THE MAXIMAL PRIME DIVISORS OF LINEAR RECURRENCES

MORGAN WARD

1. Introduction. Let

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

be a linear integral recurring sequence of order $r \geqslant 2$; that is, a particular solution of the recurrence

$$\Omega_{n+r} = P_1 \Omega_{n+r-1} + P_2 \Omega_{n+r-2} + \ldots + P_r \Omega_n, \tag{1.1}$$

where $P_1, P_2, \ldots, P_r \neq 0$ are integers, and the initial values $W_0, W_1, \ldots, W_{r-1}$ are integers.

A positive integer m is said to be a *divisor* of (W) if it divides some term W_k with positive index k.

A prime number p is said to be *regular* in (W) if every power of p is a divisor of (W). If only a finite number of powers of p are divisors of (W), p is said to be *irregular*.

If there exist in (W) s consecutive terms divisible by p, say $W_k, W_{k+1}, \ldots, W_{k+s-1}$, but p never divides $s + 1$ consecutive terms of (W), p is said to be a divisor of (W) of order s, and k is said to be a zero of p in (W) of order s. Evidently s must be less than the order r of the recurrence. A prime of order s may have zeros in (W) of order less than s, and may be regular or irregular.

A prime divisor of (W) of the maximum possible order $r - 1$ will be called *maximal*.

I give in this paper a necessary condition that p shall be a maximal prime divisor of (W) under the assumption that the characteristic polynomial

$$f(z) = z^r - P_1 z^{r-1} - \ldots - P_r \tag{1.2}$$

of the recurrence has no repeated roots. When $r = 2$, all prime divisors of (W) which are not null divisors **(1)** are maximal, and the condition reduces to a criterion for a divisor due essentially to Marshall Hall **(2)** which is both necessary and sufficient. But if r is greater than two, the condition is no longer sufficient for p to be maximal in (W). In order for the condition to be sufficient the following additional restrictions on the recurrence and the prime must be made:

(i) $f(z)$ is of odd degree and irreducible;

(ii) The prime p is chosen so that $p - 1$ is prime to the degree r of $f(z)$;

(iii) $f(z)$ is irreducible modulo p.

As is shown in the concluding section of this paper, if these conditions fail to hold, the necessary condition for p to be maximal need no longer be sufficient.

Received October 19, 1953.

https://doi.org/10.4153/CJM-1954-047-9 Published online by Cambridge University Press

It will be evident from the sufficiency proof given under the restrictions just stated that if p is unramified in the root field of $f(z)$, a set of necessary and sufficient conditions can be stated in terms of the exponents to which a certain set of integers belong in the root field modulo all prime ideal factors of p. But these conditions appear too complicated to be of interest, and will not be developed here.

The results of the paper are stated as theorems in §4; the next two sections are devoted to algebraic and arithmetical preliminaries. The proofs are given in §§5, 6 and 7, and the concluding section is devoted to numerical examples.

2. Algebraic preliminaries. Let the characteristic polynomial $f(z)$ of the recurrence have r distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_r$ so that its discriminant D is not zero.

Then the general term of (W) is of the form

$$W_n = \beta_1 \alpha_1^n + \ldots + \beta_r \alpha_r^n \tag{2.1}$$

where the β are elements of the root-field $\mathfrak{R}$ of $f(z)$ to be specified presently.

Let $\Delta(W)$ denote the persymmetric determinant of order r in which the element in the ith row and jth column is W_{i+j-2}. The non-vanishing of $\Delta(W)$ is a necessary and sufficient condition that the recurring sequence (W) be of order r. Thus it easily follows from (2.1) that

$$\beta_1 \ldots \beta_r D = \Delta(W) \neq 0. \tag{2.2}$$

Define r polynomials $f_k(z)$ by $f_0(z) = 1$, $f_k(z) = z^k - P_1 z^{k-1} - \ldots - P_k$ $(k = 1, \ldots, r-1)$. Then the polynomial

$$w(z) = W_0 f_{r-1}(z) + W_1 f_{r-2}(z) + \ldots + W_{r-1} f_0(z)$$

has rational integral coefficients and is of degree less than r. Let

$$\gamma_i = w(\alpha_i) \qquad (i = 1, 2, \ldots, r).$$

Then the γ are integers in the root field $\mathfrak{R}$. Furthermore the polynomial

$$g(z) = (z - \gamma_1) \ldots (z - \gamma_r) = z^r - Q_1 z^{r-1} - \ldots - Q_r \tag{2.3}$$

has rational integral coefficients Q, and as we shall show in a moment, $Q_r \neq 0$.

Let $f'(z) = rz^{r-1} - (r-1) P_1 z^{r-2} - \ldots$ be the derivative of $f(z)$. Since $D = \pm f'(\alpha_1) \ldots f'(\alpha_r)$, none of the numbers $f'(\alpha)$ is zero. Furthermore it turns out that

$$\beta_i = \frac{\gamma_i}{f'(\alpha_i)} \qquad (i = 1, 2, \ldots, r).$$

Hence by (2.2), no γ is zero so that $Q_r \neq 0$, and

$$W_n = \frac{\gamma_1 \alpha_1^n}{f'(\alpha_1)} + \ldots + \frac{\gamma_r \alpha_r^n}{f'(\alpha_r)}. \tag{2.4}$$

https://doi.org/10.4153/CJM-1954-047-9 Published online by Cambridge University Press

3. The restricted period of a recurrence. Let p be a prime number which does not divide the constant term P_r of the characteristic polynomial (1.2). The least positive integer n such that the congruences

$$\alpha_1^n \equiv \alpha_2^n \equiv \ldots \equiv \alpha_r^n \pmod{p} \tag{3.1}$$

hold in the root field $\mathfrak{R}$ is called the *restricted period* of p in the recurrence (1.1) or the polynomial (1.2) **(3)**.

If ρ is the restricted period of p, (3.1) holds if and only if ρ divides n. Furthermore we have the congruence

$$W_{n+\rho} \equiv CW_n \pmod{p}, \qquad C \not\equiv 0 \pmod{p}, \tag{3.2}$$

where the residue C depends only on p and the recurrence (1.1). Consequently, p is a divisor of (W) if and only if it divides one of the ρ numbers

$$W_1, W_2, \ldots, W_{\rho-1}, W_\rho.$$

Now let (L) denote that particular recurring sequence with the initial values

$$L_1 = L_2 = \ldots = L_{r-2} = 0, \qquad L_{r-1} = 1.$$

For this sequence the polynomial $w(z)$ is one, so that all the γ_i are one, and by (2.4)

$$L_n = \frac{\alpha_1^n}{f'(\alpha_1)} + \ldots + \frac{\alpha_r^n}{f'(\alpha_r)}. \tag{3.3}$$

In case $r = 2$, L_n reduces to the well-known Lucas function

$$\frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}.$$

We shall accordingly refer to (L) as the "Lucas sequence belonging to $f(z)$."

Every prime number p not dividing P_r is a maximal divisor of (L), and the first zero of order $r - 1$ of p in (L) is simply the restricted period of $f(x)$ modulo p. We accordingly call ρ the *rank* of p in (L). Furthermore, every maximal divisor of (L) is regular.

4. Statement of results. Let $\Lambda(W)$ denote the rational integer

$$\Lambda(W) = DP_r\,\Delta(W). \tag{4.1}$$

Evidently $\Lambda(W)$ is not zero. Let p be any prime not dividing $\Lambda(W)$. Let (L) be the Lucas sequence belonging to $f(z)$, and let (M) be the Lucas sequence belonging to $g(z)$ of (2.3). Since p does not divide $\Lambda(W)$, it is a maximal prime divisor of both (L) and (M).

THEOREM 4.1. *Let p be a prime number not dividing $\Lambda(W)$ of (4.1). Then a necessary condition that p be a maximal divisor of (W) is that its rank in (M) divide its rank in (L).*

https://doi.org/10.4153/CJM-1954-047-9 Published online by Cambridge University Press

THEOREM 4.2. *The condition of Theorem* 4.1 *is sufficient for p to be a maximal prime divisor of* (W) *provided that* $f(z)$ *and* p *are restricted as follows:*

(i) $f(z)$ *is of odd degree and irreducible;*
(ii) $p - 1$ *is prime to the degree* r *of* $f(z)$*;*
(iii) $f(z)$ *is irreducible modulo* p.

5. Proof of necessity of condition. We first prove Theorem 4.1. Let p be any prime not dividing $\Lambda(W)$, and assume that p is a maximal divisor of (W). Then there exists a positive integer k such that

$$W_k \equiv W_{k+1} \equiv \ldots \equiv W_{k+r-2} \equiv 0 \pmod{p},$$

but

$$W_{k+r-1} \equiv C \not\equiv 0 \pmod{p}.$$

The sequence (T) defined by $T_n = W_{n+k} - CL_n$ satisfies the recurrence (1.1) and has its r initial values $T_0, \ldots, T_{r-1}$ all divisible by p. Consequently, p divides every term of (T); in other words the congruences

$$W_{n+k} \equiv CL_n \pmod{p} \tag{5.1}$$

$$C \not\equiv 0 \pmod{p} \tag{5.2}$$

are necessary conditions for p to be maximal divisor of (W). For a fixed positive k and any rational integer C, they are also sufficient conditions for p to be maximal in (W); for since p does not divide P_r, it is maximal in (L).

Since p does not divide the discriminant D of $f(z)$, it is unramified in the root field $\mathfrak{R}$. Consequently its prime ideal factorization in $\mathfrak{R}$ is of the form

$$p = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_s \tag{5.3}$$

where the $\mathfrak{p}$ are distinct prime ideals.

Let ρ_j denote the restricted period of $f(z)$ modulo $\mathfrak{p}_j$; that is, ρ_j is the least positive integer n such that the congruences

$$\alpha_1^n \equiv \alpha_2^n \equiv \ldots \equiv \alpha_r^n \pmod{\mathfrak{p}_j} \tag{5.4}$$

hold in $\mathfrak{R}$. Evidently the restricted period ρ of $f(z)$ modulo p is the least common multiple of the ρ_j.

If $f(z)$ is normal, its Galois group is transitive over the ideals $\mathfrak{p}_j$, and the Galois group is also transitive over the $\mathfrak{p}_j$ if $f(z)$ is irreducible modulo p. In either case, on applying the substitutions of the group to the congruences (5.4), we see that the ρ_j will all be equal. Hence we may state the following lemma:

LEMMA 5.1. *If* $f(z) = 0$ *is a normal equation or if* $f(z)$ *is irreducible modulo* p, *then with the notations of* (5.3)–(5.4), $\rho = \rho_j$ $(j = 1, 2, \ldots, s)$.

Now let $\mathfrak{p}_j$ stand for any one of the prime ideal factors of p in the decomposition (5.3). Then the congruences (5.1) imply that for every n

$$W_{n+k} - CL_n \equiv 0 \pmod{\mathfrak{p}_j}, \qquad C \not\equiv 0 \pmod{\mathfrak{p}_j}. \tag{5.5}$$

On substituting for W_{n+k} and L_n from formulas (2.4) and (3.3) and then letting n range from 0 to $r - 1$, we obtain r homogeneous linear congruences

$$\sum_{i=1}^{r} (\gamma_i \alpha_i^k - C) \frac{\alpha_i^n}{f'(\alpha_i)} \equiv 0 \pmod{\mathfrak{p}_j} \qquad (n = 0, 1, \ldots, r-1).$$

Now the algebraic numbers $\alpha_i^n f'(\alpha_i)^{-1}$ are integers modulo $\mathfrak{p}_j$, and the square of their determinant is D^{-1} which is both an integer mod $\mathfrak{p}_j$ and prime to $\mathfrak{p}_j$. Consequently

(5.6) $$\gamma_1 \alpha_1^k \equiv \gamma_2 \alpha_2^k \equiv \ldots \equiv \gamma_r \alpha_r^k \equiv C \not\equiv 0 \pmod{\mathfrak{p}_j}.$$

Conversely these congruences imply the congruence (5.5). We may therefore state:

LEMMA 5.2. *If p does not divide the integer $\Lambda(W)$, then necessary and sufficient conditions that p should be a maximal divisor of the sequence (W) are that for some fixed positive integer k, the congruences* (5.6) *hold for every prime ideal factor $\mathfrak{p}_j$ of p in the root field of $f(z)$.*

Now let ρ_j be the restricted period of $f(x)$ modulo $\mathfrak{p}_j$ and σ_j the restricted period of $g(x)$ modulo $\mathfrak{p}_j$; that is, σ_j is the smallest positive value of n such that

$$\gamma_1^n \equiv \gamma_2^n \equiv \ldots \equiv \gamma_r^n \pmod{\mathfrak{p}_j}.$$

Then the restricted period σ of $g(x)$ modulo p is evidently the least common multiple of the σ_j.

On raising each term in (5.6) to the ρ_jth power, we see that σ_j must divide ρ_j. Hence σ must divide ρ, completing the proof.

6. Proof of sufficiency. It follows from the results of § 5 that if p does not divide $\Lambda(W)$, the conditions

(6.1) $$\sigma_j \text{ divides } \rho_j \qquad (j = 1, 2, \ldots, s)$$

are necessary for the congruences (5.6) to hold. To answer the question of when these conditions are sufficient, we begin by studying the congruence

(6.2) $$\gamma\alpha^k \equiv C \pmod{\mathfrak{p}}.$$

Here α as before is any root of $f(z)$, γ is an integer of the root field $\mathfrak{R}$ of $f(z)$, C is a rational integer, $\mathfrak{p}$ any prime ideal of $\mathfrak{R}$ dividing neither α nor γ, and k is a positive integer.

For brevity, we shall use the following special notations in this section. Since all congruences will be to the same modulus, we shall repress the mod $\mathfrak{p}$, writing (6.2) for example as $\gamma\alpha^k \equiv C$. $\gamma \equiv$ Int means there exists a rational integer g such that $\mathfrak{p}$ divides $\gamma - g$. Clearly

(6.3) $$\gamma \equiv \text{Int} \quad \textit{if and only if } \gamma^{p-1} \equiv 1.$$

$\gamma \equiv Pr(\alpha)$ means γ is congruent modulo $\mathfrak{p}$ to a power of α. $ex(\gamma)$ means the exponent to which γ belongs modulo $\mathfrak{p}$; that is, the least positive value of n

such that $\gamma^n \equiv 1$. $rx(\gamma)$ means the restricted exponent of γ modulo $\mathfrak{p}$; that is, the least positive value of n such that $\gamma \equiv \text{Int}$. Evidently

(6.4) $\gamma^n \equiv \text{Int}$ *if and only if* $rx(\gamma)$ *divides* n.

Let

(6.5) $$\nu = ex(\gamma), \quad \sigma = rx(\gamma), \quad \gamma^\sigma \equiv g, \quad \delta = ex(g).$$

LEMMA 6.1. *With the notations of* (6.5),

(6.6) $$\nu = \sigma\delta$$

Proof: Evidently ν divides $\sigma\delta$. Let $(\nu, p-1) = t$ so that $\nu = \nu_0 t$ and $p - 1 = lt$ with $(\nu_0, l) = 1$. Since $\gamma^{\nu_0(p-1)} \equiv 1$, $\gamma^{\nu_0} \equiv \text{Int}$ by (6.3). Consequently by (6.4), σ divides ν_0. Let $\nu_0 = \kappa\sigma$. Then

$$1 \equiv \gamma^\nu \equiv \gamma^{\nu_0 t} \equiv \gamma^{\kappa\sigma t} \equiv g^{\kappa t}.$$

Therefore $\delta | \kappa t$. Hence $\sigma\delta | \sigma\kappa t$, $\sigma\delta | \nu_0 t$ or $\sigma\delta$ divides ν. Hence $\sigma\delta = \nu$, completing the proof.

LEMMA 6.2. *If the irreducible congruence mod* $\mathfrak{p}$ *with rational integral coefficients of which* γ *is a root is of degree t, and if t is prime to* $p-1$, *where p is the rational prime corresponding to* $\mathfrak{p}$, *then the exponent* ν *to which* γ *belongs modulo* $\mathfrak{p}$ *is of the form* (6.6) *with* σ *and* δ *as before, but in addition* σ, δ *are coprime,* σ *divides* $(p^t - 1)/(p-1)$, δ *divides* $p - 1$ *and*

$$(\sigma, p-1) = 1.$$

Proof: Let the irreducible congruence be

$$z^t - R_1 z^{t-1} \ldots + (-1)^t R_t \equiv 0 \pmod{\mathfrak{p}}$$

where the R_i are rational integers. The roots of (6.6) are $\gamma, \gamma^p, \gamma^{p^2}, \ldots \gamma^{p^{t-1}}$ Hence

$$\gamma^{\frac{p^t-1}{p-1}} \equiv R_t \equiv \text{Int}.$$

Therefore by (6.4), $\sigma | (p^t - 1)/(p-1)$; obviously δ divides $p - 1$. Now $((p^t-1)/(p-1), p-1) = (t, p-1) = 1$. Hence $(\sigma, \delta) = (\sigma, p-1) = 1$ which completes the proof.

Under the hypotheses of lemma 6.2 it is not difficult to show that δ is the exponent to which R_t in (6.8) belongs modulo p.

LEMMA 6.3. *With the hypotheses of Lemma* 6.2,

$$\gamma\alpha^k \equiv \text{Int} \textit{ if and only if } \gamma^{p-1} \equiv Pr(\alpha).$$

Proof. If $\gamma\alpha^k \equiv \text{Int}$, then

$$\gamma^{p-1}\alpha^{k(p-1)} \equiv 1$$

which implies $\gamma^{p-1} \equiv Pr(\alpha)$. Assume conversely that for some integer $l \geqslant 0$, $\gamma^{p-1} \equiv \alpha^l$.

Now $(\sigma, p-1) = 1$ by Lemma 6.2. Hence integers u and r exist such that $u\sigma + r(p-1) = 1$. Hence

$$\gamma = \gamma^{u\sigma + r(p-1)} \equiv g^u \alpha^{rl}.$$

Hence for some positive k, $\gamma\alpha^k \equiv \text{Int}$, completing the proof.

LEMMA 6.4. *If the restricted exponent σ of γ is prime to $p-1$ and divides the restricted exponent of α, then $\gamma^{p-1} \equiv Pr(\alpha)$.*

Proof. Let $\rho = rx(\alpha)$. Since $\gamma^{\sigma(p-1)} \equiv 1$, $ex(\gamma^{p-1})$ divides σ. Hence $ex(\gamma^{p-1})$ divides $rx(\alpha)$ or $ex(\gamma^{p-1})$ divides $ex(\alpha)$ by applying Lemma 6.1 to α instead of to γ. Hence $\gamma^{p-1} \equiv Pr(\alpha)$; for the multiplicative group of residues prime to $\mathfrak{p}$ is cyclic.

We may draw the following conclusion from the preceding lemmas which completes our investigation of the congruence (6.2).

LEMMA 6.5. *If the degree of γ modulo $\mathfrak{p}$ is prime to $p-1$, then a necessary and sufficient condition that the congruence* (6.2) *holds is that the restricted period of γ modulo $\mathfrak{p}$ divides the restricted period of γ modulo $\mathfrak{p}$.*

7. Proof of sufficiency concluded. We may now prove Theorem 4.2 as follows: Since $f(z)$ is irreducible modulo p, p does not divide P_r and p is unramified. Consequently its prime ideal factorization is as in (5.3). Let $\mathfrak{p}_j$ denote any prime ideal factor of p. By lemma 5.1, $\rho = \rho_j$ and $\sigma = \sigma_j$ and σ divides ρ by hypothesis. Also since $f(z)$ is irreducible modulo p, the degree t of γ is a divisor of r, so that t is prime to $p-1$. Consequently by Lemma 6.5,

$$\gamma\alpha^k \equiv C \not\equiv 0 \qquad (\text{mod } \mathfrak{p}_j). \tag{7.1}$$

Here k may depend on j.

Now raise the congruence (7.1) successively to the $p, p^2, \ldots, p^{r-1}$ powers. Since $f(z)$ is irreducible mod p, its roots mod p and mod $\mathfrak{p}_j$ are the powers of any particular root α; that is, for a suitable numbering of the roots

$$\alpha_i \equiv \alpha^{p^{i-1}} \qquad (\text{mod } p) \qquad\qquad (i = 1, 2, \ldots, r).$$

Hence since $w(z)$ has rational integer coefficients,

$$\gamma^{p^{i-1}} \equiv w(\alpha^{p^{i-1}}) \equiv w(\alpha_i) \equiv \gamma_i \quad (\text{mod } p).$$

Therefore we obtain from (7.1) the congruences (5.6) and k is seen to be independent of j. But as was remarked in section 5, (5.6) implies congruences (5.1) and (5.2). Consequently p is a maximal divisor of (W), completing the proof.

8. Conclusion. A numerical example. Consider any integral recurrent sequence (W) defined by the recurrence $W_{n+3} = W_{n+2} + 4W_{n+1} + W_n$.

The characteristic polynomial of this recurrence $z^3 - z - 4z^2 - 1$ is irreducible and its discriminant is 169, a perfect square. Consequently, $f(z)$ is normal.

https://doi.org/10.4153/CJM-1954-047-9 Published online by Cambridge University Press

For every prime p congruent to 5 mod 6, $p - 1$ is prime to $r = 3$. Hence all the restrictive hypotheses of theorem 4.2 are met except possibly the irreducibility of $f(z)$ modulo p.

Consider the prime $p = 5$. Then $f(z)$ is reducible modulo 5; in fact

$$f(z) \equiv (z-1)(z-2)(z-3) \pmod{5}.$$

Consequently the restricted period of $f(z)$ modulo 5 (that is, the rank of 5 in (L)) is four. Since $g(z)$ is evidently completely reducible modulo 5, the rank of 5 in (M) always divides the rank of 5 in (L).

Now suppose the initial values of (W) are chosen so that five does not divide $\Lambda(W)$ of (4.1), which amounts to saying that the recurrence (W) is of order three modulo five. Then five may or may not be a maximal divisor of (W). For example, if $W_0 = 1$, $W_1 = 1$, $W_2 = 0$ then $\Lambda(W) = 5239$. But $W_3 = 5$ and p is maximal. If $W_0 = 1$, $W_1 = 3$, $W_2 = 5$ then $\Lambda(W) = 12337$. But $W_3 = 18$ and (W) has period four modulo 5. Hence p is not maximal in this recurrence.

To illustrate the possibility of an irregular maximal prime divisor, consider the recurrence $W_{n+3} = 7W_{n+2} + 36W_{n+1} + 29W_n$ with $W_0 = 7$, $W_1 = 7$, and $W_2 = 1$. Then if we take $p = 7$, p is obviously maximal in (W). But p is irregular. For on computing the first nineteen terms of (W) mod 49, we obtain

$$7, 7, 1, 21, 43, 8, 8, 23, 44, 45, 18, 33, 28, 44, 19, 30, 14, 14, 2.$$

Since the last three terms are double the first three,

$$W_{n+16} \equiv 2W_n \pmod{49}$$

so that no term of (W) is divisible by 7^2.

There exist for cubic sequences fairly simple criteria distinguishing regular and irregular primes. These I plan to give elsewhere.

References

1. Morgan Ward, *The null divisors of linear recurring series*, Duke Math. J., *2* (1936), 472–476.
2. Marshall Hall, *Divisors of second order sequences*, Bull. Amer. Math. Soc., *43* (1937), 78–80.
3. R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly J. Math., *48* (1920), 343–372.

California Institute of Technology