EXCEPTIONAL REAL LEHMER SEQUENCES

L. K. DURST

1. Introduction. If L and M are rational integers and L is positive, the sequence

$$(P): \quad P_0, \ P_1, \ P_2, \cdots, \ P_n, \cdots$$

is called the *Lehmer sequence* generated by

$$f(z) = z^2 - L^{1/2}z + M ,$$

if

$$\begin{aligned} P_n &= (\alpha^n - \beta^n)/(\alpha - \beta), \text{ for } n \text{ odd} , \\ &= (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), \text{ for } n \text{ even} , \end{aligned}$$

where α, β are the roots of $f(z) = 0$. Since $P_0 = 0$, $P_1 = 1$ and the remaining terms of (P) satisfy the recursion relations

$$\begin{aligned} P_{2n} &= P_{2n-1} - MP_{2n-2} \\ P_{2n+1} &= LP_{2n} - MP_{2n-1} , \end{aligned}$$

it is clear that every Lehmer sequence is a sequence of rational integers. In Lehmer [1], P_n is denoted by $\overline{U}_n$.

The sequence (P) is called *real* if $K = L - 4M$, the discriminant of $f(z)$, is positive. An index n greater than 2 is called *exceptional* if each prime dividing P_n also divides a term P_m, where $0 < m < n$. The sequence (P) is called *exceptional* if it contains a term whose index is exceptional.

This paper continues the classification of exceptional real Lehmer sequences begun by Morgan Ward [2]. The main result is the following theorem.

THEOREM 1.0. *For real Lehmer sequences, the only possible exceptional indices are six and twelve. Twelve is exceptional only in the sequences determined by*

$$L = 1, \ M = -1 \text{ and } L = 5, \ M = 1.$$

Six is exceptional if and only if

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

Received November 7, 1958.

where $s \geqq 1$, $2^{s+2} > 3K$, *and* K *is odd and positive. Thus for each odd positive value of* K, *there are infinitely many exceptional Lehmer sequences.*

For $K = 5$, $s = 2$, and for $K = 1$, $s = 1$, the expressions for L and M in Theorem 1.0 reduce to

$$L = 1,\ M = -1 \text{ and } L = 5,\ M = 1,$$

respectively. The first of these Lehmer sequences is the Fibonacci sequence F_n, and the second is closely related to the Fibonacci sequence since $P_{2n} = F_{2n}$. These two exceptional sequences (the only real Lehmer sequences in which both six and twelve are exceptional) were found by Ward. It has long been known that the Lucas sequence generated by $z^2 - 3z + 2$ has six as its only exceptional index (Ward [2]); on the other hand, the Lehmer sequence generated by the same polynomial has no exceptional indices. (Cf. Theorem 2.0.) In Theorem 1.2 of [2], "eighteen" should be deleted, since $F_{18} = 2^3.17.19$.

In this discussion, L and M are assumed to be coprime. Ward has shown that this assumption leads to no loss of generality.

2. Apparition and repetition of primes in Lehmer sequences. If p is a rational prime, and if $p \mid P_k$ but $p \nmid P_m$ for $0 < m < k$, then k is called the *rank of apparition* of p in (P). The theorem governing the apparition of rational primes in Lehmer sequences is the following *law of apparition* given by Lehmer [1] in a slightly different form.

THEOREM 2.0. *If* k *is the rank of apparition of* p *in the sequence* (P), *then*

$$k = 2p \qquad \text{if} \quad p \mid L$$

and

$$k \mid p - \sigma\varepsilon \qquad \text{if} \quad p \nmid 2LM\,,$$

where $\sigma = (K/p)$, $\varepsilon = (L/p)$ *are Legendre symbols. If* $p = 2$, *then* $k = 3$ *for* L *odd, and* $k = 4$ *for* L *even. If* $p \mid M$, *then* p *divides no term of* (P), *save* $P_0 = 0$.

Since each Lehmer sequence is a divisibility sequence (Lehmer [1]), the fundamental property of the appearance of primes is given by the following theorem.

THEOREM 2.1. *If* k *is the rank of apparition of* p *in* (P), *then* $p \mid P_n$ *if and only if* $k \mid n$.

Given L and M and a prime p dividing (P), the determination of the exact power of p dividing P_k is a generalization of the unsolved

problem of the quotients of Fermat; consequently it would appear to be premature to ask for an answer to this question. Theorem 2.1 prescribes those terms, other than P_k, containing the factor p, and the *law of repetition* tells the exact power of p dividing P_{km}, provided the highest power of p dividing P_k is supposed known. However, the law of repetition (as given by Lehmer [1]) fails to cover the repetition of the prime 2 in the case in which 2 initially appears to the first power. For the problem at hand a detailed study of this case is required and will be found in § 3.

Let $p^t \,||\, P_n$ mean that $p^t \mid P_n$ but $p^{t+1} \nmid P_n$. Then Lehmer's law of repetition may be stated as follows.

THEOREM 2.2. *If k is the rank of apparition of p in (P), $p^t \,||\, P_k$ for $t \geqq 1$, $p^t \neq 2$, and $(p, l) = 1$, then $p^{r+t} \,||\, P_{p^r kl}$.*

Following Ward [2], the associated sequence (Q) is defined as follows:

$$Q_0 = 0,\ Q_1 = 1,\ Q_2 = 1, \text{ and } Q_n = \beta^{\phi(n)} F_n(\alpha/\beta) \text{ for } n \geqq 3,$$

where $F_n(z)$ is the nth cyclotomic polynomial, of degree $\phi(n)$. Q_n is an integer for each $n \geqq 0$ and $P_n = \prod Q_d$, the product being taken over all divisors d of n. Expressed in terms of L and M, the Q's are homogeneous polynomials of degree $\frac{1}{2}\phi(n)$. A few of the Q's are exhibited here for purposes of reference:

$$Q_3 = L - M,\ Q_4 = L - 2M,\ Q_6 = L - 3M,$$
$$Q_8 = L^2 - 4LM + 2M^2,\ Q_{12} = L^2 - 4LM + M^2 .$$

3. The appearance of powers of 2. The cases in which 2 appears in (P) are given by

(i) $L = 2l + 1, \quad M = 2m + 1,$
(ii) $L = 2l, \quad M = 2m + 1.$

In case (i) the rank of 2 is 3; indeed

$$Q_3 = L - M = 2(l - m) \equiv 0 \pmod{2^t}, \qquad t \geqq 1,$$

whenever $l \equiv m \pmod{2^{t-1}}$. Suppose $l = m + 2^{t-1}n$. Then

$$Q_6 = L - 3M = 2^t n - 2M \equiv 2 \pmod 4, \text{ if } t > 1$$
$$= 2(n - M), \text{ if } t = 1.$$

Hence, if $2 \,||\, Q_3$, then $Q_6 \equiv 0 \pmod{2^s}$, $s \geqq 1$, whenever $n \equiv M \pmod{2^{s-1}}$. Thus, for suitably chosen L and M, any given power 2^t of 2 may be made to divide Q_3. As the law of repetition requires, if $t > 1$, then $2 \,||\, Q_6$. On the other hand, if $2 \,||\, Q_3$, then L and M may be chosen

so that any given power 2^s will divide Q_6; this is the case not covered by Theorem 2.2. Since L and M are odd,

$$Q_{12} = Q_3^2 - 2LM \equiv 2 \pmod 4 ,$$

whether $t = 1$ or $t > 1$.

In case (ii) the rank of 2 is 4; and

$$Q_4 = L - 2M = 2(l - M) \equiv 0 \pmod{2^t},\ t \geqq 1 ,$$

whenever $l \equiv M \pmod{2^{t-1}}$. But

$$Q_8 = L^2 - 4LM + 2M^2 \equiv 2 \pmod 4$$

since L is even and M is odd. In this case $2 \,||\, Q_8$, whatever power of 2 may divide Q_4.

The following lemma completes the discussion of the repetition of 2.

LEMMA 3.0. *If* $2^t \,||\, P_{2n}$ *and* $2^{t+1} \,||\, P_{4n}$, *then* $2^{t+2} \,||\, P_{8n}$.

Proof. For m even, $S_m = \alpha^m + \beta^m$ is a rational integer. Because $P_{4n} = P_{2n} S_{2n}$, the hypotheses imply that $2 \mid S_{2n}$. But $S_{4n} = S_{2n}^2 - 2M^{2n} \equiv 2 \pmod 4$, hence $2^{t+2} \,||\, P_{8n}$, since $P_{8n} = P_{4n} S_{4n}$.

From Lemma 3.0 it follows that when n exceeds k, the rank of 2, then $2 \,||\, Q_n$ implies $2 \,||\, Q_{2n}$.

The results of the present section show that Lemmas 3.3 and 3.4 in Ward [2] need not hold for $n = 6$ when Q_6 is even.

4. Sequences in which six is exceptional. The only cases left open in Ward's analysis are those in which Q_6 is even and, hence, K, L and M are odd.

LEMMA 4.0. *For* K *odd, six is exceptional if and only if* $L = -3K + 2^{s+2} > 0$, $M = -K + 2^s$, *where* $s \geqq 1$.

Proof. Let $L = 2l + 1$, $M = 2m + 1$, then $Q_3 = L - M = 2(l - m)$ and $Q_6 = L - 3M = 2(l - 3m - 1)$. Six is exceptional if and only if

$$l - 3m - 1 = 2^{s-1}\delta \text{ where } l - m = d\delta, \text{ and } s \leqq 1 .$$

But $2^{s-1}\delta = l - 3m - 1 = d\delta - M$, so $M = \delta(d - 2^{s-1})$, and $L = 2l + 1 = M + 2d\delta$. Since $(L, M) = 1$, δ must be ± 1. Thus the conditions become

$$L = \pm (3d - 2^{s-1}),\ M = \pm(d - 2^{s-1}) .$$

Since $K = L - 4M$, $K = \pm (3.2^{s-1} - d)$, or $d = 3.2^{s-1} \pm K$, givng

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

Because $L > 0$, the upper sign must be chosen and s must be taken large enough to make $2^{s+2} > 3K$.

The values of L and M given in Lemma 4.0 yield $Q_3 = L - M = 2\{3.2^s - K\}$ and $Q_6 = L - 3M = 2^s$.

Theorem 1.0 now follows from Lemma 4.0 and Ward's results.

REFERENCES

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

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

THE RICE INSTITUTE