MATHEMATICS OF COMPUTATION
VOLUME 39, NUMBER 159
JULY 1982, PAGES 239-247

On Euler Lehmer Pseudoprimes and Strong Lehmer Pseudoprimes With Parameters L, Q in Arithmetic Progressions

By A. Rotkiewicz

Abstract. Let $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ for n odd and $U_n = (\alpha^n - \beta^n)/(\alpha^2 - \beta^2)$ for even n, where α and β are distinct roots of the trinomial $f(z) = z^2 - \sqrt{L}z + Q$ and $L > 0$ and Q are rational integers. U_n is the nth Lehmer number connected with $f(z)$.

Let $V_n = (\alpha^n + \beta^n)/(\alpha + \beta)$ for n odd, and $V_n = \alpha^n + \beta^n$ for n even denote the nth term of the associated recurring sequence. An odd composite number n is a *strong Lehmer pseudoprime with parameters* L, Q (or slepsp(L, Q)) if $(n, DQ) = 1$, where $D = L - 4Q \neq 0$, and with $\delta(n) = n - (DL/n) = d \cdot 2^s$, d odd, where (DL/n) is the Jacobi symbol, we have either $U_d \equiv 0 \pmod n$ or $V_{d \cdot 2^r} \equiv 0 \pmod n$, for some r with $0 \leqslant r < s$.

Let $D = L - 4Q > 0$. Then every arithmetic progression $ax + b$, where a, b are relatively prime integers, contains an infinite number of odd (composite) strong Lehmer pseudoprimes with parameters L, Q. Some new tests for primality are also given.

1. First we recall the definitions of Euler pseudoprimes, which have been introduced (see Pomerance, Selfridge, Wagstaff [5]) because they are rarer than ordinary pseudoprimes.

An odd composite number n is an *Euler pseudoprime to base* c (or epsp(c)) if $(c, n) = 1$ and

$$c^{(n-1)/2} \equiv \left(\frac{c}{n}\right) \pmod n, \tag{1}$$

where (c/n) is the Jacobi symbol (see also Lehmer [4]). An odd composite n is a *strong pseudoprime* for the base c (or spsp(c)) if, with $n - 1 = d \cdot 2^s$, d odd, we have

$$c^d \equiv 1 \pmod n \quad \text{or} \quad c^{d \cdot 2^r} \equiv -1 \pmod n \quad \text{for some } r \text{ with } 0 \leqslant r < s. \tag{2}$$

Any prime p with $(p, c) = 1$ satisfies one or the other term of this alternative. Pomerance, Selfridge and Wagstaff [5] show that a strong pseudoprime is always an Euler pseudoprime, but not vice versa, so criterion (2) is indeed stronger than (1). Rotkiewicz [10], [11] proved that every arithmetic progression $ax + b$ $(x = 0, 1, 2, \dots)$ where $(a, b) = 1$, contains infinitely many ordinary pseudoprimes (that is to say, pseudoprimes for the base 2).

Received July 20, 1981.

1980 *Mathematics Subject Classification*. Primary 10A15; Secondary 10—04.

Key words and phrases. Pseudoprime, Lucas sequence, Lucas pseudoprime, Lehmer numbers, Lehmer sequence, strong pseudoprime, Euler pseudoprime, Euler Lehmer pseudoprime, strong Lehmer pseudoprime, primality testing.

©1982 American Mathematical Society
0025-5718/81/0000-0444/$03.25

It was shown by van der Poorten and Rotkiewicz [6] that *every arithmetic progression* $ax + b$ ($x = 0, 1, 2, \ldots$), *where* a, b *are relatively prime integers, contains an infinite number of odd (composite) strong pseudoprimes for each base* $c \geqslant 2$.

Baillie and Wagstaff [1] define several types of pseudoprimes with respect to Lucas sequences and prove the analogs of various theorems about ordinary pseudoprimes.

Let D, P, Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$.

The Lucas sequences U_k and V_k are defined recursively for $k \geqslant 2$ by

$$U_k = PU_{k-1} - QU_{k-2}, \qquad V_k = PV_{k-1} - QV_{k-2}.$$

We will write $U_k(P, Q)$ for U_k when it is necessary to show the dependence on P and Q. For $k \geqslant 0$, we also have

$$U_k = (\alpha^k - \beta^k)/(\alpha - \beta), \qquad V_k = \alpha^k + \beta^k,$$

where α and β are distinct roots of $x^2 - Px + Q = 0$.

For odd positive integers n, let $\varepsilon(n)$ denote the Jacobi symbol (D/n), and let $\delta(n) = n - \varepsilon(n)$. If n is prime and if $(n, Q) = 1$, then

$$U_{\delta(n)} \equiv 0 \pmod{n}. \tag{3}$$

If n is composite, but (3) still holds, then we call n a *Lucas pseudoprime with parameters P and Q* (or lpsp(P, Q)). A proper generalization of epsp(c) and spsp(c) for Lucas pseudoprimes is the following:

An odd composite number n is an *Euler Lucas pseudoprime with parameters P, Q* (elpsp(P, Q)) if $(n, QD) = 1$ and

$$U_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (Q/n) = 1, \quad \text{or}$$
$$V_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (Q/n) = -1.$$

An odd composite number n is a *strong Lucas pseudoprime with parameters P, Q* (or slpsp(P, Q)) if $(n, D) = 1$ and, with $\delta(n) = d \cdot 2^s$, d odd, we have either

(i) $U_d \equiv 0 \pmod{n}$, or

(ii) $V_{d \cdot 2^r} \equiv 0 \pmod{n}$, for some r with $0 \leqslant r < s$.

Every prime n satisfies the conditions of these four definitions (with the word "composite" omitted), provided $(n, 2QD) = 1$.

Much more general sequences than Lucas sequences are Lehmer sequences.

Let D, L, Q be integers such that $D = L - 4Q \neq 0$ and $L > 0$. Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = 1$. The Lehmer sequences U_k and V_k are defined recursively for $k \geqslant 2$ by

$$\begin{aligned} U_k &= LU_{k-1} - QU_{k-2} && \text{for } k \text{ odd},\\ U_k &= U_{k-1} - QU_{k-2} && \text{for } k \text{ even},\\ V_k &= LV_{k-1} - QV_{k-2} && \text{for } k \text{ even, and}\\ V_k &= V_{k-1} - QV_{k-2} && \text{for } k \text{ odd}. \end{aligned}$$

For $k \geqslant 0$, we also have

$$U_k = \begin{cases} (\alpha^k - \beta^k)/(\alpha - \beta) & \text{if } 2 \nmid n,\\ (\alpha^k - \beta^k)/(\alpha^2 - \beta^2) & \text{if } 2 \mid n, \end{cases}$$

and

$$V_k = \begin{cases} (\alpha^k + \beta^k)/(\alpha + \beta) & \text{for } 2 \nmid n, \\ \alpha^k + \beta^k & \text{if } 2 \mid n, \end{cases}$$

where α and β are the distinct roots of $z^2 - \sqrt{L}z + Q = 0$.

If $L = P^2$, from Lehmer numbers we get Lucas numbers. In the case of Lehmer numbers we can assume without any essential loss of generality that $(L, Q) = 1$. This is not true for Lucas numbers.

Rotkiewicz [12] gave a proper generalization of ordinary pseudoprimes for Lehmer numbers.

A composite n is a pseudoprime with parameters L, Q (or for the bases α and β) (or lepsp(L, Q)) if $(n, DL) = 1$ and

$$U_{n-\varepsilon(n)} \equiv 0 \pmod{n}, \quad \text{where } \varepsilon(n) = (LD/n).$$

Rotkiewicz [12] proved that *if* $(L, Q) = 1$, $L > 0$, $D = L - 4Q > 0$, *then every arithmetic progression* $ax + b$ $(x = 0, 1, 2, \ldots)$, *where* a, b *are relatively prime, contains an infinite number of odd (composite) pseudoprimes with parameters* L, Q *(that is to say, pseudoprimes for the bases* α *and* β*)*.

Now we shall give the definitions for Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes.

An odd composite n is an *Euler Lehmer pseudoprime with parameters* L, Q (or for the bases α and β) (or elepsp(L, Q)), if $(n, QD) = 1$ and

$$U_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (QL/n) = 1, \quad \text{or}$$

$$V_{(n-\varepsilon(n))/2} \equiv 0 \pmod{n} \quad \text{if } (QL/n) = -1, \quad \text{where } \varepsilon(n) = (DL/n).$$

An odd composite number n is *a strong Lehmer pseudoprime with parameters* L, Q (for the bases α and β) (or slepsp(L, Q)) if $(n, DQ) = 1$, and with $\delta(n) = n - (DL/n) = d \cdot 2^s$, d odd, we have either

(j) $U_d \equiv 0 \pmod{n}$, or

(jj) $V_{d \cdot 2^r} \equiv 0 \pmod{n}$, for some r with $0 \leqslant r < s$.

Every prime n satisfies the conditions of each of these four definitions (with the word "composite" omitted), provided $(n, 2QD) = 1$. The following theorem holds.

THEOREM 1. *If n is a* slepsp(L, Q), *then n is an* elepsp(L, Q).

The proof is analogous to the proof of Theorem 3 from the paper of Baillie and Wagstaff [1] on slpsp(L, Q) and may be omitted. In the present paper we shall prove the following

THEOREM 2. *Let* $D = L - 4Q > 0$, $L > 0$. *Then every arithmetical progression* $ax + b$ $(x = 0, 1, 2, \ldots)$, *where* a, b *are relatively prime integers contains an infinite number of odd strong Lehmer pseudoprimes with parameters* L, Q *(that is to say, slepsp for the bases* α *and* β*)*.

2. For each positive integer n we denote by $\phi_n(\alpha, \beta) = \bar{\phi}_n(L, Q)$ the nth cyclotomic polynomial

$$\bar{\phi}_n(L, Q) = \phi_n(\alpha, \beta) = \prod_{(m,n)=1} (\alpha - \zeta_n^m \beta) = \prod_{d \mid n} (\alpha^d - \beta^d)^{\mu(n/d)},$$

where ζ_n is a primitive nth root of unity and the product is over the $\phi(n)$ integers m with $1 \leqslant m \leqslant n$ and $(m, n) = 1$; μ is the Möbius function.

It will be convenient to write

$$\phi(\alpha, \beta; n) = \phi_n(\alpha, \beta).$$

It is easy to see that $\phi(\alpha, \beta; n) > 1$ for $D > 0$, $n > 2$. Indeed, since $\phi_n(\alpha, \beta)$ is symmetrical in α and β, we may assume that

$$\alpha = \frac{\sqrt{L} + \sqrt{D}}{2} \geqslant 1, \qquad \beta = \frac{\sqrt{L} - \sqrt{D}}{2},$$

hence for $n > 2$, $\beta > 0$, we have $\phi(\alpha, \beta; n) > |\alpha - \beta| = \sqrt{D} \geqslant 1$, and if $n > 2$, $\beta < 0$, then $\phi(\alpha, \beta; n) > |\alpha + \beta| = \sqrt{L} \geqslant 1$.

A prime factor p of U_n is called a *primitive prime factor* of U_n if $p \mid U_n$ but $p \nmid DLU_3 \cdots U_{n-1}$.

The following result is well known.

LEMMA 1. *Denote by $r = r(n)$ the largest prime factor of n. If $r \nmid \phi(\alpha, \beta; n)$, then every prime p dividing $\phi(\alpha, \beta; n)$ is a primitive prime p divisor of U_n and is $\equiv (DL/p)$* (mod n).

If $r^k \parallel \phi(\alpha, \beta; n)$, $k \geqslant 1$ (which is to say $r^k \mid \phi(\alpha, \beta; n)$ but $r^{k+1} \nmid \phi(\alpha, \beta; n)$), then r is a primitive prime divisor of U_{n/r^k}.

The number U_n for $n > n_0(\alpha, \beta) = n_0(L, Q)$ has a primitive prime divisor. The number $n_0(\alpha, \beta)$ can be effectively computed. If $D > 0$, then $n_0 = 12$.

Proof. The first part of this lemma follows from Theorems 3.2, 3.3, and 3.4 of Lehmer [2]; the second part about existence of primitive prime factors follows from the theorems of Schinzel [13] and Ward [14].

LEMMA 2 (ROTKIEWICZ [12, LEMMA 5]). *Let $\psi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 2 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} (p_1^2 - 1)(p_1^2 - 1) \cdots (p_k^2 - 1)$.*

If q is a prime such that $q^2 \parallel n$ and a is a natural number such that $a\psi(a) \mid q - 1$, then $\phi(\alpha, \beta; n) \equiv 1$ (mod a).

3. Proof of Theorem 2. If for each pair of relatively prime integers a, b there is at least one strong pseudoprime with parameters L, Q of the shape $ax + b$, where x is a natural number, then there are infinitely many such pseudoprimes. To see this just notice that we then have such pseudoprimes of the shape $adx + b$ for every natural d with $(d, b) = 1$, and we may choose d as large as we wish. This said, we may also suppose without loss of generality that a is even and b is odd and that $4DL \mid a$, since if b_1 is a prime $> 4DL$ of the form $at + b$, then every term of the progression $4DLax + b_1$ $(x = 1, 2, \ldots)$ is $\equiv b$ (mod a), its difference is $4DLa$ and $(4DLa, b_1) = 1$.

Thus, we prove the theorem if we can produce a strong pseudoprime n with parameters L, Q with $n \equiv b$ (mod a).

Given a and b as described, with $2^\lambda \parallel b - (DL/b)$, $\lambda \geqslant 1$, we commence our construction by choosing three distinct odd primes p_1, p_2, p_3 that are relatively prime to a. Furthermore,we introduce two further primes p and q, with $q > p_i$ $(i = 1, 2, 3)$, which are to satisfy certain conditions detailed below. Firstly, we require that

(a) $$2^{\lambda}p_1p_2p_3q^2 \parallel p-\varepsilon(p) \quad\text{and}\quad (LQD, p)=1.$$

Since p is prime, it satisfies the condition $U_d \equiv 0 \pmod p$ or $V_{2^r d} \equiv 0 \pmod p$ for some r, $0 \leqslant r < \lambda$ with $p-\varepsilon(p) = 2^{\lambda}d$, $(2, d) = 1$, $\varepsilon(p) = (DL/p)$.

This holds because ± 1 are the only square roots of 1 in a finite field and $U_{p-\varepsilon(p)} \equiv 0 \pmod p$, where $\varepsilon(p) = (DL/p)$. So either

(4) $$U_{(p-\varepsilon(p))/2^{\lambda}} \equiv 0 \pmod p \quad\text{or}\quad V_{(p-\varepsilon(p))/2^{\mu}} \equiv 0 \pmod p$$

for some μ, $0 < \mu \leqslant \lambda$. Slightly different proofs will be required to deal with the two terms of the alternative. However, in either case we will construct q and p so that the number

$$n_i = p\phi(\alpha, \beta; (p-\varepsilon(p))/2^{\lambda}p_i) \quad\text{or}\quad p\phi(\alpha, \beta; (p-\varepsilon(p))/2^{\mu-1}p_i) \qquad (i = 1,2,3)$$

is our required strong pseudoprime with parameters L, Q; here we take the first choice for n_i if the first term of the alternative (4) applies, and the second, with the appropriate μ, in the event the second term of the alternative (4) applies.

It will be convenient to write

$$m_i = n_i/p \qquad (i = 1,2,3)$$

and to denote the integers $(p-\varepsilon(p))/2^{\lambda}p_i$ and $(p-\varepsilon(p))/2^{\mu-1}p_i$, respectively, by s_i $(i = 1,2,3)$. We can assume that $s_i > n_0 = 12$. Hence if p divided more than one of the m_i, then by Lemma 1 we would have p as a primitive prime factor of both U_{s_i} and U_{s_j} which is absurd if $s_i \neq s_j$. So we may suppose that p divides neither m_1 nor m_2, say. Now let $\bar{r}$ be the greatest prime factor of $p-\varepsilon(p)$. By (a) we have $\bar{r} \geqslant q$ so $\bar{r} > p_1$, p_2, and thus $\bar{r}$ is the greatest prime divisor of both s_1 and s_2. Again by Lemma 1, if $\bar{r}$ were to divide both m_1 and m_2, then $\bar{r}$ would be a primitive prime factor of both $U_{s_1/\bar{r}^k}$ and $U_{s_2/\bar{r}^k}$, where $\bar{r}^k \parallel p-\varepsilon(p)$. But this is absurd, so without loss of generality $\bar{r}$ does not divide m_1. Then Lemma 1 implies that every prime factor t of m_1 is congruent to (DL/t) mod s_1. Since $D > 0$, we have that $m_1 = n_1/p$ is positive. So

(5) $$m_1 \equiv (DL/m_1) \pmod{s_1}.$$

Certainly $q^2 \parallel s_1$. So if we insist that $a\psi(a) \mid q-1$, then by Lemma 2 we have $m_1 \equiv 1 \pmod a$.

Since $4DL \mid a$, we have $m_1 \equiv 1 \pmod{4DL}$. So $(DL/m_1) = (DL/4DLg+1) = 1$ for some positive g, and from (5) it follows that

(6) $$m_1 \equiv 1 \pmod{s_1}.$$

Further, if we insist that

(b) $$2p_i(p_i^2-1) \mid q-1,$$

then by Lemma 2 (recall that $\psi(p) = 2p(p^2-1)$) we have

(7) $$m_1 \equiv 1 \pmod{p_1}.$$

In the same spirit, the requirement on q that

(c) $$3 \cdot 2^{2\lambda+1} \mid q-1$$

implies by Lemma 2 (recall that $\psi(2^{\lambda+1}) = 2 \cdot 2^{\lambda+1}3 = 2^{\lambda+2}3$) that

$$(8) \qquad m_1 \equiv 1 \pmod{2^{\lambda+1}}.$$

Recalling that, by (a), both $p_1 \parallel p - \varepsilon(p)$ and $2^\lambda \parallel p - \varepsilon(p)$, we can conclude from (6), (7) and (8) that

$$m_1 \equiv 1 \pmod{2(p - \varepsilon(p))},$$

which is to say that

$$(9) \qquad n_1 = pm_1 = p(2(p - \varepsilon(p))x + 1) = (p - \varepsilon(p))(2px + 1) + \varepsilon(p),$$

for some positive x; x is positive because, with $D > 0$ and $s_1 > 2$, certainly $\phi(\alpha, \beta; s_1) > 1$.

We have

$$\varepsilon(n_1) = (DL/pm_1) = (DL/p) \cdot (DL/m_1) = (DL/p) = \varepsilon(p).$$

Now suppose that the first term of the alternative (4) applies. By (9) we have

$$\frac{n_1 - \varepsilon(n_1)}{2^\lambda} = \frac{n_1 - \varepsilon(p)}{2^\lambda} = \frac{p - \varepsilon(p)}{2^\lambda} \cdot (2px + 1),$$

so $(m_1, p) = 1$ and

$$m_1 = \phi(\alpha, \beta; (p - \varepsilon(p))/2^\lambda p_1) \mid U_{(p-\varepsilon(p))/2^\lambda p_1}, \; p \mid U_{(p-\varepsilon(p))/2^\lambda},$$

$$n_1 = p\phi(\alpha, \beta; (p - \varepsilon(p))/2^\lambda p_1) \mid U_{(p-\varepsilon(p))/2^\lambda} \mid U_{(n_1-\varepsilon(n_1))/2^\lambda},$$

where $(n_1 - \varepsilon(n_1))/2^\lambda$ is odd. Hence n_1 is a slepsp with parameters L, Q. If the second term of the alternative (4) applies, we have, as before,

$$\frac{n_1 - \varepsilon(n_1)}{2} = \frac{p - \varepsilon(p)}{2} \cdot (2px + 1),$$

and we note that $2px + 1$ is odd. Hence we have

$$m_1 = \phi(\alpha, \beta; (p - \varepsilon(p))/2^{\mu-1}p_1) \mid V_{(p-\varepsilon(p))/2^\mu p_1}, \; p \mid V_{(p-\varepsilon(p))/2^\mu},$$

which imply that

$$n_1 = p\phi(\alpha, \beta; (p - 1)/2^{\mu-1}p_1) \mid V_{(p-\varepsilon(p))/2^\mu} \mid V_{(n_1-\varepsilon(n_1))/2^\mu},$$

so also in this case n_1 is a slepsp with parameters L, Q. It remains for us to show that conditions (a), (b), (c) can be satisfied and that n_1 lies in the appropriate arithmetic progression. We apply Dirichlet's theorem on primes in arithmetic progression to select a prime q with

$$2p_1p_2p_3(p_1^2 - 1)(p_2^2 - 1)(p_3^2 - 1) \mid q - 1, \; 3 \cdot 2^{2\lambda}a\psi(a) \mid q - 1.$$

This gives (b) and (c) and automatically yields $q > p_i$ $(i = 1, 2, 3)$. Since $(a, b) = 1$, $4DL \mid a$, we have $(DL/b) \neq 0$.

By the Chinese Remainder Theorem there exists a natural number m such that

$$(10) \qquad m \equiv (DL/b) + p_1p_2p_3q^2 \pmod{p_1^2p_2^2p_3^2q^3}, \quad m \equiv b \pmod{2^{\lambda+1}a}.$$

From (10) it follows that $(m, 2ap_1^2p_2^2p_3^2q^2) = 1$ and, by Dirichlet's theorem, there exists a positive x such that $2^{\lambda+1}ap_1^2p_2^2p_3^2q^3x + m = p$ is a prime. Since $4DL \mid a$, we have $p \equiv m \pmod{4DL}$, $m \equiv b \pmod{4DL}$, hence $\varepsilon(p) = (DL/p) = (DL/m) = (DL/b)$. Thus $2^\lambda p_1 p_2 p_3 q^2 \parallel p - \varepsilon(p)$, $(DLQ, p) = 1$. This gives (a). These remarks conclude our proof for we have $a\psi(a) \mid q - 1$, $q^2 \parallel p - \varepsilon(p)$, so Lemma 2 yields $m_1 \equiv 1 \pmod a$. Hence

$$n_1 = pm_1 \equiv b \pmod a$$

as required.

Test for Primality. Let U_n be the nth Lehmer number. The generalization of the Euler theorem for Lehmer numbers is the following (cf. Lehmer [2]).

If p is odd prime and $(p, DLQ) = 1$, then

$$\alpha^{p/2-(DL/p)/2} \equiv (LQ/p)\beta^{p/2-(DL/p)/2} \pmod p$$

or, using U_n and V_n,

$$U_{(p-\varepsilon(p))/2} \equiv 0 \pmod p \quad \text{if } (LQ/p) = 1$$

and

$$V_{(p-\varepsilon(p))/2} \equiv 0 \pmod p \quad \text{if } (LQ/p) = -1,$$

where $\varepsilon(p) = (DL/p)$.

According to Proth's theorem if $N = h \cdot 2^n + 1$, where $0 < h < 2^n$ and $(a/N) = -1$, then N is prime if and only if $a^{n-1/2} \equiv -1 \pmod N$. For the proof see Robinson [9, Theorem 9].

The following generalization of Proth's theorem holds.

THEOREM 3. *Let $N = h \cdot 2^n \pm 1$, where $0 < h < 2^n$, $n \geqslant 2$, α and β be roots of the trinomial $f(z) = z^2 - \sqrt{L}z + Q$, where $L > 0$, $D = L - 4Q \neq 0$, $(L, Q) = 1$, $\langle L, Q\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle$ (i.e., α/β is not a root of unity). Let $(DLQ, N) = 1$, $(DL/N) = \pm 1$, $(LQ/N) = -1$. Then N is prime if and only if*

$$N \mid \alpha^{h \cdot 2^{n-1}} + \beta^{h \cdot 2^{n-1}}.$$

Proof of Theorem 3. If N is prime, then $\alpha^{N/2-(DL/N)/2} \equiv (LQ/N)\beta^{N/2-(DL/N)/2} \pmod N$, and since $(DL/N) = \pm 1$, $N = 2^n h \pm 1$, $(LQ/N) = -1$, we have

$$\alpha^{(2^n h \pm 1)/2-(\pm 1)/2} \equiv -\beta^{(2^n h \pm 1)/2-(\pm 1)/2} \pmod N$$

and

$$N \mid \alpha^{2^{n-1}h} + \beta^{2^{n-1}h}.$$

Suppose now that N is not prime and $N \mid \alpha^{2^{n-1}h} + \beta^{2^{n-1}h}$. Let p be the least prime factor of N. Since α/β is not a root of unity, we have

$$p \equiv \pm 1 \pmod{2^n}.$$

From $(LQ/N) = -1$ it follows that N is not a square, and a factorization of N would yield

$$N = p \cdot q \geqslant p(p+2) \geqslant (2^n - 1)(2^n + 1) = 2^n \cdot 2^n - 1 > h \cdot 2^n - 1 = N$$

a contradiction; this completes the proof of Theorem 3. From Theorem 3 we deduce the following generalization of the Lucas-Lehmer criterion.

THEOREM 3′. *Let* $N = h \cdot 2^n \pm 1$, *where* $0 < h < 2^n$, $n \geqslant 2$, α *and* β *be roots of the trinomial* $f(z) = z^2 - \sqrt{L}z + Q$ *and* $L > 0$, $D = L - 4Q \neq 0$, $(L, Q) = 1$, $\langle L, Q\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle$. *Let* $(DLQ, N) = 1$, $(DL/N) = \pm 1$, $(LQ/N) = -1$. *Then* N *is prime if and only if*

$$v_{n-2} \equiv 0 \pmod{N},$$

where $v_i = v_{i-1}^2 - 2Q^{2^i \cdot h}$ *with* $v_0 = \alpha^{2h} + \beta^{2h}$, $i = 1, 2, \ldots$.

Proof. Let $\bar{v}_i = \alpha^{h \cdot 2^{i+1}} + \beta^{h \cdot 2^{i+1}}$. It follows from Theorem 3 that it is enough to prove that $v_i = \bar{v}_i$ for $i \geqslant 0$. This is true for $i = 0$. Suppose that $\bar{v}_i = v_i$. We have

$$v_{i+1} = v_i^2 - 2Q^{2^{i+1}h} = \left(\alpha^{2^{i+1}h} + \beta^{2^{i+1}h}\right)^2 - 2(\alpha\beta)^{2^{i+1}h}$$

$$= \alpha^{2^{i+2}h} + \beta^{2^{i+2}h} = \bar{v}_{i+1}.$$

This proves Theorem 3′. We can calculate the number $v_0 = \alpha^{2h} + \beta^{2h} = a_h$ by using the recurrence relation $a_0 = 2$, $a_1 = \alpha^2 + \beta^2 = L - 2Q$, $a_i = a_1 a_{i-1} - Q^2 a_{i-2}$.

If we put in Theorem 3′ $Q = \pm 1$, we get the following

COROLLARY 1. *Let* $N = h \cdot 2^n \pm 1$, $0 < h < 2^n$, $n \geqslant 2$, α *and* β *be roots of the trinomial* $f(z) = z^2 - \sqrt{L}z \pm 1$, $L > 0$, $\langle L, \pm 1\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle$, $(DL/N) = \pm 1$, $(\pm L/N) = -1$. *Then a necessary and sufficient condition that* N *shall be prime is that*

$$v_{n-2} \equiv 0 \pmod{N},$$

where $v_i = v_{i-1}^2 - 2$, $v_0 = \alpha^{2h} + \beta^{2h}$.

For $h = 1$, $L = 2$, $f(z) = z^2 - \sqrt{2}z - 1$, we have $v_0 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 2 + 2 = 4$, and from Corollary 1 we obtain the Lucas-Lehmer theorem on the Mersenne numbers (see Lehmer [3]). Lehmer numbers with respect to the trinomial $z^2 - \sqrt{L}z \pm 1$ correspond to Lucas numbers with respect to the trinomial $z^2 - Lz \pm L$, and it is easy to see that Corollary 1 for $N = h \cdot 2^n - 1$ corresponds to Theorem 5 of Riesel (see [8]). Riesel [8] considered the case in which h is a multiple of 3. If $h = 3$, the value $u_0 = 5778$ will fit for $n \equiv 0, 3 \pmod 4$ (Lehmer [2]), and if $h = 6a \pm 1$ and $3 \nmid N$, the value $u_0 = (2 + \sqrt{3})^h + (2 - \sqrt{3})^h$ will fit for all n (Riesel [7]).

Riesel [8] used his technique to find all primes $N = 3A \cdot 2^n - 1$ for all odd $A \leqslant 35$ and all $n \leqslant 1000$.

Theorem 3 implies immediately the following

COROLLARY 2. *Let* $N = h \cdot 2^n \pm 1$, *where* $0 < h < 2^n$, $n \geqslant 2$, α *and* β *be roots of the trinomial* $f(z) = z^2 - \sqrt{L}z + Q$, *where* $L > 0$, $D = L - 4Q \neq 0$, $(L, Q) = 1$, $\langle L, Q\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle$. *Let* $(DLQ, N) = 1$, $(DL/N) = \pm 1$, $(LQ/N) = -1$. *Then* $N = h \cdot 2^n \pm 1$ *cannot be elepsp with parameters* L, Q (*that is to say, elepsp for the bases* α *and* β).

Institute of Mathematics
Polish Academy of Sciences
ul. Sniadeckich 8
00-950 Warsaw, Poland

Department of Mathematics and Natural Sciences
Warsaw University Branch
15-424 Białystok, Poland

1. R. BAILLIE & S. WAGSTAFF, JR., "Lucas pseudoprimes," *Math. Comp.*, v. 35, 1980, pp. 1391–1417.

2. D. H. LEHMER, "An extended theory of Lucas functions," *Ann. of Math.*, v. 31, 1930, pp. 419–448.

3. D. H. LEHMER, "On Lucas's test for the primality of Mersenne's numbers," *J. London Math. Soc.*, v. 10, 1935, pp. 162–165.

4. D. H. LEHMER, "Strong Carmichael numbers," *J. Austral. Math. Soc. Ser. A*, v. 21, 1976, pp. 508–510.

5. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, JR., "The pseudoprimes to $25 \cdot 10^9$," *Math. Comp.*, v. 35, 1980, pp. 1003–1026.

6. A. J. VAN DER POORTEN & A. ROTKIEWICZ, "On strong pseudoprimes in arithmetic progressions," *J. Austral. Math. Soc. Ser. A*, v. 29, 1980, pp. 316–321.

7. H. RIESEL, "A note on the prime numbers of the forms $N = (6a + 1)2^{2n-1} - 1$ and $M = (6a - 1)2^{2n} - 1$," *Ark. Mat.*, v. 3, 1956, pp. 245–253.

8. H. RIESEL, "Lucasian criteria for the primality of $N = h \cdot 2^n - 1$," *Math. Comp.*, v. 23, 1969, pp. 869–876.

9. R. M. ROBINSON, "The converse of Fermat's theorem," *Amer. Math. Monthly*, v. 64, 1957, pp. 703–710.

10. A. ROTKIEWICZ, "Sur les nombres pseudopremiers de la forme $ax + b$," *C. R. Acad. Sci. Paris*, v. 257, 1963, pp. 2601–2604.

11. A. ROTKIEWICZ, "On the pseudoprimes of the form $ax + b$," *Proc. Cambridge Philos. Soc.*, v. 63, 1967, pp. 389–392.

12. A. ROTKIEWICZ, "On the pseudoprimes of the form $ax + b$ with respect to the sequence of Lehmer," *Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys.*, v. 20, 1972, pp. 349–354.

13. A. SCHINZEL, "On primitive prime factors of Lehmer numbers. III," *Acta Arith.*, v. 15, 1968, pp. 49–70.

14. M. WARD, "The intrinsic divisors of Lehmer numbers," *Ann. of Math.* (2), v. 62, 1955, pp. 230–236.