THE LAW OF APPARITION OF PRIMES IN A LUCASIAN SEQUENCE*

BY

MORGAN WARD

I. Introduction

1. We call a sequence of rational integers

$$(u): \ u_0, u_1, u_2, \cdots, u_n, \cdots$$

Lucasian (Ward [1]†) if it satisfies a linear recursion relation with constant integral coefficients, and if u_n divides u_m whenever n divides m. The adjective "Lucasian" is chosen in honor of the French mathematician Eduard Lucas who first developed a theory of these sequences‡ (Lucas [1], [2]). We are concerned here with the fundamental problem of determining a priori all the terms of such a sequence divisible by any preassigned modulus m.

Call the suffix k of a term u_k of (u) divisible by m a place of apparition of m in (u), and let $\mathfrak{S}_m$ denote the set of all places of apparition of m. It follows from the results established in Ward [1] that the set $\mathfrak{S}_m$ consists in general§ of all multiples of a finite number of places of apparition $\rho_1, \rho_2, \cdots, \rho_s$ called the ranks of apparition of m in (u) with the defining properties

$$u_\rho \equiv 0 \pmod{m}, \qquad u_s \not\equiv 0 \pmod{m} \text{ if } s \text{ divides } \rho.$$

The least common multiple|| $\rho = [\rho_1, \rho_2, \cdots, \rho_s]$ of the ranks of apparition of m in (u) is called simply the *rank* of m in (u). The places of apparition of m in (u) are periodic modulo ρ, and ρ divides the restricted period¶ of (u) modulo m. Furthermore if $m = a \cdot b$ where a and b are co-prime, then the set $\mathfrak{S}_m$ of places of apparition of m is the cross cut of the sets $\mathfrak{S}_a$ and $\mathfrak{S}_b$, and each rank of apparition of m is the least common multiple of ranks of apparition of a and b.

Our fundamental problem reduces then to determining the ranks of ap-

* Presented to the Society, February 26, 1938; received by the editors July 13, 1937.

† The numbers [1], [2], $\cdots$ refer to the bibliography at the close of the paper.

‡ Lucas confined himself in the main to the case when the recursion relation is of order two.

§ An exception occurs only if m divides every term of (u) beyond a certain point.

|| We use $[a, b, \cdots]$ and $(a, b, \cdots)$ to denote the least common multiple and greatest common divisor of the integers $a, b, \cdots$.

¶ The restricted period of (u) modulo m is the least positive integer μ such that $u_{n+\mu} \equiv a u_n \pmod{m}$ for all large n, where a is a constant integer. For the terminology of the theory of recurring series which we employ, see Ward [2].

parition of primes and powers of primes in (u). In the terminology of Lucas,[*] we must discover the "law of apparition" of primes in (u), and the "law of repetition" of primes in (u). I shall confine myself here to the first problem; the modulus m will invariably be a prime number p.

2. It will be well at this point to exhibit some Lucasian sequences. Let

$$f(x) = x^k - c_1x^{k-1} - \cdots - c_k, \qquad g(x) = x^l - d_1x^{l-1} - \cdots - d_l$$

be two polynomials with rational integral coefficients $c_1, \cdots, d_l$. For simplicity of exposition we assume that $f(x)$ and $g(x)$ have non-vanishing discriminants and resultant.[†] Let $\alpha_1, \cdots, \alpha_k; \beta_1, \cdots, \beta_l$ denote the roots of $f(x)=0$ and $g(x)=0$ respectively. Then none of the $k(2l+k-1)/2$ differences $\alpha_i-\beta_j$, $\alpha_i-\alpha_r$, $r\neq i$, vanish.

Consider now the sequences (U): $U_0, U_1, \cdots$; (R): $R_0, R_1, \cdots$, where

$$U_n = U_n(f) = \prod_{i<r}\left(\frac{\alpha_i^n - \alpha_r^n}{\alpha_i - \alpha_r}\right), \qquad R_n = R_n(f, g) = \prod\left(\frac{\alpha_i^n - \beta_j^n}{\alpha_i - \beta_j}\right).$$

Then U_n and R_n are rational integers, and both sequences are clearly divisibility sequences. Both sequences are also linear (Ward [1]). Hence, *both sequences are Lucasian.* The sequence U_n for $k=2$ is the classical Lucas function (Lucas [1]), while R_n for $g(x)=x-1$ is equivalent to the function studied by T. A. Pierce [1], P. Poulet [1], and D. H. Lehmer [2].[‡]

We shall call the polynomials $f(x)$ and $g(x)$ the *generators* of (R) and (U). We refer to both types of sequences as R-sequences.

The determination of the law of apparition for R-sequences is of particular importance because it appears probable that *all* Lucasian sequences may be exhibited as R-sequences or divisors of R-sequences.[§] (See next section.) I shall show here in detail that the determination of the law of apparition

[*] See Lucas [1], pp. 209, 289, 294, or Lehmer [1], pp. 421, 422.

[†] This restriction is removed in the body of the paper.

[‡] It is possible to exhibit both (R) sequences and (U) sequences as Pierce sequences. For if we let $\bar\beta=\beta^{-1}$, then $(\alpha^n-\beta^n)/(\alpha-\beta)=\beta^{n-1}[(\alpha\bar\beta)^n-1]/(\alpha\bar\beta-1)$. Accordingly if we denote the kl products $\alpha_i\bar\beta_j$ in any order by $\epsilon_1, \epsilon_2, \cdots, \epsilon_{kl}$, then

$$R_n = (-1)^{kl(n-1)}d_l^{k(n-1)}\prod_{h=1}^{kl}\left(\frac{\epsilon_h{}^n-1}{\epsilon_h-1}\right),$$

and $(\epsilon_1{}^n-1)(\epsilon_2{}^n-1)\cdots(\epsilon_{kl}^n-1)$ is the function studied by Pierce in the paper cited.

A similar result holds for (U). Since we must then deduce the properties of (R) from a polynomial $(x-\epsilon_1)\cdots(x-\epsilon_{kl})$ of higher degree than $f(x)$ or $g(x)$ with non-integral coefficients whose factorization depends in a highly complicated manner upon $f(x)$ and $g(x)$, the reduction appears to be of only formal interest.

[§] With the qualifications described in §3, I have found empirically no Lucasian sequences which are not R-sequences.

depends upon the fundamental problem of determining the period of a mark in a finite field. My results are sufficiently precise to give a good deal of specific information about the terms divisible by a given prime in any numerical example of an R-sequence.

The sequence (U) is also of importance because of the following theorem:

THEOREM 2.1. *Let the Lucasian sequence (u) belong to the polynomial $f(x)$, and let p be any prime which does not divide the discriminant of $f(x)$. Then every place of apparition of p in (u) is a place of apparition of p in the Lucasian sequence (U) generated by $f(x)$.*

3. Another extensive class of Lucasian sequences arises as follows. Consider for simplicity a sequence (U) with an irreducible generator $f(x)$. The galois group of $f(x)$ may be represented as a transitive permutation group upon the roots $\{\alpha_1\}, \{\alpha_2\}, \cdots, \{\alpha_k\}$.

Now let us represent the group as a permutation group upon the $k(k-1)/2$ *pairs* of roots $\{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_3\}, \cdots, \{\alpha_{k-1}, \alpha_k\}$.

If the group is singly transitive over the $\{\alpha_i\}$, the pairs $\{\alpha_i, \alpha_j\}$ may be separated into $\kappa \geqq 2$ transitive sets

$$\{\alpha_{i_1}, \alpha_{i'_1}\}, \{\alpha_{i_2}, \alpha_{i'_2}\}, \cdots, \{\alpha_{i_{s_i}}, \alpha_{i'_{s_i}}\}$$
$$i = 1, 2, \cdots, \kappa; s_1 + s_2 + \cdots + s_K = k(k-1)/2.$$

We have a corresponding arithmetical factorization of the general term U_n of (U) into a product of κ rational integers:

$$U_n = \prod_{i=1}^{K} U_n^{(i)}, \qquad U_n^{(i)} = \prod\left(\frac{\alpha_{i_1}^n - \alpha_{i'_1}^n}{\alpha_{i_i} - \alpha_{i'_1}}\right).$$

Each of the κ sequences $(U^{(i)})$ is obviously Lucasian.*

We shall refer to sequences obtained in this manner as *divisors* of R-sequences. The determination of the laws of apparition of primes in divisors of

* For example, suppose that $k=4$ and that $f(x)=x^4-c_1x^3-c_2x^2-c_3x-c_4\equiv x^4+(2Q-R)x^2+Q^2$ where Q and R are co-prime integers and R is not a square. Then with a proper notation, $(x-\alpha_1)(x-\alpha_2)=x^2-R^{1/2}x+Q$, $\alpha_3=-\alpha_1$, $\alpha_4=-\alpha_2$. There are two transitive sets of the $\{\alpha_i, \alpha_j\}$; namely, $\{\alpha_1, \alpha_2\}$, $\{\alpha_1, \alpha_4\}$, $\{\alpha_2, \alpha_3\}$, $\{\alpha_3, \alpha_4\}$ and $\{\alpha_1, \alpha_3\}$, $\{\alpha_2, \alpha_4\}$.

We find that $U_n = U_n^{(1)}U_n^{(2)}$ where

$$U_n^{(1)} = \left(\frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}\right)^2\left(\frac{\alpha_1^n - (-\alpha_2)^n}{\alpha_1 + \alpha_2}\right)^2, \qquad U_n^{(2)} = (4\alpha_1\alpha_2)^{n-1} = (4Q)^{n-1}.$$

Now $(\alpha_1^n-\alpha_2^n)/(\alpha_1-\alpha_2)$ is one of the important functions introduced by D. H. Lehmer in his doctor's thesis (Lehmer [1]), and $[\alpha_1^n-(-\alpha_2)^n]/(\alpha_1+\alpha_2)$ is immediately expressible in terms of Lehmer's U_n and V_n.

The function $N(\alpha^n-\beta^n)$ studied by Marshall Hall (Hall [2]) may be similarly exhibited as a divisor of a certain R-sequence.

R-sequences is an important part of our general problem. But to avoid stretching the present paper to an inordinate length, we shall give our investigations elsewhere. The problem amounts to correlating the results obtained in this paper by the use of Schatanovski's principle (§7) with results obtained from the Dedekind-Hilbert theory of the ideals of a galois field.

4. The law of apparition of primes in R-sequences is determined as follows. Consider first the sequence (R). We show (§§6, 7) that it suffices to consider primes which do not divide the resultant of the generators of (R). We have decompositions of $f(x)$ and $g(x)$ modulo p of the form

$$f(x) \equiv f_1(x)^{a_1} \cdots f_r(x)^{a_r};\ g(x) \equiv g_1(x)^{b_1} \cdots g_s(x)^{b_s} \pmod{p},$$

where the polynomials f_i and g_j are primary, irreducible and co-prime in pairs modulo p. We show in §8 that we have a corresponding decomposition of the general term of (R) modulo p

$$R_n(f, g) \equiv \prod_{i,j} \{R_n(f_i, g_j)\}^{a_i b_j} \pmod{p}.$$

In the terminology of Ward [1], the sequence (R) factors modulo p into a product of simpler sequences; for the f_i and g_j are irreducible modulo p. But then (Ward [1]) the set $\mathfrak{S}_p$ of places of apparition of p in (R) is the union of the sets of places of apparition of p in the sequences $(R(f_i, g_j))$. Therefore *in discussing the law of apparition of primes in* (R) *we may assume that the generators of* (R) *are irreducible modulo* p. A like simplification holds for the sequence (U) (§9).

5. If the generator of (U) is irreducible modulo p, the law of apparition of p in (U) takes the following beautifully simple form, affording a far-reaching generalization of the classical results of Lucas [1]:

THEOREM 5.1. *Let $f(x)$ be irreducible modulo p, and let λ be its period* modulo p. Let $k=q_1^{c_1}q_2^{c_2}\cdots q_K^{c_K}$ be the decomposition of its degree k into prime factors. Let $\rho(s)$ be defined for any positive integer s as the residual*† *of p^s-1 with respect to λ; that is, the quotient of λ by the greatest common divisor of λ and p^s-1. Then the ranks of apparition of p in (U) occur among*‡ *the κ numbers $\rho(k/q_1), \cdots, \rho(k/q_K)$, the rank of p in (U) divides $\rho(k/q_1q_2\cdots q_K)$, and p has at most κ ranks of apparition.*

We observe that the numbers $\rho(k/q)$ are known as soon as the period is known.

* The period of $f(x)$ modulo p is by definition the smallest positive value of λ such that $x^\lambda \equiv 1$ (modd $p, f(x)$).

† The operation of residuation has important arithmetical applications. I have developed some of these in the paper, Ward [3], which arose out of the present investigations.

‡ We must exclude from the set of $\rho(k/q)$ any element which is a multiple of any other.

Unlike the ranks of apparition of p in (U), the ranks of apparition of p in (R) are not obtainable from the periods of the generators $f(x)$ and $g(x)$ of (R) alone when the generators are irreducible modulo p. If $f(\alpha)=0$, $g(\beta)=0$, the ranks of apparition occur among the l periods $\sigma_1, \sigma_2, \cdots, \sigma_l$ modulo p of the algebraic numbers $\alpha\beta^{-1}, \alpha\beta^{-p}, \cdots, \alpha\beta^{-p^{l-1}}$ in the galois field of the roots of the generators (§11). In §14, we assign upper and lower limits to the periods σ in terms of the periods and restricted periods of $f(x)$ and $g(x)$.

The least common multiples of pairs of the periods σ have the following remarkable property (§13):

$$[\sigma_s, \sigma_t] = [\sigma_s, \sigma_{s\pm(m,t-s)}].$$

Here m is the least common multiple of the degrees of $f(x)$ and $g(x)$ and we adopt the convention that $\sigma_x = \sigma_y$ if $x \equiv y \pmod{l}$.

It appears unlikely that results of simplicity comparable to Theorem 5.1 exist for the law of apparition of primes in (R).

II. Reduction to R-sequences with irreducible generators

6. This section is devoted to some algebraic preliminaries. Let x; $y_1, y_2, \cdots, y_k$; $z_1, z_2, \cdots, z_l$ be $k+l+1$ indeterminates, and let $Y_1, -Y_2, \cdots, (-1)^{k-1}Y_k$; $Z_1, -Z_2, \cdots, (-1)^{l-1}Z_l$ be the $k+l$ elementary symmetric functions of the indeterminantes y, z defined by*

$$(x-y_1)(x-y_2)\cdots(x-y_k) = x^k - Y_1x^{k-1} - \cdots - Y_k,$$
$$(x-z_1)(x-z_2)\cdots(x-z_l) = x^l - Z_1x^{l-1} - \cdots - Z_l.$$

By the fundamental theorem on symmetric functions, the polynomials

$$(6.1)\qquad \Theta_{k,l}(y,z) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{y_i^n - z_j^n}{y_i - z_j}\right), \qquad \Psi_k(y) = \prod_{\substack{i,j=1\\ i<j}}^{k}\left(\frac{y_i^n - y_j^n}{y_i - y_j}\right)$$

may be expressed as polynomials in the Y and Z with integral coefficients; we write

$$(6.2)\qquad \Theta_{k,l}(y,z) = P_{k,l}(Y,Z), \qquad \Psi_k(y) = Q_k(Y).$$

Suppose now that $t_1, t_2, \cdots, t_m$ are m new indeterminates where $k \geqq m \geqq 1$, $l \geqq m \geqq 1$, and consider the effect of substituting t_1 for y_k and z_l, t_2 for y_{k-1} and z_{l-1}, t_3 for y_{k-2} and z_{l-2}, and so on, in the identity (6.2). If we let

$$(x-y_1)\cdots(x-y_{k-m}) = x^{k-m} - Y_1'x^{k-m-1} - \cdots - Y_{k-m}',$$
$$(x-z_1)\cdots(x-z_{l-m}) = x^{l-m} - Z_1'x^{l-m-1} - \cdots - Z_{l-m}',$$
$$(x-t_1)\cdots(x-t_m) = x^m - T_1'x^{m-1} - \cdots - T_m',$$

* Minus signs are introduced so that the associated difference equation used later $\Omega_{n+k} = Y_1\Omega_{n+k-1} + \cdots + Y_k\Omega_n$ may have all its signs positive.

then the polynomial $P_{k,l}$ on the right of (6.2) is transformed into a polynomial $P^*_{k,l,m}$ in the arguments Y', Z', T' with integral coefficients. Its expression in terms of y, z, t is easily found to be

$$n^m T_m'^{n-1} \Theta_{k-m,l-m}(y, z)\Theta_{k-m,m}(y, t)\Theta_{m,l-m}(t, z)\Psi_m^2(t).$$

Hence by (6.2)

$$\begin{aligned}(6.3)\quad & P^*_{k,l,m}(Y', Z', T') \\ & \quad = n^m T_m'^{n-1} P_{k-m,l-m}(Y', Z')P_{k-m,m}(Y', T')P_{m,l-m}(T', Z')Q_m^2(T').\end{aligned}$$

Now let $R_n = P_{kl}(Y, Z)$, $U_n = Q_k(Y)$, $R_n^* = P^*_{k,l,m}(Y', Z', T')$, and consider the sequences

$$\begin{aligned}(R):&\quad R_0, R_1, R_2, \cdots,\\ (U):&\quad U_0, U_1, U_2, \cdots,\\ (R^*):&\quad R_0^*, R_1^*, R_2^*, \cdots.\end{aligned}$$

THEOREM 6.1. *(R), (U), and (R^*) are Lucasian in the rings formed by adjoining respectively Y, Z; Y; Y', Z', T' to the ring of rational integers.*

Proof. The sequences evidently lie in the specified rings. Consider (R). Since its general term is a product of cyclotomic functions $(y^n - z^n)/(y-z)$ having the divisibility property, (R) has the same property; that is, R_n divides R_m if n divides m, and the division may be performed in the ring of Y and Z. The linearity of (R) over the ring follows from a general theorem in Ward [1]. Hence (R) is Lucasian. Similarly (U) is Lucasian. Then (R^*) as a product of the seven Lucasian sequences with general terms n^m, $T_m'^{n-1}$, $P_{k-m,l-m}(Y', Z')$, $P_{k-m,m}(Y', T')$, $P_{m,l-m}(T', Z')$, $Q_m(T')$, $Q_m(T')$, and is also Lucasian (Ward [1]).

7. We now consider the sequence (R) of §2 of the introduction. Let $\mathfrak{R}$ denote the ring of rational integers, and let

$$f(x) = x^k - c_1 x^{k-1} - \cdots - c_k; \qquad g(x) = x^l - d_1 x^{l-1} - \cdots - d_l$$

be two polynomials with fixed rational integral coefficients. Let $\alpha_1, \cdots, \alpha_k$; $\beta_1, \cdots, \beta_l$ be their roots, D_f and D_g their discriminants, and

$$R_{f,g} = \pm \prod (\alpha_i - \beta_j)$$

their resultant. If $R_{f,g}$ does not vanish, we define a sequence

$$(R):\quad R_0, R_1, R_2, \cdots,$$

in the notation of §6 by $R_n = \Theta_{k,l}(\alpha, \beta) = P_{k,l}(c, d)$.

If $R_{f,g}$ vanishes, then

$$f(x) = f'(x)h'(x), \qquad g(x) = g'(x)h'(x), \tag{7.1}$$

where

$$\begin{aligned} f'(x) &= x^{k-m} - c_1' x^{k-m-1} - \cdots - c_{k-m}', \\ g'(x) &= x^{l-m} - d_1' x^{l-m-1} - \cdots - d_{l-m}', \\ h'(x) &= x^{m} \quad - e_1' x^{m-1} \quad - \cdots - e_m', \qquad k \geqq m \geqq 1;\, l \geqq m \geqq 1, \end{aligned} \tag{7.2}$$

are polynomials in $\mathfrak{R}$ and $R_{f',g'} \neq 0$. Deviating for simplicity from the notation of the previous section, we now define the sequence (R) (instead of a new sequence (R^*)) by letting $R_n = P^*_{k,l,m}(c', d', e')$. In each case we obtain a Lucasian sequence over $\mathfrak{R}$.

Consider now the places of apparition of any prime number p in (R). There are two cases to consider according as p does or does not divide the resultant $R_{f,g}$.

Case 1. $R_{f,g} \not\equiv 0 \pmod p$. Then $R_n \equiv 0 \pmod p$ if and only if

$$\Theta_{k,l}(\alpha, \beta) = \prod \left(\frac{\alpha_i^n - \beta_j^n}{\alpha_i - \beta_j} \right) \equiv 0 \pmod p.$$

Case 2. $R_{f,g} \equiv 0 \pmod p$. In this case (7.1) and (7.2) hold modulo p with $R_{f',g'} \not\equiv 0 \pmod p$:

$$f(x) \equiv f'(x)h'(x) \pmod p, \qquad g(x) \equiv g'(x)h'(x) \pmod p.$$

We now make use of the following principle:

SCHATANOVSKI'S PRINCIPLE.† *If $\phi(y_1, y_2, \cdots, y_k)$ is an integral symmetric function of the indeterminates $y_1, y_2, \cdots, y_k$ with integral coefficients, and if for a natural number m*

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k) \equiv (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_k) \pmod m$$

where $f(x)$ is a polynomial with integral coefficients, then

$$\phi(\alpha_1, \alpha_2, \cdots, \alpha_k) \equiv \phi(\gamma_1, \gamma_2, \cdots, \gamma_k) \pmod m. \tag{7.3}$$

Let

$$\phi(y_1, y_2, \cdots, y_k) = \prod \left(\frac{y_i^n - \beta_j^n}{y_i - \beta_j} \right),$$

and let $\gamma_1, \gamma_2, \cdots, \gamma_k$ be the roots of $f'(x)h'(x) = 0$ in a definite order. Then on taking $m = p$, (7.3) gives us

$$R_n = R_n(f, g) \equiv R_n(f'h', g) \pmod p.$$

† See Schatanovski [1], Lubelski [1], [2]. The principle is also used constantly in Ward [2].

Here and later if $R_{f,g}$ vanishes, we can replace the congruence by an equality. A second application of Schatanovski's principle gives us

$$R_n = R_n(f, g) \equiv R_n(f'h', g'h') \equiv P^{*}_{k,l,m}(c', d', e') \pmod{p}.$$

Hence we obtain from (6.3) the congruence

$$(7.4) \qquad R_n \equiv n^m e_m'^{n-1} P_{k-m,l-m}(c', d') P_{k-m,m}(c', e') P_{m,l-m}(e', d') Q_m^2(e') \pmod{p}.$$

In particular then $R_p \equiv 0 \pmod{p}$. Since p has no proper divisors and $R_1 = 1$, we thus obtain the following theorem:

THEOREM 7.1. *p is a rank of apparition of any prime p in (R) which divides the resultant $R_{f,g}$ of the polynomials $f(x)$ and $g(x)$ which generate (R).*

Now clearly

$$c_k \equiv c'_{k-m} e'_m \pmod{p}, \quad d_l \equiv d'_{l-m} e'_m \pmod{p}, \quad (c'_{k-m}, d'_{l-m}) \not\equiv 0 \pmod{p}.$$

Hence $e'_m \equiv 0 \pmod{p}$ if and only if $c_k \equiv d_l \equiv 0 \pmod{p}$.

Also $R_{f',g'} \not\equiv 0 \pmod{p}$, $(R_{f',h'}, R_{g',h'}) \not\equiv 0 \pmod{p}$. If we assume that $R_{f',h'} \equiv 0 \pmod{p}$, we have a congruence similar to (7.4) for $P_{k-m,m}(c', e')$; with an obvious extension of notation

$$P_{k-m,m}(c', e') \equiv n^{m'} e''^{\,n-1}_{m'} P_{k-m-m',m'}(c'', e'') \cdots \pmod{p}.$$

By what we have just shown, $e''_{m'} \equiv 0 \pmod{p}$ if and only if $e'_m \equiv c'_{k-m} \equiv 0 \pmod{p}$. A like result holds if $R_{g',h'} \equiv 0 \pmod{p}$. Now it is easily seen that in case 1, p is not a null divisor of (R). Hence we obtain the theorem:

THEOREM 7.2. *p is a null divisor of the Lucasian sequence (R) if and only if p divides the constant terms c_k and d_l of the polynomials $f(x)$ and $g(x)$ which generate (R).*

Hence if p is not such a null divisor of (R), the determination of its places of apparition in case 2 reduces by virtue of (7.4) to determining its places of apparition in various sequences dividing (R) modulo p but for which p does not divide the associated resultant. For (Ward [1] Theorem 6.3) the set of places of apparition in the product of two or more sequences is the union of the sets of places of apparition in the constituent sequences, and the ranks of apparition in the product are immediately specifiable in terms of the ranks of apparition in the constituents. *It suffices therefore to consider only case* 1.

8. We next prove that it suffices to consider the case when $f(x)$ and $g(x)$ are irreducible modulo p. With our previous notation, let p be a prime which does not divide the resultant of the generators of (R). Let the decompositions of the polynomials $f(x)$ and $g(x)$ modulo p be

$$f(x) \equiv f_1(x)^{a_1} \cdots f_r(x)^{a_r} \pmod{p}, \qquad g(x) \equiv g_1(x)^{b_1} \cdots g_s(x)^{b_s} \pmod{p}.$$

Here the polynomiials $f_1(x), \cdots, g_s(x)$ have integral coefficients, and are primary, irreducible, and co-prime in pairs modulo p. Schatanovski's principle gives us then the congruence

$$R_n \equiv R_n(f, g) \equiv R_n(f_1^{a_1}f_2^{a_2} \cdots f_r^{a_r}, g_1^{b_1}g_2^{b_2} \cdots g_s^{b_s}) \pmod{p}.$$

On using the elementary multiplicative properties of resultants (Fricke [1]) this last congruence may be written

$$R_n(f, g) \equiv \{R_n(f_1, g_1)\}^{a_1 b_1} \cdots \{R_n(f_r, g_s)\}^{a_r b_s} \pmod{p}.$$

Hence it follows as in §3 that we may confine ourselves to the case where the generators of (R) are irreducible modulo p.

9. In determining the law of apparition of primes in the sequence (U), we can similarly confine ourselves to the case when the generator of (U) is irreducible modulo p. It would at first appear as if this result were a special case of the reduction for (R), since (U) is obtainable from (R) by setting $g(x) = df(x)/dx$. But the leading coefficient of df/dx is not unity but k, so that the primes dividing k would be unclassified by this method. It is however possible to parallel the reduction for (R), and the process is so similar that we shall merely indicate the main steps.

We begin as in §6 by considering the effect upon

$$\Psi_k(y) = \prod_{\substack{i,j=1 \\ i<j}}^{k} \left(\frac{y_i^n - y_j^n}{y_i - y_j}\right) = Q_k(Y) \tag{9.1}$$

of substituting, in place of $y_1, \cdots, y_k$, h distinct new indeterminates $t_{11}, \cdots, t_{1k_1}, \cdots, t_{r1}, \cdots, t_{rk_r}$ so that we have

$$(x - y_1)(x - y_2) \cdots (x - y_k) = \prod_{u=1}^{r} \prod_{i=1}^{k_u} (x - t_{ui})^{a_u},$$

$$a_1k_1 + a_2k_2 + \cdots + a_rk_r = k, \qquad k_1 + k_2 + \cdots + k_r = h,$$

and at least one a_u is greater than unity. The right side of (9.1) then becomes a polynomial in the quantities $T_1, \cdots, T_r$ defined by

$$(x - t_{u1})(x - t_{u2}) \cdots (x - t_{uk_u}) = x^{k_u} - T_{u1}x^{k_u-1} - \cdots - T_{uk_u}.$$

The value of the left side of (9.1) is then easily found to be

$$\pm\, n^l \prod_{u=1}^{r} T_{uk_u}^{A_u(n-1)} \prod_{u=1}^{r} \{Q_{k_u}(T_u)\}^{a_u^2} \prod_{\substack{u,v=1 \\ u<v}}^{r} \{P_{k_u,k_v}(T_u, T_v)\}^{a_u a_v}, \tag{9.2}$$

$$A_u = \tfrac{1}{2}a_u(a_u - 1), \qquad l = k_1A_1 + k_2A_2 + \cdots + k_rA_r$$

in analogy with formula (6.3).

Consider now the sequence (U) of §2 with the generator

$$f(x) = x^k - c_1x^{k-1} - \cdots - c_k = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

and discriminant

$$D_f = \left\{ \pm \prod_{i<j} (\alpha_i - \alpha_j) \right\}^2 .$$

If D_f does not vanish, we define the sequence

$$(U):\quad U_0,\ U_1,\ U_2, \cdots ,\quad \text{by}\quad U_n = \Psi_k(\alpha) = Q_k(c).$$

If D_f vanishes, we have

$$(9.3)\qquad f(x) = \{f_1(x)\}^{a_1}\{f_2(x)\}^{a_2} \cdots \{f_r(x)\}^{a_r},$$

where $f_u(x) = x^{k_u} - c_{u1}x^{k_u-1} - \cdots - c_{uk_u} = (x - \tau_{u1}) \cdots (x - \tau_{uk_u})$ and $D_{f_u} \neq 0$, $R_{f_u,f_v} \neq 0$, $u \neq v$. We then define U_n by means of (9.2) as

$$(9.4)\qquad U_n = \pm\, n^l \prod_{u=1}^{r} c_{uk_u}^{A_u(n-1)} \prod_{u=1}^{r} \{Q_{k_u}(c_u)\}^{a_u^2} \prod_{\substack{u,v=1\\ u<v}}^{r} \{P_{k_u,k_v}(c_u,\ c_v)\}^{a_ua_v}.$$

Now consider the places of apparition of any prime p in (U). As in the case of (R), there are two cases according as p does or does not divide the discriminant D_f.

Case 1. $D_f \not\equiv 0 \pmod{p}$. Then $U_n \equiv 0 \pmod{p}$ if and only if

$$\Psi_k(\alpha) = \prod \left(\frac{\alpha_i^n - \alpha_j^n}{\alpha_i - \alpha_j} \right) \equiv 0 \pmod{p}.$$

Case 2. $D_f \equiv 0 \pmod{p}$. In this case (9.3) holds modulo p where we may assume that the polynomials $f_u(x)$ are irreducible modulo p and relatively prime in pairs modulo p. We deduce then from Schatanovski's principle that

$$(9.5)\qquad U_n \equiv \pm\, n^l \prod_{u=1}^{r} c_{uk_u}^{A_u(n-1)} \prod_{u=1}^{r} \{Q_{k_u}(c_u)\}^{a_u^2} \prod_{\substack{u,v=1\\ u<v}}^{r} \{P_{k_u,k_v}(c_u,\ c_v)\}^{a_ua_v} \pmod{p}.$$

This congruence is the analogue of (7.4). We deduce the theorems:

THEOREM 9.1. *p is a rank of apparition of any prime p in (U) which divides the discriminant D_f of the polynomial $f(x)$ which generates (U).*

THEOREM 9.2. *p is a null divisor of the Lucasian sequence (U) if and only if p divides the last two coefficients c_k and c_{k-1} of the polynomial $f(x)$ which generates (U).*

Formula (9.5) also shows us that it suffices to consider case 1 for (U) or (R). But in case 1 for (U), we have a decomposition (9.3) of $f(x)$ modulo p with all the a_u unity. Thus a decomposition (9.5) applies with all the a_u, a_v unity, all the A_u zero, and l zero. We thus deduce that it suffices in every case to assume the generators of (U) and (R) irreducible modulo p.

Formula (9.5) shows that *the law of apparition of primes in the sequence* (U) *depends on the law of apparition in* (R), for each sequence with general term $P_{k_u,k_v}(c_u, c_v)$ is a special (R) sequence.

III. Laws of apparition for R-sequences with irreducible generators

10. We shall now determine the law of apparition of primes p in (R) when the generators of (R) are irreducible modulo p.

With our previous notation, let

$$f(x) = x^k - c_1x^{k-1} - \cdots - c_k = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k),$$
$$g(x) = x^l - d_1x^{l-1} - \cdots - d_l = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_l)$$

be the generators of (R). Both $f(x)$ and $g(x)$ are algebraically irreducible. Let $\mathfrak{K}$ denote the galois field of the roots of $f(x)=0$ and $g(x)=0$ obtained by adjoining the $k+l$ quantities $\alpha_1, \cdots, \beta_l$ to the field of rationals.

Lemma 10.1. *p is a prime ideal of $\mathfrak{K}$.*

Proof. If C is the ring of integers of $\mathfrak{K}$, it suffices to show that the quotient ring $\mathfrak{O}/[p]$ is a field. Let $\mathfrak{R}$ as before denote the ring of rational integers, and let α be any root of $f(x)=0$, β any root of $g(x)=0$. Construct the ring $\mathfrak{o}=\mathfrak{R}[\alpha, \beta]$. Clearly $\mathfrak{O}$ contains $\mathfrak{o}$. Hence $\mathfrak{O}/[p]$ contains $\mathfrak{o}/[p]$. We shall now show that $\mathfrak{o}/[p]$ contains $\mathfrak{O}/[p]$ so that

$$\mathfrak{O}/[p] = \mathfrak{o}/[p]. \tag{10.1}$$

To prove this it suffices to show that every element of $\mathfrak{O}$ is congruent modulo p to an element of $\mathfrak{o}$. Let $\overline{D}$ be the discriminant of the field $\mathfrak{K}$. Then (Hilbert [1], Theorem 85, page 144)

$$(p, \overline{D}) = 1. \tag{10.2}$$

For since both $f(x)$ and $g(x)$ are irreducible modulo p, p is prime to their discriminants.

We can choose rational integers $e_1, \cdots, e_k$; $f_1, \cdots, f_l$ such that $\theta=e_1\alpha_1+ \cdots +e_k\alpha_k+f_1\beta_1+ \cdots +f_l\beta_l$ is a primitive element of $\mathfrak{K}$. But we have the congruences in $\mathfrak{O}$

$$\alpha_i \equiv \alpha^{p^{ri}} \pmod{p}; \quad \beta_j \equiv \beta^{p^{sj}} \pmod{p}, \quad i = 1, \cdots, k; j = 1, \cdots, l, \tag{10.3}$$

where $r_1, \cdots, r_k$; $s_1, \cdots, s_l$ are the integers $1, \cdots, k$; $1, \cdots, l$ in some order. Hence θ is congruent modulo p to an element of $\mathfrak{o}$. But if N is the degree of the field $\mathfrak{K}$ and $\overline{D}$ as before its discriminant, the N elements $\overline{D}^{-1}, \theta\overline{D}^{-1}, \cdots, \theta^{N-1}\overline{D}^{-1}$ are a basis of $\mathfrak{O}$. Hence by (10.2), each element of this basis is congruent modulo p to an element of $\mathfrak{o}$. Hence (10.1) follows.

Now the ring $\mathfrak{o}/[p]$ may be obtained either by first adjoining α and β to $\mathfrak{R}$ and then forming the quotient ring, or else by first forming the quotient ring $\mathfrak{R}/[p]$ and then adjoining α and β. Since $\mathfrak{R}/[p]$ is a field, $\mathfrak{o}/[p]$ is consequently a field, so that by (10.1), $\mathfrak{O}/[p]$ is a field.

11. Now assume that for a certain value of n

$$R_n = \prod\left(\frac{\alpha_i^n - \beta_j^n}{\alpha_i - \beta_j}\right) \equiv 0 \pmod{p}.$$

Since p is prime to the resultant of $f(x)$ and $g(x)$, we see from Lemma 10.1 that this congruence can hold if and only if

$$\alpha_i^n \equiv \beta_j^n \pmod{p} \tag{11.1}$$

in $\mathfrak{O}$ for some values of the subscripts i and j.

On multiplying (11.1) by β_j^{-n}, raising to the proper power of p, and utilizing (10.3) we obtain as a necessary and sufficient condition that p divide R_n†

$$\{\alpha\beta^{-p^s}\}^n \equiv 1 \pmod{p}, \qquad 1 \leqq s \leqq l. \tag{11.2}$$

Now $\alpha\beta^{-p^s}$ is an element of the finite galois field $\mathfrak{K}^* = \mathfrak{R}[\alpha, \beta]/[p]$ of order p^m where m is the least common multiple of the degrees of $f(x)$ and $g(x)$. Let σ_s be its period. Then (11.2) holds if and only if

$$n \equiv 0 \pmod{\sigma_s}. \tag{11.3}$$

We thus obtain the following theorem:

THEOREM 11.1. *If σ_s is the period of $\alpha\beta^{-p^s}$ modulo p in $\mathfrak{O}/[p]$, then $\sigma_1, \sigma_2, \cdots, \sigma_l$ constitute a set of generators for the multiplicative set $\mathfrak{S}_p$ of places of apparition of p in (R).*

If we regard the solution of the problem of determining the period of a mark in a finite field as known, the law of apparition of p in (R) is determined: all ranks of apparitions necessarily occur in the set $\sigma_1, \sigma_2, \cdots, \sigma_l$, and to obtain them we merely reject all σ_i which are multiples of order σ_i in the set. The rank of p is then the least common multiple of the surviving σ, and the set $\mathfrak{S}_p$ is exactly specified.

12. From a more realistic standpoint, the period of a mark in a finite

† If d_l' is chosen so that $d_l' d_l \equiv 1 \pmod{p}$, an explicit expression for β^{-1} is given by the congruence

$$\beta^{-1} \equiv d_l' (\beta^{l-1} - d, \beta^{l-2} - \cdots - d_{l-1}) \pmod{p}.$$

field is not given to us by merely specifying the field and the mark, so that it becomes important to reduce the number of crude generators $\sigma_1, \cdots, \sigma_l$ of $\mathfrak{S}_p$ as much as possible. Before giving the details of this reduction, we shall consider the sequence (U) for the case when its generators are irreducible modulo p.

By a repetition of the arguments applied to (R) in the previous section, we deduce that if (U) is generated by a polynomial $f(x)$ which is irreducible modulo p, then

$$U_m \equiv 0 \pmod{p}$$

if and only if

$$m = 0 \pmod{\rho_s},$$

where ρ_s is the period of α^{p^s-1} in the field $\mathfrak{R}[\alpha]/[p]$, s is an integer $\geqq 1$ and $\leqq k$, the degree of $f(x)$, and α is any root of $f(x)=0$.

But if λ is the period of α, the period ρ_s of α^{p^s-1} is easily seen to be the residual† of p^s-1 with respect to λ. In the usual notation for residuals,

$$\rho_s = \lambda : p^s - 1. \tag{12.1}$$

We observe in particular that

$$\rho_k = 1, \qquad \rho_1 = \mu. \tag{12.2}$$

Here μ is the restricted period of $f(x)$ modulo p; that is, the least positive integer such that (Ward [2], p. 284)

$$\alpha_1^{\mu} \equiv \alpha_2^{\mu} \equiv \cdots \equiv \alpha_k^{\mu} \pmod{p}.$$

Now (Ward [4], p. 627) by (12.1)

$$\begin{aligned}[\rho_s, \rho_t] &= [\lambda : p^s - 1, \lambda : p^t - 1] = \lambda : (p^s - 1, p^t - 1)\\ &= [\lambda : p^{(s,t)} - 1]\end{aligned}$$

since the sequence $0, p-1, p^2-1, p^3-1, \cdots$ has the property that $(p^s-1, p^t-1) = p^{(s,t)}-1$ (Lucas [1], Ward [5], [6]). Thus

$$[\rho_s, \rho_t] = \rho_{(s,t)}. \tag{12.3}$$

It follows from (12.3) that if *s divides t, then ρ_t divides ρ_s*. On taking $t=k$ in (12.3) and using (12.2), we see that

$$\rho_s = \rho_d \text{ where } d = (s, k) \text{ divides } k. \tag{12.4}$$

† For the properties of residuals used here, see Ward [3], [4].

We therefore need consider only periods ρ_d where d divides k. But[†] if $d|d'|k$, then $\rho_{d'}|\rho_d$.

We therefore need consider only periods ρ_d where d divides k and no multiple of d divides k. On collecting these results, we obtain Theorem 5.1 of the introduction.

Let $\pi_{ks}=p^k-1:p^s-1$. Since λ divides $p^k-1, \lambda:p^s-1$ divides $p^k-1:p^s-1$. (Ward [4] formula (4.51)). Hence $\rho_s|\pi_{ks}$, $(s=1, 2, 3, \cdots, k)$.

We thus obtain from Theorem 5.1 the following result which gives us a useful upper limit to the ranks of apparition of p.

THEOREM 12.1. *If $f(x)$ is irreducible modulo p and of degree k, the ranks of apparition of p in the sequence (U) generated by $f(x)$ divide the numbers $p^k-1/p^{k/q_1}-1$, $p^k-1/p^{k/q_2}-1$, $\cdots$, $p^k-1/p^{k/q_K}-1$. Here $q_1, \cdots, q_K$ are the κ prime factors of k.*

If $Q=q_1q_2\cdots q_K$, it easily follows that *the rank of p in (U) must divide the number $p^k-1/p^{k/Q}-1$.*

13. We return now to the reduction of the generators of the places of apparition of p in (R). With the notation of §10, let γ be a primitive element of the finite field $\mathfrak{K}^*$. Then

$$\alpha \equiv \gamma^a, \qquad \beta \equiv \gamma^b, \qquad \alpha\beta^{-p^s} \equiv \gamma^{a-bp^s} \pmod p$$

where a and b are positive integers.[‡] Hence

$$\sigma_s = p^m - 1:(a - bp^s), \qquad (s = 1, 2, \cdots, l). \tag{13.1}$$

Here m, it will be recalled, is the least common multiple of the degrees of the generators of (R).

We extend the definition of the σ_s over the entire ring $\mathfrak{R}$ by letting

$$\sigma_r = \sigma_s \qquad \text{if} \qquad r \equiv s \pmod l. \tag{13.2}$$

The numbers σ_s have the following strange property which stands in remarkable contrast to the property of the ranks of apparition of p in (U) expressed by formula (12.3).

THEOREM 13.1. *Let p be a prime, let the generators of the sequence be irreducible modulo p, and let m be the least common multiple of their degrees. Then the least common multiples of pairs of generating elements for the places of apparition of p in (R) satisfy the relation*

$$[\sigma_s, \sigma_t] = [\sigma_s, \sigma_{s\pm(m,t-s)}]. \tag{13.3}$$

[†] We use the usual notation $a|b$ for a divides b.

[‡] If λ_1 and λ_2 are the periods of $f(x)$ and $g(x)$ modulo p, the numbers a and b are subject to the conditions

$$(a, p^m - 1) = p^m - 1:\lambda_1, \qquad (b, p^m - 1) = p^m - 1:\lambda_2.$$

Proof. For convenience write $r+s$ in place of t so that (13.3) becomes

$$[\sigma_s,\ \sigma_{r+s}] = [\sigma_s,\ \sigma_{r\pm(m,r)}]. \tag{13.31}$$

By (13.1) and elementary properties of residuals

$$\begin{aligned} [\sigma_s,\ \sigma_{r+s}] &= p^m - 1 : (p^m - 1,\ a - bp^s,\ a - bp^{r+s}), \\ [\sigma_s,\ \sigma_{s\pm(m,r)}] &= p^m - 1 : (p^m - 1,\ a - bp^s,\ a - bp^{s\pm(m,r)}). \end{aligned} \tag{13.4}$$

Thus the proof reduces to showing that the two greatest common divisors on the right of (13.4) are equal. Now

$$\begin{aligned} (p^m - 1,\ a - bp^s,\ a - bp^{r+s}) &= (p^m - 1,\ p^s b(p^r - 1),\ a - bp^s) \\ &= (p^m - 1,\ b(p^r - 1),\ a - bp^s) \end{aligned}$$

since $(p^s,\ p^m-1)=1$; and we obtain

$$(p^m-1,\ a-bp^s,\ a-bp^{r+s}) = (p^m-1,\ b(p^{(m,r)}-1),\ a-bp^s)$$

since $(p^r-1,\ p^m-1) = p^{(m,r)}-1$. Hence since $(p^{s-(m,r)},\ p^m-1)=1$ and $(p^s,\ p^m-1)=1$,

$$\begin{aligned} (p^m - 1,\ a - bp^s,\ a - bp^{r+s}) &= (p^m - 1,\ p^{s-(m,r)} b(p^{(m,r)} - 1),\ a - bp^s) \\ &= (p^m - 1,\ a - bp^{s-(m,r)},\ a - bp^s), \\ (p^m - 1,\ a - bp^s,\ a - bp^{r+s}) &= (p^m - 1,\ p^s b(p^{(m,r)} - 1),\ a - bp^s) \\ &= (p^m - 1,\ a - bp^{s+(m,r)},\ a - bp^s). \end{aligned}$$

It follows from (13.3) that the $l(l-1)/2$ least common multiples $[\sigma_s,\ \sigma_t]$, $(s, t=1, \cdots, l; s<t)$, may be grouped into a certain number of sets such that all the members of a set are equal to one another.* For example, if $l=6$, $k=2$, we find that the fifteen least common multiples are grouped into six sets:

$$\begin{aligned} &[\sigma_1, \sigma_2] = [\sigma_2, \sigma_3] = [\sigma_3, \sigma_4] = [\sigma_4, \sigma_5] = [\sigma_5, \sigma_6] = [\sigma_1, \sigma_6]; \\ &[\sigma_1, \sigma_3] = [\sigma_1, \sigma_5] = [\sigma_3, \sigma_5]; \ [\sigma_2, \sigma_4] = [\sigma_4, \sigma_6] = [\sigma_2, \sigma_6]; \\ &[\sigma_1, \sigma_4]; \quad [\sigma_2, \sigma_5]; \quad [\sigma_3, \sigma_6]. \end{aligned}$$

The case when there is only one such set is of particular interest on account of the following easily proved theorem:

THEOREM 13.2. *If all of the $l(l-1)/2$ least common multiples $[\sigma_s, \sigma_t]$ are equal to one another, then if there is more than one rank of apparition of p in (R), the rank of p in (R) is the least common multiple of the two smallest σ_t. If the smallest σ_t divides the next smallest, there is only one rank of apparition.*†

* But not necessarily unequal to least common multiples in other sets.

† It must not be supposed that there are at most two ranks of apparition. For instance if $l=3$, we might conceivably have $\sigma_1=6$, $\sigma_2=10$, $\sigma_3=15$. The least common multiples $[\sigma_s, \sigma_t]$ then equal 30.

It can be shown from (13.3) by a simple enumeration that the hypothesis of the theorem is satisfied if $l=2$, 3 or 5; $l=6$ and $k\equiv 0 \pmod 4$; $l=7$ and $k\not\equiv 0 \pmod{60}$.

14. If we raise the congruence $\alpha^n\equiv\beta^{p^s n} \pmod p$ to the p^lth and p^kth powers successively, we obtain $\alpha^{(p^l-1)n}\equiv 1 \pmod p$, $\beta^{p^s(p^k-1)n}\equiv 1 \pmod p$. Hence if λ_1 and λ_2 denote the periods of $f(x)$ and $g(x)$,

$$n\equiv 0\ (\mathrm{mod}\ \lambda_1{:}p^l-1), \qquad n\equiv 0\ (\mathrm{mod}\ \lambda_2{:}p^k-1),$$

where we are using the notation already employed in §12 for residuals. Now $\lambda_1{:}p^l-1=\lambda_1{:}(\lambda_1, p^l-1)=\lambda_1{:}(\lambda_1, p^k-1, p^l-1)$ since λ_1 divides p^k-1. But $(p^k-1, p^l-1)=p^{(k,l)}-1$. Hence $\lambda_1{:}p^l-1=\lambda_1{:}p^{(k,l)}-1$. Similarly $\lambda_2{:}p^k-1=\lambda_2{:}p^{(k,l)}-1$. Hence $n\equiv 0$ (mod $[\lambda_1{:}p^{(k,l)}-1, \lambda_2{:}p^{(k,l)}-1]$) or

$$n\equiv 0\ (\mathrm{mod}\ [\lambda_1, \lambda_2]{:}p^{(k,l)}-1). \tag{14.1}$$

(14.1) gives us a *lower limit* for every rank of apparition σ of p in (R) in terms of the periods of the generators of (R). An upper limit may be obtained as follows:

If μ_1, μ_2 denote the restricted periods of $f(x)$ and $g(x)$ respectively; then

$$\alpha_1^{\mu_1}\equiv\alpha_2^{\mu_1}\equiv\cdots\equiv\alpha_k^{\mu_1}\equiv a \pmod p, \qquad \beta_1^{\mu_2}\equiv\beta_2^{\mu_2}\equiv\cdots\equiv\beta_l^{\mu_2}\equiv b \pmod p,$$

where a and b are rational integers. Then if ϕ is the least positive value of x such that $a^x\equiv b^x \pmod p$, every other such x is easily shown to be divisible by ϕ. Now ϕ as a divisor of $p-1$ is relatively prime to the restricted periods μ_1 and μ_2 (Ward [5]) and hence relatively prime to their least common multiple $[\mu_1, \mu_2]$. It readily follows that *the least positive value of n such that*

$$\alpha_1^n\equiv\alpha_2^n\equiv\cdots\equiv\alpha_k^n\equiv\beta_1^n\equiv\beta_2^n\equiv\cdots\equiv\beta_l^n \pmod p \tag{14.2}$$

is $\mu=\phi[\mu_1, \mu_2]$. *Every other such n is divisible by* μ. Since (14.2) is satisfied for $n=[\lambda_1, \lambda_2]$ we see that $\phi \mid [\lambda_1, \lambda_2]/[\mu_1, \mu_2]$.

It is now easy to show (compare M. Hall [1] or Ward [2]) that *every rank of apparition of p in (R) divides* μ. We thus obtain the following theorem:

Theorem 14.1. *Let the generators of (R) be irreducible modulo p with degrees k and l and with periods and restricted periods* λ_1, μ_1 *and* λ_2, μ_2 *respectively. Then for every rank of apparition* σ *of p in (R),*

$$[\lambda_1, \lambda_2]{:}(p^{(l,k)}-1) \tag{14.3}$$

divides σ; σ *divides* $\phi[\mu_1, \mu_2]$. *Here* ϕ *divides* $[\lambda_1, \lambda_2]/[\mu_1, \mu_2]$, *and* $\mu=\phi[\mu_1, \mu_2]$ *is the least positive value of n such that the congruence* (14.2) *holds.*

In particular if l and k are co-prime, $[\lambda_1, \lambda_2]{:}p^{(l,k)}-1=[\mu_1, \mu_2]$. Hence if σ is a rank of apparition of p so that $\alpha_i^\sigma\equiv\beta_j^\sigma \pmod p$, (14.3) implies that μ divides σ.

THEOREM 14.2. *If the generators of* (R) *are irreducible modulo* p *and if their degrees are relatively prime, there is only one rank of apparition of* p *in* (R). *This rank is the least positive value of* n *such that the congruence* (14.2) *holds, and it is a multiple of the least common multiple of the restricted periods of the generators of* (R), *and a divisor of the least common multiple of their periods.*

IV. APPLICATIONS TO GENERAL LUCASIAN SEQUENCES

15. We shall now prove Theorem 2.1 of the introduction. Let (u): $u_0, u_1, u_2, \cdots$ be a Lucasian sequence belonging to the polynomial $f(x)=x^k- \cdots -c_k=(x-\alpha_1)\cdots(x-\alpha_k)$, and let p be any prime dividing neither its constant term* c_k nor its discriminant $D=D_f=\pm\prod_{i<j}(\alpha_i-\alpha_j)^2$.

Let $\mathfrak{K}$ now denote the galois field of the roots of $f(x)=0$ and $\mathfrak{p}$ a prime ideal divisor of p in $\mathfrak{K}$. Then the general term u_n of (u) is of the form

$$u_n = \mathrm{A}_1\alpha_1^n + \cdots + \mathrm{A}_k\alpha_k^n,$$

where $D\mathrm{A}_1, \cdots D\mathrm{A}_k$ are integers of $\mathfrak{K}$, so that $\mathrm{A}_1, \cdots, \mathrm{A}_k$ are integers modulo $\mathfrak{p}$. Since (u) is a divisibility sequence, $u_n\equiv 0 \pmod{p}$ if and only if

$$\mathrm{A}_1\alpha_1^{mn} + \mathrm{A}_2\alpha_2^{mn} + \cdots + \mathrm{A}_k\alpha_k^{mn} \equiv 0 \pmod{\mathfrak{p}}, \qquad m = 1, 2, \cdots, k.$$

Thus the determinant of this system of congruences must be divisible by $\mathfrak{p}$. This determinant may be written $c_k^n\prod_{i<j}(\alpha_i-\alpha_j)U_n$. Since $\mathfrak{p}$ is prime to the first two terms, $U_n\equiv 0 \pmod{\mathfrak{p}}$ so that $U_n\equiv 0 \pmod{p}$. Hence every place of apparition of p in (u) is also a place of apparition of p in (U).

16. Suppose that the k (not necessarily distinct) nth powers of the roots of $f(x)=0$ are grouped modulo $\mathfrak{p}$ into t incongruent sets:

$$\text{(16.1)} \qquad \alpha_{i_1}^n \equiv \alpha_{i_2}^n \equiv \cdots \equiv \alpha_{i_{s_i}}^n \equiv \zeta_i \pmod{\mathfrak{p}}, \qquad i = 1, 2, \cdots, t,$$
$$\zeta_i \not\equiv \zeta_j \pmod{\mathfrak{p}} \quad \text{if} \quad i \neq j; \quad s_1 + s_2 + \cdots + s_t = k.$$

Furthermore let

$$\text{(16.2)} \qquad \mathrm{A}_i = \mathrm{A}_{i_1} + \mathrm{A}_{i_2} + \cdots + \mathrm{A}_{i_{s_i}}, \qquad i = 1, 2, \cdots, t.$$

THEOREM 16.1. *Any prime* p *which does not divide the discriminant of* $f(x)$ *divides a term* u_n *of the Lucasian sequence* (u) *belonging to* $f(x)$ *if and only if*

$$\mathrm{A}_i \equiv 0 \pmod{\mathfrak{p}}, \qquad (i = 1, 2, \cdots, t).$$

Here A_i *is given by formulas* (16.1), (16.2)† *and* $\mathfrak{p}$ *is any prime ideal divisor of* p *in the Galois field of the roots of* $f(x)=0$.

* If we are willing to assume that $u_0=0$, we may dispense with this first assumption. Marshall Hall [1] has shown that u_0 is usually zero.

† The groupings of the roots in (16.1) depend of course on our choice of $\mathfrak{p}$.

Proof. See Ward [2], pp. 284–285.

We may make this result more explicit by the use of Schatanovski's principle. Suppose that the decomposition of $f(x)$ modulo p is

$$f(x) \equiv f_1(x)f_2(x) \cdots f_r(x) \pmod{p},$$

where $f_i(x)$ is primary and irreducible modulo p and of degree k_i, and let the roots of $f_i(x)=0$ be $\gamma_1^{(i)}, \gamma_2^{(i)}, \cdots, \gamma_{k_i}^{(i)}$.

Then by Schatanovski's principle

$$u_n \equiv \overset{(1)}{u_n} + \overset{(2)}{u_n} + \cdots + \overset{(r)}{u_n} \pmod{p},$$

where

$$\overset{(i)}{u_n} = \overset{(i)}{\Gamma_1}\left\{\overset{(i)}{\gamma_1}\right\}^n + \cdots + \overset{(i)}{\Gamma_{k_i}}\left\{\overset{(i)}{\gamma_{k_i}}\right\}^n$$

satisfies the difference equation associated with $f^{(i)}(x)$ and

$$\overset{(i)}{\Gamma_j} = u(\overset{(i)}{\gamma_j})/f'(\overset{(i)}{\gamma_j})$$

(Ward [2], p. 283).

Construct the galois field $\mathfrak{K} = \mathfrak{R}\,(\gamma_1^{(1)}, \cdots, \gamma_{k_r}^{(r)})$, and let $\mathfrak{M}$ be the ring of integers of $\mathfrak{K}$. Then as in §10, p is a prime ideal of $\mathfrak{K}$, for p is prime to the discriminants and resultants of all the $f_i(x)$. Furthermore the ring $\mathfrak{K}/[p]$ is a finite field of order p^H where $H = [k_1, k_2, \cdots, k_r]$.

Suppose that in $\mathfrak{M}$ the nth powers of the roots of $f_1(x)=0, \cdots, f_r(x)=0$ are grouped modulo p into incongruent sets as in (16.1) so that we have, omitting subscripts,

$$\left\{\gamma^{(i)}\right\}^n \equiv \left\{\gamma^{(j)}\right\}^n \pmod{p}, \qquad i \neq j. \tag{16.3}$$

Then we deduce as in §14 that

$$n \equiv 0 \; (\bmod\ [\lambda^{(i)}, \lambda^{(t)}]:p^{(k_i,k_j)} - 1). \tag{16.4}$$

Here $\lambda^{(i)}$ and $\lambda^{(j)}$ are the periods of $f^{(i)}(x)$ and $f^{(j)}(x)$ modulo p, and k_i and k_j their degrees.

In particular, if $(k_i, k_j)=1$, then $[\lambda^{(i)}, \lambda^{(j)}]:p^{(k_i,k_j)}-1 = [\mu^{(i)}, \mu^{(j)}]$, where $\mu^{(i)}$ and $\mu^{(j)}$ are the restricted periods of $f^{(i)}(x)$ and $f^{(j)}(x)$. Now $\mu^{(i)}$ divides $p^{k_i}-1/p-1$, $\mu^{(j)}$ divides $p^{k_j}-1/p-1$, and

$$\left(\frac{p^{k_i}-1}{p-1}, \frac{p^{k_j}-1}{p-1}\right) = 1.$$

Hence we obtain from (16.4) the following theorem:

Theorem 16.2. *If the degrees of $f^{(i)}(x)$ and $f^{(j)}(x)$ are relatively prime to one another, then the congruence* (16.3) *can hold if and only if n is divisible by the product of the restricted periods of $f^{(i)}(x)$ and $f^{(j)}(x)$.*

In the simple case when $f(x)$ is irreducible modulo p, we easily find as in §12 that $u_n \equiv 0 \pmod{p}$ only if $n \equiv 0 \pmod{\lambda : p^d - 1}$.* Here d is some divisor of k and λ is the period of $f(x)$. In particular then if k is a prime number, there is only one rank of apparition of p in (u), the restricted period of (u).

It seems unprofitable to investigate the law of apparition in general Lucasian sequences in very much greater detail until it is definitely known whether or not Lucasian sequences exist which cannot be exhibited as divisors of R-sequences.

References

R. Fricke

1. *Algebra*, vol. 1, Braunschweig, 1926.

M. Hall

1. American Journal of Mathematics, vol. 58 (1936), pp. 577–584.
2. Journal of the London Mathematical Society, vol. 8 (1933), pp. 162–166.

D. Hilbert

1. *Die Theorie der Algebraischen Zahlkörper.*

D. H. Lehmer

1. *An extended theory of Lucas functions*, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448.
2. Annals of Mathematics, (2), vol. 34 (1933), pp. 461–472.

S. Lubelski

1. Journal für die Reine und Angewandte Mathematik, vol. 102 (1930), pp. 66–67.
2. Prace Matematyczno-Fizyczne, vol. 43 (1936), p. 214.

E. Lucas

1. American Journal of Mathematics, 1878, pp. 184–239, 289–321.
2. *Théorie des Nombres*, Paris, 1891.

T. A. Pierce

1. Annals of Mathematics, (2), vol. 18 (1916–1917), pp. 51–64.

P. Poulet

1. L'Intermédiaire des Mathématiciens, vol. 27, pp. 86–87; (2), vol. 1, p. 47; vol. 3, p. 61.

Schatanovski

1. Bulletin de la Société Physico-Mathématique de Kazan, (2), vol. 12 (1902), pp. 33–49 (in Russian).

M. Ward

1. Annals of Mathematics, (2), vol. 39 (1938), pp. 210–219.
2. These Transactions, vol. 41 (1937), pp. 276–286.
3. American Journal of Mathematics, vol. 59 (1937), pp. 921–926.
4. Duke Mathematical Journal, vol. 3 (1937), pp. 627–636.
5. Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 279–281.
6. Annals of Mathematics, (2), vol. 38 (1937), pp. 725–732.

* Dr. Marshall Hall has informed me by letter that he has also obtained this result.

California Institute of Technology,
Pasadena, Calif.