THE LAWS OF APPARITION AND REPETITION OF PRIMES IN A CUBIC RECURRENCE

BY
MORGAN WARD

1. **Introduction.** Let

$$(W): \qquad W_0, W_1, W_2, \cdots, W_n, \cdots$$

be an integral cubic recurrent sequence; that is, the initial values W_0, W_1, W_2 of (W) are integers, and

$$W_{n+3} = PW_{n+2} - QW_{n+1} + RW_n. \tag{1.1}$$

Here P, Q, and R are given integers, and R is not zero.

In this paper we study the distribution of prime divisors and their powers in (W), endeavoring in the terminology of Lucas [1, pp. 209–210] to find their laws of apparition and of repetition. We assume throughout that the characteristic polynomial of the recursion

$$f(z) = z^3 - Pz^2 + Qz - R \tag{1.2}$$

has distinct roots. The earlier results on this topic [2; 3; 4; 5] do not give information on the distribution of multiples of a prime power in (W) save in very special cases.

The detailed plan of the paper is sufficiently indicated by the section headings. The principal new results on the distribution of prime powers are stated as theorems at the end of §§5 and 9 and the beginning of §§6 and 7.

An application of the results of §9 on null divisors is given in §11. (W) and $f(z)$ are said to be "degenerate" if any one of the ratios of the roots of $f(z)$ is a root of unity; otherwise, "nondegenerate." We prove:

THEOREM 1.1. *If the characteristic polynomial of* (W) *is irreducible over the rational field and if the sequence* (W) *is a divisibility sequence; that is,* W_n *divides* W_m *whenever* n *divides* m, *then* (W) *is degenerate and* $W_{n+3} = RW_n$, R *not a cube.*

This theorem completes partial results obtained by Marshall Hall [11] and Ward [12] in which the coefficients of the characteristic polynomial were assumed co-prime.

The paper concludes with a numerical example and mention of some unsolved problems.

2. **Value function of a prime.** Let p be a prime number, and p^{w_n} the highest power of p dividing the term W_n; that is, w_n is the p-adic value of W_n. By

Received by the editors February 1, 1954.

convention $w_n = +\infty$ if $W_n = 0$. We call the sequence of values $w_0, w_1, \cdots$ the *value function* of the prime p on (W). We write w_n or $w(p)$ according as we wish to emphasize the dependence of the value function on n or p.

Although the determination of the value function of a given prime is a problem of fundamental arithmetical importance, very little work has been done on it for recurrences of order greater than two. The results already known which are described in §3 following have been found incidentally in studying the modular periodicity of recurrences.

We shall show that for all except a finite number of primes p, the determination of $w(p)$ may be reduced to the special case when p is an ideal cube. By this we mean a prime p for which there exists a rational integer a not divisible by p such that if α, β, γ are the roots of the characteristic polynomial $f(z)$, then the differences $\alpha - a, \beta - a, \gamma - a$ are divisible by p in the root field of $f(z)$.

If p is an ideal cube, we shall show that its value function may be specified in general as soon as the initial values of (W) are known.

3. **Modular periodicity.** Let D be the discriminant of the characteristic polynomial $f(z) = (z-\alpha)(z-\beta)(z-\gamma)$ of (1.2). Since D is not zero,

$$W_n = A\alpha^n + B\beta^n + C\gamma^n \tag{3.1}$$

where A, B, C are nonzero elements of the root field $\mathfrak{R} = \mathfrak{R}_0[\alpha, \beta, \gamma]$ of $f(z)$. Here and later $\mathfrak{R}_0$ denotes the field of rationals.

Let p be a prime number which does not divide the constant term R of $f(z)$. Then if k is any positive integer, the *restricted period* [2] of $f(z)$ modulo p^k is the least positive value of n such that the congruence

$$\alpha^n \equiv \beta^n \equiv \gamma^n \pmod{p^k}$$

holds in $\mathfrak{R}$. If ρ_k is the restricted period, this congruence holds if and only if ρ_k divides n. Furthermore

$$\alpha^{\rho_k} \equiv \gamma^{\rho_k} \equiv \gamma^{\rho_k} \equiv g \pmod{p^k} \tag{3.2}$$

where g is a rational integer prime to p uniquely determined mod p^k.

Similarly, the *period* μ_k of $f(z)$ is the least positive value of n such that

$$\alpha^n \equiv \beta^n \equiv \gamma^n \equiv 1 \pmod{p^k},$$

and the congruence holds if and only if μ_k divides n. Furthermore $\mu_k = \delta_k \rho_k$, where δ_k is the exponent to which g in (3.2) belongs modulo p^k [3]. (The papers [4] and [5] contain more information on the dependence of μ_k and ρ_k on p, k, and $f(z)$.) The following lemmas summarize results given in [2], [3], and [5].

LEMMA 3.1. *The period and restricted period of $f(z)$ modulo p^k are the period and restricted period of the sequence (L) with initial values $L_0 = 0, L_1 = 0, L_2 = 1$.*

That is, μ_k is the least positive value of m such that $L_{n+m} \equiv L_n \pmod{p^k}$ and ρ_k is the least positive value of m such that $L_{n+m} \equiv gL_n \pmod{p^k}$ with $g \not\equiv 0 \pmod{p}$.

Let $\Delta(W)$ denote the determinant

$$\Delta(W) = \begin{vmatrix} W_0, & W_1, & W_2 \\ W_1, & W_2, & W_3 \\ W_2, & W_3, & W_4 \end{vmatrix}.$$

LEMMA 3.2 [3]. *For every prime p which does not divide $R\Delta(W)$, the period and restricted period of (W) modulo p^k are the period and restricted period of $f(z)$ modulo p^k and hence the same as the corresponding numbers for the recurrence (L).*

Now assume that p does not divide $R\Delta(W)$, and let $\rho = \rho_1$ be the restricted period of $f(z)$ modulo p. By Lemmas 3.1 and 3.2

$$W_{n+\rho} \equiv gW_n \pmod{p}. \tag{3.3}$$

Here g is prime to p and depends only on $f(z)$ and p and not on the sequence (W).

LEMMA 3.3 [3]. *If p is a prime not dividing $R\Delta(W)$, then p is a divisor of (W) if and only if p divides at least one of the first ρ terms $W_0, \cdots, W_{\rho-1}$ of (W).*

If $W_n \equiv 0 \pmod{p}$, $0 \leqq n < \rho$, the index n is called a *rank of apparition* of p in (W).

This lemma is an obviously unsatisfactory test for a divisor, but no other general criterion appears to be known.

Now let p^k be any power of the prime p, when as before $p \nmid R\Delta(W)$. Then by formulas (3.1), (3.2), and Lemma 3.2 there exists an integer $g \not\equiv 0 \bmod p$ such that

$$W_{n+\rho_k} \equiv gW_n \pmod{p^k}. \tag{3.4}$$

Therefore if the p-adic value w_n of W_n is less than k and if $n \equiv r \pmod{\rho_k}$, $0 \leqq r < \rho_k$, then

$$w_n = w_r. \tag{3.5}$$

By a *subsequence* of (W) we shall always understand a sequence (W') of terms of (W) whose indices lie in an arithmetical progression, so that $W'_n = W_{rn+b}$, $r > 1$ and $b \geqq 0$ fixed integers. We call r the order of the subsequence (W'). If $f(z)$ is nondegenerate, that is, if none of the ratios of its roots are roots of unity, the characteristic polynomial of any subsequence (W') has the distinct roots α^r, β^r, γ^r. We shall assume from now on that $f(z)$ is nondegenerate.

It follows from (3.5) that the value function w_n of p is determined for all

indices n such that $W_n \not\equiv 0 \pmod{p^k}$. Furthermore the terms of (W) for which w_n is not determined by (3.5) lie in a finite number of subsequences (W') of order ρ_k.

The value function $w(p)$ is consequently uniformly bounded in n if and only if it is periodic in n. This situation occurs trivially if p divides no term of (W), but it may occur as well in other cases. Whether or not $w(p)$ is bounded for an infinity of primes p appears to be unknown. On the other hand there exist special recurrences, notably the sequence (L) with initial values 0, 0, 1 of Lemma 3.1, for which $w(p)$ is unbounded for every prime p which does not divide R.

4. Classification of prime divisors. We exclude so far as possible trivial divisors dividing every term of (W) by assuming from now on that

$$(W_0, W_1, W_2) = 1. \tag{4.1}$$

We may then classify the primes with respect to the sequence (W) in three ways: first by whether or not they divide the integer $RD\Delta(W)$; secondly, by the behavior of their value functions for large n, and thirdly by the number of consecutive terms of (W) which they divide.

Any prime dividing $RD\Delta(W)$ will be called "exceptional"; under the hypotheses of this paper, there are only a finite number of such primes. All other primes will be called "ordinary."

The complexity of the modular periodicity of (W) for powers of exceptional primes is well known [4; 5]; there is a corresponding complexity in the behavior of the value function of an exceptional prime.

The only types of exceptional primes we shall discuss are the null divisors described in the next paragraph, and odd primes p with restricted period one; that is, primes for which the congruence

$$\alpha \equiv \beta \equiv \gamma \equiv a \pmod{p} \tag{4.2}$$

holds in $\mathfrak{R}$ with a a rational integer prime to p. Such primes are simply the ideal cubes defined in §2. (4.2) evidently implies that

$$f(z) \equiv (z - a)^3 \pmod{p}, \qquad a \not\equiv 0 \pmod{p}, \tag{4.3}$$

but (4.3) does not imply (4.2). If $f(z)$ is irreducible over the rational field $\mathfrak{R}$, (4.3) implies that p is the cube of a prime ideal in $\mathfrak{R}[\alpha]$. We shall continue to refer to any odd prime for which (4.2) holds as an "ideal cube" regardless of the reducibility of $f(z)$. An ideal cube divides D but not R, and divides $\Delta(W)$ if and only if $W_2 - 2aW_1 + a^2W_0 \equiv 0 \pmod{p}$ where a is as in (4.3).

We return now to the other ways of classifying primes in relation to (W). If the value function $w(p)$ is unbounded, p is called a "regular" divisor of (W); otherwise, "irregular." If w_n is positive for all large n, p is called a "null divisor" of (W) [6], and $\lim w_n$ exists. p is a regular null divisor if and only if $\lim w_n = \infty$. Such primes must divide the coefficients P, Q, and R of the re-

currence of (W) [7].

If $\lim w_n$ does not exist, p is a "proper" divisor of (W) and $\limsup w_n > 0$, $\liminf w_n = 0$.

The "multiplicity" of p in (W) is the maximum number of consecutive terms of (W) which p divides. Thus a null divisor is of infinite multiplicity, and a nondivisor is of multiplicity zero. A proper divisor of multiplicity two is called a *maximal divisor* of (W). Maximal prime divisors for a recurrence of any order are studied in [8].

If $W_k \equiv 0$, k is called a "zero" of p in (W). If $W_{k-1}W_{k+1} \not\equiv 0 \pmod{p}$, k is a simple zero of p; if p is maximal and $W_{k-1} \not\equiv 0 \pmod{p}$ but $W_k \equiv W_{k+1} \equiv 0 \pmod{p}$, k is a double zero of p. Thus a proper divisor of multiplicity one has an infinity of simple zeros in (W). An example of such a divisor is given in §12 following. On the other hand a maximal divisor of (W) may also have simple zeros.

The results of this classification are summarized in the following table:

CLASSIFICATION OF PRIME DIVISORS OF (W)

Behavior of value function	Category of prime	Multiplicity
A. $\lim w_n$ exists.	Improper divisor of (W)	
(i) $\lim w_n = 0$	Nondivisor of (W)	Zero
(ii) $\lim w_n = c$, $0 < c < \infty$	Exceptional; Irregular null divisor	Infinite
(iii) $\lim w_n = \infty$	Exceptional; Regular null divisor	Infinite
B. $\lim w_n$ does not exist; $\liminf w_n = 0$; $\limsup w_n > 0$.	Proper divisor of (W)	One or Two
(iv) $\limsup w_n = \infty$	Regular divisor of (W)	Same
(v) $\limsup w_n = c < \infty$ and w_n periodic	Irregular divisor of (W)	Same

5. **Ideal cubes.** Although there exists no general criterion for a prime to be a divisor other than Lemma 3.3, the situation is quite different for an ideal cube. This apparently exceptional case is important for the following reason.

Let p be an odd ordinary prime divisor of (W) with restricted period ρ. Then

$$\alpha^\rho = a + p\alpha_0, \qquad \beta^\rho = a + p\beta_0, \qquad \gamma^\rho = a + p\gamma_0. \tag{5.1}$$

Here α_0, β_0, γ_0 are integers of $\mathfrak{R}$ which we shall specify more exactly in §8, and a is a rational integer prime to p.

Let t be a rank of apparition of p in (W). Then $0 \leqq t < \rho$ and by the congruence (3.3), all other multiples of p appear in subsequences (W') of order ρ,

where $W_n' = W_{n\rho+t}$. If we divide each term of (W') by the greatest common divisor (W_0', W_1', W_2') of its three initial terms, we obtain a new sequence (V) having no trivial divisors. If c is the p-adic value of $(W_t, W_{t+\rho}, W_{t+2\rho})$, then $w_{n\rho+t} = v_n + c$. Here v_n is the p-adic value of V_n.

The characteristic polynomial of (V) $f_\rho(z) = (z-\alpha^\rho)(z-\beta^\rho)(z-\gamma^\rho)$ has distinct roots, since $f(z)$ was assumed to be nondegenerate. But (5.1) evidently implies that p is an ideal cube for the recurrence (V). Hence *the determination of the value functions of ideal cubes determines the value functions of all odd ordinary primes.*

If p is an ideal cube, it follows from the definition that there exists an integer $l \geqq 1$ such that

$$\alpha - a = p^l\alpha_0, \qquad \beta - a = p^l\beta_0, \qquad \gamma - a = p^l\gamma_0 \tag{5.2}$$

where α_0, β_0, γ_0 are algebraic integers of the root field which are not all divisible by p, and a is a rational integer prime to p uniquely determined modulo p^l. The integer l will be called the *order* of the ideal cube. It follows easily from (5.2) that if p is an ideal cube of order l, then

$$f(z) \equiv (z - a)^3 \pmod{p^l}. \tag{5.3}$$

The following lemma may be proved by induction from (3.3).

LEMMA 5.1. *If p is an ideal cube of order l, then there exists a polynomial of degree two*

$$g(z) = Hz^2 + Kz + M \tag{5.4}$$

with integral coefficients uniquely determined modulo p^l such that for every index n,

$$W_n \equiv g(n)a^n \pmod{p^l}. \tag{5.5}$$

The determinant of the first three of these congruences which determine H, K, and M in terms of W_0, W_1, W_2 is $-64a^6$; this is the reason p was assumed odd. Furthermore (H, K, M) is prime to p, and if $\Delta(W)$ is the determinant of Lemma 3.2, then

$$\Delta(W) \equiv -(W_2 - 2aW_1 + a^2W_0)^3 \pmod{p^l},$$
$$2a^2H \equiv W_2 - 2aW_1 + a^2W_0 \pmod{p^l}.$$

Hence $\Delta(W) \equiv 0 \pmod{p}$ if and only if $H \equiv 0 \pmod{p}$. Consequently, if $\Delta(W) \equiv 0 \pmod{p}$, p is a nondivisor of (W) if and only if $K \equiv 0 \pmod{p}$.

To discuss the more interesting case when $\Delta(W) \not\equiv 0 \pmod{p}$, let Φ denote the value which the quadratic form $X^2 + Y^2 + Z^2 - 2YZ - 2ZX - 2XY$ assumes when a^2W_0, $4aW_1$, and W_2 respectively are substituted for X, Y, and Z. Then it may be shown that

$$\Phi \equiv 4a^4(K^2 - 4HM) \pmod{p^l}. \tag{5.6}$$

It is perhaps worth noting that both the coefficients and the determinant of the form are prime to p.

The Legendre symbol $(\Phi|p)$ will be called the "character" of p and denoted by χ or $\chi(p)$. If $\chi=0$, p must divide K^2-4HM. Hence by the remarks above if $\chi=0$, p is a nondivisor of (W) only if $\Delta(W)\equiv 0 \bmod p$. We may thus state the following criteria for an ideal cube to be a nondivisor of (W).

THEOREM 5.1. *An ideal cube p is a nondivisor of (W) if and only if either p divides $\Delta(W)$ and $\chi(p)$ is zero, or p does not divide $\Delta(W)$, and $\chi(p)$ is negative.*

We can also state the laws of apparition for ideal cube in (W).

THEOREM 5.2. *An ideal cube dividing $\Delta(W)$ has precisely one rank of apparition among the first p terms of (W) if its character is not zero. An ideal cube not dividing $\Delta(W)$ has precisely two ranks of apparition if its character is positive, and one rank of apparition if its character is zero.*

THEOREM 5.3. *An ideal cube p is a maximal divisor of (W) if and only if p does not divide $\Delta(W)$ and the number Φ defined above satisfies the congruence*

$$\Phi \equiv 4a^4 \pmod{p}.$$

For later use, we state formally some simple properties of ideal cubes of character zero.

LEMMA 5.2. *Let p be an ideal cube divisor of (W) of character zero, and let t be its rank of apparition in (W). Then if $g'(z)$ denotes the derivative of the polynomial $g(z)$ defined in Lemma 5.1,*

$$W_t \equiv g(t) \equiv 0 \pmod{p} \quad \textit{and} \quad g'(t) \equiv 0 \bmod p. \tag{5.7}$$

6. **Value functions of ideal cubes.** We next determine the form of the value functions and hence the law of repetition in (W) for any ideal cube divisor of (W) not of zero character.

THEOREM 6.1. *Let p be an ideal cube divisor of (W) which is not of zero character. Then there exists at least one and at most two p-adic integers τ of the form*

$$\tau = n_0 + n_1 p + \cdots + n_{k-1}p^{k-1} + \cdots, \qquad 0 \leqq n_{k-1} < p,$$

with the following properties:

(i) *n_0 is a rank of apparition of p in (W), and the remaining n_i are uniquely determined by n_0, p, and (W).*

If $t_0=0$, $t_1=n_0, \cdots, t_k=n_0+n_1p+\cdots+n_{k-1}p^{k-1}, \cdots$ are the successive p-adic approximations to τ, then:

(ii) *$n\equiv t_k \pmod{p^k}$ implies that $W_n\equiv 0 \pmod{p^k}$;*

(iii) *$n\not\equiv t_k \pmod{p^k}$ but $n\equiv t_{k-1} \pmod{p^{k-1}}$ imply that the p-adic value w_n of W_n is precisely $k-1$.*

Proof. For our present purposes, the order of the ideal cube is irrelevant.

We shall accordingly take $l=1$ in (5.5) giving us

$$\alpha - a = p\alpha_0, \qquad \beta - a = p\beta_0, \qquad \gamma - a = p\gamma_0 \tag{6.1}$$

where a is an integer prime to p; α_0, β_0, γ_0 are distinct algebraic integers in the root field with no assumptions made about their divisibility by p. We shall prove Theorem 6.1 by mathematical induction after a series of preliminary lemmas.

LEMMA 6.1. *The elementary symmetric functions P_0, Q_0, and R_0 of α_0, β_0, γ_0 in* (6.1) *are rational integers.*

For they are both algebraic integers and rational numbers.

It follows from well-known results in the algebra of recurring series [8] that

$$\begin{aligned} \alpha_0^r &= T_r^{(0)} + T_r^{(1)}\alpha_0 + T_r^{(2)}\alpha_0^2, \\ \beta_0^r &= T_r^{(0)} + T_r^{(1)}\beta_0 + T_r^{(2)}\beta_0^2, \\ \gamma_0^r &= T_r^{(0)} + T_r^{(1)}\gamma_0 + T_r^{(2)}\gamma_0^2 \end{aligned} \tag{6.2}$$

where the $(T^{(i)})$ are integral cubic recurrences satisfying

$$T_k^{(i)} = P_0T_k^{(i)} - Q_0T_k^{(i)} + R_0T_k^{(i)}$$

with initial values $T_k^{(i)} = \delta_{ik}$ $(i, k = 0, 1, 2)$; δ_{ik} a Kronecker delta.

LEMMA 6.2. *If r and t are any integers $\geqq 0$ and if $W_t^{(r)}$ is defined by*

$$W_t^{(r)} = \sum_{\alpha} A\alpha^t\alpha_0^r = A\alpha^t\alpha_0^r + B\beta^t\beta_0^r + C\gamma^t\gamma_0^r \tag{6.3}$$

where A, B, C are as in the formula (3.1) *for W_n, then*

$$W_t^{(0)} = W_t; \quad pW_t^{(1)} = W_{t+1} - aW_t; \quad p^2W_t^{(2)} = W_{t+2} - 2aW_{t+1} + a^2W_t \tag{6.4}$$

are integers. Furthermore $p^2W_t^{(r)}$ is always an integer.

(6.4) follows immediately from the definition (6.3) and the formulas (6.1). To prove the last statement, note that (6.3) and (6.2) give

$$\begin{aligned} W_t^{(r)} &= \sum_{\alpha} A\alpha^t(T_r^{(0)} + T_r^{(1)}\alpha_0 + T_r^{(2)}\alpha_0^2) \\ &= T_r^{(0)}W_t^{(0)} + T_r^{(1)}W_t^{(1)} + T_r^{(2)}W_t^{(2)}. \end{aligned}$$

Hence $p^2W_t^{(r)}$ is integral by (6.4).

The next lemma is a simple consequence of congruence (5.6) of Lemma 5.1.

LEMMA 6.3. *If p is an ideal cube and t is any integer, then*

$$W_{t+1} - aW_t \equiv a^{t+1}\left(g'(t) + \frac{g''(t)}{2}\right) \pmod{p},$$

$$W_{t+2} - 2aW_t + a^2W_t \equiv a^{t+2}g''(t) \pmod{p}$$

where $g'(z)$, $g''(z)$ are the first and second derivatives of the polynomial $g(z)$ of Lemma 5.1.

LEMMA 6.4. *If p is an ideal cube greater than three, k a positive integer, x and t non-negative integers, then*

$$W_{xp^k+t} \equiv a^{xp^k}\{W_t + xp^k a^t g'(t)\} \bmod p^{k+1}. \tag{6.5}$$

This congruence is the basis for the inductive proof of Theorem 6.1. It may be proved as follows: By the formulas (3.1) and (6.1), (6.3):

$$W_{xp^k+t} = \sum_\alpha A\alpha^t\alpha^{xp^k} = \sum_\alpha A\alpha^t(a + p\alpha_0)^{xp^k} = \sum_\alpha \sum_r A\alpha^t \binom{xp^k}{r} a^{xp^k-r}p^r\alpha_0^r$$

$$= \sum_r \sum_\alpha A\alpha^t \binom{xp^k}{r} a^{xp^k-r}p^r\alpha_0^r = \sum_r \binom{xp^k}{r} a^{xp^k-r}p^r W_t^{(r)}.$$

Hence we may write

$$W_{xp^k+t} = \sum_1 + \sum_2 \tag{6.6}$$

where

$$\sum_1 = \sum_{r\geqq 2} \binom{xp^k}{r} a^{xp^k-r}p^r W_t^{(r)}; \qquad \sum_2 = \sum_{r\geqq 3} \binom{xp^k}{r} p^{r-2}a^{xp^k-r}(p^2W_t^{(r)}).$$

We consider these summations in order. By formulas (6.3) and (6.4):

$$\sum_1 = a^{xp^k}W_t + xp^k a^{xp^k-1}(W_{t+1} - aW_t)$$

$$+ \frac{xp^k(xp^k-1)}{1\cdot 2}(W_{t+2} - 2aW_{t+1} + a^2W_t).$$

Hence since $2k\geqq k+1$ we obtain on regrouping terms and simplifying by Lemma 6.3 the congruence

$$\sum_1 \equiv a^{xp^k}\{W_t + xp^k a^t g'(t)\} \pmod{p^{k+1}}. \tag{6.7}$$

Now consider the summation $\sum_2$. By Lemma 6.2, the numbers $p^2W_t^{(r)}$ are all integers, and a is an integer. Hence the p-adic value of the general term of $\sum_2$ is not less than the p-adic value θ of

$$\binom{xp^k}{r} p^{r-2} = \frac{xp^k(xp^k-1)\cdots(xp^k-r+1)}{1\cdot 2\cdots r} p^{r-2}.$$

If $3 \leqq r < p$, $\theta \geqq k+1$ with equality only if $r=3$ and $x \not\equiv 0 \pmod{p}$. (It is at this point that the assumption $p>3$ is vital.) If $r \geqq p$, express r in the scale of p as

$$r = r_0 + r_1 p + \cdots + r_s p^s$$

where the r_i are least positive residues of p. Then $\sum r_n \geqq 1$, and the p-adic value of the denominator of

$$\binom{xp^k}{r} p^{r-2}$$

is exactly $\sum_1^s [r/p^n] = \sum r_n(p^n-1)/(p-1)$.

The p-adic value of the numerator is at least $k+r-2$. Hence:

$$\begin{aligned} \theta &\geqq k + r - 2 - \sum r_n(p^n - 1)/(p-1) \\ &\geqq k + r_0 - 2 + \sum r_n(p^n - (p^n-1)/(p-1)) \\ &\geqq k - 2 + (p-1)\sum r_n \geqq k + p - 3 > k + 1 \end{aligned}$$

since $p \geqq 5$. Thus every term of $\sum_2$ except the first is divisible by p^{k+2}; as for the first term, it is easily seen to be congruent modulo p^{k+2} to $3^{-1}p^{k+1}xP \cdot (p^2 W_t^{(2)})$. Hence by (6.4) and Lemma 6.3,

$$\sum_2 \equiv p^{k+1}xPg''(t)a^{t+2} \pmod{p^{k+2}}. \tag{6.8}$$

The congruence (6.5) now follows immediately from (6.6) and the two congruences (6.7), (6.8). This completes the proof of the lemma.

We now prove Theorem 6.1 as follows: Let p be an ideal cube divisor of (W) greater than three with $\chi(p) \not\equiv 0$, and let n_0 be one of its ranks of apparition. Then by Lemma 5.1,

$$W_{px+n_0} \equiv 0 \pmod{p}; \qquad W_n \not\equiv 0 \pmod{p} \quad \text{if} \quad n \not\equiv n_0 \pmod{p},$$

that is, if $t_1 = n_0$, $n \equiv t_1 \pmod{p}$ *implies that* $W_n \equiv 0 \pmod{p}$; $n \not\equiv t_1 \pmod{p}$ *implies that* $w_n = 0$. Here it is understood that t_1 may be two-valued. Thus the theorem is true if $k=1$. Assume that it is true for any fixed value of $k \geqq 1$. Then multiples of p^{k+1} can appear only among the terms $W_{xp^k+t_k}$ of (W). By Lemma 6.4

$$W_{xp^k+t_k} \equiv a^{xp^k}\{W_{t_k} + xp^k a^{t_k} g'(t_k)\} \pmod{p^{k+1}}.$$

By the hypothesis of the induction, $W_{t_k} = p^k U_k$ where U_k is an integer. Also $g'(t_k) \equiv g'(t_1) \pmod{p}$. Therefore

$$W_{xp^k+t_k} \equiv a^{xp^k} p^k \{U_k + xa^{t_k} g'(t_1)\} \pmod{p^{k+1}}.$$

But $g(t_1) \equiv 0 \pmod{p}$; hence by Lemma 5.2, $g'(t_1) \not\equiv 0 \pmod{p}$; for $\chi(p) \not\equiv 0$.

Since $a \not\equiv 0 \pmod{p}$, it follows that as x runs through a complete residue system modulo p, so does $U_k + xa^{t_k} g'(t_1)$. Hence there exists a least positive

residue n_k of p with the property $W_{xp^k+t_k}\equiv 0 \pmod{p^{k+1}}$ if and only if $n\equiv n_k \pmod{p}$. Otherwise expressed, if t_{k+1} is defined to be $t_{k-1}+n_kp^k$, then $n\equiv t_{k+1} \pmod{p^{k+1}}$ implies $W_n\equiv 0 \pmod{p^{k+1}}$; $n\not\equiv t_{k+1} \pmod{p^{k+1}}$ but $n\equiv t_k \pmod{p^k}$ implies $w_n=k$.

Thus if the theorem is true for k, it is true for $k+1$. But it is true for $k=1$. Hence it is true for all $k\geqq 1$.

7. **Value functions of ideal cubes of zero character.** Let p be an ideal cube greater than three with $\chi(p)=0$ which is a divisor of (W), and let t_0 be its unique rank of apparition in (W). Then $0\leqq t_0<p$ and $W_n\equiv 0 \pmod{p}$ if and only if $n\equiv t_0 \pmod{p}$. Hence

$$w_n = 0,\ n \not\equiv t_0 \pmod{p}. \tag{7.1}$$

On taking $k=1$ and $t=t_0$ in Lemma 6.4, we obtain the congruence

$$W_{px+t_0} \equiv a^{xp}\{W_{t_0} + xpa^{t_0}g'(t_0)\} \pmod{p^2}.$$

Now by Lemma 5.2, $g'(t_0)\equiv 0 \pmod{p}$. Hence

$$W_{px+t_0} \equiv a^{xp}W_{t_0} \pmod{p^2}. \tag{7.2}$$

We may therefore state:

THEOREM 7.1. *If t_0 is the rank of apparition of any ideal cube p greater than three which is of zero character, then a sufficient condition that p be an irregular divisor of (W) is that the p-adic value w_{t_0} of W_{t_0} be one. A necessary condition for p to be a regular divisor of (W) is that w_{t_0} be greater than one.*

If $w_{t_0}=1$, the value function $w(p)$ is periodic in n with period p; for, by (7.1), $w_n=1$, $n\equiv t_0 \pmod{p}$, $w_n=0$, $n\not\equiv t_0 \pmod{p}$.

Assume that $w_{t_0}>1$. Then by the congruence (7.2), $w_n\geqq 2$ if $n\equiv t_0 \pmod{p}$. Consequently if we divide each of the terms of the subsequence W_{pn+t_0} by the greatest common divisor of its first three terms, we obtain an integral cubic recurrence (W') with no trivial divisors whose characteristic polynomial has for its roots $\alpha'=\alpha^p$, $\beta'=\beta^p$, and $\gamma'=\gamma^p$. Now $a'=a^p$ is prime to p, and by formula (6.1),

$$\alpha' - a' = p^2\alpha_0', \qquad \beta' - a' = p^2\beta_0', \qquad \gamma' - a' = p^2\gamma_0'$$

where α_0', β_0', γ_0' are algebraic integers of $\mathfrak{R}$. Thus *p is an ideal cube of order at least two for (W')*. If its character χ_1 in (W') is not zero, there is nothing new to discuss. If $\chi_1=0$, the behavior of p in (V) will be settled by determining how ideal cubes of order $l>1$ of character zero behave in the original sequence (W). Now return to the congruence (5.5) of Lemma 5.1:

$$W_n \equiv (Hn^2 + Kn + M)a^n \pmod{p^l}.$$

Here $H\not\equiv 0 \pmod{p}$ by the remarks preceeding Theorem 5.1. Hence since

$$4HW_n \equiv \{(2Hn + K)^2 + 4HM - K^2\} \pmod{p^l} \tag{7.3}$$

and $4HM-K^2\equiv 0 \pmod{p}$, $W_n\equiv 0 \pmod{p}$ if and only if $2Hn+K\equiv 0 \pmod{p}$. This congruence is always soluble, for $2H$ is prime to p. However, if n is any solution, the p-adic value of $(2Hn+K)^2$ is a positive even number. By (5.6), if the p-adic value of $4HM-K^2$ is less than l, then it is the same as the p-adic value of Φ. We denote this value by q. Evidently $q\geqq 1$. We may therefore state

THEOREM 7.2. *If p is an ideal cube divisor of (W) greater than three of zero character and order l greater than one, and if the p-adic value q defined above is less than l, then a sufficient condition that p be an irregular divisor of (W) is that q be odd.*

Evidently necessary conditions that p be a regular divisor of (W) are either $q\geqq l$, or q even, and less than l. Hence assume that $q=2r<l$, and consider the congruences

$$2Hn + K \equiv 0 \pmod{p^k} \qquad (k = 1, 2, 3, \cdots).$$

Taking $k=1$, there exists a least positive residue m_0 of p such that the p-adic value of $(2Hn+K)$ is greater than zero if and only if $n\equiv m_0 \pmod{p}$. Replacing n by $px+m_0$, there exists a least positive residue m_1 such that the p-adic value of $(2Hn+K)$ is greater than one if and only if $n\equiv pm_1+m_0 \pmod{p^2}$. Proceeding in this manner, we can construct a p-adic integer

$$\mu = m_0 + m_1p + m_2p^2 + \cdots$$

with convergents $\mu_0=0$; $\mu_k=m_0+m_1p+\cdots+m_{k-1}p^{k-1}$, $k\geqq 1$, with the property that the p-adic value of $2Hn+K$ is exactly k if and only if

$$n \equiv \mu_k \pmod{p^k}, \qquad n \not\equiv \mu_{k+1} \pmod{p^{k+1}}. \tag{7.4}$$

Since for this choice of n, the p-adic value of $(2Hn+K)^2$ is evidently $2k$, *the congruence* (7.3) *fixes the p-adic value of W_n for all n incongruent to μ_r modulo p^r*; namely $w_n=2k$ if $k<r$ and $w_n=r$ if $k>r$.

The same reasoning applies if $q\geqq l$ for $2k<l$; namely $w_n=2k$ if $2k<l$, if and only if (7.4) holds.

If however $k=r$ so that the p-adic values of $(2Hn+K)^2$ and $4HM-K^2$ in (7.3) are both equal to q, *then multiples of p^q appear in (W) only among the terms $W_{xp^r+\mu_r}$*. On dividing each of these terms by the greatest common divisor of the three initial terms with $x=0$, 1, and 2, we obtain a new sequence (W') with no trivial divisors for which p is an ideal cube of order $l+r$. In case $q\geqq l$, we obtain similarly a sequence for which p is an ideal cube of order $2l$.

In either case the whole procedure applied to (W) may be repeated for (W') and so on. Evidently what usually happens is that the character of p will be different from zero, but we have been unable to exclude the possibility that there exist sequences (W) for which p is regular, but nevertheless of

zero character in each one of an infinite chain of subsequences $(W)\supset(W')\supset(W'')\cdots$. This then is the only case when the value function of an ideal cube would be indeterminate.

8. **Orders and characters of ordinary primes.** The concepts of the order and character of an ideal prime may be extended to ordinary primes.

If p is an ordinary prime with rank of apparition ρ, then modifying the notation of (5.1) slightly, we may write

$$\alpha^\rho = a + p^l\alpha_0, \qquad \beta^\rho = a + p^l\beta_0, \qquad \gamma^\rho = a + p^l\gamma_0, \qquad l \geqq 1, \tag{8.1}$$

where a is prime to p and α_0, β_0, γ_0 are integers of $\mathfrak{R}$ not all divisible by p. We call the exponent l in (8.1) the order of p.

THEOREM 8.1. *If p is an ordinary prime with restricted period ρ, its order l is the p-adic value of the greatest common divisor of L_ρ and $L_{\rho+1}$ where (L) is the recurrence with initial values* 0, 0, 1.

Thus if $l(p)$ is the value function of (L), l is the minimum of l_ρ and $l_{\rho+1}$.

The theorem follows from the formula

$$\alpha^n = RL_{n-1} + (L_{n+1} - PL_n)\alpha + L_n\alpha^2 \tag{8.2}$$

which holds for any root α of $f(z)$ [9]. For by Lemma 3.1, $L_\rho\equiv L_{\rho+1}\equiv 0 \pmod{p}$ and $L_{\rho-1}\not\equiv 0 \pmod{p}$. Hence on letting $n=\rho$ in (8.2) and comparing with (8.1), we see that $a=RL_{\rho-1}$ and $(L_{\rho+1}-PL_\rho)\alpha+L_\rho\alpha^2\equiv 0 \pmod{p^l}$. Since p is prime to $R=\alpha\beta\gamma$, and α is any one of the three distinct roots of $f(z)$, we deduce that the congruences $L_{\rho+1}-PL_\rho+L_\rho\alpha\equiv L_{\rho+1}-PL_\rho+L_\rho\beta\equiv L_{\rho+1}-PL_\rho+L_\rho\gamma\equiv 0$ must hold in $\mathfrak{R}$ mod p^l, but not mod p^{l+1}. Subtracting the first two, $L_\rho(\alpha-\beta)\equiv 0 \pmod{p^l}$. But since p is ordinary, p is prime to D in the rational field and consequently prime to $\alpha-\beta$ in $\mathfrak{R}$. Hence $L_\rho\equiv 0 \pmod{p^l}$ and $L_{\rho+1}\equiv 0 \pmod{p^l}$. Since these congruences are false mod p^{l+1}, l is the p-adic value of $(L_\rho, L_{\rho+1})$.

Now in analogy with the procedure of §5, let $\Phi(X, Y, Z)$ denote the quadratic form $X^2+Y^2+Z^2-2YZ-2XZ-2XY$ and let $\Phi_{\rho t}$ denote its numerical value when $R^2L_{\rho-1}^2W_t$, $4RL_\rho W_{t+\rho}$ and $W_{t+2\rho}$ each divided by $(W_t, W_{t+\rho}, W_{t+2\rho})$ are substituted for X, Y, and Z respectively. Here t as before is any rank of apparition of p in (W). We then define the *t-character* χ_t of p to be the Legendre symbol $(\Phi_{\rho,t}\,|\,p)$.

If $\chi_t=0$, let $\phi_{\rho t}$ denote the p-adic value of $\Phi_{\rho t}$. Then the theorems of §§5, 6, and 7 may be immediately applied to determining the value function of p in the subsequence (W') defined by $W_n' = W_{n\rho+t}$. A numerical example of the procedure is given in §12 following.

9. **Null divisors.** Since the initial values of (W) are co-prime, a prime dividing almost all W_n must divide R [6]. Consequently, (W) can have only a finite number of null divisors. Regular null divisors divide P, Q, and R but need not divide any initial value, but irregular null divisors must divide

both R and W_2, and may divide either P or Q, but not both. (For necessary and sufficient conditions, see [7]. Irregular null divisors have been studied for linear recurrences of any order in [6] and [7].) The following theorem is a special case of results given in [7].

THEOREM 9.1. *Let p be an irregular null divisor of (W) and let b be the p-adic value of the first elementary divisor of the matrix of the determinant $\Delta(W)$ of Lemma 3.2. Then for all large n, $w_n = c$, where $0 < c \leqq b$.*

b is finite; for $\Delta(W)$ is not zero.

Consider next the regular null divisors of (W), that is the $r \geqq 1$ distinct prime factors $p_1, p_2, \cdots, p_r$ of (P, Q, R).

Let $p = p_r$, and let k, l, m be the p-adic values of P, Q, R. Then

$$P = p^k P_0, \qquad Q = p^l Q_0, \qquad R = p^m R_0 \tag{9.1}$$

where P_0, Q_0, R_0 are prime to p unless P or Q is zero when we take P_0 or Q_0 zero on the corresponding p-adic value as $+\infty$. Also let

$$d = \min \{k, l/2, m/3\}. \tag{9.2}$$

Then we shall prove in the following section

THEOREM 9.2. *Let (W) admit in all $r \geqq 1$ regular null divisors $p_1, p_2, \cdots, p_r$, and let $p = p_r$. Then there exists a set of $c \geqq 1$ integral cubic recurrences*

$$(W'_x) \qquad (x = 0, 1, \cdots, c-1)$$

all satisfying the same recurrence and such that

(i) *The regular null divisors of each recurrence are precisely $p_1, p_2, \cdots, p_{r-1}$;*

(ii) *If $n = ct + x$, $0 \leqq x < c$, then*

$$W_n = p^{\phi_n} W'_{xt}$$

where $\phi_n = s(n-2) + r(t-2)$.

Here s and r are non-negative integers defined along with c, x, and t in terms of n and d of (9.2) as follows:

Form of d	s	c	r	t	x
integer	d	1	0	n	0
$d = l/2$; *fraction*	$[l/2]$	2	1	$[n/2]$	0 *or* 1
$d = m/3$; *fraction*	$[m/3]$	3	1 *or* 2	$[n/3]$	0, 1, *or* 2

Finally, if the characteristic polynomial of (W) is nondegenerate, so is the characteristic polynomial of each sequence (W'_x).

10. Proof of theorem on regular null divisors. With the notation of (9.1) and (9.2) of the preceding section, let $s = [d]$ be the greatest integer in d. Then

$$k' = k - s \geqq 0, \quad l' = l - 2s \geqq 0, \quad m' = m - 3s \geqq 0. \tag{10.1}$$

There are several cases to discuss.

Case 1. $s \geqq 1$; d an integer.

Case 2. $s \geqq 1$; d not an integer.

Case 3. $s=0$, $d=l/2$.

Case 4. $s=0$, $d=m/3$.

In Cases 1 and 2, s is positive, and we let

$$\alpha = p^s\alpha', \qquad \beta = p^s\beta', \qquad \gamma = p^s\gamma',$$

$$(10.2) \quad P' = \alpha' + \beta' + \gamma', \qquad Q' = \alpha'\beta' + \beta'\gamma' + \gamma'\alpha', \qquad R' = \alpha'\beta'\gamma'.$$

Then $P=p^sP'$, $Q=p^{2s}Q'$, and $R=p^{3s}R'$. Hence by (9.1),

$$(10.3) \qquad P' = p^{k'}P_0, \qquad Q' = p^{l'}Q_0, \qquad R' = p^{m'}R_0$$

where k', l', m' are given by (10.1). Thus P', Q', R' are integers whose p-adic values are k', l', m' and α', β', γ' are algebraic integers.

Next let $A'=p^{2s}A$, $B'=p^{2s}B$, $C'=p^{2s}C$ where A, B, C are as in formula (3.1) for W_n, and let $W_n' = A'\alpha'^n + B'\beta'^n + C'\gamma'^n$. Then $W'_{n+3} = P'W'_{n+2} - Q'W'_{n+1} + R'W'_n$ and $W_0' = p^{2s}W_0$, $W_1' = p^sW_1$, $W_2' = W_2$. Consequently (W') *is an integral cubic recurring sequence whose characteristic polynomial is degenerate if and only if the characteristic polynomial of* (W) *is degenerate.* Furthermore by formula (3.1), $W_n = p^{(n-2)s}W_n'$. Consequently the p-adic values $w(p)$ and $w'(p)$ of (W) and (W') are connected by the relation $w_n = (n-2)s + w_n'$.

We now separate Case 1 and Case 2. In Case 1, at least one of k', l', m' in (10.1) is zero. Therefore by comparing the formulas (9.1) and (10.3), we see that in Case 1, $p_r=p$ *is not a regular null divisor of* (W'), *while* $p_1, p_2, \cdots, p_{r-1}$ *are regular null divisors of* (W').

In Case 2, either $d=l/2$, l odd, or $d=m/3$, m not divisible by three. If $d=l/2$, then $l=2s+1$. Consequently l' in (10.3) is one, and $k' \geqq 1$, $m' \geqq 2$. Therefore with an extension of notation, $d'=1/2$ and $s'=0$ for (W'), so that Case 3 following will apply to (W'). If $d=m/3$, then $m=3s+1$ or $3s+2$. Consequently m' in (10.3) is either one or two and $l' \geqq m'$, $2m'$, $k' \geqq m'$. Hence $d'=m'/3$, $s'=0$ and Case 4 following will apply to (W').

Now consider Case 3. Then $k \geqq 1$, $l=1$, $m \geqq 2$.

Now let $\alpha'=\alpha^2$, $\beta'=\beta^2$, $\gamma'=\gamma^2$ and define P', Q', R' as in (10.2) and (10.1) of the previous two cases. Then

$$(10.4) \qquad P' = P^2 - 2Q, \qquad Q' = Q^2 - 2PR, \qquad R' = R^2.$$

Hence $k' \geqq 1$, $l'=2$, and $m' \geqq 4$. Thus $d'=1$ and Case 1 is applicable to any sequence (W_x') with characteristic polynomial $Z^3 - P'z^2 + Q'z - R'$.

Now let

$$A_x' = A\alpha^x, \qquad B_x' = B\beta^x, \qquad C_x' = C\gamma^x, \qquad x = 0 \text{ or } 1,$$

and let

$$W'_{xt} = A'_x\alpha'^t + B'_x\beta'^t + C'_x\gamma'^t \qquad (x = 0 \text{ or } 1;\ t = 0, 1, \cdots).$$

Then if $n=2t+x$, $0\leqq x\leqq 1$, $t=[n/2]$ and $W_n=W'_{xt}$. But it follows from (10.4) that (P, Q, R) and (P', Q', R') have the same prime factors. Thus (W) and (W'_x) have the same regular null divisors.

Since, for each sequence (W), $s'=a'=1$ the results of Case 1 give $W'_{xt}=p^{t-2}W^*_{xt}$ where sequences (W^*_x) have $p_1, \cdots, p_{r-1}$ but not $p_r=p$ as regular null divisors.

Thus changing the notation slightly, we summarize Case 3 by saying that if $n=2t+x$, $0\leqq x\leqq 1$, then

$$W_n = p^{t-2}W'_{xt}, \qquad t = [n/2],$$

where (W_x) has $p_1, p_2, \cdots, p_{r-1}$ as its regular null divisors.

In Case 4, if $m=2$, then $k\geqq 1$, $l\geqq 2$ but if $m=1$, $k\geqq 1$, $l\geqq 1$. In either event we make the substitution $\alpha'=\alpha^3$, $\beta'=\beta^3$, $\gamma'=\gamma^3$ obtaining as in Case 3 three sequences (W'_x) having the same regular null divisors as (W) but to each of which Case 1 is applicable. Evidently in both Case 3 and Case 4 the sequence (W'_x) has nondegenerate characteristic polynomial if (W) has. The details of the proof are similar to those in Case 3; the results are summarized in Theorem 9.1 itself.

11. **Application to cubic divisibility sequences.** We shall next prove Theorem 1.1 of the introduction. Assume that the recurrence (W) is a divisibility sequence; that is W_n *divides* W_m *if* n *divides* m. For brevity we call (W) degenerate or nondegenerate according as its characteristic polynomial is degenerate or nondegenerate. It is easily shown that if (W) is nondegenerate, no term of (W) can vanish except W_0.

By a subsequence of a divisibility sequence (W), we mean a sequence (W') whose general term is of the form $W'_n=W_{kn}/W_k$. Here W_k is any nonzero term of (W). Evidently the subsequences of a divisibility sequence are also divisibility sequences, and if (W) is nondegenerate, so are all its subsequences. Furthermore if the first two initial values of (W) are zero and one [11; 12] every subsequence has the same property.

Now assume that the characteristic polynomial of the divisibility sequence

$$f(z) = z^3 - Pz + Qz - R \tag{1.2}$$

is irreducible over the field of rationals. It is then easily shown that (W) is degenerate if and only if $P=Q=0$ and R is not a perfect cube. In this case $W_{n+3}=RW_n$ and if $W_0=0$, $W_1=1$, then (W) is a divisibility sequence if and only if W_2 divides R.

We shall prove the main part of Theorem 1.1 by showing that the assumption that $f(z)$ is both irreducible and nondegenerate gives a contradiction. We say that a recurrence (W) is "almost always" a divisibility sequence if whenever n divides m, the quotient W_m/W_n is an integer modulo p for all

but a finite number of primes p.

LEMMA 11.1. *If the cubic recurrence* (W) *has no null divisors, and if* (W) *is almost always a divisibility sequence, then the characteristic polynimial of* (W) *is reducible.*

This lemma is substantially due to Marshall Hall [11]; his proof is by contradiction. He assumes $f(z)$ irreducible, and proves that this implies the existence of an infinite number of primes q such that $f(z)$ is irreducible modulo q and

$$W_q^6 \equiv 1 \pmod{q}. \tag{11.1}$$

He then proves that the validity of (11.1) for an infinity of such q implies $f(z)$ reducible.

Hall in [11] actually assumes that (W) is a divisibility sequence, and that the coefficients Q and R of $f(z)$ are co-prime; the only use made of this latter assumption is to show that (W) has no null divisors. It turns out that (11.1) still holds for an infinity of primes q for which $f(z)$ is irreducible under the weaker assumption that (W) is almost always a divisibility sequence. Hence the rest of Hall's proof applies, giving the lemma.

LEMMA 11.2. *If the characteristic polynomial of the cubic recurrence* (W) *has co-prime coefficients and if* (W) *is almost always a divisibility sequence, then* (W) *has an infinite number of subsequences having no null divisors.*

The proof given in [12] for the case when (W) is a divisibility sequence carries over with only slight modification to the present case when (W) is almost always a divisibility sequence.

Now assume that (W) is a divisibility sequence whose characteristic polynomial $f(z)$ is both irreducible and nondegenerate. If the coefficients of $f(z)$ are co-prime, we have an immediate contradiction with Lemmas 11.2 and 11.1. If the coefficients of $f(z)$ are not co-prime, the sequences (W_0') of Theorem 9.1 will be almost always divisibility sequences, satisfying the same conditions as (W). Hence after a finite number of applications of Theorem 9.1, we shall obtain a sequence which is almost always a divisibility sequence whose characteristic polynomial has co-prime coefficients and is both irreducible and nondegenerate, contradicting Lemmas 11.1 and 11.2.

12. **Conclusion—a numerical example.** The determination of the value functions of the exceptional primes not treated in this paper—among which the primes two and three should be included—require an extensive use of ideal theory. It is possible, however, to prove in an elementary way from the results of this paper and a result of Mahler's [14] that *every nondegenerate cubic sequence has an infinite number of prime divisors.* This theorem is already known to be true for quadratic sequences [13].

There are some unsolved problems of interest suggested by the investiga-

tion. Are there sequences with an infinite number of irregular prime divisors? Has every nondegenerate sequence only a finite number of non-divisors? Do there exist ideal cubes which are regular divisors but of zero character in each of an infinite chain of subsequences? What simplifications occur if the characteristic polynomial of the recurrence is irreducible over the rational field or irreducible and normal? Does there exist any other criterion for a divisor than Lemma 3.3? (It is shown in [3] that if ρ is large enough, p will be a divisor.)

As an illustration of the theory, consider the recurrence defined by

$$W_{n+3} = 12W_{n+2} + 5W_{n+1} + 8W_n$$

with initial values 1, 2, and 3. The characteristic polynomial has discriminant $D = 61564 = 2^2 \cdot 15391$ where 15391 is a prime. Since it is irreducible, its group is the symmetric group of order six.

Consider the prime $p = 13$. Then $\Delta(W) \equiv 3 \pmod{13}$. Hence $RD\Delta(W) \not\equiv 0 \pmod{13}$ and p is regular. Since

$$z^3 - 12z^2 - 5z - 8 \equiv (z - 3)(z - 4)(z - 5) \pmod{13}$$

the restricted period ρ of $f(z)$ modulo 13 is a divisor of 12. In fact on computing (W) mod 13, we obtain 1, 2, 3, 2, 3, 5, 0, 10, 4, 7, 2, 0; 1, 2, 3, $\cdots$. Hence $\rho = 12$ and

$$W_{n+12} \equiv W_n \pmod{13}$$

and 13 is a divisor of (W) with the ranks $t = 6$ and $t = 11$.

To find the order of t, we compute $\rho + 2 =$ fourteen terms of the sequence (L): 0, 0, 1, 12, $\cdots$ finding $L_{11} \equiv 148$, $L_{12} \equiv 52$, $L_{13} \equiv 65 \pmod{13^2}$. Hence by the formula (8.2)

$$\alpha^{12} \equiv 1 + 117\alpha + 52\alpha^2 \pmod{169}.$$

Thus 13 is of order one, and again $\rho = 12$. Furthermore

$$a = RL_{\rho-1} \equiv 1 \pmod{169}.$$

Since 13 is of order one, we can compute $\Phi_{\rho t}$ by computing (W) mod 13^2 to find W_t, $W_{t+\rho}$, $W_{t+2\rho}$ and $(W_t, W_{t+\rho}, W_{t+2\rho})$. On carrying out the computations for $t = 6$, $\rho = 12$, we find that

$$W_6 \equiv 13, \qquad W_{18} \equiv 39, \qquad W_{30} \equiv 65 \pmod{13^2}.$$

(In fact $W_{12n+6} \equiv 26n + 13 \pmod{169}$.) Hence $(W_6, W_{18}, W_{30}) \equiv 13 \pmod{13^2}$ so that the initial values of the subsequence (W') with $W_n' = W_{12n+6}$ are congruent modulo 13 to 1, 3, and 5. Thus by formula 8.3,

$$\Phi_{12,6} \equiv 3 \pmod{13}.$$

Consequently, $\chi_{12,6} = (3/13)$ is positive, so that 13 is a regular divisor of

the subsequence (W').

On making similar calculations for the rank $t=11$, we find that $W_{11}\equiv 91$, $W_{23}\equiv 143$, $W_{35}\equiv 26 \pmod{13^2}$ so that in this case $W_0'\equiv 7$, $W_1'\equiv 11$, and $W_2'\equiv 2 \pmod{13}$ giving $\Phi_{12,11}\equiv 1 \pmod{13}$. Hence thirteen is again of positive character and regular in the subsequence (W').

An example of an irregular prime divisor of a sequence is given at the close of [9]; such examples are easily constructed by using the theory developed in §§5 and 6 of this paper.

References

1. E. Lucas, *Theorie des fonctions numeriques simplement periodiques*, Amer. J. Math. vol. 1 (1878) pp. 184–240.

2. P. R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Math. vol. 48 (1920) pp. 343–372.

3. M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*. Trans. Amer. Math. Soc. vol. 33 (1931) pp. 153–165.

4. H. T. Engstrom, *On sequences defined by linear recurrence relations*, Trans. Amer. Math. Soc. vol. 33 (1931) pp. 210–218.

5. M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. vol. 44 (1938) pp. 196–218.

6. M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 600–628.

7. ———, *The null divisors of linear recurring series*, Duke Math. J. vol. 2 (1936) pp. 472–476.

8. ———, *The maximal prime divisors of linear recurrences*, not yet published.

9. E. T. Bell, *Notes on recurring series of the third order*, Tôhoku Math. J. vol. 24 (1924) pp. 168–184.

10. M. Hall, *Divisibility sequences of the third order*, Amer. J. Math. vol. 58 (1936) pp. 577–584.

11. M. Ward, *Linear divisibility sequences*, Trans. Amer. Math. Soc. vol. 41 (1937) pp. 276–286.

12. ———, *The prime divisors of second order recurring sequences*, not yet published.

13. Kurt Mahler, *Eine arithmetical Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Amsterdam Acad. vol. 38 (1935) pp. 50–60.

California Institute of Technology,
Pasadena, Calif.