EXCEPTIONAL REAL LUCAS SEQUENCES

L. K. Durst

1. Introduction. If l and m are any pair of non-zero rational integers, the sequence

$$(U): \quad U_0 = 0, \quad U_1 = 1, \quad U_n = l U_{n-1} - m U_{n-2}, \quad n \geq 2,$$

is called the *Lucas sequence* generated by the polynomial $z^2 - lz + m$. If $l^2 \neq 4m$ and α, β are the roots of the generator of (U),

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad n \geq 0$$

(Lucas [6]). Each (U) is a *divisibility sequence*: $n \mid m$ implies $U_n \mid U_m$. An index n, greater than 2, is *exceptional* in (U) if every prime dividing U_n also divides $U_1 U_2 U_3 \cdots U_{n-1}$. In the study of exceptional indices it suffices to take $l > 0$. For if (U) and (U') are generated by $z^2 - lz + m$ and $z^2 + lz + m$, respectively, then $U_n = (-1)^{n-1} U'_n$. In all that follows we therefore suppose $l > 0$. If $l^2 > 4m$, (U) will be called *real*.

Birkhoff and Vandiver [1] have shown that when α and β are co-prime rational integers the only (U) with any exceptional indices is the so-called [6] Fermat sequence generated by $z^2 - 3z + 2$, whose only exceptional index is six. Carmichael [2, Theorem 23] has shown that when l and m are co-prime integers, $l^2 > 4m$, the only possible exceptional indices are six and twelve and that twelve is exceptional only in the Fibonacci sequence ($l = 1, m = -1$). Lekkerkerker [5] has shown that even if l and m are not co-prime, provided $l^2 > 4m$, (U) has only finitely many exceptional indices.

In this paper we show that for $(l, m) = 1$ there are infinitely many real Lucas sequences in which six is exceptional (Theorems 2, 3) and that for $(l, m) > 1$ there exist infinitely many real Lucas sequences with any prescribed finite set of exceptional indices (Theorem 5).

The problem is attacked by reducing it to a study of Lehmer's divisibility sequences (Lehmer [4]), for which the corresponding problem has been solved (Ward [8], Durst [3]). In the course of the discussion we obtain a new proof of Lekkerkerker's theorem and an extension of it to Lehmer's sequences (Theorem 4).

If $l^2 = 4m$, then $m = a^2$ and $U_n = na^{n-1}$. Here n is exceptional unless it is a prime not dividing a. For $l^2 < 4m$ very little is known. In particular, it is not known whether any such sequences have infinitely many exceptional indices.

2. Lehmer sequences. If L and M are rational integers, $L > 0$, the sequence

$$(P): \quad P_0 = 0 \,, \quad P_1 = 1 \,, \quad P_{2n} = P_{2n-1} - MP_{2n-2} \,, \quad P_{2n+1} = LP_{2n} - MP_{2n-1}$$

is called the *Lehmer sequence* generated by the polynomial $z^2 - L^{\frac{1}{2}}z + M$. Let $K = L - 4M$. If $K \neq 0$ and α, β are the roots of the generator of (P),

$$P_{2n} = (\alpha^{2n} - \beta^{2n})/(\alpha^2 - \beta^2) \,,$$
$$P_{2n+1} = (\alpha^{2n+1} - \beta^{2n+1})/(\alpha - \beta) \,.$$

If the Lucas sequence (U) is generated by $z^2 - lz + m$, then the Lehmer sequence (P) generated by the same polynomial $z^2 - L^{\frac{1}{2}}z + M$, $L = l^2$, $M = m$, will be called the Lehmer sequence *associated* with (U). Clearly

$$U_{2n} = lP_{2n} \,, \qquad U_{2n+1} = P_{2n+1} \,,$$

and

$$U_1 U_2 \cdots U_{n-1} = l^{[\frac{1}{2}(n-1)]} P_1 P_2 \cdots P_{n-1} \,.$$

Thus we have the following theorem.

THEOREM 1. *An index n is exceptional in (U) if and only if*
(i) *n is exceptional in (P), or*
(ii) *each prime dividing P_n but not $P_1 \cdots P_{n-1}$ divides l.*
Cases (i) and (ii) are treated in §§ 3 and 4, respectively.

3. Lucas sequences whose associated Lehmer sequences have exceptional indices. If L and M are co-prime and $K > 0$, the Lehmer sequence (P) generated by $z^2 - L^{\frac{1}{2}}z + M$ has six as an exceptional index if and only if

$$L = 2^{s+2} - 3K \,, \qquad M = 2^s - K \,,$$

where $s \geq 1$, $2^{s+2} > 3K$, and K is odd (Durst [3]). Since $2^{s+2} - 3K \equiv (-1)^s \pmod{3}$, $L = l^2 = 2^{s+2} - 3K$ implies $s = 2t$ and $l = 2^{t+1} - j$, where j is odd and $1 \leq j < 2^{t+1}$. But, then $3K = 2^{2t+2} - l^2 = j(2^{t+2} - j)$; and either $j = 3r$ or $2^{t+2} - j = 3r$, where r is odd, positive, and less than $2^{t+1}/3$. Thus

$$K = r(2^{t+2} - 3r) \,, \quad L = (2^{t+1} - 3r)^2 \,, \quad M = (2^t - r)(2^t - 3r)$$

and we have the following theorem.

THEOREM 2. *If $(l, m) = 1$ and $l^2 > 4m$, then six is an exceptional index in both the Lucas sequence (U) and the Lehmer sequence (P) generated by $z^2 - lz + m$ if and only if*

$$l = 2^{t+1} - 3r , \qquad m = (2^t - r)(2^t - 3r) ,$$

where $t \geqq 1$, $2^{t+1} > 3r$, and r is odd and positive.

Note that for $r = t = 1$, (U) is the Fibonacci sequence $(l = 1$, $m = -1)$.

4. Lucas sequences whose associated Lehmer sequences have no exceptional indices. Since $P_1 = P_2 = 1$ and $P_6/P_3 = L - 3M$, every prime dividing P_6 but not P_3 must divide $Q_6 = L - 3M = K + M$. But $(L, M) = 1$ implies $(P_4 P_5, P_6) = 1$ by Theorem 2.1 of [3], and P_6 is even if and only if P_3 is. Thus for p an odd prime, $p \mid P_6$ but $p \nmid P_1 P_2 P_3 P_4 P_5$ if and only if $p \mid Q_6$. On the other hand, if $p \mid L$, then $p \mid P_{2p}$ by Theorem 2.0 of [3], so $p \mid (Q_6, L)$ if and only if L is odd and $p = 3$. Now $Q_6 = 2^2 3^u$, $l = 3^s \lambda$, $t \geqq 0$, $u \geqq 1$, $s \geqq 1$, and $(\lambda, 6) = 1$ give $3M = l^2 - Q_6 = 3^{2s} \lambda^2 - 2^2 3^u$ or $M = 3^{2s-1} \lambda^2 - 2^2 3^{u-1}$. But $s \geqq 1$ and $(L, M) = 1$ imply $u = 1$. Finally $K = Q_6 - M = 2^{t+2} - 3^{2s-1} \lambda^2 > 0$, and we have the following theorem.

THEOREM 3. *If $(l, m) = 1$ and $l^2 > 4m$, then six is an exceptional index in (U) but not an exceptional index in its associated (P) if and only if*

$$l = 3^s \lambda , \qquad m = 3^{2s-1} \lambda^2 - 2^t$$

where $s \geqq 1$, $t \geqq 0$, $\lambda \equiv \pm 1 \pmod 6$ and $3^{2s-1} \lambda^2 < 2^{t+2}$.

Note that for $s = \lambda = 1$, $t = 0$, (U) is the Fermat sequence $(l = 3$, $m = 2)$.

5. Sylvester's sequences and Lekkerkerker's theorem. In his study of Lehmer's sequences, Ward [8] adapted a method originally introduced by Sylvester [7] in connection with Lucas sequences. With each Lehmer sequence (P) we associate the *Sylvester sequence*

$$(Q): \quad Q_0 = 0 , \quad Q_1 = 1 , \quad Q_2 = 1 , \quad Q_n = \beta^{\phi(n)} C_n(\alpha/\beta) , \quad n \geqq 3 ,$$

where $C_n(x)$ is the nth cyclotomic polynomial. Each Q_n is a rational integer and $P_n = \Pi Q_d$, $Q_n = \Pi P_d^{\mu(\delta)}$, where μ is the Möbius function, $\delta = n/d$, and the products are taken over all divisors d of n. Evidently an index is exceptional in (P) if and only if it is exceptional in (Q).

Suppose $L = D\bar{L}$, $M = D\bar{M}$ and let (P) and $(\bar{P})$ be the Lehmer sequences generated by $z^2 - L^{\frac{1}{2}} z + M$ and $z^2 - \bar{L}^{\frac{1}{2}} z + \bar{M}$, respectively, (Q) and $(\bar{Q})$ being their associated Sylvester sequences. Lemma 1 below is easily proved by induction using the recursion relations. Lemma 2 states that Q_n is a homogeneous function of L, M.

LEMMA 1.

$$P_{2n} = D^{n-1} \bar{P}_{2n} , \qquad P_{2n+1} = D^n \bar{P}_{2n+1} .$$

LEMMA 2. $Q_n = D^{\frac{1}{2}\phi(n)}\bar{Q}_n \quad if \quad n > 2 .$

Proof. There are three cases: $n = m$, $n = 2m$, $n = 2^r m$, where m is odd and $r > 1$. In the first case,

$$
\begin{aligned}
Q_n = Q_m &= \Pi P_d^{\mu(\delta)} \qquad\qquad (d\delta = m) \\
&= \Pi \{D^{\frac{1}{2}(d-1)}\bar{P}_d\}^{\mu(\delta)} \\
&= D^{\frac{1}{2}\{\Sigma d\mu(\delta) - \Sigma\mu(\delta)\}} \Pi \bar{P}_d^{\mu(\delta)} \\
&= D^{\frac{1}{2}\{\phi(n) - \varepsilon(n)\}}\bar{Q}_n ,
\end{aligned}
$$

where $\varepsilon(n) = 1$ if $n = 1$, $\varepsilon(n) = 0$ if $n > 1$. In the second and third cases ($n = 2^r m$, $r \geq 1$),

$$
Q_n = \prod_{s=0}^{r} \prod_{d\delta = m} P_{2^{r-s}d}^{\mu(2^s\delta)} = \prod_{d\delta = m} (P_{2^r d}/P_{2^{r-1}a})^{\mu(\delta)} ,
$$

since δ is odd, $\mu(2\delta) = -\mu(\delta)$ and $\mu(2^s\delta) = 0$ if $s \geq 2$. In the second case ($r = 1$),

$$
P_{2d} = D^{d-1}\bar{P}_{2d} , \qquad P_d = D^{\frac{1}{2}(d-1)}\bar{P}_d ,
$$

and

$$
\begin{aligned}
Q_n = Q_{2m} &= \Pi\{D^{\frac{1}{2}(d-1)}(\bar{P}_{2d}/\bar{P}_d)\}^{\mu(\delta)} \\
&= D^{\frac{1}{2}\{\Sigma d\mu(\delta) - \Sigma\mu(\delta)\}} \Pi (\bar{P}_{2d}/\bar{P}_d)^{\mu(\delta)} \\
&= D^{\frac{1}{2}\{\phi(m) - \varepsilon(m)\}}\bar{Q}_{2m} \\
&= D^{\frac{1}{2}\{\phi(n) - \varepsilon(m)\}}\bar{Q}_n .
\end{aligned}
$$

While in the third case ($r > 1$),

$$
P_{2^r d} = D^{2^{r-1}d-1}\bar{P}_{2^r d} , \qquad P_{2^{r-1}a} = D^{2^{r-2}d-1}\bar{P}_{2^{r-1}a}
$$

and

$$
\begin{aligned}
Q_n &= \Pi\{D^{2^{r-2}d}(\bar{P}_{2^r d}/\bar{P}_{2^{r-1}a})\}^{\mu(\delta)} \\
&= D^{2^{r-2}\Sigma d\mu(\delta)} \Pi (\bar{P}_{2^r d}/\bar{P}_{2^{r-1}a})^{\mu(\delta)} \\
&= D^{2^{r-2}\phi(m)}\bar{Q}_{2^r m} \\
&= D^{\frac{1}{2}\phi(n)}\bar{Q}_n .
\end{aligned}
$$

If p divides Q_n but not $Q_1 Q_2 \cdots Q_{n-1}$, p is called[1] a *primitive factor* of Q_n. Clearly different members of (Q) share no primitive factors. Lemma 2 implies that an index n, greater than 3, is exceptional in (P) if and only if

(i) n is exceptional in $(\bar{P})$ or

(ii)   every primitive prime factor of $\bar{Q}_n$ is a factor of D. Now for

---

[1] By Lehmer [4]. Lucas [6] calls it a *diviseur propre*, Carmichael [2] a characteristic factor, and Ward [8] an intrinsic divisor.

$(\bar{L}, \bar{M}) = 1$ and $\bar{L} > 4\bar{M}$, $(\bar{P})$ has only finitely many exceptional indices. (It has at most two of them [3].) Since D has a finite number of distinct prime divisors, only finitely many indices fall into case (ii), and we have the following theorem.

THEOREM 4. *If* $L > 4M$, *the Lehmer sequence* (P) *generated by* $z^2 - L^{\frac{1}{2}}z + M$ *has only finitely many exceptional indices.*

As a corollary, we deduce Lekkerkerker's theorem. If (U) is the Lucas sequence generated by $z^2 - lz + m$, and (P) its associated Lehmer sequence,

$$U_{2n} = lP_{2n}, \qquad U_{2n+1} = P_{2n+1},$$

so that an index n is exceptional in (U) if and only if n is exceptional in (P), or the primitive prime factors of Q_n divide l, (Q) being the Sylvester sequence associated with (P). In view of Theorem 4, the number of such indices is finite if $l^2 > 4m$.

6. **Exceptional indices for real sequences with** (L, M) **greater than one.** In this section we show that Theorem 4 and Lekkerkerker's theorem are the best such theorems possible, in the sense that generally no more specific statement can be made regarding the distribution of exceptional indices of real Lehmer and Lucas sequences.

THEOREM 5. *There are infinitely many real Lehmer sequences and infinitely many real Lucas sequences with any prescribed finite set* $\{n_1, \cdots, n_N\}$ *of exceptional indices.*

Proof. Suppose $(\bar{U})$ is the Lucas sequence generated by $z^2 - \bar{l}z + \bar{m}$, where $\bar{l} = 1$ and $\bar{m} = -2$. Then $(\bar{U})$ and its associated Lehmer sequence $(\bar{P})$, which are identical, have no exceptional indices. Suppose $(\bar{Q})$ is the Sylvester sequence associated with $(\bar{P})$ and let $d = p_1^{a_1} \cdots p_M^{a_M}$, where $a_1, \cdots, a_M$ are any positive integers and $p_1, \cdots, p_M$ are the primitive prime factors of $\bar{Q}_{n_1}, \cdots, \bar{Q}_{n_N}$. Since the maximal square-free divisors of (l^2, m) and (l, m) are the same, the Lehmer sequence (P) and the Lucas sequence (U) generated by $z^2 - lz + m$, $l = d\bar{l}$, $m = d\bar{m}$, have the required exceptional indices.

It is easy to construct real sequences with $(l, m) > 1$ which have no exceptional indices. For example, if $\bar{l} = 1$, $\bar{m} = -2$, then $\bar{U}_{11} = 683$, $\bar{U}_{22} = 1,398,101$, so 23 and 89 are primitive factors of $\bar{U}_{22}$. Thus the sequences (U) and (P) generated by $z^2 - 23z - 46$ have no exceptional indices since $(\bar{U})$ has none.

Given a single example of a complex sequence $(l^2 < 4m)$ known to have no exceptional indices, it would be possible to extend Theorem 5 to include complex sequences as well as real sequences. Since no such examples seem to be known at present (Carmichael [2], Ward [8]), this extension

must wait. However, given any sequence, real or complex, the proof of Theorem 5 provides a method for constructing any number of other sequences whose sets of exceptional indices contain all those of the given sequence as well as any finite set of additional exceptional indices.

REFERENCES

1. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math., (Second Series), **5** (1903-1904), 173-180.

2. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math., (Second Series), **15** (1913-1914), 30-70.

3. L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math., **9** (1959), 437-441.

4. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., (Second Series), **31** (1930), 419-448.

5. C. G. Lekkerkerker, *Prime factors of the elements of certain sequences of integers*, Proc., Koninklijke Nederlandse Akademie van Wetenschappen (Series A), **56** (1953), 265-280.

6. Edouard Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184-240, 289-321.

7. J. J. Sylvester, *On the divisors of cyclotomic functions*, Amer. J. Math., **2** (1879), 357-381, Comptes Rendus, **90** (1880), 287-289, 345-347. Collected Mathematical Papers, volume **3**, 317-339, 428-432.

8. Morgan Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math., (Second Series), **62** (1955), 230-236.

WM. M. RICE UNIVERSITY