we deduce that

$$\begin{aligned} (15) \quad S(z) &:= \\ &:= \sum_{1 < a \leq z} \frac{\lambda(a)}{a \log^2(\frac{x}{a})} = -\frac{1}{\log^2(x)} + \frac{L(z)}{z \log^2(x/z)} - \int_1^z L(t) \left( \frac{1}{t \log^2(x/t)} \right)' dt = \\ &= -\frac{1}{\log^2 x} + \frac{L(z)}{z \log^2(x/z)} + \int_1^z L(t) \left( -\frac{1}{t \log^2(x/t)} \right)' dt \leq \\ &\leq -\frac{1}{\log^2(x)} + \frac{C^{-1}}{\log^2(x/z)} + C^{-1} \int_1^z t \left( -\frac{1}{t \log^2(x/t)} \right)' dt \leq \\ &\leq -\frac{1}{\log^2 x} + \frac{C^{-1}}{\log^2 x} + C^{-1} \left( \frac{1}{\log(x/z)} - \frac{1}{\log x} \right). \end{aligned}$$

Applying this result with  $z = x^{1-u}$ , then for large  $x$  we have

$$\begin{aligned} (16) \quad M_1(x, u) &\leq 16Cx(1+o(1)) \left\{ o(1) + C^{-1} \frac{1-u}{u} \right\} \frac{1}{\log x} = \\ &= \left( 16 \frac{1-u}{u} + o(1) \right) \pi(x). \end{aligned}$$

It can be deduced in the same way that

$$(17) \quad M_2(x, u) \leq \left( 16 \frac{1-u}{u} + o(1) \right) \pi(x).$$

From (16), (17) and using the fact  $1 > u > \frac{32}{33}$ , there is a constant  $x_0(u)$  such that for all  $x > x_0(u)$  we have

$$T(x, x^u) \geq \pi(x) - \pi(x^u) - 2 \left( 16 \frac{1-u}{u} + o(1) \right) \pi(x) =$$

$$= \left(1 - 32 \frac{1-u}{u} + o(1)\right) \pi(x) \gg \pi(x),$$

because  $1 > u > \frac{32}{33}$  and the prime number theorem implies that

$$\frac{\pi(x^u)}{\pi(x)} = o(1).$$

**Remark.** If  $\Pi(x, y) = |\{p \leq x : P(p-1) \leq y\}|$ , then by using some results of Hooley [10] and Goldfeld [5], Pomerance [18] showed that for all  $u > 625/512e$  and for all large  $x$

$$\Pi(x, x^u) \gg \pi(x).$$

Recently, Freidlander [4] improved this result by showing that the last relation holds for  $u > 1/(2\sqrt{e})$ .

#### 4. The proof of Theorem 1

**Lemma 4.** *Let*

$$E = \sup \{c : T(x, x^{1-c}) \gg \pi(x)\}.$$

*Then for any small  $\varepsilon > 0$  there is  $x_0(\varepsilon, U)$  such that*

$$(18) \quad P(U, x) > \exp \left\{ (\log x)^{\frac{E}{E+1}-\varepsilon} \right\}.$$

*holds for all  $x > x_0(\varepsilon, U)$ .*

**Proof.** We note from Lemma 3 that  $E > \frac{1}{33}$ , and so we may assume that  $E > \varepsilon > 0$ .

Let  $y$  be a large real number. We denote by  $A$  the least common multiple of all positive integers not exceeding  $\log y / \log_2 y$  and let  $p_0$  be the least prime number of the form  $4LKA t + 1$ . Let

$$z := (\log y)^{(1-E+\varepsilon/2)^{-1}},$$

$$V := \left\{ p \in \mathcal{P} : \frac{\log y}{\log_2 y} < p \leq z \quad \text{and} \quad P[(p-1)(p+1)] \leq \frac{\log y}{\log_2 y} \right\},$$

$$\mathcal{A} := \{p \in V : [p - 1, p + 1] \mid A \text{ and } (p, u(p_0)) = 1\},$$

$$Q := \prod_{p \in \mathcal{A}} p$$

and

$$S := \{r \leq y : r \mid Q \text{ and } (p_0 Q, U_r) = 1\}.$$

We note that

$$\frac{\log y}{\log_2 y} = z^{1 - [E - \varepsilon/2 + (\log_2 z^{1-E+\varepsilon/2})/\log z]},$$

which using the definition of  $E$  shows that

$$|V| = T\left(z, \frac{\log y}{\log_2 y}\right) > \delta \frac{z}{\log z}$$

for some positive absolute constant  $\delta$ .

We shall prove that  $|S| \geq y^{E-\varepsilon}$ .

If  $p \in V$  and  $[p - 1, p + 1]$  is not a divisor of  $A$ , then there is a prime power  $q^c > \log y / \log_2 y$  with  $c \geq 2$  such that  $q^c \mid p - 1$  or  $q^c \mid p + 1$ . By using the fact  $p \leq z$ , the number of such prime powers is

$$(20) \quad < 2 \sum \left[ \frac{2z}{q^c} \right] \ll z \left( \frac{\log_2 y}{\log y} \right)^{1/2} = o\left(\frac{z}{\log z}\right).$$

It is obvious that if  $p \in V$  and  $p \mid u(p_0)$ , then  $p \mid p_0 - (LK/p_0)$ . On the other hand, by using the prime number theorem, we have

$$A = \exp\left(\Psi\left(\frac{\log y}{\log_2 y}\right)\right) \sim \exp\left(\frac{\log y}{\log_2 y}\right),$$

where  $\Psi(x)$  denotes the Chebyshev's function (see e.g. [9], Theorem 420, Theorem 434), and so

$$p_0 < (4LK A)^{20} < \exp(40 \log y / \log_2 y)$$

if  $y$  is enough large (see [7]). Thus

$$(21) \quad \begin{aligned} |\{p \in V, p \mid u(p_0)\}| &\leq \\ &\leq \nu(p_0 - (LK/p_0)) \leq \log(p_0 - (LK/p_0)) / \log z \leq \\ &\leq \log(p_0 + 1) / \log z \leq 2 \log p_0 < \\ &< 80 \log y / \log_2 y = \left(80 \frac{\log y \log z}{z \log_2 y}\right) \frac{z}{\log z} = o\left(\frac{z}{\log z}\right). \end{aligned}$$

By using (19), (20) and (21), we have

$$(22) \quad |A| \geq |V| - |\{p \in V, [p-1, p+1] \nmid A\}| - |\{p \in V : p|u(p_0)\}| > \frac{\delta}{2} \frac{z}{\log z}$$

for all large  $y$ .

It can be seen that for all divisors  $r$  of  $Q$  we have  $(p_0, U_r) = 1$  and  $(Q, U_r) = 1$ . Thus

$$(23) \quad S = \{r \leq y : r|Q\}.$$

Since all prime divisors of  $Q$  is  $\leq z$ , one can deduce that  $r \in S$  if  $r$  has at most  $\lceil \log y / \log z \rceil$  prime divisors. Then, it follows from a result of Pomerance [19] that

$$|S| \geq y^{E-\epsilon}.$$

(see the proof of Theorem 1 of [19]).

We now prove (18).

Since

$$A \sim \exp\left(\frac{\log y}{\log_2 y}\right),$$

therefore

$$p_0 > A > \exp\left(\frac{\log y}{2 \log_2 y}\right) > z \geq P(Q) \quad \text{and} \quad p_0 > n_0 |LMK|.$$

Then, it follows from Theorem 3 that

$$(24) \quad n = \prod_{r \in S'} \Phi_{p_0 r}$$

is Lehmer pseudoprime with respect to the sequence  $U$  if  $S' \subseteq S$  and  $|S'| \geq 2$ . Since there is a constant  $c = c(U)$  such that  $\Phi_n < e^{cn}$ , it follows that if  $n$  is of the form in (24) then

$$\begin{aligned} n &= \exp\left\{\sum_{r \in S'} \log |\Phi_{p_0 r}|\right\} \leq \exp\left\{cp_0 \sum_{r \in S'} r\right\} \leq \\ &\leq \exp\left\{cp_0 \sum_{r \in S} r\right\} < \exp\left\{cy^{40/\log_2 y} y \cdot y^{E-\epsilon}\right\} \leq \\ &\leq \exp(y^{E+1}) = x, \end{aligned}$$

if

$$y = (\log x)^{(E+1)^{-1}} \quad \text{and } x \text{ is enough large.}$$

On the other hand  $|S| \geq y^{E-\epsilon}$ , we can assume that  $|S| = \lfloor y^{E-\epsilon} \rfloor$ , and so the number of those  $n$  of the form in (24) is

$$\geq 2^{|S|} - |S| - 1 > 2^{y^{E-\epsilon}-1} - y^{E-\epsilon} - 1 \geq \exp \left\{ (\log x)^{\frac{E}{E+1}-\epsilon} \right\}$$

for all large  $x$ . Thus

$$P(U, x) \geq \exp \left\{ (\log x)^{\frac{E}{E+1}-\epsilon} \right\},$$

which proves (18). Lemma 4 is proved.

The proof of Theorem 1 follows directly from Lemma 3 and Lemma 4, because

$$\frac{E}{E+1} - \epsilon = \frac{1}{34} - \epsilon > \frac{1}{35}.$$

### 5. The proof of Theorem 2

Let  $U = U(L, M)$  be a non-degenerate Lehmer sequence and let  $d \geq 2$  be a given integer for which  $(d, M) = 1$ . Then, it is obvious that  $\bar{u}(d)$  exists, i.e.

$$U_{\bar{u}(d)} \equiv 0 \quad \text{and} \quad U_{\bar{u}(d)+1} \equiv 1 \pmod{d}.$$

In the following  $c_7, c_8, \dots$  denote positive absolute constants.

Let  $0 < \delta < 1/33$  be a fixed real number. Then, it follows from Lemma 3 that for all large  $y$

$$T(y, y^{1-\delta}) > c_7 \frac{y}{\log y}.$$

Thus, if  $p_1 < p_2 < \dots < p_t$  denote the those primes  $p$  which satisfy the conditions

$$(25) \quad y^{1-\delta} < p \leq y \quad \text{and} \quad P[(p-1)(p+1)] \leq y^{1-\delta},$$

then  $t > c_7 y / \log y$ . For these primes  $p$  we have

$$P[u(p_i)] \leq P[(p_i - 1)(p_i + 1)] \leq y^{1-\delta},$$

and so

$$(26) \quad (u(p_i), p_1 \dots p_t) = 1 \quad (i = 1, \dots, t).$$

Let

$$(27) \quad m := [p_1 - 1, p_1 + 1, \dots, p_t - 1, p_t + 1] = q_1^{e_1} \dots q_s^{e_s},$$

where  $q_1 < \dots < q_s$  are primes and  $e_1, \dots, e_s$  are positive integers. By (25) and (27)

$$q_i^{e_i} \leq y + 1 \quad \text{and} \quad q_i \leq y^{1-\delta} \quad (i = 1, \dots, t).$$

Then, by using the prime number theorem, we have

$$\begin{aligned} \log m &= \log \prod_{i=1}^s q_i^{e_i} \leq \log \prod_{i=1}^s (y + 1) < \sum_{i=1}^s \log y^2 \leq \\ &\leq 2 \log y \sum_{q \leq y^{1-\delta}} 1 < 3 \log y \frac{y^{1-\delta}}{(1-\delta) \log y} < y^{1-c_8}, \end{aligned}$$

i.e.  $m < \exp(y^{1-c_8})$ .

Let now

$$Q' := p_1 \dots p_t$$

and let  $p_0$  be the smallest prime of the form  $4LK\bar{u}(d)m\mathbf{x} + 1$ . Then

$$p_0 < (4LK\bar{u}(d)m)^{20} < \exp(y^{1-c_9}).$$

Furthermore, let

$$S := \{r : r|Q', r < \exp(y^{1-c_9}) \text{ and } (p_0 Q', U_r) = 1\}.$$

It is easy to show by using (26) and the definition of  $Q'$  that  $(Q', U_r) = 1$  for all  $r|Q'$ , consequently

$$S := \{r : r|Q', r < \exp(y^{1-c_9}) \text{ and } (p_0, U_r) = 1\}.$$

Let  $Q := Q' \cdot d$ , where  $d$  is a given positive integer. One can deduce that

$$\bar{u}(Q) | 2\bar{u}(d)m.$$



Thus, it follows from Theorem 3 that for any subset  $S' \subseteq S$  with  $|S'| \geq 2$  the numbers of the form

$$(28) \quad n = \prod_{r \in S'} \Phi_{p_0 r}$$

are Lehmer pseudoprimes and

$$n \equiv 1 \pmod{d}.$$

Since  $|U_k| < e^{c_{10}k}$ , for the numbers  $n$  defined in (28) we have

$$\begin{aligned} n &= \prod_{r \in S'} \Phi_{p_0 r} \leq \prod_{r \in S'} |U_{p_0 r}| < \exp \left( c_{10} p_0 \sum_{r \in S'} r \right) < \\ &< \exp \left( c_{10} e^{y^{1-c_9}} e^{2y^{1-c_9}} \right) < \exp \left( e^{4y^{1-c_9}} \right) = x \end{aligned}$$

if

$$\log x := e^{4y^{1-c_9}}.$$

Thus, the number of Lehmer pseudoprimes  $\leq x$  and  $\equiv 1 \pmod{d}$  is

$$(29) \quad \geq 2^{|S|} - |S| - 1.$$

By using the same method that was used in [3], one can prove that

$$2^{|S|} - |S| - 1 > \exp((\log x)^{c_{11}}),$$

which with (29) proves Theorem 2. The proof of Theorem 2 is complete.

### References

- [1] Baillie R. and Wagstaff S.S. Jr., Lucas pseudoprimes, *Math. Comp.*, **35** (1980), 1391-1417.
- [2] Erdős P., On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen*, **4** (1956), 201-206.
- [3] Erdős P., Kiss P. and Sárközy A., A lower bound for the counting function of Lucas pseudoprimes, *Math. Comp.*, **41** (1988), 315-323.

- [4] **Freidlander J.B.**, Shifted primes without large prime factors, *Number Theory and Applications*, ed. R.A.Mollin, Kluwer, 1989, 393-402.
- [5] **Goldfeld M.**, On the number of primes  $p$  for which  $p + a$  has a large prime factor, *Mathematika*, **16** (1969), 23-27.
- [6] **Gordon D.M. and Pomerance C.**, The distribution of Lucas and elliptic pseudoprimes, *Math. Comp.*, **196** (1991), 825-838.
- [7] **Graham S.**, On Linnik's constant, *Acta Arith.*, **39** (1981), 161-179.
- [8] **Halberstam H. and Richert H.E.**, *Sieve methods*, Academic Press, 1974.
- [9] **Hardy G.H. and Wright E.M.**, *An introduction to the theory of numbers*, Oxford Univ. Press, London, 1954.
- [10] **Hooley C.**, On the greatest prime factor of  $p+a$ , *Mathematika*, **20** (1973), 135-143.
- [11] **Joó I. and Phong B.M.**, On super Lehmer pseudoprimes, *Studia Sci. Math. Hungar.*, **25** (1990), 121-124.
- [12] **Kiss P.**, Some results on Lucas pseudoprimes, *Ann. Univ. Sci. Bud. Sect. Math.*, **28** (1986), 153-159.
- [13] **Lehmer D.H.**, An extended theory of Lucas' functions, *Ann. Math.*, **31** (1930), 419-448.
- [14] **Lehmer D.H.**, On converse of Fermat's theorem, *Amer. Math. Monthly*, **43** (1936), 347-354.
- [15] **Phong B.M.**, On super Lucas and super Lehmer pseudoprimes, *Studia Sci. Math. Hungar.*, **23** (1988), 435-442.
- [16] **Phong B.M.**, Lucas- és Lehmer- pseudoprím számokról (On Lucas and Lehmer pseudoprime numbers), *Matematikai Lapok*, **33** (1986), 79-92.
- [17] **Phong B.M.**, Rotkiewicz egy problémájának általánosított megoldása (Generalized solution of Rotkiewicz's problem), *Matematikai Lapok*, **34** (1987), 109-119.
- [18] **Pomerance C.**, Popular values of Euler's function, *Mathematika*, **27** (1980), 84-89.
- [19] **Pomerance C.**, On the distribution of pseudoprimes, *Math. Comp.*, **37** (1981), 587-593.
- [20] **Pomerance C.**, A new lower bound for the pseudoprime counting function, *Illinois J. Math.*, **26** (1982), 4-9.
- [21] **Pomerance C.**, Two methods in elementary analytic number theory, *Number Theory and Applications*, ed. R.A.Mollin, Kluwer, 1989, 135-161.
- [22] **Rotkiewicz A.**, On some problems of W.Sierpinski, *Acta Arith.*, **21** (1972), 251-259.

- [23] **Rotkiewicz A.**, 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.
- [24] **Rotkiewicz A.**, On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters  $L, Q$  in arithmetic progressions, *Math. Comp.*, **39** (1982), 239-247.
- [25] **Schinzel A.**, Primitive divisors of the expression  $A^n - B^n$  in algebraic number fields, *J. reine angew. Math.*, **268/269** (1974), 27-33.
- [26] **Stewart C.L.**, Primitive divisors of Lucas and Lehmer numbers, *Transcendence theory*, ed. A.Baker and D.W.Masser, Acad. Press, London-New York, 1977, 79-92.
- [27] **Stewart C.L.**, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.*, **35** (1977), 425-447.

**Bui Minh Phong**  
Department of Computer Algebra  
Eötvös Loránd University  
XI. Bogdánfy u. 10/B  
H-1117 Budapest, Hungary