THE LINEAR p-ADIC RECURRENCE OF ORDER TWO

Dedicated to Hans Rademacher on the occasion of his seventieth birthday

BY

MORGAN WARD

I. Introduction and summary of results

1. Let P and $Q \neq 0$ be fixed elements of R_p, the p-adic completion of the rational field R, and consider a second order linear recurrence

$$(W): \quad W_0, \quad W_1, \quad \cdots, \quad W_n, \quad \cdots$$

defined by

$$W_{n+2} = PW_{n+1} - QW_n \qquad (n = 0, 1, 2, \cdots) \tag{1.1}$$

whose initial values W_0, W_1 are elements of R_p. If P, Q, W_0, W_1 are p-adic integers, all the W_n are p-adic integers, and we say that (W) is integral.

Any element $X \neq 0$ of the field R_p may be written as $X = p^x U$, where U is a unit of R_p. We call x the (p-adic) value of X, writing $x = \phi(X)$, with the usual convention that if $X = 0$, $x = +\infty$. In particular, we write

$$w_n = \phi(W_n) \qquad (n = 0, 1, 2, \cdots). \tag{1.2}$$

The sequence (w) is called the value function of the recurrence (W).

We solve completely here the problem of determining the value function of any such recurrence (W); indeed we shall give specific formulas for (w). Since R_p contains the rational field R, our results give a far-reaching generalization of Lucas's "Laws of apparition and repetition" for the appearance of multiples of p in the special recurrences (Lucas [4]):

$$(L): \quad L_0 = 0, \quad L_1 = 1, \quad \cdots, \quad L_n, \quad \cdots,$$

$$(S): \quad S_0 = 2, \quad S_1 = P, \quad \cdots, \quad S_n, \quad \cdots.$$

It should be possible to carry out a similar generalization for the functions (L) and (S) discussed by Lehmer in his thesis (Lehmer [3]), where P is replaced by the square root of an integer of R, but this will not be done here.

2. Let

$$f(z) = z^2 - Pz + Q \tag{2.1}$$

be the polynomial associated with the recurrence (1.1), and let D denote its discriminant. If p divides D, we call p a discriminantal divisor of $f(z)$ or of (W).

It turns out that the only case presenting any difficulty occurs when P

Received August 31, 1960.

and Q are both p-adic units, and (W) is integral. If the value w_n of W_n is positive, we call n a zero of (W) modulo p of order w_n. If (w) is bounded, the recurrence is said to have bounded zeros. In Chapter V of the paper, we give necessary and sufficient conditions that (W) has bounded zeros, and in particular no zeros.

If (W) has zeros, we may assume that $W_0 \equiv 0 \pmod{p}$, and W_1 is a unit. Let $l_n = \phi(L_n)$ be the value function of the p-adic Lucas function (L). If p is not a discriminantal divisor, let r be the rank of apparition of p in (L), that is, the first positive zero of (L) modulo p. (As in the classical case, r divides $p - (D/p)$.) If p is a discriminantal divisor, let $r = 1$. Then there exists an explicitly calculable p-adic integer ν such that the value function of (W) is given by

$$
\begin{aligned}
w_n &= 0 && \text{if} \quad n \not\equiv 0 \pmod{r}, \\
w_n &= l_r + \phi(\nu - n/r) && \text{if} \quad n \equiv 0 \pmod{r}.
\end{aligned} \tag{2.2}
$$

If we represent ν in the canonical form

$$
\nu = \sum_0^\infty a_n p^n, \qquad 0 \leqq a_i < p,
$$

and let $A_n = a_0 + a_1 p + \cdots + a_n p^n$ for $n = 0, 1, 2, \cdots$, then (2.2) gives the following *law of repetition* for powers of p in the terms $W_0, W_r, W_{2r}, \cdots$ of (W) which are divisible by p:

If $m \equiv A_{n-1} \pmod{p^n}$, *but* $m \not\equiv A_n \pmod{p^{n+1}}$, *then the order of* p *in* W_{mr} *is* $n + l_r$.

Lucas's law of apparition for the sequence (L) is the special case when ν is zero.

We show conversely that if p is odd, then there exists a recurrence (W) whose value function (w) is given by (2.2). Furthermore, (W) is unique up to a unit multiplier.

In the special case where P and Q, W_0 and W_1 are rational integers, these results show that for any choice of n we may choose the initial values of (W) in such a way that the law of repetition for powers of p up to the $n + l_r - 1$ power is anything we please. The simplicity of Lucas's law of repetition is thus quite exceptional.

3. The concluding chapter of the paper gives a generalization of the relation between Lucas (L) and (S) recurrences. Assume that p is odd. Two integral sequences (W) and (V) with the same characteristic polynomial $z^2 - Pz + Q$ are said to be *polar* if $\Psi(W_0, W_1, V_0, V_1) = 0$ where Ψ denotes the bilinear polar form of $z^2 - Pzw + Qw^2$. For example, (L) and (S) are polar. We show that the relationships between the laws of apparition and repetition of the prime p in (L) and (S) discovered by Lucas extend to any two polar sequences.

It would be interesting to determine whether there is a p-adic analogue of

the cyclotomic sequence (Q) of Sylvester for any two polar sequences. It is not hard to show that (W) in the cases of most interest is p-adically a divisibility sequence.

It is of some interest that the case when the prime p is ramified in the root field of $z^2 - Pz + Q$ does not require special treatment. For cubic sequences over the rational field (Ward [6]), the ramified case is troublesome. Even though the results for the laws of apparition of unramified primes are qualitatively similar to those obtained here, their proof requires a complicated induction (Ward [6]). It would be of some interest therefore to study the p-adic cubic linear recurrences to see whether they actually need a different treatment from quadratic p-adic recurrences.

The general plan of the present investigation is sufficiently indicated by the chapter headings. The relevant information about p-adic fields summarized in Chapter III may be found in Hasse [2].

II. Reduction to integral sequences

4. To avoid trivial cases, when the determination of the value function of (W) is immediate, we shall assume that not both W_0 and W_1 are zero, and that $W_1^2 - PW_1W_0 + QW_0^2 \neq 0$; for otherwise (W) satisfies a recursion of order one. We shall also assume that the characteristic polynomial (2.1) has distinct nonzero roots which do not differ merely in sign. Thus throughout the remainder of the paper, P, Q, and D are assumed to be different from zero.

Let $\phi(P) = a$ and $\phi(Q) = b$, so that $P = p^aU$, $Q = p^bV$, where U and V are units. Also let $W_0 = p^{w_0}U_0'$, $W_1 = p^{w_1}U_1'$ where U_0' and U_1' are units. Finally, let

$$W_n = p^{nc+d}W_n'$$

where c and d are integers at our disposal. Then

$$W_{n+2}' = p^{a-c}UW_{n+1}' - p^{b-2c}VW_n' \qquad (n = 0, 1, \cdots),$$

and

$$W_0' = p^{w_0-d}U_0', \qquad W_1' = p^{w_1-d-c}U_1'.$$

We choose c so that $a - c$ and $b - 2c$ shall be nonnegative and as small as possible. Then if $d = \text{Min}\{w_0, w_1 - c\}$, W_0' and W_1' are integers, and at least one is a unit. Evidently the value function of (W) is known as soon as the value function of the integral recurrence (W') is determined.

The appropriate choices of c are as follows. If $2a \geqq b$, then

$$a - c = \tfrac{1}{2}((2a - b) + (b - 2c)) \geqq \tfrac{1}{2}(b - 2c),$$

and we choose $c = [b/2]$. If $b > 2a$, then

$$b - 2c = (b - 2a) + 2(a - c) > 2(a - c),$$

and we choose $c = a$.

If we let $P' = p^{a-c}U$ and $Q' = p^{b-2c}V$, then

$$W_{n+2}' = P'W_{n+1}' - QW_n',$$

and the reduction procedure just described leads to the following possibilities for the integers P' and Q'.

Case	Choice of c	Value of $\phi(P')$	Value of $\phi(Q')$
I. $2a \geqq b$, b even	$\frac{1}{2}b$	$\frac{1}{2}(2a - b)$	0
II. $2a > b$, b odd	$\frac{1}{2}(b - 1)$	$\frac{1}{2}(2a - b - 1)$	1
III. $b > 2a$	a	0	$(b - 2a) > 0$

We shall show next that only Case I need be discussed, and that P' may be assumed to be a unit unless p is two, when P' may be double a unit.

The two subsequences

$$W'_0, W'_2, \cdots W'_{2n}, \cdots \quad \text{and} \quad W'_1, W'_3, \cdots, W'_{2n+1}, \cdots$$

of (W') both satisfy the recurrence

$$W^*_{n+2} = P^*W^*_{n+1} - Q^*W^*_n$$

where $P^* = P'^2 - 2Q'$ and $Q^* = Q'^2$. Hence in Case I if P' is not a unit, then P^* and Q^* are both units unless p is two, when the value of P^* is one. In Case II, the value of P^* is at least one if P' is not a unit, while the value of Q^* is two. Consequently a substitution of the form $W^*_n = p^nW^{**}_n$ leads to a recursion for (W^{**}) of type I.

5. It remains to discuss Case III, and Case II when P' is a unit. In either case $z^2 - P'z + Q' \equiv z(z - P') \pmod{p}$, P' a unit. Hence by Hensel's lemma, $z^2 - P'z + Q'$ splits in R_p. Let its roots be γ and δ. Evidently one root is a unit. Let it be δ. Then $\phi(\gamma) = \phi(Q') = c' > 0$. Evidently $\gamma - \delta$ is a unit. Hence the general term of (W') may be put in the form

$$W'_n = \Gamma\gamma^n + \Delta\delta^n \tag{5.1}$$

where Γ and Δ are both integers of R.

At least one of $W'_0 = \Gamma + \Delta$ and $W'_1 = \Gamma\gamma + \Delta\delta$ is a unit. Let $d = \phi(\Delta)$. If $d = 0$, $\phi(W'_n) = 0$ if $n \neq d$. If $d > 0$, Γ is a unit. Hence by (5.1), $\phi(W'_n) = nc'$ if $n < d/c'$, and $\phi(W'_n) = d$ if $n > d/c'$. If c' divides d, so that $d = kc'$, $\phi(W'_k)$ is not completely determined; all that can be said in general is that $\phi(W'_k) \geqq kc'$.

We may summarize the results of these reductions in the following theorem.

THEOREM 5.1. *The rank function of any linear p-adic quadratic recurrence can be determined provided that the rank function of any integral recurrence can be determined in the following two cases*:

Case 1. *p odd, Q and P units*;

Case 2. *p even, Q a unit, P a unit, or double a unit.*

III. Properties of the root field

6. Let α and β denote the roots of $f(z)$, distinct and nonzero by (4.2), and let $\mathfrak{R}_p$ denote the root field $R_p(\alpha, \beta)$. Then $\mathfrak{R}_p$ is either R_p or the simple quadratic extension $R_p(\sqrt{D})$ according as D is or is not a square in R_p. If

p is a discriminantal divisor, $d = \phi(D)$ is positive. p ramifies in $\mathfrak{R}_p$ if and only if d is odd. If p is not a discriminantal divisor, it is said to be ordinary. In particular, two is ordinary if and only if P is a dyadic unit.

Let $\pi = p$ or $\sqrt{p}$ according as p is unramified or ramified, and let $e = \phi(\pi)$ be 1 or $\frac{1}{2}$ accordingly. Every element $\xi \neq 0$ of $\mathfrak{R}_p$ may be uniquely represented as a series in π:

$$\xi = \sum_N^\infty \rho_n \pi^n, \qquad \rho_N \neq 0, \quad N > -\infty,$$

whose coefficients ρ_n are either zero or roots of unity in $\mathfrak{R}_p$.

We define $\phi(\xi) = Ne$ as the value of ξ in $\mathfrak{R}_p$. ξ is a unit if $\phi(\xi) = 0$ and a principal unit when p is odd if $\phi(\xi) = 0$ and $\rho_0 = 1$. If p is even, we require in addition for principal units that $\rho_1 = 0$ if p is unramified, and $\rho_1 = \rho_2 = \rho_3 = 0$ if p is ramified. Thus when $p = 2$ and ξ is a principal unit,

$$\phi(\xi - 1) \geqq 2.$$

Every unit u of $\mathfrak{R}_p$ may be written uniquely as

$$u = \zeta\psi. \tag{6.1}$$

Here ζ is a root of unity, and ψ is a principal unit. If p is odd, ζ is either a $(p-1)^{\text{st}}$ or $(p^2-1)^{\text{st}}$ root of unity. If p is even, ζ is a twelfth root of unity. The order of ζ, that is, the least positive integer n such that $\zeta^n = 1$, is called the order of the unit u. If the order is r, ζ is said to be a primitive r^{th} root of unity. Thus a principal unit is of order one. We shall make repeated use of the following simple lemma.

LEMMA 6.1. *With the notations of formula* (6.1), *if* $u_1 = \zeta_1\psi_1$ *and* $u_2 = \zeta_2\psi_2$ *are units of* $\mathfrak{R}_p$, *then* $u_1 \equiv u_2 \pmod{\pi}$ *if and only if* $\zeta_1 = \zeta_2$.

By $\xi \equiv \eta \pmod{\pi}$ we mean as usual that the p-adic value of $\xi - \eta$ in $\mathfrak{R}_p$ is positive.

7. If ψ is a principal unit, we define the logarithm of ψ by the formula

$$\log\psi = -\sum_{n=1}^\infty (1-\psi)^n/n. \tag{7.1}$$

Then $\log\psi = \psi - 1 + (\psi - 1)\tau$ where $\phi(\tau) > 0$. Consequently

$$\phi(\log\psi) = \phi(\psi - 1) > 0. \tag{7.2}$$

We call the value of $\log\psi$ or of $\psi - 1$ the *logarithmic value* of the principal unit ψ. Note that when p is two, the logarithmic value of ψ is at least two.

The exponential function e^θ is defined for all θ with $\phi(\theta) > 0$ by

$$e^\theta = \sum_0^\infty \theta^n/n!,$$

and

$$e^{\log\psi} = \psi. \tag{7.3}$$

We shall make repeated use of the elementary formulas

$$\log(\psi_1\psi_2) = \log\psi_1 + \log\psi_2, \qquad \log(\psi_1/\psi_2) = \log\psi_1 - \log\psi_2.$$

Finally if ν is any integer of $\mathfrak{R}_p$, we define ψ^ν to mean $e^{\nu \log \psi}$. Thus

$$\log \psi^\nu = \nu \log \psi. \tag{7.4}$$

(7.2) and (7.3) give the useful lemma

LEMMA 7.1. *If ψ is a principal unit of $\mathfrak{R}_p$ and ν is any integer of $\mathfrak{R}_p$, then the logarithmic value of ψ^ν is given by the formula*

$$\phi(\log \psi^\nu) = \phi(\nu \log \psi) = \phi(\psi^\nu - 1) = \phi(\nu) + \phi(\psi - 1). \tag{7.5}$$

IV. The zeros mod p of integral recurrences

8. If the rank function (w) of (W) is bounded, we say that (W) has bounded zeros. Let

$$\begin{aligned} \Phi &= \Phi(z, w) = z^2 - Pzw + Qw^2, \\ \Psi &= \Psi(z, w; z', w') = zz' - (P/2)(zw' + z'w) + Qww' \end{aligned} \tag{8.1}$$

denote the quadratic and bilinear forms associated with the polynomial $f(z)$. We call the p-adic integer $\Phi(W_1, W_0)$ the invariant of the recurrence (W). It is easily shown that

$$\Phi(W_{n+1}, W_n) = Q^n \Phi(W_1, W_0). \tag{8.2}$$

Hence the p-adic value of $\Phi(W_{n+1}, W_n)$ is independent of n.

THEOREM 8.1. *Let (W) be an integral recurrence. Then a sufficient condition that all terms of (W) are units is that the invariant of (W) be a multiple of p.*

It follows that a necessary condition that (W) have zeros is that the invariant of (W) be a unit. This condition always holds if $\mathfrak{R}_p$ is a quadratic extension of R_p, and in particular when p is two and P and Q are odd.

Proof. Since (W) is an integral recurrence, not both W_0 and W_1 are divisible by p. Hence since Q is always a unit, $\Phi(W_1, W_0) \equiv 0 \pmod{p}$ implies that both W_0 and W_1 are units. It follows by induction from (8.2) that W_n is a unit for every n.

For example, the invariant of the Lucas function $S_n = \alpha^n + \beta^n$ is D. Consequently (S) has no zeros modulo p if p is a discriminantal divisor.

Let (V) be a second integral recurrence belonging to $f(z)$ with initial values V_0 and V_1. Then it is easily shown that

$$\Psi(W_{n+1}, W_n ; V_{n+1}, V_n) = Q^n \Psi(W_1, W_0 ; V_1, V_0). \tag{8.3}$$

If $\Psi(W_1, W_0 ; V_1, V_0) = 0$, we say that (W) and (V) are *polar sequences*. We develop the properties of polar sequences in Chapter VI. If (W) is self-polar, it satisfies a recurrence of order one, and the determination of (w) is trivial.

V. The rank function for ordinary primes

9. Let (W) be an integral recurrence satisfying the conditions of Theorem 5.1 whose invariant is a unit of R_p, and assume that p is ordinary and hence

unramified in $\mathfrak{R}_p$. If p is two, this entails P and Q both odd.

The general term of (W) may be written

$$W_n = (\mathrm{A}\alpha^n - \mathrm{B}\beta^n)/(\alpha - \beta), \tag{9.1}$$

where

$$\mathrm{A} = W_1 - W_0\beta, \qquad \mathrm{B} = W_1 - W_0\alpha \tag{9.2}$$

are both integers in $\mathfrak{R}_p$. It follows from (8.1) and (9.2) that

$$\mathrm{AB} = \Phi(W_1, W_0).$$

Consequently, *both* A *and* B *are units in* $\mathfrak{R}_p$. We may therefore write with the notation of formula (6.1)

$$\mathrm{A}/\mathrm{B} = \rho_2\psi_2. \tag{9.3}$$

Since both $\alpha + \beta$ and $\alpha\beta$ are units in R_p, *both* α *and* β *are units in* $\mathfrak{R}_p$. Consequently

$$\beta/\alpha = \rho_1\psi_1. \tag{9.4}$$

Furthermore $\rho_1 \neq 1$ since $\phi(\alpha - \beta)^2 = \phi(D) = 0$. Let A/B be of order s, and β/α of order r. These orders have an interesting arithmetical interpretation. For let (L) denote the p-adic Lucas recurrence of $f(z)$ defined by $L_0 = 0$, $L_1 = 1$ so that $\mathrm{A} = \mathrm{B} = 1$, and $L_n = (\alpha^n - \beta^n)/(\alpha - \beta)$.

Since α, β, and $\alpha - \beta$ are all units, $l_n = \phi(L_n) = \phi((\beta/\alpha)^n - 1)$. Hence the value l_n is zero if r does not divide n.

Consequently r is the first zero of (L) mod p, or the rank of apparition of p in (L), and l_r is the logarithmic value of the principal unit ψ_1^r.

THEOREM 9.1. *The rank of apparition of* p *in* (L) *divides* $p - (D/p)$.

Here (D/p) is 1 if D is a square in R_p, and -1 if D is not a square.

It is shown in the next chapter that this theorem is also true when p divides D if we then let $(D/p) = 0$.

Proof. If $(D/P) = +1$, p is odd and $\mathfrak{R}_p = R_p$. Consequently

$$\alpha^{p-1} \equiv \beta^{p-1} \pmod{p}, \qquad L_{p-1} \equiv 0 \pmod{p},$$

and r divides $p - 1$.

If $(D/p) = -1$, $\mathfrak{R}_p$ is a quadratic extension of R_p. Let $\mathfrak{I}_p$ be the ring of integers of $\mathfrak{R}_p$. Then $\mathfrak{I}_p/(\pi)$ is isomorphic to the finite field of order p^2. Consequently

$$\alpha^p \equiv \beta, \quad \beta^p \equiv \alpha \pmod{\pi}, \qquad L_{p+1} \equiv 0 \pmod{\pi}, \qquad L_{p+1} \equiv 0 \pmod{p},$$

and r divides $p + 1$, which completes the proof.

If $g(z)$ denotes the polynomial $(z - \mathrm{A})(z - \mathrm{B}) = z^2 - P'z + Q'$ where $P' = 2W_1 - PW_0$ and $Q' = W_1^2 - PW_1W_0 + QW_0^2$ are in R_p with Q' a unit, then s is the rank of apparition of p in the Lucas recurrence (L') of $g(z)$ de-

fined by

$$L'_n = (A^n - B^n)/(A - B). \tag{9.5}$$

Now by (9.1), (9.3), and (9.4),

$$W_n = (B\alpha^n/(\alpha - \beta))\{\rho_2 \psi_2 - \rho_1^n \psi_1^n\}. \tag{9.6}$$

Here $B\alpha^n/(\alpha - \beta)$ is a unit in $\mathfrak{R}_p$. Consequently by Lemma 6.1, $W_n \equiv 0 \pmod{p}$ if and only if $\rho_2 = \rho_1^n$.

LEMMA 9.1. *If ρ_1 and ρ_2 are roots of unity in $\mathfrak{R}_p$ of orders r and s, then there exists a positive integer n such that $\rho_2 = \rho_1^n$ if and only if s divides r.*

Proof. The lemma is evident, since the roots of unity in $\mathfrak{R}_p$ form a finite cyclic group.

We may thus state

THEOREM 9.2. *If (W) is an integral sequence and p is an ordinary prime, the sequence (W) has zeros if and only if the rank of apparition of p in (L') divides the rank of apparition of p in (L).*

This theorem along with Theorem 10.1 contains as a special case results obtained by Ward [5] and Hall [1] for rational integral sequences by more involved methods.

It follows that if (W) has zeros mod p, they lie in an arithmetical progression of constant difference r. There is no essential loss in generality in assuming then that $W_0 \equiv 0 \pmod{p}$. Then by formula (9.1) $w_0 = \phi(W_0) = \phi(A/B - 1) > 0$. Thus in formula (9.3), ρ_2 is 1, A/B is a principal unit, and $\phi(W_n) = 0$ unless r divides n.

THEOREM 9.3. *If p is an ordinary prime and (W) is an integral recurrence with $W_0 \equiv 0 \pmod{p}$, then the zeros of (W) are bounded if the p-adic value of W_0 is less than the p-adic value of L_r. Here r is the rank of apparition of p in the Lucas sequence (L).*

The value function (w) of (W) is then given by the formulas

$$w_n = 0, \quad n \not\equiv 0 \pmod{r}; \qquad w_n = w_0, \quad n \equiv 0 \pmod{r}.$$

This case is definitely exceptional, since the usual value for l_r will be one; it is however worth noting that P and Q can be chosen so that l_r is as large as we please.

Proof. Since A and B are units, w_0 is the logarithmic value of A/B. Similarly l_r is the logarithmic value of $(\beta/\alpha)^r$. Under the hypotheses of the theorem, one obtains from (9.6)

$$W_{rn} = (B\alpha^{rn}/(\alpha - \beta))((A/B - 1)((\beta/\alpha)^{rn} - 1)).$$

Here $B\alpha^{rn}/(\alpha - \beta)$ is a unit, and by formula (7.1),

$$\phi(A/B - 1) < \phi((\beta/\alpha)^{rn} - 1).$$

Consequently $w_{rn} = \phi(W_{rn}) = \phi(\mathrm{A}/\mathrm{B} - 1) = w_0$. The determination of (w) follows immediately, completing the proof.

10. We come now to the case of real interest when $w_0 \geqq l_r$. Then A/B and $(\beta/\alpha)^r$ are both principal units, and we may write

$$(10.1) \qquad (\beta/\alpha)^r = \psi_1, \qquad \mathrm{A}/\mathrm{B} = \psi_2, \qquad \phi(\log \psi_2) \geqq \phi(\log \psi_1).$$

Consequently

$$(10.2) \qquad \nu = (\log \psi_2)/(\log \psi_1)$$

is an integer of $\mathfrak{R}_p$.

LEMMA 10.1. *ν is an integer of R_p.*

Proof. We need consider only the case when $\mathfrak{R}_p$ is a quadratic extension of R_p. Then $\mathfrak{R}_p$ is normal over R_p with a Galois group of order two. Let $\bar{\xi}$ denote the result of applying the generating automorphism of the group to any element ξ of $\mathfrak{R}_p$. Then ξ is in R_p if and only if $\bar{\xi} = \xi$.

Now $\bar{\alpha} = \beta, \bar{\beta} = \alpha$, so that by (9.2), $\bar{\mathrm{A}} = \mathrm{B}, \mathrm{B} = \mathrm{A}$. Consequently $\bar{\psi}_1 = \psi_1^{-1}$ and $\bar{\psi}_2 = \psi_2^{-1}$. But by formula (7.1), if ψ is a principal unit, $\overline{\log \psi} = \log \bar{\psi}$. Hence by formula (10.2),

$$\bar{\nu} = (\log \bar{\psi}_2)/(\log \bar{\psi}_1) = (-\log \psi_2)/(-\log \psi_1) = \nu,$$

which completes the proof.

It follows from this lemma and the results of Section 7 that

$$(10.3) \qquad \psi_2 = \psi_1^{\nu}, \qquad \nu \text{ an integer of } R_p.$$

Hence by formulas (9.6) and (10.1),

$$W_{mr} = \frac{\mathrm{B}\alpha^{mr}}{\alpha - \beta}\{\psi_2 - \psi_1^m\} = \frac{\mathrm{B}\alpha^{mr}}{\alpha - \beta}\psi_1^m\{\psi_1^{\nu - m} - 1\}.$$

Now $\mathrm{B}\alpha^{mr}\psi_1^m/(\alpha - \beta)$ is a unit. Hence by Lemma 7.1

$$w_{mr} = \phi(W_{mr}) = \phi(\psi_1^{\nu - m} - 1) = \phi(\nu - m) + \phi \log \psi_1 = \phi(\nu - m) + l_r.$$

We have thus proved the following result:

THEOREM 10.1. *Under the hypotheses:*

(i) *(W) is integral and its associated polynomial $z^2 - Pz + Q$ has unit coefficients and distinct roots,*
(ii) *p is not a discriminantal divisor,*
(iii) $W_0 \equiv 0 \pmod{p}$, $W_1 \not\equiv 0 \pmod{p}$,
(iv) $w_0 = \phi(W_0) \geqq l_r = \phi(L_r)$,

the value function (w) of (W) is given by the formula

$$(10.4) \qquad w_n = 0 \qquad \text{if} \quad n \not\equiv 0 \pmod{r},$$

$$w_n = \phi(\nu - n/r) + l_r \qquad \text{if} \quad n \equiv 0 \pmod{r}.$$

Here ν is the p-adic integer

$$\log\{(W_1 - W_0\beta)/(W_1 - W_0\alpha)\} - \log\{\alpha^r/\beta^r - 1\}.$$

It will be recalled that r is the rank of apparition of p in the Lucas recurrence (L).

VI. The value function for discriminantal divisors

11. There remains the case when p is a discriminantal divisor, so that $(\alpha - \beta) \equiv 0 \pmod{\pi}$. Then β/α is a principal unit in $\mathfrak{R}_p$, and we may write

$$\beta/\alpha = \psi_1, \tag{11.1}$$

which is simply formula (10.1) with $r = 1$. Now $W_0 = (\mathrm{A} - \mathrm{B})/(\alpha - \beta)$ is an integer, so that A/B is also a principal unit in $\mathfrak{R}_p$, say

$$\mathrm{A}/\mathrm{B} = \psi_2. \tag{11.2}$$

Evidently $\phi(\log \psi_2) \geqq \phi(\log \psi_1)$, so that

$$\nu = (\log \psi_2)/(\log \psi_1) \tag{11.3}$$

is an integer in $\mathfrak{R}_p$. Hence Lemma 10.1 applies, and ν is an integer in R_p. Hence proceeding as in Section 10,

$$W_{mr} = L_r\left(\frac{\mathrm{A}\alpha^{rm} - \mathrm{B}\beta^{rm}}{\alpha^r - \beta^r}\right).$$

For p is a discriminantal divisor for the polynomial $(z - \alpha^r)(z - \beta^r)$.

On the other hand the case when p is a discriminantal divisor may be included in the previous case by taking $r = 1$ when $L_1 = 1$, so that $l_1 = 0$ and $W_{mr} = W_n$.

The results of this section and Theorems 8.1 and 9.2 give the following criteria for the value function of (W) to be unbounded.

THEOREM 11.1. *Necessary and sufficient conditions that an integral recurrence (W) have unbounded zeros are*

(i) $W_1^2 - PW_1W_0 + QW_0^2$ *is a unit of* R_p, *and either*

(ii) p *is a discriminantal divisor of* $z^2 - Pz + Q$, *or*

(iii) p *is ordinary, and* $(W_1 - \beta W_0)/(W_1 - \alpha W_0)$ *is a unit in* $\mathfrak{R}_p$ *whose order divides the order of the unit* β/α.

It is convenient finally to state the results obtained on the rank function as a separate theorem.

THEOREM 11.2. *If p is a discriminantal divisor of $f(z)$, every integral recurrence belonging to $f(z)$ has unbounded zeros. Furthermore*

$$\nu = \log\{(W_1 - W_0\beta)/(W_1 - W_0\alpha)\} - \log\{\beta/\alpha - 1\}$$

is a p-adic integer, and the rank function (w) of (W) is given by the formula

$$w_n = \phi(\nu - n).$$

If we define r in formula (10.4) to be one when p is a discriminantal divisor, the last statement of Theorem 11.2 is a special case of formula (10.4); for since $L_1 = 1$, $l_r = 0$ when $r = 1$.

The law of repetition for powers of primes stated in the introduction follows immediately.

VII. The determination of a sequence by its zeros

12. If p is odd, the law of repetition of p in (W) essentially determines (W). More precisely, we have the following theorem.

THEOREM 12.1. *Let p be an odd prime, and let ν be an arbitrarily chosen integer of $\mathfrak{I}_p$. Then there exists an integral recurrence (W) whose rank function (w) is given by formula* (10.4). *Furthermore (W) is uniquely determined by (w) up to a unit factor.*

Proof. Let r be one if p is a discriminantal divisor, and otherwise let r be the rank of p in (L). Then

$$\psi_1 = (\beta/\alpha)^r$$

is a principal unit. Let ν be an element of $\mathfrak{I}_p$. Then $\frac{1}{2}\nu$ and $-\frac{1}{2}\nu$ are also in $\mathfrak{I}_p$. Consequently

$$\mathrm{A} = \psi_1^{1/2}, \qquad \mathrm{B} = \psi_1^{-1/2}$$

are both units in $\mathfrak{R}_p$, and

$$\mathrm{A}/\mathrm{B} = \psi_1, \qquad \mathrm{AB} = 1. \tag{12.1}$$

Now let

$$W_n = (\mathrm{A}\alpha^n - \mathrm{B}\beta^n)/(\alpha - \beta) \qquad (n = 0, 1, \cdots).$$

Then (W) is easily seen to satisfy the conditions of the theorem. But if (W') were a second such sequence, by the results of Section 10, we would have, with an obvious notation, $\mathrm{A}'/\mathrm{B}' = \mathrm{A}/\mathrm{B}$ and $\mathrm{A}'\mathrm{B}'$ a unit of $\mathfrak{I}_p$. Hence, $\mathrm{A}'/\mathrm{A} = \mathrm{B}'/\mathrm{B}$ is a unit c of $\mathfrak{I}_p$. Thus $W'_n = cW_n$.

A similar result holds when p is two if ν is even. But if ν is odd, (12.1) does not determine A and B.

VIII. Polar sequences

13. With the terminology of Section 8, let (W) and (V) be polar sequences. Then by formulas (8.1), (8.2), and (8.3)

$$W_{n+1}V_{n+1} - (P/2)(W_{n+1}V_n + W_nV_{n+1}) + QW_nV_n = 0. \tag{13.1}$$

We shall assume throughout the discussion that either p is odd, P, W both units, or p is even, P is not a unit and Q a unit. Thus $P/2$ on the right of (13.1) is integral. We shall also assume that at least one of W_0, W_1 and one of V_2, V_1 is a unit. Consequently in neither (W) nor (V) can two consecutive terms be divisible by p.

LEMMA 13.1. *Two polar sequences can have no common zeros modulo p.*

For if (W) and (V) are polar and $W_n \equiv V_n \equiv 0 \pmod{p}$, then by (13.1), $W_{n+1} V_{n+1} \equiv 0 \pmod{p}$, so that either (W) or (V) has consecutive zeros.
Let

$$W_n = (\mathrm{A}\alpha^n - \mathrm{B}\beta^n)/(\alpha - \beta), \qquad V_n = (\Gamma\alpha^n - \Delta\beta^n)/(\alpha - \beta),$$

and as in Section 9, let

$$\beta/\alpha = \rho_1 \psi_0, \qquad \mathrm{A}/\mathrm{B} = \rho_2 \psi_2, \qquad \Gamma/\Delta = \rho_3 \psi_3, \tag{13.2}$$

where ψ_0, ψ_2, ψ_3 are principal units, ρ_1, ρ_2, ρ_3 are roots of unity, and the order r of ρ_1 is the rank of p in (L). With a prior notation,

$$(\beta/\alpha)^r = \psi_0^r = \psi_1. \tag{13.3}$$

It is easily shown (Section 8) that the invariants and polar form of (W) and (V) are given by the formulas

$$\Phi(W_1, W_0) = \mathrm{AB}, \qquad \Phi(V_1, V_0) = \Gamma\Delta,$$

$$\Psi(W_1, W_0; V_1, V_0) = \mathrm{A}\Delta + \mathrm{B}\Gamma. \tag{13.4}$$

It follows that (W) *and* (V) *are polar if and only if*

$$\rho_2 = -\rho_3, \qquad \psi_2 = \psi_3. \tag{13.5}$$

The next lemma is a simple consequence of (13.4).

LEMMA 13.2. *If (W) and (V) are polar sequences with unit invariants, and if $W_n = (\mathrm{A}\alpha^n - \mathrm{B}\beta^n)/(\alpha - \beta)$, then V_n may be put in the form*

$$V_n = C(\mathrm{A}^n + \mathrm{B}^n) \tag{13.6}$$

where C is a unit of R_p. Consequently all sequences (V) with unit invariant polar to (W) have the same rank function.

If k_2 and k_3 are the orders of ρ_2 and ρ_3, (13.5) implies that $k_2 k_3$ is even; k_1 divides $2k_j$; if k_i is even, k_j divides k_i. Here $i, j = 2$ or 3. We thus obtain the following restrictions on k_2 and k_3:

(13.7)
(i) k_2, k_3 are not both odd.
(ii) $k_2 \equiv 0 \pmod{4} \iff k_3 \equiv 0 \pmod{4} \iff k_2 = k_3$.
(iii) $k_i \equiv 2 \pmod{4} \iff k_j$ odd and $k_i = 2k_j$, $i, j = 2$ or 3.

THEOREM 13.1. *If (W) and (V) are polar, and p is a discriminantal divisor, at most one of (W) and (V) has zeros modulo p.*

Proof. In view of Theorem 8.1, it suffices to show that the hypotheses imply that not both of the invariants of (W) and (V) are units. In the contrary case, A, B, Γ, and Δ are units in R_p. But since W_0 and V_0 are both integers and π divides $\alpha - \beta$, π divides $\mathrm{A} - \mathrm{B}$ and $\Gamma - \Delta$. Hence both A/B and Γ/Δ are principal units, so that $\rho_2 = \rho_3 = 1$, contradicting (13.5).

A simple illustration is the polar pair of Lucas sequences (L) and (S) whose invariants are 1 and D respectively.

14. We assume from now on that p is not a discriminantal divisor. By Lemma 9.1 and Theorem 9.2, (W) has zeros if and only if k_2 divides r, *and* similarly for (V). Hence we have by (13.7)

LEMMA 14.1. *If the rank of p in (L) is odd, at most one of a pair of polar sequences can have zeros; if the rank is even, either both polar sequences have zeros, or neither has zeros.*

It follows from formula (13.6) that

$$L_n V_n = CW_{2n} - CQ^n W_0 . \tag{14.1}$$

Now assume that (W) has zeros modulo p, and that the rank r of p in (L) is even. We may also assume that $W_0 \equiv 0 \pmod{p}$. Since $W_r \equiv 0 \pmod{p}$, on taking $n = r/2$ in (14.1) we see that $V_{r/2} \equiv 0 \pmod{p}$. *Thus all the zeros of (V) lie in an arithmetical progression of constant difference r and initial value $r/2$*; that is, the zeros of (V) are all odd multiples of $r/2$. In the special case when P and Q are rational integers and $(W) = (L)$, $(V) = (S)$, this is Lucas's law of apparition of primes in (S).

We conclude by determining the law of repetition for (V). Since $W_0 \equiv 0 \pmod{p}$ and $V_{r/2} \equiv 0 \pmod{p}$, we have $A/B = \psi_2$, $(\beta/\alpha)^{r/2} = -\psi_4$ where ψ_4 is a unit. Evidently $\psi_1 = \psi_4^2$ where ψ_1 is given by (13.3). Then proceeding as in Section 10, if $\nu = (\log \psi_2)/(\log \psi_1)$ and $\mu = (\log \psi_2)/(\log \psi_4)$, $\mu = 2\nu$. Thus we have as a consequence of Theorem 10.1

THEOREM 14.1. *If the rank r of p in (L) is even and (W) has zeros, then under the hypotheses of Theorem* 10.1, *the value function (v) of any sequence (V) with unit invariant polar to (W) is given by the formulas*

$$v_n = 0 \qquad \text{if} \quad n \not\equiv r/2 \pmod{4},$$

$$v_n = \phi(2\nu - (2n - r)/2r) + l_r \qquad \text{if} \quad n \equiv r/2 \pmod{r}.$$

REFERENCES

1. MARSHALL HALL, *Divisors of second-order sequences*, Bull. Amer. Math. Soc., vol. 43 (1937), pp. 78–80.
2. HELMUT HASSE, *Zahlentheorie*, Berlin, Akademie-Verlag, 1949.
3. D. H. LEHMER, *An extending theory of Lucas' functions*, Ann. of Math. (2), vol. 31 (1930), pp. 419–448.
4. E. LUCAS, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., vol. 1 (1878), pp. 184–240.
5. MORGAN WARD, *Prime divisors of second order recurring sequences*, Duke Math. J., vol. 21 (1954), pp. 607–614.
6. ———, *The laws of apparition and repetition of primes in a cubic recurrence*, Trans. Amer. Math. Soc., vol. 79 (1955), pp. 72–90.

PASADENA, CALIFORNIA