

Collected Papers of Morgan Ward

Masum Billal

February 4, 2020

About This Collection

This book is a collection of papers authored by Morgan Ward. Morgan Ward may not be that well known among most of the students now a days but his work has been really influential in many ways. He has some research results in some very important and interesting areas, specially recurring series. He authored 82 papers according to Lehmer [1]. The papers collected here are kept as the original ones. However, there are some papers that I could not get. By my count, I got 68 of those 82 papers here. A particular chapter contains the papers published in that year.

An important note please do not use this book for any commercial purposes. I do not own any copyright of the papers in any way. For adding the missing ones to this collection or for any suggestion, feel free to contact me at billalmasum93@gmail.com

Masum Billal
February 4, 2020

Contents

1 1927	1
2 1928	21
3 1929	33
4 1930	45
5 1931	63
6 1932	123
7 1933	137
8 1934	195
9 1935	225
10 1936	259
11 1937	279
12 1938	305
13 1939	367
14 1942	407
15 1945	415
16 1948	419
17 1949	465

18 1950	471
19 1951	495
20 1954	499
21 1955	509
22 1959	555
23 1960	561
24 1961	571
25 1962	581

Chapter 1

1927

A GENERALIZATION OF RECURRENTS

BY MORGAN WARD

1. *Introduction.* It is well known that if

$$\phi(x) = \sum_{r=0}^{\infty} \phi_r x^r, \quad \psi(x) = \sum_{s=0}^{\infty} \psi_s x^s$$

are two singly infinite series, then the coefficients in the expansion of $\phi(x)/\psi(x)$, $\log \phi(x)$, $e^{\phi(x)}$ can all be expressed as determinants in the quantities ϕ_r , ψ_s . These expressions are called *recurrents* and have been used by several writers* to evaluate determinants involving the binomial coefficients, Bernoulli numbers, etc.

In the present paper, the analogous results are given for the quotient of two *doubly* infinite series, and the logarithm and exponential of a doubly infinite series. The extension to m -tuply infinite series is briefly sketched in §8.

It is believed the expressions obtained are new; there is no reference to any such work in the four volumes of Muir's *History*. We assume throughout that all the series involved are absolutely convergent, so that the derangements and multiplications employed are justified. As a matter of fact, we are dealing essentially with infinite sets of quantities A_{rs} , B_{rs} , C_{rs} , \dots , ($r, s = 0, 1, 2, \dots$); the "variables" which appear in the series are merely convenient carriers for their coefficients.

We shall use, wherever convenient, the convention employed by writers on relativity for summations, namely,

$$U_{rs} x^r y^s,$$

which is taken to mean

$$\sum_{r=0}^{\infty} \sum_{s=0}^{\infty} U_{rs} x^r y^s,$$

the summations being understood.

* Muir's *History*, vols. II, III, IV, Chapters on recurrents.

2. *Degree and Rank.* Given a doubly infinite series

$$(1) \quad U(x, y) = U_{rs}x^r y^s,$$

we shall invariably write U in the order

$$U_{00} + U_{10}x + U_{01}y + U_{20}x^2 + U_{11}xy + U_{02}y^2 + \dots,$$

or as

$$(2) \quad U(x, y) = \sum_{l=0}^{\infty} \sum_{k=0}^l U_{l-k,k} x^{l-k} y^k.$$

We define

$$l = (l - k) + k, \quad u_{lk} = \frac{l(l+1) + 2(k+1)}{2},$$

as the *degree* and *rank* respectively of the coefficient $U_{l-k,k}$. Hence the degree of a coefficient is the degree of the term it multiplies. The rank of a coefficient is simply its place in the series (2). For since from (2) there are $l+1$ terms of degree l , the coefficient U_{l0} appears in the $[(1+2+3+\dots+l)+1]$ st place, that is,

$$u_{l0} = \frac{l(l+1)}{2} + 1.$$

The coefficient $U_{l-k,k}$ is k terms to the right of U_{l0} , so that its rank is

$$\frac{l(l+1)}{2} + 1 + k = \frac{l(l+1) + 2(k+1)}{2} = u_{lk}.$$

Thus for U_{rs} , the degree is $r+s$, and the rank is

$$(3) \quad u_{rs} = \frac{(r+s)(r+s+1) + 2(s+1)}{2}.$$

Moreover, it follows from the meaning of rank, that given any positive integer n , the equation

$$(4) \quad n = u_{rs}$$

determines a unique pair of non-negative integers r, s , and hence a unique coefficient U_{rs} in the series (2). Let k be any integer not greater than $r+s$. Then, by (3),

$$u_{r+s-k,k} = \frac{(r+s)(r+s+1) + 2(k+1)}{2};$$

hence

$$u_{r+s-k,k} + s - k = \frac{(r+s)(r+s+1) + 2(s+1)}{2} = u_{rs}.$$

In particular

$$(5) \quad u_{r+s,0} + s = u_{rs}, \quad s \leq r + s.$$

3. Coefficients for a Product.

If

$$A(x, y) = A_{qr}x^qy^r,$$

$$B(x, y) = B_{st}x^sy^t,$$

then we know that

$$A(x, y) \cdot B(x, y) = C_{uv}x^uy^v,$$

where

$$(6) \quad C_{uv} = \sum_{\sigma=0}^u \sum_{\tau=0}^v A_{u-\sigma, v-\tau} B_{\sigma\tau}.$$

4. Coefficients for a Quotient.

Consider now

$$P(x, y) = P_{uv}x^uy^v,$$

$$Q(x, y) = Q_{qr}x^qy^r,$$

and let

$$(7) \quad \frac{P(x, y)}{Q(x, y)} = Z(x, y) = Z_{st}x^sy^t,$$

where the coefficients Z_{st} are to be determined.

First, we can assume $Q_{00} \neq 0$. For, if $Q_{00} = Q_{10} = Q_{01} = \dots = 0$, $Q_{ii} \neq 0$, multiply both sides of (7) by x^iy^i , replacing $Q(x, y)/x^iy^i$ by $Q'(x, y)$ and $x^iy^iZ(x, y)$ by $Z'(x, y)$ with $Z'_{00} = Z'_{10} = Z'_{01} = \dots = 0$, $Z'_{ii} = Z_{00}$. We then have a new equality of the same form as (7) with $Q'_{00} = Q_{ii} \neq 0$. Thus $P(x, y) = Q(x, y)Z(x, y)$, or, by (6),

$$(8) \quad P_{uv} = \sum_{\sigma=0}^u \sum_{\tau=0}^v Q_{u-\sigma, v-\tau} Z_{\sigma\tau}, \quad (u, v = 0, 1, 2, \dots).$$

It may be noted in passing, that just as recurrents are related to difference equations with constant coefficients, so may (7), if $Q(x, y)$ be a polynomial, be looked upon as a linear partial difference equation with constant coefficients to determine Z_{uv} .

Let us introduce the symbol

$$(\lambda_{r-k,k} ; u - r + k, v - k),$$

defined by the relations

$$(9) \quad \begin{cases} \lambda_{r-k,k} = \frac{r(r+1) + 2(k+1)}{2}, \\ (\lambda_{r-k,k} ; u - r + k, v - k) = 0, \text{ if } r > u + k, \text{ or } k > v, \\ \quad \quad \quad = Q_{u-r+k,v-k}, \text{ if } k \leq v \text{ and } r \leq u + k. \end{cases}$$

Then (8) may be written

$$(10) \quad \sum_{r=0}^{u+v} \sum_{k=0}^r (z_{r-k,k} ; u - r + k, v - k) Z_{r-k,k} = P_{uv},$$

$$(p_{uv} = 1, 2, 3, \dots).$$

For $\lambda_{r-k,k} = z_{r-k,k}$, by definition of rank in (3). Moreover setting $r - k = \sigma$, $k = \tau$ in (10), we see that every term that occurs in (8) occurs in (10), and conversely.

Finally, by virtue of (9) we may replace (10) by

$$(11) \quad \sum_{r=0}^n \sum_{k=0}^r (z_{r-k,k} ; u - r + k, v - k) Z_{r-k,k} = P_{uv},$$

$$(p_{uv} = 1, 2, 3, \dots),$$

where n is any integer $\geq u + v$. Take $n = z_{ij}$ and consider the set of $n = p_{ij}$ equations (11), in the n unknowns Z_{00} , Z_{10} , Z_{01} , \dots , Z_{ij} ,

$$(12) \quad \begin{cases} Q_{00}Z_{00} & = P_{00}, \\ Q_{01}Z_{00} + Q_{00}Z_{10} & = P_{10}, \\ \dots & \dots \\ Q_{ij}Z_{00} + (2; i-1, j+1)Z_{10} + \dots + Q_{00}Z_{ij} & = P_{ij}. \end{cases}$$

Since $Q_{00} \neq 0$, we have, solving for Z_{ij} by determinants,

$$(13) \quad Q_{00}^n Z_{ij} = \begin{vmatrix} Q_{00} & 0 & 0 & \cdots & 0 & P_{00} \\ Q_{10} & Q_{00} & 0 & \cdots & 0 & P_{10} \\ Q_{01} & 0 & Q_{00} & \cdots & 0 & P_{01} \\ Q_{20} & Q_{10} & 0 & \cdots & 0 & P_{20} \\ Q_{11} & Q_{01} & Q_{10} & \cdots & 0 & P_{11} \\ Q_{02} & 0 & Q_{01} & \cdots & 0 & P_{02} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ Q_{ij}, (2 ; i-1, j+1), (3, i-2, j+2), \dots, P_{ij} \end{vmatrix},$$

where (13) is constructed on the following scheme. The elements in the s th column ($s < n$) consist of $s-1$ zeros, then the coefficients of $Q(x, y)$ of degree zero, one, two, three, \dots , in their proper order, the groups of coefficients of the same degree being separated by r' zeros, where $s = z_{r'-k', k'}$ determines r' . In fact, we see from (11), that the elements in the s th column are given by the expression

$$(14) \quad (s ; u - r' + k', v - k'),$$

where r' and k' are determined from the equation

$$z_{r'-k', k'} = s,$$

in accordance with (4), and (u, v) has the successive values

$$(15) \quad (0, 0), (1, 0), (0, 1), (2, 0), (1, 1), \dots, (u, v), \dots, (i, j),$$

$n = \lambda_{ij}$ in number, (u, v) appearing in the λ_{uv} th place in (15). Now the $\sigma+1$ terms (uv) of constant degree $u+v=\sigma$, $(0 \leq \sigma \leq i+j)$, appear in the order

$$(16) \quad (\sigma, 0), (\sigma - 1, 1), \dots, (\sigma - k, k), \dots, (0, \sigma).$$

If n is replaced u by $\sigma-v$, (14) becomes

$$(s ; \sigma - r' + k' - v, v - k'),$$

so that for $v=0, 1, 2, \dots, \sigma$, we have the values of (14) for the sequence (16). But this expression vanishes, by (9), unless

- (a) $v-k' \geq 0$,
- (b) $\sigma-r'+k'-v \geq 0$.

Thus the first k' terms of (16) yield k' zeros. Replace v by $r+k'$, where to satisfy (a) and (b) $0 \leq r \leq \sigma-r' \leq 0$. We thus obtain from the next $\sigma-r'+1$ terms of (15),

$$(s; \sigma-r', 0), (s; \sigma-r'-1, 1), \dots, (s; 0, \sigma-r'),$$

or by (9),

$$Q_{\sigma-r', 0}, Q_{\sigma-r'-1, 1}, \dots, Q_{0, \sigma-r'},$$

the coefficients of $Q(x, y)$ of degree $\sigma-r'$ in their proper order. The remaining terms of (16) produce $\sigma+1-k'-(\sigma-r'+1)=r'-k'$ zeros.

Since the sequence of degree $\sigma+1$ following (16) produces k' zeros followed by

$$Q_{\sigma+1-r', 0}, Q_{\sigma-r', 1}, \dots, Q_{0, \sigma+1-r'},$$

we see that the coefficients of degree $\sigma-r'=0, 1, 2, 3, \dots$ are separated by r' zeros, as stated. Q_{00} appears when $\sigma-r'=0$. From (a) and (b),

$$v = k', \quad u = \sigma - v = r' - k'.$$

Hence Q_{00} appears in the $\lambda_{r'-k', k'}$ or the s th place in the column; i. e., in (13), the elements Q_{00} lie along the main diagonal. The last column in (13) consists of the elements $P_{00}, P_{10}, P_{01}, \dots, P_{ij}$ in order of rank.

5. *Final Coefficients in the s th Column.* There is some doubt about the last few elements in the s th column, but this is obviated as follows. Take $s=z_{i+j-\tau, \tau}$, ($0 \leq \tau \leq j-1$), i. e., consider the $(n-j)$ th, $(n-j-1)$ th, \dots , $(n-1)$ th columns of (13).

We have then $s=n-j+\tau$ so that the s th column contains $n-j+\tau$ zeros, Q_{00} , followed by $i+j$ zeros by our results in §4. But since there are only n elements in the column, Q_{00} is followed by $j-\tau-1$ zeros, since $j-\tau-1$ is always

less than $i+j$. Hence we can reduce (13) to a determinant of the $(n-j)$ th order multiplied by Q_{00}^j to some power, for the j columns just considered consist entirely of zeros save along the main diagonal where Q_{00} appears.

Now $n = z_{ij}$ and $z_{i+j,0} + j = n$, by (5). Hence, setting $n-j=\nu$, we have

$$n - j = z_{i+j,0} = \frac{(i+j)(i+j+1)}{2} + 1 = \nu.$$

The elements in the ν th row are now

$$\begin{aligned} Q_{ii}, (2; i-1, j+1), (3; i-2, j+2), \dots, \\ (\nu-1; i-\nu+2, j+\nu-2), P_{ij} \end{aligned}$$

so that the s th column terminates with

$$(s; i-s+1, j+s-1)$$

and in the $(\nu-1)$ th row the elements are

$$\begin{aligned} (z_{r-k,k}; k-r, i+j-1-k) = \delta_{r+1,k+i} Q_{0,i+j-1-r}, \\ (r, k = 0, 1, 2, \dots, i+j-1), \end{aligned}$$

where δ_{uv} is the Kronecker symbol.

Thus we have

$$Q_{0,i+j-1,0}, Q_{0,i+j-2,0,0}, Q_{0,i+j-3,0,0,0}, \dots, Q_{00} P_{0,i+j-1},$$

so that our evaluation of Z_{ij} gives us

$$(17) \quad Q_{00}^{\nu} Z_{ij} = \left| \begin{array}{cccc} Q_{00} & 0 & \cdots & P_{00} \\ Q_{10} & Q_{00} & \cdots & P_{01} \\ Q_{01} & 0 & \cdots & P_{10} \\ Q_{20} & Q_{10} & \cdots & P_{20} \\ Q_{11} & Q_{01} & \cdots & P_{11} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{1,i+j-2} & \vdots & \ddots & \vdots \\ Q_{0,i+j-1} & 0 & \cdots & \cdot \\ Q_{ij} & (2; i-1, j+1), \dots & & P_{ij} \end{array} \right|,$$

where

$$\nu = \frac{(i+j)(i+j+1)}{2} + 1.$$

6. *Expression of the Z's as Recurrents.* There remains still one more simplification; the quantities $Z_{i+j,0}, Z_{0,i+j}$ can be expressed as recurrents. For we obtain from (7), §4, by the ordinary multiplication rule

$$(18) \quad P_{uv} = \sum_{t=0}^u \sum_{s=0}^v Q_{ts} Z_{u-t, v-s}, \quad (u, v = 0, 1, 2, 3, \dots).$$

This result may be written

$$(19) \quad P_{uv} - R_{uv} = \sum_{t=0}^u Q_{t0} Z_{u-t, v}, \quad (u = 0, 1, 2, 3, \dots),$$

where

$$(20) \quad R_{uv} = \sum_{t=0}^u \sum_{s=1}^v Q_{ts} Z_{u-t, v-s},$$

so that

$$R_{u0} = 0,$$

$$R_{u1} = \sum_{t=0}^u Q_{t1} Z_{u-t, 0},$$

$$R_{u2} = \sum_{t=0}^u Q_{t1} Z_{u-t, 1} + \sum_{t=0}^u Q_{t2} Z_{u-t, 0},$$

etc.

The formula (19) gives for $u = 0, 1, 2, 3, \dots, i+j$, the set of $i+j+1$ equations

$$Q_{00} Z_{0v} = P_{0v} - R_{0v},$$

$$Q_{10} Z_{0v} + Q_{00} Z_{1v} = P_{1v} - R_{1v},$$

$$Q_{20} Z_{0v} + Q_{10} Z_{1v} + Q_{00} Z_{2v} = P_{2v} - R_{2v},$$

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \end{array}$$

$$Q_{i+j,0} Z_{0v} + Q_{i+j-1,0} Z_{1v} + Q_{i+j-2,0} Z_{2v} + \dots$$

$$+ Q_{00} Z_{i+j,v} = P_{i+j,v} - R_{i+j,v},$$

so that

$$(21) \quad Q_{00}^{i+j+1} Z_{i+j,v} = \begin{vmatrix} Q_{00} & 0 & \cdots & P_{0v} - R_{0v} \\ Q_{10} & Q_{00} & \cdots & P_{1v} - R_{1v} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{i+j,0} & \cdots & \cdots & P_{i+j,v} - R_{i+j,v} \end{vmatrix}.$$

In particular

$$(22) \quad Q_{00}^{i+j+1} Z_{i+j,0} = \begin{vmatrix} Q_{00} & 0 & \cdots & P_{00} \\ Q_{10} & Q_{00} & \cdots & P_{10} \\ \vdots & \vdots & \ddots & \vdots \\ Q_{i+j,0} & \cdots & \cdots & P_{i+j,0} \end{vmatrix}.$$

which gives the required expression for $Z_{i+j,0}$ as a recurrent. From symmetry the expression for $Z_{0,i+j}$ is derived from (22) by simply interchanging the subscripts of all the terms in (21).

We may observe that, having obtained the quantities Z_{u0} by (22), we know R_{u1} , so that we can calculate the quantities $Z_{i+j-1,1}$ by means of (21). Proceeding thus step by step, we can finally calculate Z_{ij} .

There are a number of relations among the determinants (17), (22). For example, suppose we interchange x and y in the equation (7),

$$\frac{P(x,y)}{Q(x,y)} = Z(x,y).$$

The effect is merely to interchange the subscripts of the coefficients throughout. Hence in (17), we can interchange the subscripts of Z_{ij} , the Q 's and the P 's and obtain an expression for Z_{ji} , v , the order of the determinant, being unaffected by the process. Again, we may write (7) as

$$\frac{P(x,y)}{Z(x,y)} = Q(x,y),$$

so that we can interchange the roles of the Q 's and Z 's in (17).

7. Final Expressions for the Z's. The first eleven coefficients in the development of

$$\frac{P(x, y)}{Q(x, y)} = Z_{00} + Z_{10}x + Z_{01}y + \cdots + Z_{03}y^3 + \cdots$$

are

$$Z_{00} = Q_{00}^{-1} P_{00},$$

$$Z_{10} = Q_{00}^{-2} \begin{vmatrix} Q_{00} & P_{00} \\ Q_{10} & P_{10} \end{vmatrix}, \quad Z_{01} = Q_{00}^{-2} \begin{vmatrix} Q_{00} & P_{00} \\ Q_{01} & P_{01} \end{vmatrix},$$

$$Z_{20} = Q_{00}^{-3} \begin{vmatrix} Q_{00} & 0 & P_{00} \\ Q_{10} & Q_{00} & P_{10} \\ Q_{20} & Q_{10} & P_{20} \end{vmatrix}, \quad Z_{02} = Q_{00}^{-3} \begin{vmatrix} Q_{00} & 0 & P_{00} \\ Q_{01} & Q_{00} & P_{01} \\ Q_{02} & Q_{01} & P_{02} \end{vmatrix},$$

$$Z_{11} = Q_{00}^{-4} \begin{vmatrix} Q_{00} & 0 & 0 & P_{00} \\ Q_{10} & Q_{00} & 0 & P_{10} \\ Q_{01} & 0 & Q_{00} & P_{01} \\ Q_{11} & Q_{01} & Q_{10} & P_{11} \end{vmatrix},$$

$$= Q_{00}^{-4} \begin{vmatrix} Q_{00} & 0 & 0 & P_{00} \\ Q_{01} & Q_{00} & 0 & P_{01} \\ Q_{10} & 0 & Q_{00} & P_{10} \\ Q_{11} & Q_{10} & Q_{01} & P_{11} \end{vmatrix},$$

$$Z_{30} = Q_{00}^{-4} \begin{vmatrix} Q_{00} & 0 & 0 & P_{00} \\ Q_{10} & Q_{00} & 0 & P_{10} \\ Q_{20} & Q_{10} & Q_{00} & P_{20} \\ Q_{30} & Q_{20} & Q_{10} & P_{30} \end{vmatrix},$$

$$Z_{03} = Q_{00}^{-4} \begin{vmatrix} Q_{00} & 0 & 0 & P_{00} \\ Q_{01} & Q_{00} & 0 & P_{01} \\ Q_{02} & Q_{01} & Q_{00} & P_{02} \\ Q_{03} & Q_{02} & Q_{01} & P_{03} \end{vmatrix},$$

$$Z_{21} = Q_{00}^{-7} \begin{vmatrix} Q_{00} & 0 & 0 & 0 & 0 & 0 & P_{00} \\ Q_{10} & Q_{00} & 0 & 0 & 0 & 0 & P_{10} \\ Q_{01} & 0 & Q_{00} & 0 & 0 & 0 & P_{01} \\ Q_{20} & Q_{10} & 0 & Q_{00} & 0 & 0 & P_{20} \\ Q_{11} & Q_{01} & Q_{10} & 0 & Q_{00} & 0 & P_{11} \\ Q_{02} & 0 & Q_{01} & 0 & 0 & Q_{00} & P_{02} \\ Q_{21} & Q_{11} & Q_{20} & Q_{01} & Q_{10} & 0 & P_{21} \end{vmatrix},$$

$$Z_{12} = Q_{00}^{-7} \begin{vmatrix} Q_{00} & 0 & 0 & 0 & 0 & 0 & P_{00} \\ Q_{01} & Q_{00} & 0 & 0 & 0 & 0 & P_{01} \\ Q_{10} & 0 & Q_{00} & 0 & 0 & 0 & P_{10} \\ Q_{02} & Q_{01} & 0 & Q_{00} & 0 & 0 & P_{02} \\ Q_{11} & Q_{10} & Q_{01} & 0 & Q_{00} & 0 & P_{11} \\ Q_{20} & 0 & Q_{10} & 0 & 0 & Q_{00} & P_{20} \\ Q_{12} & Q_{11} & Q_{02} & Q_{10} & Q_{01} & 0 & P_{12} \end{vmatrix}.$$

8. *Quotient of two m -tuply Infinite Series.* The same method can be applied to the development of the quotient of two triply, or indeed of two m -tuply infinite series. We need only to generalize the formulas for degree and rank of §2, for product of two series in §3 and to introduce a symbol corresponding to the $(\lambda_{r-k,k}; u-r+k, v-k)$ of §4 to obtain the analog of (17); the analog of (21) is obtained with equal ease. Thus for the m -tuply infinite series,

$$A(x_1, \dots, x_m) = A_{i_1 i_2 \dots i_m} x_1^{i_1} x_2^{i_2} \dots x_m^{i_m},$$

$i_1 + i_2 + \dots + i_m$ is the *degree* of the coefficient A_i above and

$$(23) \quad a_{i_1 i_2 \dots i_m} = \sum_{r=1}^m \binom{i_r + i_{r+1} + \dots + i_m + m - r}{m - r + 1} + 1$$

is its *rank*, when A is written so that the terms of degree 0, 1, 2, \dots , r , $r+1$, \dots succeed each other in order, and the terms of degree r are arranged in alphabetic order.

For the product of two such series, we have the formula

$$A(x_1, \dots, x_m) \cdot B(x_1, \dots, x_m) = C(x_1, \dots, x_m),$$

where

$$(24) \quad C_{i_1, \dots, i_m} = \sum_{r=0}^j A_{i_1-r_1, i_2-r_2, \dots, i_m-r_m} B_{r_1, r_2, \dots, r_m}.$$

If we define $Z(x_1, \dots, x_m)$ by

$$(25) \quad \frac{P(x_1, \dots, x_m)}{Q(x_1, \dots, x_m)} = Z(x_1, \dots, x_m),$$

then our new symbol is

$$\Delta_{s_j} = (\lambda_{s_j}; j_1 - s_1 + s_2, j_2 - s_2 + s_3, \dots, \\ j_{m-1} - s_{m-1} + s_m, j_m - s_m),$$

defined by $\Delta_{s_j} = 0$ if $j_r - s_r + s_{r+1}$ is negative for any r between 0 and $m+1$, and

$$(26) \quad \Delta_{s_j} = Q_{i_1-s_1+s_2, \dots, i_m-s_m},$$

if $j_r - s_r + s_{r+1}$ is positive for every r between 0 and $m+1$, and by convention $s_{m+1} = 0$. But our final results in the general case are completely obscured by the symbolism introduced to express them.

9. *Expansion of a Logarithm.* We can readily obtain the expansion of

$$(27) \quad \log Q(x, y) = Z(x, y)$$

where

$$Q(x, y) = Q_{qr} x^q y^r, \quad Q_{00} \neq 0,$$

$$Z(x, y) = Z_{st} x^s y^t.$$

For, operating on (27) with

$$x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y},$$

we obtain a result of the form

$$\frac{P(x,y)}{Q(x,y)} = W(x,y),$$

where

$$W_{st} = (s+t)Z_{st}, \quad P_{uv} = (u+v)Q_{uv},$$

by Euler's theorem on homogeneous functions and our convention as to the order of an infinite series.

Thus $Z_{00} = \log Q_{00}$; the other coefficients are derived from our previous expressions by replacing Z_{ij} by $Z_{ij}/(i+j)$ and P_{uv} by $(u+v)Q_{uv}$.

10. *Expansion of an Exponential.* For $e^{Q(x,y)}$, a slightly different procedure is necessary. Let

$$(28) \quad \begin{cases} e^{Q(x,y)} = W(x,y), \\ \theta = x\frac{\partial}{\partial x} + y\frac{\partial}{\partial y}. \end{cases}$$

We shall have

$$(29) \quad \begin{cases} Q(x,y) = Q_{qr}x^qy^r, & \theta Q = (q+r)Q_{qr}x^qy^r, \\ W(x,y) = W_{st}x^sy^t, & \theta W = (s+t)W_{st}x^sy^t. \end{cases}$$

Then

$$(30) \quad \theta e^Q = \theta Q e^Q = (\theta Q) \cdot W = \theta W.$$

Hence, by (6),

$$(31) \quad (u+v)W_{uv} = \sum_{\sigma=0}^u \sum_{\tau=0}^v (u+v-\sigma-\tau)Q_{u-\sigma,v-\tau}W_{\sigma\tau}.$$

Now as in §4 introduce a symbol

$$(\lambda_{r-k,k}; u-r+k, v-k)$$

defined as in (9), with one modification, namely, while

$$\lambda_{r-k,k} = \frac{r(r+1) + 2(k+1)}{2}$$

and

$$\begin{aligned} (\lambda_{r-k,k}; u - r + k, v - k) &= 0, \quad \text{if } r > u + k, \text{ or } k > v, \\ &= (u + v - r)Q_{u-r+k, v-k}, \\ &\quad \text{if } k \leq v \text{ and } r \leq u + k, \end{aligned}$$

we have

$$(\lambda_{r-k,k}; u - r + k, v - k) = -(u + v),$$

for $k = v$ and $r = u + v$. Then (31) may be written in the form

$$(32) \quad \sum_{r=0}^{u+v} \sum_{k=0}^r (W_{r-k,k}; u - r + k, v - k) W_{r-k,k} = 0,$$

just as (10) was equivalent to (8) in §4. Also $(\lambda_{00}; 0, 0) = 0$, but from (28) we see that

$$e^{Q_{00}} = W_{00} = -P_{00}, \text{ say.}$$

Thus (28) becomes equivalent to (10) if we replace in each equation P_{uv} by 0 for $u+v>0$ and $(\lambda_{uv}; 0, 0)$ by $-(u+v)$, instead of by Q_{00} . We thus obtain the following set of w_{ij} equations for W_{ij} :

$$\begin{aligned} -W_{00} &= P_{00}, \\ 1 \cdot Q_{10}W_{00} - 1 \cdot W_{10} &= 0, \\ 1 \cdot Q_{01}W_{00} + 0 \cdot W_{10} - 1 \cdot W_{01} &= 0, \\ 2 \cdot Q_{20}W_{00} + 1 \cdot Q_{10}W_{10} + 0 \cdot W_{01} - 2W_{20} &= 0, \\ 2 \cdot Q_{11}W_{00} + 1 \cdot Q_{01}W_{10} + 1 \cdot Q_{10}W_{01} + 0 \cdot W_{20} - 2W_{11} &= 0, \\ 2 \cdot Q_{02}W_{00} + 0 \cdot W_{10} + 1 \cdot Q_{01}W_{01} + 0 \cdot W_{20} \\ &\quad + 0 \cdot W_{11} - 2W_{02} = 0, \\ \dots &\dots \\ (i+j)Q_{ii}W_{00} + \dots &= -(i+j)W_{ii} = 0. \end{aligned}$$

The determinant of this system is

$$\begin{aligned}
 & (-1)(-1)^2(-2)^3(-3)^4 \cdots \\
 & \quad (-i-j+1)^{i+j}(-i-j) \\
 & = (-1)^{\frac{i+j}{2}} 1^2 \cdot 2^3 \cdot 3^4 \cdots (i+j-1)^{i+j} (i+j)^j.
 \end{aligned}$$

Just as before, if we solve for W_{ij} , we can reduce the determinant we obtain corresponding to (12) to one of the ν th order,

$$\nu = \frac{(i+j)(i+j+1)}{2} + 1.$$

But we can also develop this expression with respect to its last row which is $P_{00}, 0, 0, \dots, 0$, obtaining a determinant of the $(\nu-1)$ st order with a factor $(-1)^{\nu-1}$. Hence our final form for W_{ij} is

$$1^2 \cdot 2^3 \cdot 3^4 \cdots (i+j-1)^{i+j} W_{ij}$$

$$= - \left| \begin{array}{ccccccc}
 Q_{10} & -1 & 0 & 0 & 0 & \cdots & 0 \\
 Q_{01} & 0 & -1 & 0 & 0 & \cdots & 0 \\
 2Q_{20} & Q_{10} & 0 & -2 & 0 & \cdots & 0 \\
 2Q_{11} & Q_{01} & Q_{10} & 0 & -2 & \cdots & 0 \\
 2Q_{02} & 0 & Q_{01} & 0 & 0 & \cdots & 0 \\
 \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
 \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
 & & & & & & 0 \\
 \cdots & \cdots & \cdots & \cdots & \cdots & - (i+j-1) & \\
 (i+j) Q_{ii} (2, i-1, j+1) & & & & & \cdots &
 \end{array} \right|.$$

As before, we can interchange subscripts of all the Q 's to obtain W_{ii} . We can also express $W_{i+j,0}$ and $W_{0,i+j}$ as recurrents; thus

$$(i+j-1)!W_{i+j,0} = - \begin{vmatrix} Q_{10} & -1 & & 0 \\ 2Q_{20} & Q_{10} & -2 & 0 \\ 3Q_{30} & 2Q_{20} & Q_{10} & -3 \\ \vdots & \vdots & \vdots & \vdots \\ & & & -(i+j) \\ (i+j)Q_{i+j,0} \dots & & & Q_{10} \end{vmatrix}$$

with a similar expression for $W_{0,i+j}$.

11. *Conclusion.* It hardly seems necessary to give numerical examples of these expansions. As in the case of recurrents, from expressions of such generality any desired example may be derived by a mere substitution of numbers for letters in the general formulas. The quotient of two polynomials, the reciprocal of a series or a polynomial, for example, are included as special cases.

It appears from the expressions for Z_{21} and Z_{12} in §7, that a further immediate reduction of the order of the determinants (17) is sometimes possible; but to explicate this reduction in the general case would be to mar the simplicity and symmetry of our developments.

In conclusion I should like to thank Professor E. T. Bell for criticism and suggestions in the writing of this paper.

CALIFORNIA INSTITUTE OF TECHNOLOGY

A CORRECTION

In the paper by H. W. March, *The Heaviside operational calculus*, this Bulletin, vol. 33(1927), on page 312, in the line following equation (2), change "negative" to "positive."

The author is glad to acknowledge his indebtedness to Professor G. N. Lewis for his interest and helpful suggestions; to Dr. Simon Freed for his kind advice throughout the work in a field with which the author was not familiar; and to Beatrice Wulf with whom much of the experimental work was done.

* NATIONAL RESEARCH FELLOW IN CHEMISTRY.

¹ Becquerel, *Compt. rend.*, **92**, 348 (1881).

² Schumeister, *Sitz. Akad. Wiss. Wien*, II, **83**, 45 (1881).

³ Lewis, *Valence and the Structure of Atoms and Molecules*, Chemical Catalog Co., 1923, pages 130, 147 et seq; *Chemical Reviews*, **1**, 234 (1924).

⁴ See, for example, Stoner, *Magnetism and Atomic Structure*, E. P. Dutton and Co., 1926, page 40.

⁵ The expression for oxygen was calculated from an average value of the volume susceptibility using the three recent values listed by Stoner in Table IX of his book, see ref. 4. The expression for air was obtained from this and from the composition of air, taking account of the oxygen only.

GENERAL ARITHMETIC

BY MORGAN WARD

CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA

Communicated October 15, 1927

The abstract theory of a mathematical system consisting of a set of elements and two operations "multiplication," and, later, "addition" is developed by postulational methods with examples.

The more important results are the following. An "arithmetic" may be roughly described as a system in which

1. Every element is completely specified by a finite number of cardinal numbers.

2. "Division" is not always possible, and we can find when one element divides another element in a finite number of steps.

3. Unique resolution into "prime factors" is always possible.

For the case when multiplication is commutative we replace these vague requirements by an exact set of postulates, the necessary and sufficient conditions for a system to form an arithmetic. We give a general theory of recurring sequences, exhibiting the connections with the Dedekind field theory which we develop following Kronecker, as an arithmetic of forms without assuming the so-called "fundamental theorem of algebra." We next show that all systems of ideals and ideal numbers are abstractly equivalent and may be replaced by the system of rational integers, making ideals and ideal numbers unnecessary in algebraic arithmetic.

An arithmetic may be defined over any arbitrary class of distinct de-

numerable elements, and conversely any arithmetic determines such a class, giving connections with the algebra of logic. These connections are destroyed if we assume "multiplication" is not commutative.

For the case when multiplication is not a commutative, we replace "division" by "left division" and "right division," with analogous changes for other relations such as "equivalence." We then develop the theory of the greatest common divisor, least common multiple, equivalence with respect to unit factors and so on. It is shown that for an arithmetic, we must assume the units of the system are commutative with all the other elements of the system. Any "arithmetic" may be converted into a group by adjunction, and the theory of congruence and the fundamentals of Kronecker's theory of forms carry over almost unchanged. The complete development will be published shortly in a mathematical journal.

ON THE STRUCTURE OF A PLANE CONTINUOUS CURVE¹

BY W. L. AYRES

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA

Communicated October 11, 1927

If x and y are distinct points of a continuous curve M , the set of all points $[z]$, such that z lies on some arc of M with end-points x and y , is called the *arc-curve* xy and is denoted by $M(x + y)$. This was defined in a previous paper, "Concerning the Arc-Curves and Basic Sets of a Continuous Curve."² Among other results this paper contained the following theorems for the case where M lies in a plane:

- A.—The arc-curve xy is itself a continuous curve.
- B.—If K is a maximal connected subset of $M - M(x + y)$, then K has only one limit point in $M(x + y)$.
- C.—If P is a point of a set K such that $K - P$ is the sum of two non-vacuous mutually separated sets K_1 and K_2 , and A and B are distinct points of $K_1 + P$, then no point of K_2 is a point of any arc whose end-points are A and B and which lies wholly in K .

It is the purpose of this paper to characterize types of points of a continuous curve and types of continuous curves by a set which is the limit of the arc-curve xy as y approaches x . Throughout the paper the letter M is used to denote a plane continuous curve and all point sets mentioned are considered as subsets of M . The theorems listed above will be referred to as "Theorem A," etc.

THEOREM 1.—*If the point x lies on no simple closed curve of M and α is any arc of M whose end-points are x and any other point z of M , then x is a limit point of the points of M which lie on α and separate x and z in M .³*

Chapter 2

1928

Γ . Let $\bar{\lambda}_1, \dots, \bar{\lambda}_r$ be any set of complex numbers and let the resulting numerical equation

$$f(x; \bar{\lambda}_1, \dots, \bar{\lambda}_r) \equiv x^n + a_1 x^{n-1} + \dots + a_n = 0 \quad (2)$$

have the group Γ_0 with respect to $K(a_1, \dots, a_n)$. Then Γ_0 is a sub-group of Γ .

We shall next consider a normal division algebra A , in n^2 units, over K . It is known that if u_1, \dots, u_m are a basis of A and $\lambda_1, \dots, \lambda_m$ are independent variables in K , the general element of A ,

$$a = \lambda_1 u_1 + \lambda_2 u_2 + \dots + \lambda_m u_m, \quad m = n^2$$

is a root of a uniquely defined rank equation $f(x, \lambda_1, \dots, \lambda_m) = 0$ with leading coefficient unity and further coefficient polynomials, with coefficients in K , of $\lambda_1, \dots, \lambda_m$. Also the degree of f is n . We have proved, using theorem 1 and the known theory of division algebras, the theorem:

THEOREM 2. Let A be a normal division algebra over K . Then the group of its rank equation with respect to K is the symmetric group.

Applying the Hilbert irreducibility theorem we have

THEOREM 3. Every normal division algebra A , in n^2 units, over F contains an infinity of elements each satisfying an equation of degree n , with leading coefficient unity and further coefficients in K , such that the group of the equation with respect to K is the symmetric group.

¹ NATIONAL RESEARCH FELLOW.

POSTULATES FOR AN ABSTRACT ARITHMETIC

By MORGAN WARD

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY

Communicated October 29, 1928

1. *Introduction.*—In a previous communication ("General Arithmetic," These PROCEEDINGS, November, 1927) I have described an "arithmetic" as a system in which

(a) Every element is completely specified by a finite number of cardinal numbers.

(b) "Division" is not always possible, and we can find when one element divides another in a finite number of steps.

(c) Unique resolution into "prime factors" is always possible.

I here give a precise definition of an abstract arithmetic, that is, one whose elements are marks in the technical sense, and state a few of its simpler properties. The principal advance over the work summarized

in "General Arithmetic" lies in the fact that I no longer assume that "multiplication" is commutative.

2. *Definition of an Arithmetic.*—A system Σ consisting of a denumerable set of elements a, b, \dots and a function $x \circ y$ is said to form an *abstract arithmetic* if the following six conditions are satisfied:

Postulate 1; Closure.—For any two elements a, b of Σ , $a \circ b$ is a uniquely determined element of Σ .

Postulate 2; Associativity.—For any three elements a, b, c of Σ ,

$$(a \circ b) \circ c = a \circ (b \circ c).$$

Postulate 3; Existence of Identity.—There exists an element i of Σ such that $i \circ i = i$.

Postulate 4; Cancelativity.—If a, b, c, b', c' are any five elements of Σ , and if

$$b \circ a \circ c = b' \circ a \circ c',$$

then

$$b \circ c \curvearrowleft b' \circ c'. \quad (1)$$

(for the meaning of the symbol \curvearrowleft , see §4 (iv))

$$b = b' \text{ if } c = c' \quad (2)$$

$$c = c' \text{ if } b = b'. \quad (3)$$

Postulate 5; Integrality.—(1) There exists at least one integral element.

(2) Every integral element has only a finite number of distinct integral divisors. (For the meanings of *integral element* and *distinct integral divisor*, see §4(iii), (iv).)

Postulate 6; Primitivity.—If a divides $b \circ c$, then a is not prime to both b and c . (For meanings of *divide* and *prime*, see §4 (v), (vii).)

3. *Properties of the Postulates.*—The six postulates above are consistent; and, with the possible exception of Pos. 2, they are independent. Pos. 3, though not strictly necessary, greatly simplifies the statement of Pos. 4. It is satisfied in all the instances of an arithmetic of practical interest. If Pos. 5 (1) is contradicted, Pos. 5 (2) asserted, Σ is a finite group. If both parts of Pos. 5 are contradicted, omitting the word *integral* Σ is an infinite discrete group. The consequences of asserting the first part of Pos. 5 and contradicting the second are not known; they would appear to be trivial.

If Pos. 6 is contradicted, the introduction of ideals is necessary to restore unique factorization. These ideals can be constructed abstractly; they are additional marks which we adjoin to Σ . Their complete theory is known. Postulates 1, 2, 4—(2) (3) are due to Dickson (*Transactions A. M. S.*, vol. 6, 1905, pp. 205–208) and serve to define a semi-group.

4. *Elementary Properties of an Arithmetic.*—The following results are easily deduced from the postulates in §2.

(i) THE IDENTITY.—The element i of Pos. 3 is unique. It is called the identity of Σ , and denoted by 1. For every element s of Σ ,

$$1 \circ s = s \circ 1 = s$$

(ii) UNITS.—If for any element a of Σ there exists an element a' , such that

$$a \circ a' = 1,$$

a is called a *unit* and a' its inverse.

1 is a unit, and the units of Σ form a group, denoted by E . We use $\epsilon, \epsilon', \dots$ to denote units. If

$$a \circ b \circ \dots \circ k = \epsilon, \text{ then } a, b, \dots k$$

are all units.

(iii) INTEGRAL ELEMENTS.—Every element of Σ which is not a unit is called an integral element, and Σ contains an infinite number of integral elements.

(iv) EQUIVALENCE.—Two integral elements a, b are said to be equivalent if there exists units ϵ, ϵ' such that

$$\epsilon \circ a \circ \epsilon' = b$$

NOTATION.

$$a \sim b$$

The relation \sim is transitive, symmetric and reflexive. It is trivial in E , but not all integral elements are equivalent. Two elements which are not equivalent are said to be distinct.

THEOREM A.—If $b \circ a \circ c \sim b' \circ a' \circ c'$ and $a \sim a'$, then $b \circ c \sim b' \circ c'$.

(v) DIVISION.— a is said to divide b if there exists two elements x, y of Σ , such that

$$x \circ a \circ y = b.$$

NOTATION.

$$a D b$$

The relation D is transitive, non-symmetric and reflexive. The necessary and sufficient condition that two elements of Σ be equivalent is that they both divide each other.

THEOREM B.—If $a D b$ and $a \sim a'$, $b \sim b'$, then $a' D b'$.

(vi) IRREDUCIBLE ELEMENTS.—An element of Σ whose only integral divisor is itself is said to be irreducible. Equivalent elements are simultaneously reducible or irreducible.

(vii) COMMON DIVISORS.—Let b, c be two distinct integral elements of Σ . Every integral element a which divides both b and c is called a common divisor of b and c .

(viii) CO-PRIME ELEMENTS.—Two elements a and b of Σ without any common divisors are said to be co-prime. We also say a is prime to b .

NOTATION.

$a P b$

The relation P is intransitive, symmetric and irreflexive.

5. *Fundamental Theorem of Arithmetic*.—“Every integral element of Σ can be resolved in one way only into a product of irreducible elements, provided we take no account of unit factors, nor of the order in which the irreducible elements occur.”

Proof.—Let s be any integral element of Σ . By Pos. 5, s has only a finite number of distinct irreducible divisors. Suppose that

$$s \curvearrowleft a_1 \circ a_2 \circ \dots \circ a_k \curvearrowleft b_1 \circ b_2 \circ \dots \circ b_l$$

are two resolutions of s into products of irreducible factors, so that a, b' are irreducible, but not necessarily distinct. (See §4 (v).) Consider any a_u ($1 \leq u \leq k$)

Since $a_u D s, a_u D (b_1 \circ \dots \circ b_l)$ by theorem B. Therefore, by Pos. 6, either

- (a) a_u and b_1 have a common factor, or
- (b) a_u and $b_2 \circ \dots \circ b_l$ have a common factor. Now clearly if (a) is true $a_u \curvearrowleft b_1$; but if (a) is false

$$a_u D (b_2 \circ \dots \circ b_l)$$

since a_u is irreducible. Hence, by Pos. 6 again, either

- (a') a_u and b_2 have a common factor, or
- (b') a_u and $b_3 \circ \dots \circ b_l$ have a common factor. If (a') is true,

$$a_u \curvearrowleft b_2.$$

Proceeding in this way we see that

$$a_u \curvearrowleft b_v \quad (1 \leq v \leq l).$$

But $a_1 \circ \dots \circ a_k \curvearrowleft b_1 \circ \dots \circ b_l$ hence

$$\begin{aligned} a_1 \circ a_2 \circ \dots \circ a_{u-1} \circ a_{u+1} \circ \dots \circ a_k \curvearrowleft \\ b_1 \circ b_2 \circ \dots \circ b_{v-1} \circ b_{v+1} \circ \dots \circ b_l \end{aligned}$$

by theorem A.

Thus every a divides a b and, similarly, every b divides an a , so that $l =$

k and $b_1 \circ \dots \circ b_l$ consists of the irreducible factors a of s taken perhaps in a different order.

6. *Instances of an Arithmetic.*—The rational integers, the complex integers and Dedekind ideals are instances of an abstract arithmetic. The set of all square non-singular matrices of order m taken over an arbitrary ring satisfy the first five of these postulates, with \circ interpreted as multiplication.

The first two requirements for an arithmetic in §1 are in part a limitation upon the possible instances of an arithmetic; for instance, if a set of marks is denumerable, each element may be completely specified by precisely one cardinal number, so that the first requirement is trivial. The second requirement is more complicated and cannot be discussed fully here.

ON THE CHARACTERISTIC VALUES OF LINEAR INTEGRAL EQUATIONS

BY EINAR HILLE AND J. D. TAMARKIN

PRINCETON UNIVERSITY AND BROWN UNIVERSITY

Communicated November 7, 1928

1. We consider the integral equation

$$f(x) = \varphi(x) - \lambda \int_a^b K(x, s)\varphi(s)ds, \quad (1)$$

where the kernel is supposed to belong to the class (L^2) , i.e., $K(x, s)$ and its square are Lebesgue integrable in $a \leq x, s \leq b$. The equation is known to possess a resolvent kernel which is the quotient of two entire functions of λ , defined by Fredholm's formulas with the modifications due to Hilbert.¹ The characteristic values of the equation are the zeros of the denominator $D_K^*(\lambda)$ in this quotient. The order ν of $D_K^*(\lambda)$ is ≤ 2 , and if $\nu = 2$ the function belongs to the minimal type; its genus is at most unity. This result is due to Carleman.²

2. The proof given by Carleman is ingenious but also rather complicated. It is possible, however, to base the proof upon a simple and well-known method, namely, that of infinitely many equations in infinitely many unknowns. Let $\{\omega_i(x)\}$ be a complete orthonormal system for the interval (a, b) . Then $\{\omega_i(x)\overline{\omega_j(s)}\}$ constitutes a complete orthonormal system for the square $a \leq x, s \leq b$. Put

$$f_i = \int_a^b f(s)\overline{\omega_i(s)}ds, \quad \varphi_i = \int_a^b \varphi(s)\overline{\omega_i(s)}ds,$$

way as to render the calculation difficult, and special functions have been invented for the graphing, to avoid these inconvenient figures and permit an accurate determination of the area.

Any advances which permit an increased accuracy in graphical calculations will be welcomed by the chemist.

18. Conclusion. It has been the purpose of this article to point out some of the mathematical needs of modern chemistry. It would be appreciated if courses in mathematics could emphasize some of these things, along with the calculations of volumes, lengths of curves, and moments of inertia and other calculations which are included for the benefit of the engineer. The present courses should not be changed, however, for mathematics is much more valuable to the student of chemistry as a mental training than as a source of technical methods. In physical chemistry the chief aim is to emphasize the research point of view and to interest the student in the mechanism of natural phenomena and there is no better way to develop the necessary originality in a student than to have him solve hundreds and thousands of problems in pure mathematics.

A SIMPLIFICATION OF CERTAIN PROBLEMS IN ARITHMETICAL DIVISION

By MORGAN WARD, California Institute of Technology

1. Like all inverse operations, the process of dividing one integer by another requires certain tentative steps irresolvable into the direct operations of addition and multiplication. Any method of division has then a three-fold aim: to reduce as far as possible (1) the number of these tentative steps, (2) the difficulty of each step, and (3) the amount of addition, multiplication and mere copying necessary to combine the results of the separate steps into the correct quotient. These aims conflict to a certain extent and our ordinary "long" division is a sort of compromise between them. It may in fact be considerably improved as regards the third requirement.¹

The object of this paper is to exhibit a method of division satisfying the requirements above and applicable to a class of problems where solution by ordinary division is excessively laborious, if not impossible. Our main result is given in section 4; its proof, which rests upon the most elementary properties of congruences and power residues, is developed in sections 2 and 3. The concluding section is devoted to numerical examples.

¹ See a discussion of "long" division by L. S. Dederick in this Monthly, vol. 33 (1926), pp. 143-144.

2. In what follows small italic and Greek letters stand for positive integers or zero.

Denote the quotient obtained on dividing a by $b \neq 0$ by

$$(1) \quad [a/b] = q \text{ so that } a = qb + r \quad 0 \leq r < b.$$

Then $q=0$ when $b>a$ and is otherwise a positive integer. It is to be understood that b is never zero in the symbol $[a/b]$. Let us develop some of the properties of the symbol.

First, if $b=b_1 \cdot b_2$, it is easily shown¹ that

$$(I) \quad \left[\frac{a}{b_1 b_2} \right] = \left[\frac{\left[\frac{a}{b_1} \right]}{b_2} \right] = \left[\frac{\left[\frac{a}{b_2} \right]}{b_1} \right]$$

Suppose $a=a_1 \cdot a_2$. Let $[a_1/b]=q_1$ and $[a_2/b]=q_2$ so that $a_1=bq_1+r_1$ and $a_2=bq_2+r_2$ ($0 \leq r_1, r_2 < b$). Then $a_1 a_2 = (bq_1 q_2 + q_1 r_2 + q_2 r_1)b + r_1 r_2$. Hence

$$(II) \quad \left[\frac{a_1 a_2}{b} \right] = b \left[\frac{a_1}{b} \right] \left[\frac{a_2}{b} \right] + r_2 \left[\frac{a_1}{b} \right] + r_1 \left[\frac{a_2}{b} \right] + \left[\frac{r_1 r_2}{b} \right].$$

The following special cases of II are to be noted:

First, if $r_2=0$,

$$(IIa) \quad \left[\frac{a_1 a_2}{b} \right] = b \left[\frac{a_1}{b} \right] \left[\frac{a_2}{b} \right] + r_1 \left[\frac{a_2}{b} \right] = a_2 \left[\frac{a_1}{b} \right] + r_1 \left[\frac{a_2}{b} \right].$$

Secondly, if $q_2=0$, then $a_2 < b$, $[a_2/b]=0$, $r_2=a_2$, and

$$(IIb) \quad \left[\frac{a_1 a_2}{b} \right] = a_2 \left[\frac{a_1}{b} \right] + \left[\frac{a_2 r_1}{b} \right].$$

Also if $a=a_1+a_2$,

$$(III) \quad \begin{aligned} \left[\frac{a}{b} \right] &= \left[\frac{a_1}{b} \right] + \left[\frac{a_2}{b} \right] + \left[\frac{(r_1 + r_2)}{b} \right], \quad \text{where} \\ 0 \leq \left[\frac{(r_1 + r_2)}{b} \right] &\leq 1. \end{aligned}$$

3. Assume now that a is greater than b and prime to it,

$$(2) \quad U_m = \left[\frac{a^m}{b} \right]. \quad \text{Then} \quad (2a) \quad U_0 = U_1 = 0.$$

We seek the general expression for U_m .

¹ Reid: *Elements of the Theory of Algebraic Numbers*, p. 27.

Let r be the least positive integer for which

$$(3) \quad a^{r+1} \equiv a \pmod{b}.$$

That is, r is the exponent to which a belongs, modulo b , so that a, a^2, a^3, \dots, a^r are all distinct. Let $a^s \equiv a_s \pmod{b}$ ($0 \leq a_s < b$) and

$$(4) \quad V_s = [aa_s/b], \text{ so that } V_0 = 0, \quad V_s < b.$$

Then by (3), (4), $V_s = V_t$ when and only when $s \equiv t \pmod{r}$.

By (IIb), $U_m = [a \cdot a^{m-1}/b] = a[a^{m-1}/b] + [a \cdot a_{m-1}/b]$, $m \geq 1$; or, by (2) and (4),

$$(5) \quad U_m = aU_{m-1} + V_{m-1}.$$

Thus $U_2 = aU_1 + V_1 = V_1$; $U_3 = aU_2 + V_2 = aV_1 + V_2$. Assume for some $s \geq 2$

$$U_s = a^{s-2}V_1 + a^{s-3}V_2 + \dots + aV_{s-2} + V_{s-1} = \sum_{K=1}^{s-1} a^{s-1-K}V_K.$$

Then

$$U_{s+1} = aU_s + V_s = \sum_{K=1}^{s-1} a^{s-K}V_K + V_s = \sum_{K=1}^s a^{s-K}V_K$$

or

$$U_{s+1} = \sum_{K=1}^{(s+1)-1} a^{(s+1)-1-K}V_K,$$

so that, by induction, for any $m \geq 1$

$$(6) \quad U_m = \sum_{K=1}^{m-1} a^{m-1-K}V_K.$$

Now suppose

$$(7) \quad m - 1 = kr + \alpha \quad (0 \leq \alpha < r, \quad k \geq 0).$$

Divide K in (6) by r and let the quotient be τ and the remainder σ ($0 \leq \tau \leq k$, $0 \leq \sigma < r$). Set $K = \tau_1r + \sigma_1$ ($0 \leq \sigma \leq \alpha$) and $K = \tau_2r + \sigma_2$ ($\alpha < \sigma \leq r-1$). Then (6) may be written

$$\begin{aligned} U_m &= \sum_{\tau_1=0}^k \sum_{\sigma_1=0}^{\alpha} a^{(k-\tau_1)r+\alpha-\sigma_1} V_{\tau_1r+\sigma_1} + \sum_{\tau_2=0}^{k-1} \sum_{\sigma_2=\alpha_1}^{r-1} a^{(k-1-\tau_2)r+\alpha+r-\sigma_2} V_{\tau_2r+\sigma_2} \\ &= \sum_{\tau_1=0}^k a^{(k-\tau_1)r} \sum_{\sigma_1=0}^{\alpha} a^{\alpha-\sigma_1} V_{\sigma_1} + \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} \sum_{\sigma_2=\alpha_1}^{r-1} a^{\alpha+r-\sigma_2} V_{\sigma_2} \\ &= \sum_{\tau_1=0}^k a^{(k-\tau_1)r} \sum_{\sigma_1=0}^{\alpha} a^{\alpha-\sigma_1} V_{\sigma_1} + \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} \sum_{\sigma_1=1}^{r-1-\alpha} a^{\alpha+\sigma_1} V_{\alpha+\sigma_1} \end{aligned}$$

on replacing in the second expression $r - \sigma_2$ by σ_1 and changing the order of summation. But

$$\sum_{\tau_1=0}^k a^{(k-\tau_1)r} = \frac{a^{(k+1)r} - 1}{a^r - 1}; \quad \sum_{\tau_2=0}^{k-1} a^{(k-1-\tau_2)r} = \frac{a^{kr} - 1}{a^r - 1}.$$

Hence we obtain the following theorem.

4. THEOREM: "Let b be any integer greater than a but not a power of a , and let m be any positive integer. Let k and α denote the quotient and remainder obtained on dividing $m-1$ by the least positive integer r for which $a^{r+1}-a$ is divisible by b . Then the quotient on dividing a^m by b is given by

$$(IV) \quad \left[\frac{a^m}{b} \right] = \frac{a^{(k+1)r} - 1}{a^r - 1} (a^{\alpha-1}V_1 + a^{\alpha-2}V_2 + \cdots + aV_{\alpha-1} + V_\alpha) \\ + \frac{a^{kr} - 1}{a^r - 1} a^\alpha (aV_{\alpha+1} + a^2V_{\alpha+2} + \cdots + a^{r-\alpha-1}V_{r-1}),$$

where $V_i = [a \cdot a_i / b]$ ($1 \leq i \leq r-1$) and a_i is the least positive residue of a^i modulo b ."

The numbers V_i must be found by trial. They are always less than b and can be readily computed in conjunction with the a_i 's; for from (4) we have $V_s = [a \cdot a_s / b]$, $a_{s+1} \equiv a^{s+1} \equiv a \cdot a^s \equiv a \cdot a_s \pmod{b}$, $0 \leq a_{s+1} < b$, or $a \cdot a_s = b \cdot V_s + a_{s+1}$, so that V_s is the quotient and a_{s+1} the remainder on dividing $a \cdot a_s$ by b . We can thus determine V_1, V_2, \dots, V_{r-1} step by step. If we have found by any means the residue system $a_1, a_2, \dots, a_s, \dots, a_{r-1}$, say by a table of indices modulo $b/(b, a)$, we have

$$(8) \quad V_s = (a \cdot a_s - a_{s+1})/b$$

which for small b 's gives V_s by inspection.

The expressions in brackets in IV are indeed numbers in the scale a .

If the V 's are assumed known, IV involves only additions and multiplications, for the first terms in each line are merely the sums of geometric progressions. Hence we have here a *formula* for the quotient of a^m by b .

There are several special cases of IV. First $\alpha=0$ if $m-1$ is exactly divisible by r , and IV becomes

$$\left[\frac{a^m}{b} \right] = \frac{a^{kr} - 1}{a^r - 1} (aV_1 + a^2V_2 + \cdots + a^{r-1}V_{r-1}) \\ = \frac{a^m - 1}{a^r - 1} (a^{r-1}V_{r-1} + a^{r-2}V_{r-2} + \cdots + aV_1)$$

so that we have the result:

$$(IVa) \quad \left[\frac{a^m}{b} \right] \equiv 0 \pmod{a} \quad \text{if } m \equiv 0 \pmod{r}.$$

If $b = a^r - 1$, $V_1 = V_2 = V_3 = \dots = V_{r-2} = 0$, $V_{r-1} = 1$, and

$$(IVb) \quad \left[\frac{a^m}{b} \right] = \frac{a^{kr} - 1}{a^r - 1} a^{r-1}.$$

If $a = 10$, the expressions in round brackets in IV become ordinary numbers with digits $V_1 \dots V_\alpha$; $V_{r-1} \dots V_{\alpha+1}$, and the geometric progressions are numbers of the form

$$(IVc) \quad 100 \dots 0100 \dots 0100 \dots 01 \dots$$

where the 1's are separated by $r-1$ zeros.

The formulas I-IV enable us to solve any problem in division by separating a and b into sums and products in suitable ways. But IV is the only result essentially novel. Let us apply it to some numerical examples.

5. Example 1. To find the quotient when 10^{11} is divided by 13.

Here

$$\begin{aligned} a &= 10, \quad b = 13, \quad m = 11, \quad a_1 = 10, \quad a \cdot a_1 = 100 = 7 \cdot 13 + 9. \\ \therefore v_1 &= 7, \quad a_2 = 9, \quad a \cdot a_2 = 90 = 6 \cdot 13 + 12; \quad \therefore v_2 = 6, \quad a_3 = 12, \\ &\quad a \cdot a_3 = 120 = 9 \cdot 13 + 3; \\ \therefore v_3 &= 9, \quad a_4 = 3, \quad a \cdot a_4 = 30 = 2 \cdot 13 + 4; \quad \therefore v_4 = 2, \quad a_5 = 4, \\ &\quad a \cdot a_5 = 40 = 3 \cdot 13 + 1; \\ \therefore v_5 &= 3, \quad a_6 = 1, \quad r = 6, \quad m - 1 = 6 + 4. \quad \therefore k = 1, \quad \alpha = 4. \end{aligned}$$

$$\begin{aligned} \left[\frac{10^{11}}{13} \right] &= \left[\frac{10^{12} - 1}{10^6 - 1} \right] \cdot 7692 + \frac{10^6 - 1}{10^6 - 1} \cdot 10^4 \cdot 32 \\ &= (10^6 + 1) \cdot 7692 + 10^4 \cdot 32 = 7692307692. \end{aligned}$$

The work here is exactly the same as in the ordinary process of short division:

$$13) \overline{100000000000}.$$

Example 2. To find the quotient when 9^μ , where $\mu = (9^8)$, is divided by 19. Here $a = 9$, $b = 19$, $m = 9^8$, and 9, 5, 7, 6, 16, 11, 4, 17, 1 are the residues of $a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9$, so that $r = 9$.

$$m - 1 = 9^8 - 1 = (9^8 - 1)9 + 8, \quad \text{so that } k = 9^8 - 1, \quad \alpha = 8.$$

Using (8), we readily find 4, 2, 3, 2, 7, 5, 1, 8 for $V_1, V_2, V_3, V_4, V_5, V_6, V_7, V_8$. Therefore if $\mu = (9^9)$ and $\nu = 9^8$,

$$\left[\frac{9^\mu}{19} \right] = \left(\frac{9^\nu - 1}{9^9 - 1} \right) (4 \cdot 9^7 + 2 \cdot 9^6 + 3 \cdot 9^5 + 2 \cdot 9^4 + 7 \cdot 9^3 + 5 \cdot 9^2 + 1 \cdot 9 + 8)$$

Example 3. To find the quotient when $2^{257} - 1$ is divided by 1023.

Here $a = 2$, $b = a^{10} - 1$, $r = 10$, and IVb is applicable. Since $2^{257} \equiv 2^7 \pmod{1023}$,

$$\left[\frac{2^{257} - 1}{1023} \right] = \left[\frac{2^{257}}{1023} \right] = \frac{2^{250} - 1}{2^{10} - 1} \cdot 2^9 = 2^9 + 2^{19} + 2^{29} + \cdots + 2^{249}.$$

FORMAL UNIFICATION OF GRADIENT, DIVERGENCE, AND CURL, BY MEANS OF AN INFINITESIMAL OPERATIONAL VOLUME

By VLADIMIR KARAPETOFF, Cornell University

In vector analysis, the results of the three differential operations known as taking the gradient, the divergence, and the curl of a function are radically different from each other, both from a mathematical and from a physical point of view. Nevertheless there is some formal connection among the operations themselves in that the same Hamiltonian operator "nabla" or "del" (∇) is used in all three.¹ This permits to denote the three operations as ∇ , $\nabla \cdot$, and $\nabla \times$, respectively. In elementary text-books on vector analysis, the three operations and the Hamiltonian operator itself are introduced in Cartesian coördinates, thus perhaps leaving in the mind of the reader an unconscious impression that it is absolutely necessary to begin a problem by using the projections of both the operator and the operand.

On the other hand, the very purpose of vector analysis being to do away with resolving directed quantities into their components, as much as possible, a direct and unified interpretation of the foregoing differential operators in space is quite desirable. [In some advanced German works² this unification has been obtained by defining the gradient, the divergence, and the curl as follows:

$$(A) \quad \nabla P = \lim_{\Delta \rightarrow 0} (1/\Delta v) \int_S ds P ; \quad (B) \quad \nabla \cdot F = \lim_{\Delta \rightarrow 0} (1/\Delta v) \int_S d\mathbf{s} \cdot F ;$$

$$(C) \quad \nabla \times F = \lim_{\Delta \rightarrow 0} (1/\Delta v) \int_S ds \times F .$$

¹ In this article, by the Hamiltonian operator is meant the operator ∇ expressed in orthogonal coordinates, that is,

$$\nabla = i(\partial/\partial x) + j(\partial/\partial y) + k(\partial/\partial z)$$

² C. Runge, *Vector Analysis* (English Translation), p. 95; W. von Ignatowsky, *Die Vektoranalysis*, vol. 1, p. 16; J. Spielrein, *Lehrbuch der Vektorrechnung*, p. 111.

Chapter 3

1929

Theorem IV. *The summation on the right referring to all pairs (t, r) of integers $t > 0, r > 0, r$ odd, such that $n = tr$,*

$$F(n) = -1/n[\{1 + (-1)^n\}\sigma(\frac{1}{2}n)f(0) + 2 \sum (-1)^t \tau_f(t)].$$

To see first that this implies the $Q(n)$ part of theorem I, take $f(x) = 1$ for all integer values of x , as clearly is permissible under the definition of $f(x)$. A short reduction of the resulting right hand member gives the required relation.

To prove theorem IV, observe that we may take $f(n) = \cos nx$, where x is a parameter, for all integers n , and get a true theorem provided theorem IV is true. But conversely, if the cosine form of the theorem is an identity in x , we can infer the general form as stated.¹ The cosine form, however, follows by a straightforward reduction from the identity.²

$$\log(1 + \sum' q^{n^2}) = \log \theta_3 + 2 \sum \frac{(-1)^n q^n}{n(1 - q^{2n})} (1 - \cos 2nx),$$

where Σ' refers to $n = \pm 1, \pm 2, \pm 3, \dots$, Σ to $n = 1, 2, 3, \dots$, and

$$\log \theta_3 = \sum [\log(1 - q^{2n}) + 2 \log(1 + q^{2n-1})],$$

where Σ refers to $n = 1, 2, 3, \dots$. The expansions are valid for q, x suitably restricted, and similarly for the series obtained by expanding the logarithms by the logarithmic series. Comparison of coefficients of like powers of q in the result gives the stated cosine identity, as can be easily verified.

There is a similar but more complicated generalization of the $T(n)$ part of theorem I. Omitting this, we need only state the classic identity which implies the theorem as stated:

$$1 + \sum_{n=1}^{\infty} q^{n(n+1)/2} = \prod(1 - q^n)\prod(1 + q^n)^2,$$

from which, by taking logarithms and expanding, the result follows.

ON CERTAIN FUNCTIONAL RELATIONS

By MORGAN WARD, California Institute of Technology

1. *Introductory problem.* If $y = f(x)$ is an analytic function of x for $0 \leq |x| < r$ and if $f(0) = 0, f'(0) \neq 0$ so that

$$(1) \quad y = a_1 x + a_2 x^2 + a_3 x^3 + \dots \quad (a_1 \neq 0),$$

then the inverse function $x = f^{-1}(y)$ is also analytic for $0 \leq |y| < \rho = \rho(r)$ and vanishes with y .

¹ This is a simple instance of what was called paraphrase in several previous papers, e.g., Transactions of the American Mathematical Society, vol. 22 (1921), p. 1.

² See almost any text on elliptic functions, e.g., Tannery-Molk, vol. 3, p. 116.

Suppose that the function $f^{-1}(x)$ is identical with¹ $f(x)$, so that

$$(2) \quad x = a_1y + a_2y^2 + a_3y^3 + \dots$$

The coefficients a_1, a_2, a_3, \dots must then satisfy certain algebraic conditions. These conditions express the fact that the result of substituting for the successive powers of x in (1) their expressions in terms of y from (2) must reduce to the identity $y=y$. In particular, we see that $a_1^2=1$. There are two totally different cases according as $a_1=+1$ or $a_1=-1$. If $a_1=+1$, the remaining coefficients a_2, a_3, \dots , all vanish; if however $a_1=-1$, the situation is more complicated. We find that

$$\begin{aligned} a_3 &= -a_2^2, \quad a_5 = 2a_2^4 - 3a_2a_4 \\ a_7 &= -13a_2^6 + 18a_2^3a_4 - 4a_2a_6 - 2a_4^2 \\ a_9 &= 145a_2^8 - 221a_2^5a_4 + 35a_2^3a_6 + 50a_2^2a_4^2 - 5a_2a_8 - 5a_4a_6 \\ &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ x^n &= (-y)^n \left\{ 1 - na_2y + \frac{n(n+1)}{2!}a_2^2y^2 - \left(\frac{n(n-1)(n+4)}{3!}a_2^3 + na_4 \right)y^3 \right. \\ &\quad \left. + \left(\frac{n(n-3)(n+2)(n+7)}{4!}a_2^4 + n(n+2)a_2a_4 \right)y^4 - \dots \right\} \end{aligned}$$

By a somewhat lengthy induction, we can establish the following theorem:

Theorem 1: Given

$$\begin{aligned} y = f(x) &= a_1x + a_2x^2 + a_3x^3 + \dots \\ x = f(y) &= a_1y + a_2y^2 + a_3y^3 + \dots \quad (a_1^2 = 1) \end{aligned}$$

Then if $a_1=1$,

$$a_n = 0 \quad (n = 2, 3, 4, \dots)$$

But if $a_1=-1$,

$$a_{2n+1} = P_n(a_2, a_4, \dots, a_{2n}) = P_n(-a_2, -a_4, \dots, -a_{2n}),$$

where P_n is a uniquely determined polynomial in a_2, a_4, \dots, a_{2n} with integral coefficients.²

The following result is immediate.

Theorem 2: The necessary and sufficient condition that x and y be related as in theorem 1 is that there exist an analytic function $F(x, y)$ of x and y satisfying the conditions,

¹ A simple example of such a function is $y=x/(x-1) = -x-x^2-x^3-\dots$.

² I have not yet succeeded in obtaining the explicit expression for P_n .

$$F(x, y) = F(y, x) = F(0, 0) = 0; \quad F_x(0, 0) \neq 0.$$

2. *Extended problem.* Suppose that $y = \Phi(a, b; x)$ is a function of x and the two real parameters a and b which satisfies the following conditions:

- (i) $\Phi(a, b; x)$ is an analytic function of x on and within the square \mathfrak{S} bounded by the lines $a = \pm h$, $b = \pm h$ in the $a \cdot b$ plane for $0 \leq |x| < r = r(h)$;
- (ii) $\Phi(a, b; x)$ vanishes with x throughout \mathfrak{S} .

We may consequently write

$$y = \Phi(a, b; x) = \phi_1(a, b)x + \frac{\phi_2(a, b)x^2}{2!} + \frac{\phi_3(a, b)}{3!}x^3 + \dots,$$

where

$$\phi_n(a, b) = (\partial^n \Phi / \partial x^n).$$

If, moreover, $\phi_1(a, b) \neq 0$ in \mathfrak{S} , the inverse function $x = \Phi^{-1}(y)$ exists for $0 \leq |y| < \rho(h)$. Let us assume finally that

- (iii) $\Phi^{-1}(x) = \Phi(b, a; x)$ for $0 \leq |x| < r(h)$ throughout \mathfrak{S} . We shall then have

$$x = \Phi(b, a; y) = \phi_1(b, a)y + \frac{\phi_2(b, a)y^2}{2!} + \frac{\phi_3(b, a)y^3}{3!} + \dots$$

and as in section 1 it is necessary that

$$(3) \quad \phi_1(a, b) \cdot \phi_1(b, a) = 1.$$

Let us determine some of the properties of functions which satisfy the conditions (i), (ii), and (iii). We shall refer to such functions as "Φ-functions."

3. *Canonical form for functions.* From (3) we see that $\phi_1(a, b)$ and $\phi_1(b, a)$ can never vanish in \mathfrak{S} and must both be of the same sign in \mathfrak{S} . If we write

$$y = |\phi_1(a, b)|^{1/2}v, \quad x = |\phi_1(b, a)|^{1/2}u,$$

the series defining Φ in section 2 become either

$$(I) \quad \begin{aligned} v &= u + \psi_2 u^2 + \psi_3 u^3 + \dots \\ u &= v + \psi'_2 v^2 + \psi'_3 v^3 + \dots \end{aligned}$$

if $\phi_1(a, b)$ and $\phi_1(b, a)$ are positive in \mathfrak{S} , or

$$(II) \quad \begin{aligned} v &= -u + \psi_2 u^2 + \psi_3 u^3 + \dots \\ u &= -v + \psi'_2 v^2 + \psi'_3 v^3 + \dots \end{aligned}$$

if $\phi_1(a, b)$ and $\phi_1(b, a)$ are negative in \mathfrak{S} ; where in both cases

$$(4) \quad \begin{aligned} \psi_n &= \psi_n(a, b) = \frac{\phi_n(a, b)}{n!} |\phi_1(b, a)|^{(n+1)/2} \\ \psi'_n &= \psi_n(b, a) = \frac{\phi_n(b, a)}{n!} |\phi_1(a, b)|^{(n+1)/2} \\ (n &= 2, 3, \dots). \end{aligned}$$

If we write $a=b$ in (I) and (4), we see from the first part of theorem 1 that

$$\phi_n(a, a) = 0. \quad (n = 2, 3, \dots).$$

From (3) and (4) follows

Theorem 3. *If $y = F(a, b; x)$ is any Φ -function whose coefficients are polynomials in a and b , then the coefficient of every power of x in F save the first is divisible by $a-b$.*

The two canonical forms of Φ -function in (I) and (II) show us that we have a correspondence with the two types of solution of $y=f(x)$, $x=f^{-1}(y)$ in theorem 1. Let us call Φ -functions of the first type "proper functions" and Φ -functions of the second type "improper functions." $y=x$ is the simplest proper function, but in contrast to the first part of theorem 1, we have a theorem analogous to theorem 2 for both proper and improper functions. We shall confine our statement to the former type of function in the canonical form (I).

Theorem 4. *The necessary and sufficient condition that v be a proper Φ -function of u is that u and v be connected by an implicit relation of the form*

$$(5) \quad u - v + F(a, b; u, v) - F(b, a; v, u) = 0,$$

where for sufficiently small positive values of $|u|$ and $|v|$, $F(a, b; u, v)$ is an analytic function of both u and v in some region \mathfrak{R} in the ab -plane which includes the origin, and where

$$F(a, b; 0, 0) = F(b, a; 0, 0),$$

$$F_x(a, b; 0, 0) = F_x(b, a; 0, 0),$$

$$F_y(a, b; 0, 0) = F_y(b, a; 0, 0),$$

for all values of a and b in \mathfrak{R} .

In fact these conditions allow us to substitute for v a series in u with undetermined coefficients Ψ_n which we know will be convergent, and to determine the $\Psi_n = \Psi_n(a, b)$ by equating the coefficients of u, u^2, u^3, \dots , to zero in the resulting identity; in particular, we shall have $\Psi_1 = 1$. Now if instead we substitute for u a series in v with undetermined coefficients Ψ'_n , the equations determining Ψ'_n are obtained from those determining Ψ_n by merely inter-changing a and b , so that $\Psi'_n(a, b) = \Psi_n(b, a)$ and v is a proper function of u . Conversely, if (I) holds, by halving and subtracting the two series we obtain

$$u - v + \frac{1}{2} \sum_{n=2}^{\infty} \psi_n(a, b) u^n - \frac{1}{2} \sum_{n=2}^{\infty} \psi_n(b, a) v^n = 0,$$

where, by our definition of a Φ -function, $\frac{1}{2} \sum_{n=2}^{\infty} \psi_n(a, b) u^n$ satisfies all the conditions imposed upon $F(a, b, u, v)$ in the theorem.

5. Example. As an illustration of a proper Φ -function, suppose temporarily that a, b are real, but never zero. Consider the relation

$$(6) \quad (1 + bx)^a = (1 + ay)^b.$$

By the binomial theorem, if $|x| < 1/|b|$, $|y| < 1/|a|$

$$\begin{aligned} x - y + \frac{(a-1)bx^2}{1 \cdot 2} + \frac{(a-1)(a-2)b^2x^3}{1 \cdot 2 \cdot 3} + \dots \\ - \frac{(b-1) \cdot ay^2}{1 \cdot 2} - \frac{(b-1)(b-2)a^2y^3}{1 \cdot 2 \cdot 3} - \dots = 0, \end{aligned}$$

so that

$$x - y + F(a, b ; x, y) - F(b, a ; y, x) = 0,$$

where

$$F(a, b ; x, y) = \sum_{n=1}^{\infty} \frac{(a-1)(a-2) \cdots (a-n)}{(n+1)!} b^n x^{n+1}.$$

Now $F(a, b ; x, y)$ satisfies all the conditions of theorem 4, even when a, b are zero, so that we have

$$y = x + J(a, b ; x); \quad x = y + J(b, a ; y),$$

where we easily see that

$$(7) \quad J(a, b ; x) = \sum_{n=1}^{\infty} \frac{(a-b)(a-2b) \cdots (a-nb)}{(n+1)!} x^{n+1}.$$

Moreover if $\lambda \neq 0$,

$$\lambda J\left(\lambda a, \lambda b ; \frac{x}{\lambda}\right) = J(a, b ; x)$$

and if $ab \neq 0$,

$$1 + ax + aJ(a, b ; x) = (1 + bx)^{a/b}.$$

We can define $J(a, b ; x)$ by the series (7) and then prove that $x + J(a, b ; x)$ is actually a proper Φ -function. This has been done by O. Jezek.¹ We conclude with a few easily proved but curious properties of the function $J(a, b ; x)$. If

$$x = t + J(b, ab ; t) \quad \text{and} \quad y = t + J(a, ab ; t),$$

then

$$\begin{aligned} x + J(ab, b ; x) &= y + J(ab, a ; y); \\ y - x &= J(a, b ; x); \quad x - y = J(b, a ; y). \end{aligned}$$

If

$$\begin{aligned} x &= t - J(a, abc ; t) + J(b, abc ; t) + J(c, abc ; t), \\ y &= t + J(a, abc ; t) - J(b, abc ; t) + J(c, abc ; t), \\ z &= t + J(a, abc ; t) + J(b, abc ; t) - J(c, abc ; t), \end{aligned}$$

then

¹ O. Jezek, *Ueber die Reihenumkehrung*, Wiener Sitzungsberichte Zweite Abteilung, vol. XCIX (1890), pp. 191–203.—See also Whittaker and Watson, *Modern Analysis*, 3rd edition, p. 147, example 14.

$$\begin{aligned}x - y &= J(a, b ; y + z), \quad y - x = J(b, a ; x + z) \\y - z &= J(b, c ; z + x), \quad z - y = J(c, b ; y + x), \\z - x &= J(c, a ; x + y), \quad x - z = J(a, c ; z + y), \\J(abc, c ; x + y) &= J(abc, a ; y + z) = J(abc, b ; z + x).\end{aligned}$$

GENERALIZATIONS IN GEOMETRY AS SEEN IN THE HISTORY OF DEVELOPABLE SURFACES

By FLORIAN CAJORI, University of California

"The mathematicians of the eighteenth century would have been astonished to a high degree, had they been told that there exist developable surfaces which are not ruled surfaces." Perhaps this passage from the pen of Picard¹ surprises many mathematicians even of the present time; it challenges the historian to endeavor to trace the evolution of ideas. The result alluded to is no less surprising to us than was to Euler in the eighteenth century the fact that i^i , where $i = \sqrt{(-1)}$, has a real value. In a letter to Goldbach, Euler showed his interest by computing this value to ten decimal places. Picard's statement is no less surprising than the declaration about integral numbers made by Galileo in the seventeenth century: "Neither is the number of squares less than the totality of all numbers, nor the latter greater than the former."

Period of Primitive Intuition

Aristotle remarked that "a line by its motion produces a surface."² When this line was a straight line, ruled surfaces would result, which clearly included the cone and cylinder. But Aristotle's statement does not necessarily carry the implication that there are ruled surfaces which can be spread out upon a plane. Nevertheless, early students of geometry must have recognized as intuitively evident the fact that, without stretching or tearing, the curved surface of cylinders and cones could be unbent upon a plane. Explanations of this property are not generally given. We have found the developed surface of a right cone drawn as the sector of a circle, in a practical work on mensuration,³ without any novelty being claimed for it. In the same treatise the cylinder is described as being "in form of a Rolling stone used in Gardens," an expression conveying the picture of a surface rolled over a plane so that all its points are brought into coincidence with the plane.

¹ Émile Picard, *La science moderne et son état actuel*, Paris, p. 53.

² Aristotle, *De Anima*, I, 4, 409, a4; T. L. Heath's *Thirteen Books of Euclid*, vol. 1, 2nd edition (1926), p. 170.

³ William Hawney, *The Complete Measurer*, ninth Edition (1755), p. 159. See also p. 154. (First edition, London, 1717).

CERTAIN EXPANSIONS INVOLVING DOUBLY INFINITE SERIES.*

BY MORGAN WARD.

1. Introduction. The present paper extends the results of a previous article† on the same subject. If

$$P(x, y) = \sum_{r,s=0}^{\infty} P_{rs} x^r y^s, \quad Q(x, y) = \sum_{r,s=0}^{\infty} Q_{rs} x^r y^s$$

are power series in x and y , I showed in R how to express the coefficients of P/Q , $\exp Q$, $\log Q$ as simple determinants in the coefficients P_{rs} , Q_{rs} and here I shall apply these results to the expansion of

$$[P_1(x, y)]^{m_1} \cdot [P_2(x, y)]^{m_2} \cdots [P_t(x, y)]^{m_t}$$

where m_1, m_2, \dots, m_t are any real numbers.

The analogous expansion problem for singly infinite series has been solved by Mangeot‡; David§ and Segar|| had previously dealt with the simple case of a single power series raised to an arbitrary power.

2. Notation. In this paper, if P , Q , P_i , etc. are power series in x , y the corresponding coefficients are denoted by P_{rs} , Q_{rs} , $P_{i,rs}$, etc. The Einstein summation convention is used, so that for instance, we shall write $Q = Q_{ij} x^i y^j$ instead of $\sum_{i,j=0}^{\infty} Q_{ij} x^i y^j$. The terms of a series Q will always be taken to be arranged in the usual numerical order; viz.

$$(1) \quad Q_{00} + Q_{10} x + Q_{01} y + Q_{20} x^2 + Q_{11} xy + Q_{02} y^2 + \dots$$

When the series is arranged in this manner, the term Q_{ij} occurs in the $(\frac{1}{2}(i+j)(i+j+1)+(j+1))$ place. ¶ We shall call the number $\frac{1}{2}(i+j)(i+j+1)+(j+1)$ the *rank* of the coefficient Q_{ij} and denote it by q_{ij} .

3. Evaluation of coefficients. Suppose then that

$$(2) \quad \begin{aligned} P_\tau &= P_\tau(x, y) = P_{\tau,rs} x^r y^s & (\tau = 1, 2, \dots, t) \\ W(x, y) &= W_{ij} x^i y^j = P_1^{m_1} \cdot P_2^{m_2} \cdots P_t^{m_t}. \end{aligned}$$

* Received October 4, 1927; in revised form, February 4, 1929.

† A Generalization of Recurrents. Bull. Amer. Math. Soc., vol. 33 (1927), pp. 477-492. I shall refer to this paper as R. A correction is given p. 580 in the second footnote (†).

‡ Annales de l'Ec. Norm., vol. 14 (1897), pp. 247-250.

§ Journ. de Math., vol. 8, ser. 3 (1882), pp. 61-72.

|| Messenger of Math., vol. 21, ser. 2 (1892), pp. 177-188. See vol. 4, chapter 8 of Muir's *History* for other references.

¶ R, section 2.

Our object is to show how to express W_{ij} in terms of the coefficients of the P series. We may assume first of all that

$$P_{\tau,00} \neq 0 \quad (\tau = 1, 2, \dots, t).$$

Let

$$(3) \quad [P_\tau(x, y)]^{m_\tau} = \exp Q_\tau(x, y) \quad (\tau = 1, 2, \dots, t)$$

so that

$$(4) \quad Q_\tau(x, y) = Q_{\tau,rs} x^r y^s = m_\tau \log P_\tau(x, y).$$

On substituting from (3) into (2) we obtain

$$(5) \quad W(x, y) = \exp Q(x, y)$$

where

$$(6) \quad \begin{aligned} Q(x, y) &= Q_1(x, y) + Q_2(x, y) + \dots + Q_t(x, y), \\ Q_{rs} &= Q_{1,rs} + Q_{2,rs} + \dots + Q_{t,rs}. \end{aligned}$$

Our next step is to express W_{ij} as a determinant* in the Q 's; but we shall explain the formation of this determinant more fully than in R.

4. Fundamental determinants. Consider first of all the determinants

$$\Delta_1 = 1, \quad \Delta_2 = \begin{vmatrix} Q_{10} & -1 \\ Q_{01} & \cdot \end{vmatrix}_2, \quad \Delta_3 = \begin{vmatrix} Q_{10} & -1 & \cdot & \cdot & \cdot \\ Q_{01} & \cdot & -1 & \cdot & \cdot \\ 2Q_{20} & Q_{10} & \cdot & -2 & \cdot \\ 2Q_{11} & Q_{01} & Q_{10} & \cdot & -2 \\ 2Q_{02} & \cdot & Q_{01} & \cdot & \cdot \end{vmatrix}_5,$$

$$\Delta_4 = \begin{vmatrix} Q_{10} & -1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ Q_{01} & \cdot & -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 2Q_{20} & Q_{10} & \cdot & -2 & \cdot & \cdot & \cdot & \cdot \\ 2Q_{11} & Q_{01} & Q_{10} & \cdot & -2 & \cdot & \cdot & \cdot \\ 2Q_{02} & \cdot & Q_{01} & \cdot & \cdot & -2 & \cdot & \cdot \\ 3Q_{30} & 2Q_{20} & \cdot & Q_{10} & \cdot & \cdot & -3 & \cdot \\ 3Q_{21} & 2Q_{11} & 2Q_{20} & Q_{01} & Q_{10} & \cdot & \cdot & -3 \\ 3Q_{12} & 2Q_{02} & 2Q_{11} & \cdot & Q_{01} & Q_{10} & \cdot & \cdot \\ 3Q_{03} & \cdot & 2Q_{02} & \cdot & \cdot & Q_{01} & \cdot & \cdot \end{vmatrix}_9$$

and so on.

The dots indicate zeros and the subscripts 2, 5, 9, ... the orders of $\Delta_2, \Delta_3, \Delta_4, \dots$. In general, Δ_n is a determinant of order $n(n+1)/2 - 1$ whose mode of formation is fairly apparent from the examples just given.[†]

We next introduce a set of N numerical functions[‡] somewhat analogous to Kronecker's δ_{ij} symbol:

* R, section 10, p. 489.

† R, pp. 490-91; 481-82.

‡ R, p. 480; p. 489.

$$(q_{t-s}; i+s-t, j-s) \quad \begin{pmatrix} t = 0, 1, \dots, i+j-1 \\ s = 0, 1, \dots, t \\ N = \frac{1}{2}(i+j)(i+j+1) = q_{i+j_0}-1 \end{pmatrix}.$$

The relations defining these functions are as follows:

$$(q_{t-s}; i+s-t, j-s) = 0$$

if either $i+s-t < 0$ or $j-s < 0$ and

$$(q_{t-s}; i+s-t, j-s) = (i+j-t) Q_{i-t+s, j-s}$$

if neither $i+s-t < 0$ nor $j-s < 0$.

The general coefficient W_{ij} in (5) is then given by*

$$(7) \quad \begin{array}{c} (i+j)e^{-Q_{00}} 1^2 \cdot 2^2 \cdot 3^4 \cdots \\ \cdots (i+j-1)^{i+j} W_{ij} = \end{array} \quad \begin{array}{c} 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \Delta_{i+j} \\ \cdot \\ \cdot \\ \cdot \\ -(i+j-1) \\ \dots \dots \dots (q_{t+s}; i+s-t, j-s) \dots \dots \end{array}$$

The determinant on the right side of (7) consists of the determinant A_{i+j} bordered by

$$\begin{aligned}
& (q_{00}; i, j), \quad (q_{10}; i-1, j), \quad (q_{01}; i, j-1), \quad (q_{20}; i-2, j), \\
& (q_{11}; i-1, j-1), \quad (q_{02}; i, j-2), \quad \dots, \quad \dots, \\
& \dots, \quad \dots, \quad \dots, \quad \dots, \\
& \dots, \quad \dots, \quad (q_{t-s,s}; i+s-t, j-s), \quad \dots, \\
& \dots, \quad \dots, \quad \dots, \quad \dots, \\
& \dots, \quad \dots, \quad \dots, \quad (q_{0,i+j-1}; i, 1-i)
\end{aligned}$$

in the last row, and by

$$0, \quad 0, \quad 0, \quad \dots, \quad -(i+j-1), \quad (q_0 i_{j-1}; i, 1-i)$$

in the last column.[†]

* R., p. 491.

[†]In R, p. 491, the factor $(i+j)e^{-q_{00}}$ was omitted from the left-hand side of (7), and the last row of the determinant on the right-hand side of (7) was given incorrectly as $(q_{00}; i, j)$, $(q_{10}; i-1, j+1)$, $(q_{01}; i-2, j+2)$, ... etc. instead of the correct expressions above. Similar corrections should be made on p. 483 (interpreting the numerical functions appearing there as in (9) p. 480), and in the procedure sketched in section 9R for $\log Q(x, y)$.

5. Illustrative example. To show the ease with which the general formula (7) may be applied, we shall evaluate the coefficient W_{21} . Here $i = 2, j = 1, i+j = 3, N = \frac{3 \cdot 4}{2} = 6$, so that we must border the determinant Δ_3 with the row

$(q_{00}; 2, 1), (q_{10}; 1, 1), (q_{01}; 2, 0), (q_{20}; 0, 1), (q_{11}; 1, 0), (q_{02}; 2, -1)$
and with the column

$$0, 0, 0, 0, -2, (q_{02}; 2, -1).$$

That is, with the row

$$3 Q_{21}, 2 Q_{11}, 2 Q_{20}, Q_{01}, Q_{10}, 0$$

and the column

$$0, 0, 0, 0, -2, 0.$$

Thus*

$$3 e^{-q_{00}} 1^2 \cdot 2^3 W_{21} = \begin{vmatrix} Q_{10} & -1 & 0 & 0 & 0 & 0 \\ Q_{01} & 0 & -1 & 0 & 0 & 0 \\ 2 Q_{20} & Q_{10} & 0 & -2 & 0 & 0 \\ 2 Q_{11} & Q_{01} & Q_{10} & 0 & -2 & 0 \\ 2 Q_{02} & 0 & Q_{01} & 0 & 0 & -2 \\ 3 Q_{21} & 2 Q_{11} & 2 Q_{20} & Q_{01} & Q_{10} & 0 \end{vmatrix}_6$$

6. Final evaluation of coefficients. We have thus expressed the W_{ij} as determinants in the Q_{rs} . But we can express the Q_{rs} as sums of determinants in the $P_{\tau, rs}$; for since by (4) $Q_{\tau}(x, y) = m_{\tau} \log P_{\tau}(x, y)$ we can apply the method developed in R section 9 to expand a logarithm. We need only to substitute in R (17) p. 483 $m_{\tau} \log P_{\tau,00} = Q_{\tau,00}$ for Z_{00} ; $\frac{i+j}{m_{\tau}} Q_{\tau,ij}$ for Z_{ij} ($i+j > 0$); $i+j P_{\tau,ij}$ for P_{ij} ; and $P_{\tau,ij}$ for Q_{ij} . Since P_{00} vanishes, we obtain thus†

$$(8) \quad P_{\tau,00}^{N-1} \frac{i+j}{m_{\tau}} Q_{\tau,ij} = \begin{vmatrix} P_{\tau,10} & P_{\tau,00} & 0 & \cdot & 0 & P_{\tau,10} \\ P_{\tau,01} & 0 & P_{\tau,00} & \cdot & 0 & P_{\tau,01} \\ P_{\tau,20} & P_{\tau,10} & 0 & \cdot & 0 & 2 P_{\tau,20} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{\tau,0i+j-1} & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{\tau ij}, & (2; i-1, j), & \dots, & (i+j) P_{\tau,ij} & & \end{vmatrix},$$

* This result may be readily checked from the equations at the foot of p. 490 in R.

† We have applied the correction mentioned in the footnote to section 4 to the last row of the determinant.

where $N = \frac{1}{2}(i+j)(i+j+1)+1$ and $1 \leq \tau \leq t$. By combining (8), (6) and (7) we can finally express the coefficients of $W(x, y)$ in terms of the coefficients of $P_1(x, y), P_2(x, y), \dots, P_t(x, y)$.

7. A special case. In case $t = 1$ we may proceed more simply. We have

$$(9) \quad W(x, y) = [P(x, y)]^m, \quad P_{00} \neq 0.$$

Take the logarithms of both sides of (9) and then operate with

$$W(x, y) P(x, y) \left\{ x \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} \right\}.$$

We obtain

$$P_{rs} x^r y^s (u+v) W_{uv} x^u y^v = m(r+s) P_{rs} x^r y^s W_{uv} x^u y^v$$

or transposing and equating the coefficient of $x^r y^s$ to zero,

$$\sum_{\tau=0}^p \sum_{\sigma=0}^q [m(r+q)-(m+1)(\sigma+\tau)] P_{r-\tau, q-\sigma} W_{\sigma\tau} = 0 \quad (r, q, = 0, 1, 2, \dots).$$

These equations may be identified with the equations (8) on p. 479 of R on taking in R

$$\begin{aligned} P_{uv} &= 0 \quad (u \neq 0, v \neq 0), & P_{00} &= P_{00}^n, \\ Q_{u-\sigma, v-\tau} &= [m(r+q)-(m+1)(\sigma+\tau)] P_{p-\tau, q-\sigma} \quad (u \neq 0, v \neq 0), \\ Q_{00} &= 1, \\ W_{\sigma\tau} &= Z_{\sigma\tau}. \end{aligned}$$

It follows that they may be solved in the same manner by introducing a properly defined numerical function.

8. Conclusion. The method I have applied here for obtaining simple determinants for the expansions of various elementary functions of doubly infinite series by the introduction of suitably defined numerical functions can theoretically be extended to m -tuply infinite series.* The numerical functions which must be introduced are unfortunately of such complexity* as to reduce the results to a mere jumble of symbols. A successful application of the method to the problem of reverting two doubly infinite series would be of more interest and of some practical importance. It would seem, however, to be rather difficult.†

* R, section 8, p. 487.

† I have treated the problem for singly infinite series in a note which is to appear shortly in the Rendiconti del Circolo di Palermo.

Chapter 4

1930

A CERTAIN CLASS OF POLYNOMIALS.*

BY MORGAN WARD.

Contents.

	Page
1. Definition of a Regular Sequence of Polynomials	43
2. Fundamental Properties of Regular Sequences	43
3. Harmonic Sequences	44
4. Condition a Harmonic Sequence be Regular	45
5, 6. Properties of the Simplest Regular Sequence	45, 47
7. Definition and Properties of Cyclic Sequences	47
8. Additional Properties of Cyclic Sequences	49

1. The remarkable properties which a sequence of polynomials

$$Y_0(x), Y_1(x), Y_2(x), \dots$$

of degrees 0, 1, 2, ... in x possesses when the two functional equations

$$\frac{d Y_n(x)}{dx} = Y_{n-1}(x), \quad Y_n(-x-1) = (-1)^n Y_n(x)$$

are satisfied have been systematically developed by N. Nielsen.† It is of some interest to consider sequences of polynomials satisfying the more general equations

$$(1) \quad \frac{d Y_n(x)}{dx} = Y_{n-1}(x), \quad (n = 0, 1, 2, \dots)$$
$$(2) \quad Y_n(ax+b) = \tau_n Y_n(x),$$

where a, b are any complex numbers. Such a sequence we call a *regular* sequence. The main properties of regular sequences are as follows:

2. If a is not a root of unity, there is only one regular sequence; namely

$$Y_n(x) = \frac{c}{n!} \left(x + \frac{b}{a-1} \right)^n, \quad \tau_n = a^n \quad (n = 0, 1, 2, \dots).$$

If however, a is a root of unity, say a primitive n th root, there exist an infinite number of regular sequences. Let

$$(k_0 + k_1 t + k_2 t^2 + \dots) e^{xt} = K_0(x) + K_1(x) t + K_2(x) t^2 + \dots$$

* Received February 4, 1929.

† *Traité Élémentaire des Nombres de Bernoulli*, Paris 1923.

be the generating function of any such sequence. Then if $r\pi \leq n < (r+1)\pi$, k_n may be expressed as a linear function of $k_0, k_\pi, k_{2\pi}, \dots, k_{r\pi}$

$$k_n = \sum_{s=0}^r k_{s\pi} H'_{n-s\pi},$$

where H'_0, H'_1, H'_2, \dots depend only on a and b and are independent of the particular regular sequence $[K_n(x)]$ we have selected. Moreover, if a is a given π th root of unity, all possible solutions (1) and (2) are obtained by giving $k_0, k_\pi, k_{2\pi}, \dots$ the proper values.

3. We now proceed to the proof of these results. A sequence of polynomials

$$H_0(x), H_1(x), H_2(x), \dots$$

of degrees 0, 1, 2, ... in x which satisfies (1) is said to be *harmonic*.* The following properties of harmonic sequences are easily proved.*

(i) If $[H_n(x)]$ is a harmonic sequence, there exists a sequence of constants

$$[h_n]: h_0, h_1, h_2, \dots, h_n, \dots,$$

such that for all values of n ,

$$H_n(x) = \frac{h_0 x^n}{n!} + \frac{h_1 x^{n-1}}{(n-1)!} + \frac{h_2 x^{n-2}}{(n-2)!} + \dots + h_n, \quad H_n(0) = h_n.$$

We denote such a sequence by $[H_n(x), h_n]$.

(ii) If†

$$\begin{aligned} H(x, t) &= H_0(x) + H_1(x)t + H_2(x)t^2 + \dots, \\ h(t) &= h_0 + h_1t + h_2t^2 + \dots \end{aligned}$$

are the generating functions of the sequences $[H_n(x)], [h_n]$

$$H(x, t) = e^{xt} h(t).$$

(iii) If b is any constant,

$$H_n(x+b) = H_n(b) + \frac{xH_{n-1}(b)}{1!} + \frac{x^2 H_{n-2}(b)}{2!} + \dots + \frac{x^n H_0(b)}{n!}.$$

(iv) Let $[K_n(x), k_n]$ be a second harmonic sequence. Then there exists a unique ordinary sequence $[\alpha_n]$ such that for all values of n

$$K_n(x) = \alpha_0 H_n(x) + \alpha_1 H_{n-1}(x) + \dots + \alpha_n H_0(x).$$

* Nielsen, l. c., chap. III, section XI.

† This property of harmonic sequences is substantially due to Appell: Annales de l'École Normale, (2) 10 (1880), 119–120.

4. We pass now to regular sequences. If in (2), $a = 0$ or 1 , the sequences are trivial, so that we shall exclude these cases in all that follows. It is clear that for any sequence $[L_n(x)]$ satisfying (2)

$$(3) \quad \tau_n = a^n, \quad L_n(b) = a^n L_n(0) \quad (n = 0, 1, 2, \dots).$$

Now suppose $[H_n(x)]$ is a harmonic sequence for which

$$H_n(b) = a^n H_n(0) \quad (n = 0, 1, 2, \dots).$$

Then by (iii) and our hypothesis

$$H_n(ax+b) = \sum_{s=0}^n H_{n-s}(b) a^s \frac{x^s}{s!} = \sum_{s=0}^n a^{n-s} H_{n-s}(0) a^s \frac{x^s}{s!},$$

$$H_n(ax+b) = a^n H_n(x)$$

by (i). Hence we have proved

THEOREM 1. *The necessary and sufficient condition that a harmonic sequence $[H_n(x), h_n]$ be regular is that*

$$(4) \quad H_n(b) = a^n H_n(0) \quad (n = 0, 1, 2, \dots).$$

5. If we expand the left side of (4) by (i), we obtain

$$(5) \quad \sum_{r=0}^n \frac{h_{n-r} b^r}{r!} = a^n h_n \quad (n = 0, 1, 2, \dots),$$

so that

$$\begin{aligned}
 h_0 &= h_0, \\
 \frac{b h_0}{1!} + h_1 &= a h_1, \\
 \frac{b^2 h_0}{2!} + \frac{b h_1}{1!} + h_2 &= a^2 h_2, \\
 \frac{b^3 h_0}{3!} + \frac{b^2 h_1}{2!} + \frac{b h_2}{1!} + h_3 &= a^3 h_3, \\
 \dots &\dots \\
 \frac{b^r h_0}{r!} + \frac{b^{r-1} h_1}{(r-1)!} + \frac{b^{r-2} h_2}{(r-2)!} + \frac{b^{r-3} h_3}{(r-3)!} + \dots + \frac{b h_r}{1!} + h_r &= a^r h_r,
 \end{aligned}$$

If we assume $a^k \neq 1$ ($1 \leq k \leq r$) we can solve the first $r+1$ of these equations for h_r in terms of h_0, a, b by determinants. We thus obtain after a few simplifications

$$(6) \quad h_r = \frac{h_0 b^r \Delta_r(a)}{(a-1)(a^2-1)\cdots(a^r-1)},$$

where $\Delta_r(a)$ is given by

$$\Delta_r(a) = \begin{vmatrix} \frac{1}{1!} & 1-a & 0 & 0 & \cdots & 0 & 0 \\ \frac{1}{2!} & \frac{1}{1!} & 1-a^2 & 0 & \cdots & 0 & 0 \\ \frac{1}{3!} & \frac{1}{2!} & \frac{1}{1!} & 1-a^3 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \frac{1}{1!} & 1-a^{r-1} \\ \frac{1}{r!} & \frac{1}{(r-1)!} & \frac{1}{(r-2)!} & \frac{1}{(r-3)!} & \cdots & \frac{1}{2!} & \frac{1}{1!} \end{vmatrix}$$

Moreover this value of h_r is unique. We find by solving for h_0 , h_1 and h_2 , provided $a^k \neq 1$

$$h_0 = \frac{h_0 \lambda^0}{0!}, \quad h_1 = \frac{h_0 \lambda^1}{1!}, \quad h_2 = \frac{h_0 \lambda^2}{2!}$$

where

$$(7) \quad \lambda = \frac{b}{a-1}.$$

Hence let us assume

$$(8) \quad h_r = \frac{h_0 \lambda^r}{r!}, \quad a^{r+1} \neq 1 \quad (0 \leq r \leq k).$$

From (5) and our hypothesis

$$(a^{k+1}-1)h_{k+1} = \sum_{r=0}^k \frac{h_r b^{k+1-r}}{(k+1-r)!} = h_0 b^{k+1} \sum_{r=0}^k \frac{1}{r! (k+1-r)! (a-1)^r}.$$

Then

$$\begin{aligned} (k+1)! (a-1)^{k+1} (a^{k+1}-1) h_{k+1} &= h_0 b^{k+1} \sum_{r=0}^k \binom{k+1}{r} (a-1)^{k+1-r} \\ &= h_0 b^{k+1} (a^{k+1}-1), \end{aligned}$$

so that by (7) and (8)

$$h_{k+1} = \frac{h_0 \lambda^{k+1}}{(k+1)!}.$$

Thus by induction (6) holds for all values of r , provided a is not a root of unity. On comparing (6) and (8) we deduce

THEOREM 2. *The determinant $\Delta_r(a)$ has the value*

$$\Delta_r(a) = (1+a)(1+a+a^2) \cdots (1+a+a^2+\cdots+a^r)/r!$$

Moreover $\Delta_r(1) = 1$, $\Delta_r(0) = 1/r$, and $\Delta_r(a)$ vanishes if a is any primitive π th root of unity ($2 \leq \pi \leq r$).

6. From (8) and (i) it follows that

$$(9) \quad H_n(x) = \sum_{r=0}^n \frac{h_0}{r!(n-r)!} \lambda^{n-r} x^r = \frac{h_0}{n!} (x + \lambda)^n.$$

If (9) holds,

$$\frac{dH_n(x)}{dx} = H_{n-1}(x), \quad H_n(ax+b) = \frac{h_0}{n!} \left(ax + b + \frac{b}{a-1} \right)^n = a^n H_n(x),$$

so that (9) is a regular sequence whether or not a is a root of unity. On collecting these results, we have

THEOREM 3. A sequence $[H_n(x)]$ satisfying the two functional equations

$$(1) \quad \frac{dY_n(x)}{dx} = Y_{n-1}(x),$$

$$(2) \quad Y_n(ax+b) = a^n Y_n(x), \quad (a \neq 0, 1),$$

is always given by

$$(8) \quad h_n = \frac{h_0 \lambda^n}{n!},$$

$$(9) \quad H_n(x) = \frac{h_0 (x + \lambda)^n}{n!},$$

where h_0 is an arbitrary constant, and

$$(7) \quad \lambda = \frac{b}{a-1}.$$

Moreover if a is not a root of unity, this solution of (1) and (2) is unique.

7. The first result stated in section 2 is now proved. The regular sequences for which a is a root of unity are of much greater interest. It will be convenient in studying them to define $H_n(x)$ to mean the polynomial $\frac{(x + \lambda)^n}{n!}$ which gives the simplest regular sequence and to define

a cyclic sequence of order π to mean any solution of (1) and (2) for which a is a primitive π th root of unity. Then

$$(10) \quad a^r = 1$$

when and only when $r \equiv 0 \pmod{\pi}$.

THEOREM 4. If $[K_n(x), k_n]$ is a cyclic sequence of order π then $K_n(x)$ may be uniquely represented in the form

$$(11) \quad K_n(x) = \alpha_0 H_n(x) + \alpha_\pi H_{n\pi}(x) + \dots + \alpha_{r\pi} H_{n-r\pi}(x)$$

where $\alpha_0, \alpha_\pi, \dots, \alpha_{r\pi}$ are constants, and $r\pi \leq n < (r+1)\pi$. Moreover every sequence of the form (11) is a cyclic sequence of order π .

For since $[K_n(x)]$ and $[H_n(x)]$ are both harmonic sequences, there exists by (iv) a unique ordinary sequence $[\alpha_r]$ such that

$$K_n(x) = \alpha_0 H_n(x) + \alpha_1 H_{n-1}(x) + \dots + \alpha_n H_0(x).$$

Hence the first part of the theorem will be proved if we can show $\alpha_r = 0$, $r \not\equiv 0 \pmod{\pi}$. Now

$$\begin{aligned} K_n(ax+b) &= \sum_{r=0}^n H_{n-r}(ax+b) = \sum_{r=0}^n \alpha_r a^{n-r} H_{n-r}(x), \\ K_n(ax+b) &= a^n K_n(x) = \sum_{r=0}^n \alpha_r a^n H_{n-r}(x). \end{aligned}$$

Write $x+\lambda = y$ so that $H_{n-r}(x) = \frac{y^{n-r}}{(n-r)!}$. Then we have identically in y

$$\sum_{r=0}^n \frac{\alpha_r a^{n-r}}{(n-r)!} y^{n-r} = \sum_{r=0}^n \frac{\alpha_r a^n y^{n-r}}{(n-r)!}$$

so that by equating coefficients of corresponding powers of y ,

$$\alpha_r (a^r - 1) = 0 \quad (r = 0, 1, 2, \dots, n).$$

(11) now follows from (10). The last part of the theorem is obvious from (9) and (10).

If we write in (11) first $x = -\lambda$ and then $x = 0$ we obtain

THEOREM 5. *For any cyclic sequence $[K_n(x)]$ of order π ,*

$$\begin{aligned} K_n(-\lambda) &= 0, \quad n \not\equiv 0 \pmod{\pi}, \\ &= \alpha_n, \quad n \equiv 0 \pmod{\pi}, \end{aligned}$$

$$(12) \quad a^{-n} K_n(b) = K_n(0) = k_n = \frac{\alpha_0 \lambda^n}{n!} + \frac{\alpha_\pi \lambda^{n-\pi}}{(n-\pi)!} + \dots + \frac{\alpha_{r\pi} \lambda^{n-r\pi}}{(n-r\pi)!},$$

where $r\pi \leq n < (r+1)\pi$ and $n = 0, 1, 2, \dots$

We have from (12)

$$\begin{aligned} k_0 &= \alpha_0, \\ k_\pi &= \frac{\alpha_0 \lambda^\pi}{\pi!} + \alpha_\pi, \\ k_{2\pi} &= \frac{\alpha_0 \lambda^{2\pi}}{(2\pi)!} + \frac{\alpha_\pi \lambda^\pi}{\pi!} + \alpha_{2\pi}, \\ k_{3\pi} &= \frac{\alpha_0 \lambda^{3\pi}}{(3\pi)!} + \frac{\alpha_\pi \lambda^{2\pi}}{(2\pi)!} + \frac{\alpha_{2\pi} \lambda^\pi}{\pi!} + \alpha_{3\pi}, \\ &\dots \end{aligned}$$

Hence $\alpha_0, \alpha_\pi, \alpha_{2\pi}, \dots$ are uniquely determined in terms of $k_0, k_\pi, k_{2\pi}, \dots$. Since (12) gives k_n for all values of n in terms of $\alpha_0, \alpha_\pi, \alpha_{2\pi}, \dots$ we have proved

THEOREM 6. *If $[K_n(x), k_n]$ is any cyclic sequence of order π and if the values of $k_0, k_\pi, k_{2\pi}, \dots$ are given, then all the other k_n are uniquely determined.*

8. We shall now give the explicit expression for k_n as a function of $k_0, k_\pi, k_{2\pi}, \dots$ proving the last result in section 2. It is convenient to borrow a definition from the calculus of generating functions.

Given any sequence of constants

$$[c_n]: \quad c_0, c_1, c_2, \dots \quad (c_0 \neq 0),$$

the sequence

$$[c'_n]: \quad c'_0, c'_1, c'_2, \dots$$

determined by the equations:

$$c'_0 c_0 = 1$$

$$c_0 c'_n + c_1 c'_{n-1} + c_2 c'_{n-2} + \dots + c_n c'_0 = 0 \quad (n = 1, 2, 3, \dots)$$

is called the *inverse* of the sequence $[c_n]$. It is clear that the generating functions $c(t), c'(t)$ of the two sequences are reciprocals of each other. Assume that $k_0 \neq 0$, and consider the expression

$$A(z^\pi) = \frac{k_0 + k_\pi z^\pi + k_{2\pi} z^{2\pi} + \dots}{1 + \frac{\lambda^\pi}{\pi!} z^\pi + \frac{\lambda^{2\pi}}{(2\pi)!} z^{2\pi} + \dots} = u_0 + u_\pi z^\pi + u_{2\pi} z^{2\pi} + \dots$$

On clearing of fractions, we have the following set of equations to determine $u_0, u_\pi, u_{2\pi}, \dots$,

$$k_0 = u_0,$$

$$k_\pi = \frac{u_0 \lambda^\pi}{\pi!} + u_\pi,$$

$$k_{2\pi} = \frac{u_0 \lambda^{2\pi}}{(2\pi)!} + \frac{u_\pi \lambda^\pi}{\pi!} + u_{2\pi},$$

$$\dots \dots \dots \dots \dots \dots$$

Since these equations become identical with the equations (12) on replacing u by α we have proved

THEOREM 7. *The generating function of the sequence $\alpha_0, \alpha_\pi, \alpha_{2\pi}, \dots$ in Theorem 5 is given by*

$$A(z^\pi) = \frac{K(z^\pi)}{H(z^\pi)}$$

where

$$K(z^\pi) = \sum_{n=0}^{\infty} k_{n\pi} z^{n\pi},$$

$$H(z^\pi) = \sum_{n=0}^{\infty} \frac{1}{(n\pi)!} \lambda^{n\pi} z^{n\pi} = \frac{1}{\pi} \{ e^{a\lambda z} + e^{a^2 \lambda z} + \dots + e^{a^n \lambda z} \}.$$

The reciprocal of $H(z^\pi)$ generates the sequence inverse to $\left[\frac{\lambda^{n\pi}}{(n\pi)!} \right]$ since by (8)

$$h_{n\pi} = \frac{\lambda^{n\pi}}{(n\pi)!}$$

we write

$$(13) \quad \frac{1}{H(z^\pi)} = H'(z^\pi) = h'_0 + h'_\pi z^\pi + h'_{2\pi} z^{2\pi} + \dots$$

If $\pi = 2$, $a = b = -1$, the case Nielsen has studied*,

$$H'(z^\pi) = \operatorname{sech} \frac{z}{2} = E_0 + \frac{E_2 z^2}{2^2 2!} + \frac{E_4 z^4}{2^4 4!} + \dots$$

where E_0, E_2, E_4, \dots are Euler's numbers.

Moreover it is clear that

$$(14) \quad \alpha_{n\pi} = k_{n\pi} h'_0 + k_{(n-1)\pi} h'_\pi + \dots + k_0 h'_{n\pi}.$$

Let $[H_n''(x), h_n'']$ denote the cyclic sequence defined by

$$H_n''(x) = \frac{h'_0(x+\lambda)^n}{n!} + \frac{h'_\pi(x+\lambda)^{n-\pi}}{(n-\pi)!} + \frac{h'_{2\pi}(x+\lambda)^{n-2\pi}}{(n-2\pi)!} + \dots$$

$$\dots + \frac{h'_{r\pi}(x+\lambda)^{n-r\pi}}{(n-r\pi)!},$$

where as usual $r\pi \leq n \leq (r+1)\pi$. Then by (12), if $[K_n(x), k_n]$ is any cyclic sequence

$$k_n = \sum_{s=0}^r \frac{\alpha_{s\pi} \lambda^{n-s\pi}}{(n-s\pi)!} = \sum_{t=0}^r \sum_{s=t}^r \frac{k_{t\pi} h'_{(s-t)\pi} \lambda^{n-s\pi}}{(n-s\pi)!}$$

on substituting from (14) for $\alpha_{s\pi}$ and changing the order of summation.
Now

$$\sum_{s=t}^r \frac{h'_{(s-t)\pi} \lambda^{n-s\pi}}{(n-s\pi)!} = \sum_{u=0}^{u=r-t} \frac{h'_{u\pi} \lambda^{n-t\pi-u\pi}}{(n-t\pi-u\pi)!} = H_{n-t\pi}''(0) = h_{n-t\pi}''.$$

Furthermore if

$$H'(t^\pi) e^{tx} = H'_0(x) + H'_1(x)t + H'_2(x)t^2 + \dots$$

* Nielsen, l. c., chapter VI.

Then

$$H'_n(x) = \frac{h'_0 x^n}{n!} + \frac{h'_{\pi} x^{n-\pi}}{(n-\pi)!} + \cdots + \frac{h'_{r\pi} x^{n-r\pi}}{(n-r\pi)!} = H''_n(x-\lambda).$$

Hence we have proved

THEOREM 8. *If $[K_n(x), k_n]$ is any cyclic sequence of order π*

$$k_n = \sum_{s=0}^r k_{s\pi} H'_{n-s\pi}(\lambda),$$

where $r\pi \leq n < (r+1)\pi$, $\lambda = \frac{b}{a-1}$ and the generating function of the polynomials $H'_n(x)$ is

$$\pi e^{tx} [e^{at} + e^{a^2 t} + \cdots + e^{a^\pi t}]^{-1}.$$

CALIFORNIA INSTITUTE, PASADENA, CALIFORNIA.

October 29, 1928.

POSTULATES FOR THE INVERSE OPERATIONS IN A GROUP*

BY
MORGAN WARD

1. Introduction. Suppose that we are given a collection of marks which we shall call “ \mathfrak{S} -symbols,” and a rule which assigns to any two \mathfrak{S} -symbols x and y a unique third \mathfrak{S} -symbol z . We may then regard z as a one-valued “function” of x and y defined over the collection \mathfrak{S} and write

$$(1) \quad z = F(x, y).$$

It may happen that the function F is of such a character that when the \mathfrak{S} -symbols z, x are given in (1), an \mathfrak{S} -symbol y is uniquely determined, and when the \mathfrak{S} -symbols y, z are given in (1), an \mathfrak{S} -symbol x is uniquely determined. In this case we may associate with the function $F(x, y)$ two other one-valued functions $y = G(z, x)$, $x = H(y, z)$ defined over the collection \mathfrak{S} . These functions are called the first and second *inverses* of the function F . The primary object of this paper is to state the restrictions which must be imposed upon F in order that one of its inverses may define with \mathfrak{S} an abstract group.

It is convenient, in developing the properties of the system $\{\mathfrak{S}; \circ\}$ consisting of the \mathfrak{S} -symbols, F , and one or more postulates, to replace (1) by the notation†

$$z = x \circ y.$$

In any interpretation of the \mathfrak{S} , we may look upon \circ as an *operation* which we perform upon x and y to obtain z . We shall continue to call \circ an operation even when no interpretation of the \mathfrak{S} -symbols is in mind, and we shall similarly replace $y = G(z, x)$ and $x = H(y, z)$ by

$$y = z \Delta x \quad \text{and} \quad x = y \square z.$$

For example, suppose that the \mathfrak{S} -symbols stand for the rational integers, and that $F(x, y) = x - y$. Then $z = x - y$; $y = -z + x$; $x = y + z$, so that \circ is subtraction, \square , addition, and Δ , the negative of subtraction. Our problem in this instance would be first of all to frame a definition of “subtraction,” and then to define “addition” in terms of “subtraction.”

* Presented to the Society, April 5, 1930; received by the editors of the Bulletin in January, 1929, and transferred to the Transactions.

† Read “ z equals x dot y .”

2. Postulates for the operation \circ . Consider first the system $\{\mathfrak{S}; \circ\}$ consisting of (i) a collection \mathfrak{S} of two or more distinct elements a, b, c, \dots , (ii) a function $F(x, y) = x \circ y$ defined over \mathfrak{S} , and (iii) the following four postulates:

POSTULATE 1. *If a, b are any elements of \mathfrak{S} , then $a \circ b$ is an element of \mathfrak{S} uniquely determined by a and b .*

POSTULATE 2. *If a, b are any elements of \mathfrak{S} , then $a \circ a = b \circ b$.*

POSTULATE 3. *If a, b, c are any elements of \mathfrak{S} , and 1 is the element of definition 1 below, $(a \circ b) \circ c = a \circ (c \circ (1 \circ b))$.*

POSTULATE 4. *If a, b are any elements of \mathfrak{S} , and 1 is the element of Definition 1 below, and if $1 \circ a = 1 \circ b$, then $a = b$.*

THEOREM 1. *There exists a unique element i of \mathfrak{S} such that $i \circ i = i$.*

By Postulate 1, $a \circ a = i$ is an element of \mathfrak{S} , and by Postulate 2, $i \circ i = a \circ a = i$. Moreover, if j were any second element such that $j \circ j = j$, then by Postulate 2,

$$j = j \circ j = i \circ i = i.$$

DEFINITION 1. *The element i of Theorem 1 is called the “identity” of \mathfrak{S} and denoted by 1, so that Theorem 1 states that for any element a of \mathfrak{S}*

$$a \circ a = 1 \circ 1 = 1.$$

Postulates 1, 3 and 4 are true in any Abelian group, or any Abelian semi-group containing an identity. Postulate 4 is in fact a weakened form of Dickson's third postulate for a semi-group.* Postulate 2 is far more drastic, and serves to give the system its peculiar character.

3. Consistency and independence of postulates. The consistency and independence of the four postulates given in §2 is proved by the following table, which gives examples of systems in which Postulates 1–4 are all true, Postulate 1 false and Postulates 2, 3, 4 true and so on.

It should be noted that in order to prove that Postulate 1 is independent, we must change the statement of the remaining postulates slightly. Thus Postulate 2 should read *If a, b are any two elements of \mathfrak{S} , and if $a \circ a, b \circ b$ are both in \mathfrak{S} , then $a \circ a = b \circ b$.* The similar emendations of Postulate 3 and Postulate 4 are left to the reader.

* L. E. Dickson, *On semi-groups and the general isomorphism between infinite groups*, these Transactions, vol. 6 (1905), p. 205. Also see Theorem 5, §4, Theorem 10, §6.

TABLE I

 \mathfrak{S} $x \circ y$

Consistency		
1.	All four true	Rational integers
2.	All four true	Rationals, 0 excluded
Independence		
3.	Postulate 1 false	Rational integers, 2 excluded
4.	Postulate 2 false	Rational integers
5.	Postulate 3 false	Rational integers
6.	Postulate 4 false	Rationals, 0 excluded

4. **Deductions from postulates.** The five theorems which follow give important properties of the system $\{\mathfrak{S}; \circ\}$ defined in §2, and lead up to the fundamental theorem of the next section. The proofs of the theorems are given in some detail in order to bring out clearly the implications of the various postulates.

THEOREM 2. *If a is any element of \mathfrak{S} , then $a \circ 1 = a$.*

We have $1 \circ a = (1 \circ 1) \circ a = 1 \circ (a \circ (1 \circ 1)) = 1 \circ (a \circ 1)$ by Theorem 1 and Postulate 3. Therefore, by Postulate 4, $a = a \circ 1$.

THEOREM 3. *If a is any element of \mathfrak{S} , then $1 \circ (1 \circ a) = a$.*

We have $1 \circ a = (1 \circ a) \circ 1 = 1 \circ (1 \circ (1 \circ a))$, by Theorem 2 and Postulate 3. Therefore, by Postulate 4, $a = 1 \circ (1 \circ a)$.

THEOREM 4. *If a, b, c are any three elements of \mathfrak{S} , then $a \circ (b \circ c) = (a \circ (1 \circ c)) \circ b$.*

We have $a \circ (b \circ c) = a \circ [b \circ (1 \circ (1 \circ c))] = (a \circ (1 \circ c)) \circ b$, by Theorem 3 and Postulate 3.

THEOREM 4.1. *If a, b are any elements of \mathfrak{S} , then $1 \circ (a \circ b) = b \circ a$.*

We have $1 \circ (a \circ b) = (1 \circ (1 \circ b)) \circ a = b \circ a$ by Theorem 4 and Theorem 3.

THEOREM 5. *If a, b, c are any elements of \mathfrak{S} and if (i) $b \circ a = c \circ a$, then $b = c$; and if (ii) $a \circ b = a \circ c$, then $b = c$.*

(i) is clear from Postulate 4, since by Theorem 4 and Postulate 2

$$(1 \circ a) \circ (b \circ a) = [(1 \circ a) \circ (1 \circ a)] \circ b = 1 \circ b;$$

$$(1 \circ a) \circ (c \circ a) = [(1 \circ a) \circ (1 \circ a)] \circ c = 1 \circ c.$$

(ii) follows from (i) and Theorem 4.1.

THEOREM 6. *If a, b, c are any three elements of \mathfrak{S} , the three relations*

$$(2) \quad a \circ b = c,$$

$$(3) \quad b = (1 \circ c) \circ (1 \circ a),$$

$$(4) \quad a = c \circ (1 \circ b)$$

are all equivalent to one another.

Note that in accordance with our definitions in §1, (3) and (4) give the first and second inverses of the operation \circ in terms of \circ itself.

(2) implies (3); for if $a \circ b = c$, then by Theorem 4.1,

$$1 \circ c = 1 \circ (a \circ b) = b \circ a.$$

Hence

$$(1 \circ c) \circ (1 \circ a) = (b \circ a) \circ (1 \circ a) = b \circ [(1 \circ a) \circ (1 \circ a)] = b \circ 1 = b,$$

by Postulate 3, Postulate 4 and Theorem 2. Conversely, (3) implies (2); for all the steps in the reasoning above are reversible.

(3) is equivalent to (4); for writing $(1 \circ c)$, $(1 \circ a)$, b for a , b , c in (2), we see from what we have just proved that (3) is equivalent to

$$1 \circ a = (1 \circ b) \circ (1 \circ (1 \circ c)).$$

Hence

$$1 \circ a = (1 \circ b) \circ c = 1 \circ (c \circ (1 \circ b))$$

by Theorem 3 and Postulate 3. Hence by Postulate 2, (3) is equivalent to (4), so that each of (2), (3) and (4) implies the other two.

5. The operation \square . We shall now study the second inverse of \circ as defined by equation (4) of Theorem 6.

DEFINITION 2. *If x, y are any two elements of \mathfrak{S} ,*

$$x \square y = y \circ (1 \circ x).$$

FUNDAMENTAL THEOREM. *\mathfrak{S} forms a group with respect to the operation \square .*

(i) By Definition 2, Theorem 1 and Postulate 1, if a and b are any elements of \mathfrak{S} , $a \square b$ is an element of \mathfrak{S} uniquely determined by a and b .

(ii) If a, b, c are any elements of \mathfrak{S} , then

$$a \square (b \square c) = (a \square b) \square c.$$

For by Definition 2,

$$(a \square b) \square c = c \circ [1 \circ (b \circ (1 \circ a))];$$

$$a \square (b \square c) = [c \circ (1 \circ b)] \circ (1 \circ a).$$

Now

$$[c \circ (1 \circ b)] \circ (1 \circ a) = c \circ [(1 \circ a) \circ (1 \circ (1 \circ b))] = c \circ [(1 \circ a) \circ b],$$

by Postulate 3, Theorem 2. And by Theorem 4, Theorem 2,

$$c \circ [1 \circ (b \circ (1 \circ a))] = c \circ [(1 \circ (1 \circ (1 \circ a))) \circ b] = c \circ [(1 \circ a) \circ b].$$

(iii) The set contains an element i such that for any element a of the set, $i \square a = a \square i = a$.

For by Definition 2, Theorems 1, 2, 4, \mathfrak{S} contains 1 and

$$\begin{aligned} 1 \square a &= a \circ (1 \circ 1) = a \circ 1 = a, \\ a \square 1 &= 1 \circ (1 \circ a) = a, \end{aligned}$$

so that we may take $i = 1$.

(iv) If a is any element of \mathfrak{S} , the set also contains an element a' such that $a \square a' = i$.

For by Definition 2, Postulate 2,

$$a \square (1 \circ a) = (1 \circ a) \circ (1 \circ a) = 1.$$

Hence we may take $a' = 1 \circ a$, and the system $\{\mathfrak{S}; \square\}$ satisfies the four postulates for a group.*

Consider the inverses of \square in their relation to the original operation \circ .

THEOREM 7. *If $b \square c = a$, then $c = (1 \circ b) \square a = a \circ b$, and $b = a \square (1 \circ c) = (1 \circ c) \circ (1 \circ a)$.*

This is clear from Definition 2 and Theorem 6.

Thus the first inverse of \square is \circ , while the second inverse of \square is, by equation (3), the same as the first inverse of \circ .

6. The operation Δ . We shall now study the operation defined by equation (3).

DEFINITION 3. *If x, y are any two elements of \mathfrak{S} ,*

$$x \Delta y = (1 \circ x) \circ (1 \circ y).$$

Since as we might expect, the operation Δ is very similar to the original operation \circ , we shall merely state its more important properties. The following four theorems which correspond roughly to Theorems 1 to 6 may all be proved from Definition 3 and the results already given.

THEOREM 8. (i) $a \Delta a = 1$; (ii) $a \Delta 1 = 1 \circ a$; (iii) $1 \Delta a = a$; (iv) $(a \Delta 1) \Delta 1 = a$; (v) $(a \Delta b) \Delta 1 = b \Delta a$; (vi) $1 \circ (a \Delta b) = b \Delta a$.

THEOREM 9. (i) $a \Delta (b \Delta c) = ((b \Delta 1) \Delta a) \Delta c$; (ii) $(a \Delta b) \Delta c = b \Delta ((a \Delta 1) \Delta c)$.

* Speiser, *Die Theorie der Gruppen*, Berlin, 1927, pp. 10–11.

THEOREM 10. *If $a\Delta b = a\Delta c$, then $b = c$; if $b\Delta a = c\Delta a$, then $b = c$.*

THEOREM 11. *If $b = c\Delta a$, then $a \circ b = c$, and $b \square c = a$.*

For example, Theorem 9 (ii) may be proved as follows.

By Definition 3, $(a\Delta b)\Delta c = [1 \circ (a\Delta b)] \circ (1 \circ c)$. Therefore,

$$\begin{aligned}(a\Delta b)\Delta c &= [b\Delta a] \circ (1 \circ c) = [(1 \circ b) \circ (1 \circ a)] \circ (1 \circ c) \\ &= (1 \circ b) \circ [(1 \circ c) \circ (1 \circ (1 \circ a))],\end{aligned}$$

by Theorem 8 (vi), Definition 3, and Postulate 2. Hence by Theorem 3, Postulate 2, Definition 3,

$$\begin{aligned}(a\Delta b)\Delta c &= (1 \circ b) \circ [(1 \circ c) \circ a] = (1 \circ b) \circ [1 \circ (a \circ (1 \circ c))]; \\ (a\Delta b)\Delta c &= b\Delta[a \circ (1 \circ c)].\end{aligned}$$

Putting $b = 1$ in this last result,

$$\begin{aligned}(a\Delta 1)\Delta c &= 1\Delta[a \circ (1 \circ c)] \\ &= a \circ (1 \circ c)\end{aligned}$$

by Theorem 8 (iii). Hence

$$(a\Delta b)\Delta c = b\Delta((a\Delta 1)\Delta c).$$

7. Postulates for the operation Δ . It remains to give a set of postulates for the operation Δ which shall be consistent and independent.

THEOREM 12. *The system $\{\mathfrak{S}; \Delta\}$ satisfies the following four conditions:*

POSTULATE 1. *If a, b are any elements of \mathfrak{S} , $a\Delta b$ is an element of \mathfrak{S} uniquely determined by a and b .*

POSTULATE 2. *If a, b are any elements of \mathfrak{S} , $a\Delta a = b\Delta b$.*

POSTULATE 5. *If a, b, c are any elements of \mathfrak{S} , and 1 is the element of Theorem 1 and Theorem 8, $(a\Delta b)\Delta c = b\Delta((a\Delta 1)\Delta c)$.*

POSTULATE 6. *If a, b are any elements of \mathfrak{S} , and 1 is the element of Theorem 1 and Theorem 8, and if $a\Delta 1 = b\Delta 1$, then $a = b$.*

The proof is clear from Theorems 8–11.

Table I of §3 may easily be modified so as to show that these postulates are consistent and independent.

8. Condition that \square be commutative. We shall now give a condition that the operation \square be commutative, so that $\{\mathfrak{S}; \square\}$ will form an Abelian group.

THEOREM 13. *A necessary and sufficient condition that the operation \square of Definition 2 be commutative is that, for every pair of elements a, b of \mathfrak{S} , $a\Delta b = b \circ a$.*

The condition is necessary; for if \square is commutative, and if a, b are any two elements of \mathfrak{S} , then

$$(5) \quad a \square b = b \square a.$$

Then by Definition 2,

$$b \circ [b \circ (1 \circ a)] = b \circ [a \square b] = b \circ [b \square a] = b \circ [a \circ (1 \circ b)].$$

But

$$b \circ [b \circ (1 \circ a)] = (b \circ a) \circ b; \quad b \circ [a \circ (1 \circ b)] = 1 \circ a,$$

by Theorem 4, Theorem 3 and Theorem 1. Hence (5) implies that

$$(b \circ a) \circ b = 1 \circ a.$$

By Theorem 6 and Definition 3, this last equation is equivalent to

$$b \circ a = (1 \circ a) \circ (1 \circ b) = a \Delta b.$$

The condition is moreover sufficient, for all the steps in the reasoning just given are reversible.

We close with a table giving the relations between the various operations and their inverses.

TABLE II

Operation	First Inverse	Second Inverse
$z = x \circ y$	$y = z \Delta x$	$x = y \square z$
$x = y \square z$	$z = x \circ y$	$y = z \Delta x$
$y = z \Delta x$	$x = y \square z$	$z = x \circ y$

I wish to express my thanks to the editors of this journal for some extremely helpful criticisms and suggestions.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

Chapter 5

1931

THE CHARACTERISTIC NUMBER OF A SEQUENCE OF INTEGERS SATISFYING A LINEAR RECURSION RELATION*

BY
MORGAN WARD

1. Introduction. Let

$$(W)_n : \quad W_0, W_1, \dots, W_n, \dots$$

denote a sequence of integers satisfying the linear difference equation of order $r=3$

$$(1.1) \quad \Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n, \quad R \neq 0,$$

where P, Q, R, W_0, W_1, W_2 are fixed integers,† and let $m > 1$ be any positive integer. If

$$W_n \equiv A_n \quad (\text{mod } m; 0 \leq A_n \leq m-1; n = 0, 1, \dots)$$

we shall call $(A)_n$ the *reduced sequence* corresponding to $(W)_n$ modulo m .

If after s terms in the reduced sequence, a cycle of t terms keeps repeating itself indefinitely, $(W)_n$ will be said to *admit the period t , modulo m* . The least period that $(W)_n$ admits (modulo m) is called its *characteristic number*.‡

In this paper, I give a number of new results on the form of the characteristic number of a sequence. The principal result is the following:

If $m = p_1^{a_1} \cdots p_k^{a_k}$ is the resolution of m into its prime factors, then the characteristic number of any sequence modulo m is the least common multiple of its characteristic numbers modulis $p_1^{a_1}, \dots, p_k^{a_k}$.

The restriction to the case of a difference equation of order 3 is mainly for convenience of notation and ease of illustration. The theorems in the first seven sections of the paper, which include my main result, may be immediately extended to the general case of a difference equation of order r .

* Presented to the Society, November 29, 1929; received by the editors in January, 1930.

† The arithmetical properties of such sequences do not seem to have been extensively investigated. Besides the references in Dickson's *History*, there is an important paper by Carmichael on the linear recursion relation (1.1) for general r (*Quarterly Journal of Mathematics*, vol. 48 (1920), pp. 343–372). We shall refer to this paper as Carmichael I, giving page reference. Many of Carmichael's results are summarized in a more recent paper (*American Mathematical Monthly*, vol. 36 (1929), pp. 132–143). Draeger (*Ueber rekurrente Reihen von höherer, insbesondere von der dritten Ordnung*, Dissertation, Jena, 1919) has discussed (1.1) in detail and given some arithmetical results for the cases $m = 2, 3$ and $P \equiv 0 \pmod{m}$).

‡ Carmichael I, p. 345. We shall omit the phrase "modulo m " when no confusion can arise.

2. Periodicity of sequences. We shall employ the notation

$$A_0, A_1, \dots, A_{\lambda-1}; \dot{A}_\lambda, A_{\lambda+1}, \dots, \dot{A}_{\lambda+\mu-1}$$

for a reduced sequence $(A)_n$ having λ non-repeating terms $A_0, A_1, \dots, A_{\lambda-1}$ and μ repeating terms* $\dot{A}_\lambda, A_{\lambda+1}, \dots, \dot{A}_{\lambda+\mu-1}$. If $\lambda=0$, $(W)_n$ is said to be *purely periodic* modulo m .

If μ is the characteristic number of $(W)_n$, then a necessary and sufficient condition that $(W)_n$ admit the period r is that $\dagger \mu | r$.

THEOREM 2.1. *Every sequence $(W)_n$ becomes periodic,‡ modulo m . Moreover, if μ is the characteristic number of $(W)_n$ and λ the maximum number of non-repeating terms in the reduced sequence $(A)_n$ corresponding to $(W)_n$, then*

$$\lambda \leq m^3 - 1; 1 \leq \mu \leq m^3 - \lambda.$$

Call an ordered set of three consecutive elements of $(A)_n$ a triad. Then the first m^3+3 terms of $(A)_n$ contain the m^3+1 triads

$$(2.1) \quad A_0, A_1, A_2; A_1, A_2, A_3; \dots; A_{m^3}, A_{m^3+1}, A_{m^3+2}$$

of which at most m^3 are distinct, since $0 \leq A_n \leq m-1$. Hence if λ, μ are the least values of s, t such that

$$A_s = A_{s+t}, A_{s+1} = A_{s+t+1}, A_{s+2} = A_{s+t+2}$$

in (2.1), the first part of the theorem follows from the linearity of (1.1). The remainder of the theorem follows from the inequalities

$$s \leq m^3 - 1; s + t + 2 \leq m^3 + 2.$$

3. Reduction to prime powers. We shall now show that there is no loss of generality in supposing that m is a power of a prime.

THEOREM 3.1. *Let $(W)_n$ be any particular solution of the difference equation (1.1), and assume that $m=a \cdot b$ where $(a, b)=1$; $a, b > 1$. Then the characteristic number of $(W)_n$ modulo m is the L.C.M. of its characteristic numbers modulis a and b .*

Let $\mu(x) \equiv \mu_x$ denote the characteristic number of $(W)_n$ modulo x , and let κ denote the L.C.M. of μ_a and μ_b where, by hypothesis, $a \cdot b = m$; $(a, b) = 1$.

$(W)_n$ admits the period μ_m modulis a and b ; therefore $\mu_a | \mu_m$, $\mu_b | \mu_m$, so that $\kappa | \mu_m$.

* It is understood that λ is the greatest number of non-repeating terms, and μ the smallest number of repeating terms in the reduced sequence.

† We use the customary abbreviations (a, b) for the greatest common divisor of the integers a and b , $a | b$ for a divides b , and L.C.M. of a and b for the least common multiple of a and b .

‡ For another proof, see Carmichael I, p. 344.

$(W)_n$ also admits the period κ modulis a and b ; therefore

$$(3.1) \quad W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{a}, \quad W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{b} \quad (n = 0, 1, \dots)$$

where λ is the number of non-repeating terms in the reduced sequence $(A)_n$ corresponding to $(W)_n$ modulo $m = a \cdot b$.

Since $(a, b) = 1$, (3.1) implies that

$$W_{\lambda+\kappa+n} - W_{\lambda+n} \equiv 0 \pmod{m; n = 0, 1, \dots}.$$

Hence $(W)_n$ admits the period κ modulo m and $\mu_m | \kappa$. Since $\kappa | \mu_m$, $\kappa = \mu_m$. The following fundamental result is a direct corollary of this theorem.

THEOREM 3.11. *Let $(W)_n$ be any particular solution of the difference equation (1.1) and let*

$$m = p_1^{a_1} \cdots p_k^{a_k}$$

be the resolution of m into its prime factors. Then the characteristic number of $(W)_n$ modulo m is the L.C.M. of its characteristic numbers modulis $p_1^{a_1}, \dots, p_k^{a_k}$.

To illustrate this theorem, consider the difference equation

$$\Omega_{n+3} = \Omega_{n+2} + \Omega_{n+1} + \Omega_n$$

with the particular solution $(U)_n$ whose first few terms are

$$1, 0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, \dots$$

Let $\mu(m)$ denote the characteristic number of $(U)_n$ modulo m . Taking $(U)_n$ modulis 2, 3, 4, 5, 6, 7, 9, 42, we find that $\mu(2) = 4$, $\mu(3) = 13$, $\mu(4) = 8$, $\mu(6) = 52$, $\mu(7) = 48$, $\mu(9) = 39$, and $\mu(42) = 624$. Thus $\mu(42)$, for example, equals $3 \cdot 13 \cdot 16$ which is the L.C.M. of $\mu(2)$, $\mu(3)$ and $\mu(7)$; and $\mu(6)$ is the L.C.M. of $\mu(2)$ and $\mu(3)$.

4. Purely periodic sequences. We shall now give some conditions that a sequence $(W)_n$ be purely periodic, modulo m . It is easily shown that a sufficient condition* that the sequence $(W)_n$ be purely periodic is that $(R, m) = 1$. This condition is not, however, a necessary one. On the other hand, we shall prove

THEOREM 4.1. *A necessary condition that the sequence $(W)_n$ be purely periodic modulo m is that*

$$(4.1) \quad W_2 \equiv PW_1 - QW_0 \pmod{d},$$

where d is the greatest common divisor of R and m .

* Carmichael, I, p. 344, §2.

Assume that $(W)_n$ is purely periodic modulo m , and has the characteristic number μ . Then if $(m, R) = d$, $d \mid m$ and $d \mid R$, so that

$$W_{\mu+2} \equiv PW_{\mu+1} - QW_\mu + RW_{\mu-1} \equiv PW_{\mu+1} - QW_\mu \pmod{d},$$

giving (4.1) immediately.

Unfortunately, this condition is not sufficient for pure periodicity. Consider for example the difference equation

$$\Omega_{n+3} = 2\Omega_{n+2} + \Omega_{n+1} + 3\Omega_n, \text{ with } m = 9.$$

Here $d=3$, and if we take $W_0=0$, $W_1=0$, $W_2=3$, then $W_2 \equiv 2W_1 + W_0 \pmod{3}$. Nevertheless, in this case $(A)_n$ is $0; 0, 3, 6, 6, 0, 6, 3, 3$.

We can, however, prove as in Theorem 3.1 that if $(W)_n$ is purely periodic modulis a and b , where $(a, b)=1$, then $(W)_n$ is purely periodic modulo $a \cdot b$. Consequently, we have the following criterion for pure periodicity:

THEOREM 4.2. *If $m=p_1^{a_1} \cdots p_k^{a_k}$ is the decomposition of m into its prime factors, then a necessary and sufficient condition that $(W)_n$ be purely periodic modulo m is that it be purely periodic modulis $p_1^{a_1}, \dots, p_k^{a_k}$.*

We shall consider henceforth only purely periodic solutions of (1.1).

5. Singular and non-singular sequences. Let $(W)_n$ stand as usual for a particular solution of (1.1), and let $D=D(W)$ denote the determinant

$$\begin{vmatrix} W_0 & W_1 & W_2 \\ W_1 & W_2 & W_3 \\ W_2 & W_3 & W_4 \end{vmatrix}.$$

The solution $(W)_n$ is said to be non-singular (modulo m) if $(D, m)=1$ and singular if $(D, m)=d>1$.

THEOREM 5.1. *All purely periodic non-singular sequences satisfying (1.1) have the same characteristic number, τ , modulo m . Moreover, the characteristic number modulo m of any singular sequence is a divisor of τ .*

Let $(W)_n$ be any solution of (1.1), and $(T)_n$ any non-singular solution, and let the characteristic numbers of $(W)_n$ and $(T)_n$ modulo m be μ and τ respectively. Then we can determine integers K_0, K_1, K_2 such that

$$(5.1) \quad W_n \equiv K_0 T_n + K_1 T_{n+1} + K_2 T_{n+2} \pmod{m; n=0, 1, \dots}$$

where

$$(5.2) \quad 0 \leq K_0, K_1, K_2 \leq m-1.$$

For on account of the linearity of (1.2), (5.1) will be true provided that it is true for $n=0, 1$, and 2.

But a sufficient condition that the congruences

$$W_i \equiv K_0 T_i + K_1 T_{i+1} + K_2 T_{i+2} \pmod{m} ; i = 0, 1, 2$$

have a solution satisfying the conditions (5.2) is that $(D(T), m) = 1$.

From (5.1), we see that $(W)_n$ admits all the periods of $(T)_n$, so that $\mu | \tau$. If $(W)_n$ is also non-singular, a repetition of the argument shows that $\tau | \mu$, so that $\tau = \mu$.

The characteristic number τ is called the *principal period* of (1.1) modulo m .

It is easily shown that if $(m, c) = 1$, the sequences $(W)_n$ and cW_0, cW_1, \dots or for short $c(W)_n$, have the same characteristic number* modulo m . If $(m, c) > 1$, this is not usually the case.

For instance, consider the difference equation and particular solution given to illustrate Theorem 3.11. The characteristic number of $(U)_n$ modulo 6 is 52. Nevertheless, the characteristic number of $3(U)_n$ modulo 6 is only 4.† Now 4 is the characteristic number of $(U)_n$ modulo $2 = 6/3$. We have here an illustration of the following theorem:

THEOREM 5.2. *If $(W)_n$ is any particular solution of (1.1) and c is any integer, the characteristic number of $c(W)_n$ modulo m equals the characteristic number of $(W)_n$ modulo m/d , where d is the greatest common divisor of m and c .*

Let $c = c' \cdot d$, $m = m' \cdot d$; $(m', c') = 1$. From the congruences

$$cW_{n+3} \equiv cPW_{n+2} - cQW_{n+1} + cRW_n \pmod{m},$$

we obtain

$$(5.3) \quad c'W_{n+3} \equiv c'PW_{n+2} - c'QW_{n+1} + c'RW_n \pmod{m'; n = 0, 1, \dots}.$$

Since $(c', m') = 1$, the characteristic number of $c'(W)_n$ modulo m' is the same as the characteristic number, κ , of $(W)_n$ modulo m' . Let μ denote the characteristic number of $c(W)_n$ modulo m . From (4.3), $(W)_n$ admits the period μ modulo m' , so that $\kappa | \mu$.

But we also have

$$W_{k+\kappa} - W_k \equiv 0 \pmod{m'; k = 0, 1, \dots}.$$

Hence $c'W_{k+\kappa} - c'W_k \equiv 0 \pmod{m'}$, $cW_{k+\kappa} - cW_k \equiv 0 \pmod{m}$, so that $c(W)_n$ admits the period κ , modulo m . Thus $\mu | \kappa$, so that $\mu = \kappa$.

* If the periodic parts of $(A)_n$ and $c(A)_n$ are merely cyclic permutations of each other, c is called a multiplier of $(W)_n$. The theory of the multipliers of a sequence is considered in §9, for m a prime p .

† Note that $D(3U) = 27$, which is not prime to the modulus 6.

We can derive the following important consequence from Theorem 5.2.

THEOREM 5.3. *Let $(S)_n$ be any singular solution of (1.1) and let d be the greatest common divisor of $D(S)$ and m . Then the characteristic number of $(S)_n$ modulo m is a multiple of the principal period of (1.1) modulo m/d .**

If $(T)_n$ is any non-singular solution and if $(D(S), m) = d$, then it is easily shown that we can determine constants K_0, K_1, K_2 such that

$$dT_n \equiv K_0 S_n + K_1 S_{n+1} + K_2 S_{n+2} \pmod{m; n = 0, 1, \dots},$$

where $0 \leq K_0, K_1, K_2 \leq m-1$. Hence $d(T)_n$ admits the periods of $(S)_n$. The theorem now follows immediately from Theorem 5.2, since $(T)_n$ is also a non-singular solution of (1.1) modulo m/d .

6. The binomial congruence. Consider the binomial congruence

$$(6.1) \quad x^n \equiv 1 \pmod{m, F(x)}$$

where it should be noted that

$$F(x) = x^3 - Px^2 + Qx - R$$

is the characteristic function of the difference equation (1.1).

The problem which immediately suggests itself is to find those values of n for which (6.1) is an identity in x . We shall see that they are the periods of the non-singular sequences of (1.1), modulo m .

If

$$(U)_n : \quad U_0, U_1, U_2, \dots, U_n, \dots$$

denotes that particular solution of

$$(1.1) \quad \Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n, \quad R \neq 0,$$

with the initial values $U_0 = 1/R, U_1 = 0, U_2 = 0$, then it may be shown by induction that

$$(6.2) \quad x^n = U_{n+1}x^2 + (U_{n+2} - PU_{n+1})x + RU_n + Q_n(x)F(x),$$

where

$$Q_0(x) = 0; \quad Q_n(x) = \sum_{r=1}^n U_r x^{n-r} \quad (n = 1, 2, \dots).$$

Suppose that

$$U_n \equiv H_n \pmod{m; 0 \leq H_n \leq m-1; n = 0, 1, \dots}.$$

* One might conjecture from Theorem 4.3 that all singular solutions $(S)_n$ for which the greatest common divisor of $D(S)$ and m has the same value would have the same characteristic number, but it is easy to construct examples showing that this is not the case.

(6.2) then gives us the fundamental formula

$$x^n \equiv H_{n+1}x^2 + (H_{n+2} - PH_{n+1})x + RH_n \pmod{m, F(x)}.$$

Hence $x^n \equiv 1 \pmod{m, F(x)}$ identically in x when and only when $U_{n+1} \equiv U_{n+2} \equiv 0 \pmod{m}$ and $RU_n \equiv 1 \pmod{m}$. Thus we have the following theorem:

THEOREM 6.1. *Necessary and sufficient conditions that (6.1) hold identically in x for $n=\mu$ are that R be prime to m , and that the sequence $(U)_n$ admit the period μ modulo m .*

We shall assume henceforth that $(R, m) = 1$. Since

$$D(U) = \begin{vmatrix} R^{-1}, & 0, & 0 \\ 0, & 0, & 1 \\ 0, & 1, & P \end{vmatrix} = (-R)^{-1},$$

the characteristic number of $(U)_n$ is the principal period τ of (1.2) modulo m . It then follows from Theorem 6.1 that the least value of n for which (6.1) is an identity in x is τ .*

If we put $x=\alpha$ in the identity (6.2), where α is a root of $F(x)=0$, we have the congruence

$$\alpha^n \equiv 1 \pmod{m}.$$

Thus τ is divisible by the exponent to which α belongs modulo m , which gives us the following theorem:

THEOREM 6.2. *The principal period of (1.1) modulo m is divisible by the L.C.M. of the exponents to which the roots of $F(x)=0$ belong, modulo m .*

7. Characteristic number for powers of a prime. Assume now that

$$m=p^t \quad (t \geq 1)$$

is a power of a prime, p .

THEOREM 7.1. *If $(W)_n$ is any solution of (1.1) and $\mu^{(t)} = \mu(p^t)$, $\mu = \mu(p)$ the characteristic numbers of $(W)_n$ modulo $m=p^t$ and modulo p respectively, then*

$$(7.1) \quad \mu^{(t)} = p^b \mu$$

where† $0 \leq b \leq t-1$.

By Theorem 6.1, $x^{\mu^{(t)}} \equiv 1 \pmod{p^t, F(x)}$, so that $x^{\mu^{(t)}} \equiv 1 \pmod{p, F(x)}$ and $\mu | \mu^{(t)}$. Also,

* Compare the relationship between the binomial congruence $x^n \equiv 1 \pmod{m}$ and the difference equation $\Omega_{n+1} \equiv R\Omega_n \pmod{m}$; $(R, m) = 1$. The characteristic number of any solution of the difference equation is an admissible value of n for the congruence.

† Carmichael (I, p. 352) gives the limits $0 \leq b \leq t$ for b .

$$(7.2) \quad x^\mu = 1 + pP(x) + F(x)Q(x)$$

where $P(x)$ and $Q(x)$ are polynomials in x with integral coefficients. On raising both sides of (7.2) to the p^{t-1} power, we see that $x^{\mu p^{t-1}} \equiv 1 \pmod{p^t}$, $F(x)$. By Theorem 6.1, $\mu^{(t)} \mid \mu p^{t-1}$; since $\mu \mid \mu^{(t)}$, (7.1) follows.

For illustrations of this theorem, see the examples following Theorem 3.11.*

By the same method of proof used in Theorem 7.1, we can establish the following result:

THEOREM 7.2. *If $\sigma \geq 1$ and $x^{\mu(p)} \equiv 1 \pmod{p^\sigma, F(x)}$ but $x^{\mu(p)} \not\equiv 1 \pmod{p^{\sigma+1}, F(x)}$, then*

$$\begin{aligned} \mu(p^t) &= \mu(p) \quad \text{if} \quad \sigma \geq t \geq 1, \\ \mu(p^t) &= p^{t-\sigma}\mu(p) \quad \text{if} \quad t \geq \sigma. \end{aligned}$$

The problem of determining the exponent b in (7.1) is thus a generalization of Abel's famous problem† of finding the highest power of p which will divide $a^{p-1} - 1$.

8. Characteristic number for prime modulus. Assume now that m is a prime, p . The factorization of $F(x)$ modulo p may be described by a partition of three; for example, if $F(x)$ is irreducible, we shall say it is of "type [3]", if it can be factored into an irreducible quadratic factor and a linear factor, we shall say that it is of "type [2, 1]" and so on. In any case, the factorization is unique; denote the roots which correspond to linear factors by small italic letters a, b, c and the roots which correspond to irreducible quadratic or cubic factors by small greek letters α, β, γ .

Let $L(\alpha)$; $L(a)$ denote the exponents to which the roots $\alpha; a$ belong modulo p and $L(\alpha, b); L(\alpha, \beta, c)$, etc., the L.C.M. of the exponents to which $\alpha, b; \alpha, \beta, c$ etc. belong modulo p .

Finally, let Δ denote the discriminant of $F(x)$, and W the matrix

$$\begin{pmatrix} W_0, & W_1, & W_2 \\ W_1, & W_2, & W_3 \\ W_2, & W_3, & W_4 \end{pmatrix}.$$

Then it is easily shown from the known algebraic theory of (1.1) that the characteristic number of $(W)_n$ is given by the following table:

* b in (7.2) may be zero; for example, take $F(x) = x^3 - 2x^2 + x - 1$ and $p = 2$. The first few terms of $(U)_n$ are 1, 0, 0, 1, 2, 3, 5, 9, 16, 28, Taking the sequence modulo 2 and modulo 4, we obtain 1, 0, 0, 1, 0, 1, 1, and 1, 0, 0, 1, 2, 3, 1 so that $\mu(2^2) = \mu(2) = 7$.

† Crelle's Journal, vol. 3 (1828), p. 212. See also Dickson's *History*, Chapter IV.

CHARACTERISTIC NUMBERS MODULO p

Case	Type of $F(x)$	Quadratic character* of Δ modulo p	Algebraic form of W_n in terms of roots of $F(x) \equiv 0 \pmod{p}$		
			Rank of W	Characteristic number	
I	[3]	+1	$A\alpha^n + B\beta^n + C\gamma^n$	3	$L(\alpha) = L(\beta) = L(\gamma).$
II	[2, 1]	-1	$A\alpha^n + B\beta^n + C\gamma^n$ $A\alpha^n + B\beta^n$ Cc^n	3 2 1	$L(\alpha, c) = L(\beta, c),$ $L(\alpha) = L(\beta),$ $L(W_1/W_0).$
III	[1, 1, 1]	+1	$Aa^n + Bb^n + Cc^n$ $Aa^n + Bb^n \brace$ $Bb^n + Cc^n \brace$ $Cc^n + Aa^n \brace$ $Aa^n; Bb^n; Cc^n$	3 2 1	$L(a, b, c),$ $\begin{cases} L(a, b), \\ L(b, c), \\ L(c, a), \end{cases}$ $L(W_1/W_0).$
IV	[1 ² , 1]	0 $PQ - 9R \not\equiv 0$	$(A + Bn)a^n + Cc^n \brace$ $Bna^n + Cc^n \brace$ $Bna^n \brace$ $(A + Bn)a^n \brace$ $Aa^n + Cc^n$ $Aa^n; Cc^n$	3 2 2 1	$pL(a, c),$ $pL(a),$ $L(a, c),$ $L(W_1/W_0).$
V	[1 ³]	0 $PQ - 9R \equiv 0$	$(A + Bn + Cn^2)a^n \brace$ $(Bn + Cn^2)a^n \brace$ $(A + Cn^2)a^n \brace$ Cn^2a^n $(A + Bn)a^n$ Aa^n	3 2 1	$pL(a),$ $pL(a),$ $L(W_1/W_0).$

The problem of determining the characteristic number for a prime modulus is thus equivalent to the problem of determining the exponent to which a given element in a Galois field of order p^3 , p^2 or p belongs.†

* There exists no convenient criterion for distinguishing the cases when $F(x)$ is of type [3], and of type [1, 1, 1]. See Dickson's *History*, vol. I, pp. 252–256.

† If we call a difference equation *primitive* (modulo p) when there is only one sequence belonging to it, then, just as in the allied theory of primitive marks in a Galois field, or primitive roots of p^n , we can show that for every prime p , there exist primitive difference equations of any order r .

We shall devote the concluding two sections of the paper to studying case I. The characteristic number modulo p of all sequences satisfying (1.1) is then the same, and equals the exponent to which any root of $F(x)=0$ belongs in the Galois field $[p^3]$ associated with $F(x)$. We shall call this number the *period* of $F(x)$, and denote it by τ . It is of course a divisor of p^3-1 .

If α, β, γ are the roots of $F(x)=0$, and $S_n = \alpha^n + \beta^n + \gamma^n$, then*

$$(8.1) \quad \beta \equiv \alpha^p, \quad \gamma \equiv \alpha^{p^2}; \quad R \equiv \alpha^{1+p+p^2}; \quad S_n \equiv \alpha^n + \alpha^{pn} + \alpha^{p^2n}.$$

9. Multipliers of cycles. If $(A)_n$ is any reduced sequence of residues, so that

$$A_{n+3} \equiv PA_{n+2} - QA_{n+1} + RA_n \quad (0 \leq A_n \leq p-1, n = 0, \pm 1, \dots)$$

the τ residues $A_0, \dots, A_{\tau-1}$ are said to form a cycle (A) belonging to $F(x)$. Two such cycles are said to be equal if either can be obtained from the other by a cyclic permutation of its elements.

Let L be any residue. If the cycle $LA_0, \dots, LA_{\tau-1}$ equals the cycle (A) , then L is called a multiplier of (A) ; we have

$$(9.1) \quad LA_n \equiv A_{n+l} \quad (n = 0, \dots, \tau-1).$$

Since any other cycle (B) of $F(x)$ may be expressed in the form

$$B_n \equiv K_0 A_n + K_1 A_{n+1} + K_2 A_{n+2} \quad (n = 0, \dots, \tau-1),$$

where K_0, K_1, K_2 are residues, the following theorem is apparent:

THEOREM 9.1. *If L is a multiplier of one cycle of $F(x)$, it is a multiplier of all the cycles of $F(x)$, and the integer l in equation (9.1) does not depend on the particular cycle (A) used in defining L .*

We shall call l the span of L .

The following three theorems are easily established:

THEOREM 9.2. *The multipliers of the cycles of $F(x)$ form a group with respect to multiplication modulo p .*

THEOREM 9.3. *Two multipliers with the same span are identical modulo p .*

THEOREM 9.4. *The group of the multipliers of the cycles of $F(x)$ is cyclic, and a generator is the unique multiplier of least span.*

Let M denote this unique multiplier. From Theorem 9.4, there follows:

* It is understood that all congruences in which the modulus is not indicated are to be taken to the modulus p over the field of the p residues $0, 1, \dots, p-1$. For the properties of Galois fields which are assumed, see Dickson, work cited.

THEOREM 9.41. *The span of M divides the span of every other multiplier.*

THEOREM 9.5. *If $p^2 + p + 1 \equiv \pi \pmod{\tau}$, then R is a multiplier of span π .*

Since $p^3 \equiv 1 \pmod{\tau}$,

$$p^2\pi \equiv p\pi \equiv \pi \pmod{\tau}.$$

By (8.1),

$$RS_n \equiv \alpha^\pi(\alpha^n + \alpha^{pn} + \alpha^{p^2n}) \equiv \alpha^{n+\pi} + \alpha^{p(n+\pi)} + \alpha^{p^2(n+\pi)} \equiv S_{n+\pi}.$$

Hence by Theorem 9.1, R is a multiplier of span π .

As an immediate consequence of these theorems, we see that R is congruent to a power of M , modulo p , and that the span of M divides π .

THEOREM 9.6. *If $\epsilon(M)$ is the exponent to which the multiplier M belongs modulo p , and if μ is its span, then*

$$(9.2) \quad \tau = \epsilon(M)\mu$$

where τ is the period of $F(x)$.*

$\mu | \tau$; for if $\tau = s\mu + t$ ($0 \leq t \leq \mu - 1$), then by (9.1)

$$M^{\tau-s}A_n \equiv A_{n+(\tau-s)\mu} \equiv A_{n+t} \quad (n=0, \dots, \tau-1)$$

so that $\mu | t$; $t=0$. Similarly, $\epsilon(M) | \tau$ so that $\epsilon(M) \cdot \mu | \gamma\tau$ where $\gamma = (\epsilon(M), \mu) = 3$ or 1. But

$$A_n \equiv M^{\epsilon(M)}A_n \equiv A_{n+\epsilon(M)\mu} \quad (n=0, \dots, \tau-1).$$

Hence $\tau | \epsilon(M)\mu$, so that either $\tau = \epsilon(M)\mu$ or $3\tau = \epsilon(M)\mu$.

The latter case can occur only when $(\epsilon(M), \mu) = 3$; but then

$$A_{n+\tau} \equiv A_n \equiv M^{\epsilon(M)/3} \cdot A_n$$

so that $M^{\epsilon(M)/3} \equiv 1$, contradicting the definition of $\epsilon(M)$.

We shall call μ the *restricted period* of $F(x)$; since it is a divisor of $p^2 + p + 1$, we may write

$$(9.3) \quad p^2 + p + 1 = \kappa \cdot \mu.$$

We easily find that

$$(9.31) \quad M^\kappa \equiv R, \quad M^3 \equiv R^\mu,$$

* (9.2) is a special case of a theorem given in Carmichael I, p. 355. Carmichael calls μ the restricted period of the sequence whose characteristic number is τ .

so that

$$(9.32) \quad \epsilon(R) \mid \epsilon(M) \mid 3\epsilon(R),$$

where $\epsilon(R)$ is the exponent to which R belongs, modulo p .

If $p \equiv 2 \pmod{3}$, then $p^2 + p + 1 \equiv 1 \pmod{3}$ and it follows from Theorem 9.6 and equation (9.32) that $\tau = \epsilon(R)\mu$ where $\mu \mid p^2 + p + 1$ and $(\mu, 3) = 1$. The concluding section of the paper is devoted to the more interesting case when $p \equiv 1 \pmod{3}$.

10. Period for primes of form $3m+1$. We shall assume throughout this section that

$$(10.1) \quad p = 3^k n + 1, \quad (n, 3) = 1; \quad k \geq 1.$$

Then $p^2 + p + 1 \equiv 0 \pmod{3}$, $\not\equiv 0 \pmod{9}$, and from (9.3),

$$(10.2) \quad \kappa\mu/3 \equiv 1 \pmod{\epsilon(M)} \equiv 1 \pmod{\epsilon(R)}.$$

THEOREM 10.1. *If p is of the form $3^k n + 1$, and μ denotes the restricted period of $F(x)$, then $\mu \equiv 0 \pmod{3}$ when and only when $\epsilon(R) \equiv 0 \pmod{3^k}$.*

If this last condition holds, then

$$(10.3) \quad \tau = \epsilon(R)\mu, \quad M \equiv R^{\mu/3} \pmod{p}.$$

Let $\mu = 3\mu'$. Then $(\mu', 3) = 1$, $(\kappa, 3) = 1$, and from (10.2) $\kappa\mu' \equiv 1 \pmod{\epsilon(M)}$. From (9.31), $R \equiv M^\kappa \pmod{p}$ and

$$(10.31) \quad M \equiv R^{\mu'} \pmod{p}.$$

Hence by (9.32), $\epsilon(M) = \epsilon(R)$. Assume that

$$\epsilon(M) = 3^s \cdot \sigma, \quad (\sigma, 3) = 1; \quad s \leq k;$$

then by (9.2), $\tau = 3^{s+1}\tau'$;

$$\tau'; \quad (\tau', 3) = 1.$$

Now it is easily seen that $\alpha^{\tau'}$ is a primitive 3^{s+1} root of unity, modulo p , and hence a residue of p if and only if $s < k$. Assume that $s < k$. Then if $\alpha^{\tau'} \equiv Q$, $\alpha^{p\tau'} \equiv \alpha^{p^s\tau'} \equiv Q$, so that by (8.1),

$$QS_n \equiv S_{n+\tau'},$$

and by Theorem 9.1, Q is a multiplier. By Theorem 9.4, $3^{s+1} = \epsilon(Q)$; but $\epsilon(Q) \mid \epsilon(M)$. Hence $s = k$ and

$$(10.32) \quad \epsilon(R) = \epsilon(M) \equiv 0 \pmod{3^k}.$$

Conversely, if $\epsilon(R) \equiv 0 \pmod{3^k}$, then (10.32) follows from (9.32). If $\mu \not\equiv 0 \pmod{3}$, then $\kappa \equiv 0 \pmod{3}$, and (9.32) gives

$$M^{\epsilon(M)/3} \equiv 1 \equiv R^{\epsilon(M)/3} \equiv R^{\epsilon(R)/3} \pmod{p},$$

contrary to the definition of $\epsilon(R)$. Equation (10.3) now follows from Theorem 9.6, (10.32) and (10.31).

THEOREM 10.2. *If $\epsilon(R) \equiv 0 \pmod{3}$, $\not\equiv 0 \pmod{3^k}$, then $\tau = 3\epsilon(R)\mu$, where $\mu | (p^2 + p + 1)/3$.*

The last part of the theorem follows immediately from Theorem 10.1, so that it is sufficient, in view of Theorem 9.6, to prove that $\epsilon(M) = 3\epsilon(R)$. But this equality follows from (9.31), (9.32), since $(\mu, \epsilon(R)) = 1$.

THEOREM 10.21. *If R is not a cubic residue of p , τ is of the form $3\epsilon(R)\sigma$, where $\sigma | (p^2 + p + 1)/3$.*

If R is not a cubic residue of p , $\epsilon(R) \equiv 0 \pmod{3}$, and the theorem follows from Theorems 10.1 and 10.2.

If $\epsilon(R) \not\equiv 0 \pmod{3}$, then $(\mu, 3) = 1$, but I have not found a criterion to distinguish whether $\tau = 3\epsilon(R)\mu$ or $\tau = \epsilon(R)\mu$. The discovery of such a criterion would fill a serious lacuna in the theory. To illustrate the two cases possible, take $p = 7$. Then $p^2 + p + 1 = 57 = 3 \cdot 19$, so that $\mu = 19$. For the irreducible polynomial modulo 7, $F(x) = x^3 + x - 1$, $\epsilon(R) = 1$ and we find by direct computation that the period τ is $57 = 3\epsilon(R)\mu$. However, for $x^3 - 3x^2 + 4x - 1$, the period is only $19 = \epsilon(R)\mu$.

Finally, the case $p = 3$ may be easily treated by a direct enumeration of the possible cases.*

* Draeger's Thesis contains such an enumeration for certain forms of $F(x)$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

THE ALGEBRA OF RECURRING SERIES.*

BY MORGAN WARD.

1. **Introduction.** It is well known that if the function

$$(1.1) \quad F(x) \equiv x^3 - Px^2 + Qx - R, \quad R \neq 0$$

is irreducible in the field \mathfrak{F} of its coefficients, then the properties of those solutions of the linear difference equation

$$(1.2) \quad \Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n$$

which lie in \mathfrak{F} are ultimately based on the algebra of the field $\mathfrak{F}(\alpha)$ obtained by adjoining to \mathfrak{F} a root α of $F(x) = 0$.¹

The object of this paper is to develop a general method for obtaining formal properties of the solutions of (1.2) from simple algebraic identities in $\mathfrak{F}(\alpha)$. The process is as follows:

We set up a one-to-one correspondence between the field $\mathfrak{F}(\alpha)$ and a certain class of square matrices of order three with elements lying in \mathfrak{F} . We then group these matrices into sets which are particular solutions of a matrix difference equation of order one. Finally, we associate with each set a number of particular solutions of the scalar difference equation (1.2). Our method then consists of translating identities in $\mathfrak{F}(\alpha)$ into identities between matrices, and these in turn into relations between solutions of (1.2).² The treatment is simple and direct, and leads to a number of interesting formulas.³

The method may easily be extended to a difference equation of any order whose characteristic function is irreducible. We confine ourselves to the case of a third order equation, both for its interest in view of Lucas' claim to have discovered a remarkable connection between (1.2) and the theory of the elliptic functions,⁴ and for simplicity of notation.

* Received January 7, 1930.

¹ See for example, Bell, Tohoku Mathematical Journal, vol. 24, Numbers 1, 2 (1924), page 168. This paper gives a concise exposition of the algebraic theory of (1.2). We shall refer to it as "Bell", giving page reference. For the elementary theory of the linear difference equation of order r , see Bachmann, Niedere Zahlentheorie. The equation of order three is treated with considerable detail by Draeger, Thesis, Jena 1919. For other references, see Dickson's History, vol. I.

² See Section 5.

³ In this connection, see Bell, p. 168.

2. Basic definitions. The most general solution of the difference equation (1.2) lying in the field \mathfrak{F} of its coefficients is given by

$$(2.1) \quad \Omega_n = (K_0 + K_1 \alpha + K_2 \alpha^2) \alpha^n + (K_0 + K_1 \beta + K_2 \beta^2) \beta^n + (K_0 + K_1 \gamma + K_2 \gamma^2) \gamma^n, \quad (n = 0, \pm 1, \dots).$$

Here α, β, γ are the roots of the irreducible equation $F(x) = 0$, and K_0, K_1, K_2 are arbitrary elements of \mathfrak{F} .

If

$$\Omega_n = A_n, \quad (n = 0, \pm 1, \dots)$$

is any particular solution of (1.2) obtained by giving the constants K_0, K_1, K_2 in (2.1) definite values, A_0, A_1, A_2 are called the *initial values* of the sequence $(A)_n$. We write

$$(A)_n \sim [A_0, A_1, A_2].$$

Any sequence $(A)_n$ is completely determined as soon as we have specified its initial values.

There are four particular solutions of (1.2) of sufficient importance to have a special notation; we shall invariably write $(X)_n, (Y)_n, (Z)_n, (S)_n$ for the sequences defined by⁴

$$(2.2) \quad \begin{aligned} (X)_n &\sim [1, 0, 0]; & (Y)_n &\sim [0, 1, 0]; \\ (Z)_n &\sim [0, 0, 1]; & (S)_n &\sim [3, P, P^2 - 2Q]. \end{aligned}$$

Finally, we have the well known formulas

$$(2.3) \quad \begin{aligned} P &= \alpha + \beta + \gamma, & Q &= \alpha\beta + \beta\gamma + \gamma\alpha, & R &= \alpha\beta\gamma; \\ S_n &= \alpha^n + \beta^n + \gamma^n, & R^n S_{-n} &= \alpha^n \beta^n + \beta^n \gamma^n + \gamma^n \alpha^n. \end{aligned}$$

3. Introduction of matrices. Let M_n denote the square matrix of order three

$$(3.1) \quad M_n = \begin{pmatrix} X_n, & Y_n, & Z_n \\ X_{n+1}, & Y_{n+1}, & Z_{n+1} \\ X_{n+2}, & Y_{n+2}, & Z_{n+2} \end{pmatrix}, \quad (n = 0, \pm 1, \dots).$$

⁴ For properties of the first three, see Bell's paper. The solution

$$(Z)_n : 0, 0, 1, P, P^2 - Q, P^3 - 2PQ + R, \dots$$

is important in Combinatory Analysis; in fact, $Z_{n+2}, n > 0$ is the homogeneous product sum of α, β, γ of degree n . See MacMahon, Combinatory Analysis, Cambridge, (1915), vol. I, p. 3. S_n is the familiar sum of the n th powers of the roots of $F(x) = 0$.

Then by direct calculation from (2.2) and (1.2), we find that

$$(3.2) \quad \mathbf{M}_0 = \begin{pmatrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{pmatrix}, \quad \mathbf{M}_1 = \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ R, & -Q, & P \end{pmatrix}, \quad \mathbf{M}_2 = \begin{pmatrix} 0, & 0, & 1 \\ R, & -Q, & P \\ PR, & R-PQ, & P^2-Q \end{pmatrix}.$$

Thus $\mathbf{M}_0 = \mathbf{I}$, the identity matrix. We shall often write \mathbf{M} for \mathbf{M}_1 , omitting the subscript one.

The following properties of the matrices (3.1) are easily proved by induction:

$$(3.3) \quad \begin{aligned} \mathbf{M}_{n+1} &= \mathbf{M} \cdot \mathbf{M}_n = \mathbf{M}^{n+1}, \\ \mathbf{M}_n \cdot \mathbf{M}_m &= \mathbf{M}_m \cdot \mathbf{M}_n = \mathbf{M}_{m+n}, \\ \mathbf{M}_{n+3} &= P\mathbf{M}_{n+2} - Q\mathbf{M}_{n+1} + R\mathbf{M}_n, \quad (m, n = 0, \pm 1, \dots). \\ \mathbf{M}_n &= X_n \mathbf{M}_0 + Y_n \mathbf{M}_1 + Z_n \mathbf{M}_2. \end{aligned}$$

The first of these formulas shows that \mathbf{M}_n is a particular solution of the matric difference equation of order one

$$(3.4) \quad \Omega_{n+1} = \mathbf{M} \cdot \Omega_n$$

and the third formula shows that \mathbf{M}_n is a particular solution of (1.2). We shall hereafter refer to the matrices (3.1) as the *sequence* $(\mathbf{M})_n$.

Combining the second and fourth of the formulas (3.3) gives the more general formula

$$\mathbf{M}_{n+m} = X_n \mathbf{M}_m + Y_n \mathbf{M}_{m+1} + Z_n \mathbf{M}_{m+2}, \quad (m, n = 0, \pm 1, \dots).$$

By transforming \mathbf{M} to the diagonal form and applying (3.3), (2.3), we can prove⁵

THEOREM 3.1. *The characteristic function of the matrix \mathbf{M}_n is $\lambda^3 - S_n \lambda^2 + R^n S_{-n} \lambda - R^n$.*

The most general solution of (3.4) is

$$\Omega_n = \mathbf{M}_n \cdot \Omega_0, \quad (n = 0, \pm 1, \dots)$$

where the elements of the matrix Ω_0 are arbitrary. Let

$$\Omega_n = \mathbf{P}_n$$

⁵ We may note in passing a useful formula immediately obtainable from Theorem 3.1 and (3.1); namely,

$$S_n = X_n + Y_{n+1} + Z_{n+2}, \quad (n = 0, \pm 1, \dots).$$

be a particular solution obtained by letting

$$(3.41) \quad \Omega_0 = P_0 = \begin{pmatrix} U_0, & V_0, & W_0 \\ U_1, & V_1, & W_1 \\ U_2, & V_2, & W_2 \end{pmatrix},$$

where U_0, \dots, W_2 are fixed elements of \mathfrak{F} . Then from (3.3),

$$(3.5) \quad \begin{aligned} P_{m+n} &= M_n \cdot P_m, \\ P_{n+3} &= P P_{n+2} - Q P_{n+1} + R P_n, \end{aligned} \quad (m, n = 0, \pm 1, \dots).$$

From (3.5), we obtain the following theorem:

THEOREM 3.2. *If the sequence of matrices (P_n) is a particular solution of the matric difference equation (3.4), where the value of P_0 is given by (3.41), then*

$$P_n = \begin{pmatrix} U_n, & V_n, & W_n \\ U_{n+1}, & V_{n+1}, & W_{n+1} \\ U_{n+2}, & V_{n+2}, & W_{n+2} \end{pmatrix}, \quad (n = 0, \pm 1, \dots),$$

where $(U)_n \sim [U_0, U_1, U_2]$, $(V)_n \sim [V_0, V_1, V_2]$, $(W)_n \sim [W_0, W_1, W_2]$ are particular solutions of the scalar difference equation (1.2).

It is easily shown that the converse of this theorem is also true.

4. Associated fields. We shall now establish an isomorphism between $\mathfrak{F}(\alpha)$ and a certain class of matrices with elements in \mathfrak{F} .

THEOREM 4.1. *The class \mathfrak{M} of all matrices of the form*

$$P = UI + VM + WM^2$$

where U, V, W are any elements of \mathfrak{F} forms a field which is simply isomorphic with the field $\mathfrak{F}(\alpha)$ obtained by adjoining a root α of $F(x) = 0$ to \mathfrak{F} .

Proof. It is clear from formulas (3.2), (3.3), that any matrix P of \mathfrak{M} can vanish when and only when U, V and W vanish.

\mathfrak{M} is obviously closed under addition and subtraction; by (3.3), $M^3 = PM^2 - QM + RI$; consequently, \mathfrak{M} is also closed under multiplication. Furthermore, multiplication is commutative, and distributive with respect to addition.

Any element π of the field $\mathfrak{F}(\alpha)$ may be put in the unique canonical form

$$\pi = U + V\alpha + W\alpha^2$$

where U, V, W are elements of \mathfrak{F} . Set \mathfrak{M} and $\mathfrak{F}(\alpha)$ into one-to-one correspondence by pairing the elements π and P for which U, V, W have the same values; we write in this case $\pi \sim P$.

Then if $\pi_1 \sim \mathbf{P}_1$, $\pi_2 \sim \mathbf{P}_2$, $\pi_3 \sim \mathbf{P}_3$, it is easily verified that

$$\pi_1 \pm \pi_2 \sim \mathbf{P}_1 \pm \mathbf{P}_2; \quad \pi_1 \cdot \pi_2 \sim \mathbf{P}_1 \cdot \mathbf{P}_2; \quad \pi_1(\pi_2 \pm \pi_3) \sim \mathbf{P}_1(\mathbf{P}_2 \pm \mathbf{P}_3).$$

Furthermore, if $\pi \pi' = 1$, $\pi \sim \mathbf{P}$, $\pi' \sim \mathbf{P}'$, then $\mathbf{P} \cdot \mathbf{P}' = I$.

Hence \mathfrak{M} forms a field simply isomorphic with $\mathfrak{F}(\alpha)$.

As a corollary to this theorem, we have

THEOREM 4.11. *The characteristic equation of any matrix \mathbf{P} of \mathfrak{M} is the same as the equation which the corresponding element π of $\mathfrak{F}(\alpha)$ satisfies in \mathfrak{F} .*

We shall use the notations $\text{Det } \mathbf{P}$ and $\text{Adj } \mathbf{P}$ for the determinant and adjoint of any matrix \mathbf{P} , and $N(\pi)$ for the norm of any number π of $\mathfrak{F}(\alpha)$. It is easily seen from Theorem 4.11 that

$$(4.12) \quad \text{If } \mathbf{P} \sim \pi, \quad \text{then } \text{Det } \mathbf{P} = N(\pi);$$

$$(4.13) \quad \text{If } \mathbf{P} \sim \pi \neq 0, \quad \text{then } \text{Adj } \mathbf{P} \sim N(\pi)/\pi.$$

THEOREM 4.2. *The necessary and sufficient condition that any matrix of order three with elements in \mathfrak{F} be commutative with \mathbf{M} is that it lies in the field \mathfrak{M} .*

Proof. The sufficiency of the condition follows from Theorem 4.1. To establish the necessity, suppose that \mathbf{L} is a matrix of order three over \mathfrak{F} commutative with \mathbf{M} . Then

$$(4.2) \quad \mathbf{L} \cdot \mathbf{M} = \mathbf{M} \cdot \mathbf{L}; \quad \mathbf{L} \cdot \mathbf{M}^2 = \mathbf{M}^2 \cdot \mathbf{L}.$$

There exists a non-singular matrix \mathbf{T} transforming \mathbf{M} into the diagonal form \mathbf{M}^* . By (4.2), $\mathbf{T}^{-1} \cdot \mathbf{L} \cdot \mathbf{T} = \mathbf{L}^*$ must also be in the diagonal form. Let $\alpha, \beta, \gamma; \alpha', \beta', \gamma'$ be the diagonal elements in $\mathbf{M}^*; \mathbf{L}^*$, and consider the traces of $\mathbf{L}^*, \mathbf{M}^* \cdot \mathbf{L}^*, (\mathbf{M}^*)^2 \cdot \mathbf{L}^*$. They are the same as the traces of $\mathbf{L}, \mathbf{M} \cdot \mathbf{L}, \mathbf{M}^2 \cdot \mathbf{L}$. Hence

$$\alpha' + \beta' + \gamma' = I, \quad \alpha\alpha' + \beta\beta' + \gamma\gamma' = J, \quad \alpha^2\alpha' + \beta^2\beta' + \gamma^2\gamma' = K,$$

where I, J, K are elements of \mathfrak{F} . Solving these equations for α', β', γ' we find that

$$\alpha' = U + V\alpha + W\alpha^2, \quad \beta' = U + V\beta + W\beta^2, \quad \gamma' = U + V\gamma + W\gamma^2$$

where U, V, W are elements of \mathfrak{F} . Thus

$$\begin{aligned} \mathbf{L}^* &= UI + VM^* + WM^{*2}, \\ \mathbf{L} &= \mathbf{T} \cdot \mathbf{L}^* \cdot \mathbf{T}^{-1} = UI + VM + WM^2. \end{aligned}$$

THEOREM 4.3. *Let $(P)_n$ denote the sequence of matrices defined in Theorem 3.2. Then a necessary and sufficient condition that $(P)_n$ should lie in \mathfrak{M} is that the sequences $(U)_n$, $(V)_n$, $(W)_n$ be connected by the relations*

$$(4.3) \quad \begin{aligned} V_n &= W_{n+1} - P W_n, \\ U_n &= W_{n+2} - P W_{n+1} + Q W_n = R W_{n-1}, \end{aligned} \quad (n = 0, \pm 1, \dots).$$

Proof. We easily find that

$$P_n \cdot M = M \cdot P_n$$

when and only when the relations (4.3) hold. The result now follows from Theorem 4.2.

Let $(P)_n$ now denote a sequence of matrices whose elements satisfy the relations⁶ (4.3). Then

$$P_n = I M_0 + J M_1 + K M_2$$

where I, J, K lie in \mathfrak{F} . By comparing the elements in the first row of both sides of this identity, we find from (3.2) that

$$I = U_n, \quad J = V_n, \quad K = W_n$$

so that

$$P_n = U_n M_0 + V_n M_1 + W_n M_2, \quad (n = 0, \pm 1, \dots).$$

5. Derivation of formulas. We are now in a position to illustrate the method of translating identities in $\mathfrak{F}(\alpha)$ into relations between solutions of (1.2). With the notation of Theorem 4.1, we write $\pi \sim P_0$ for

$$\pi = U_0 + V_0 \alpha + W_0 \alpha^2, \quad P_0 = U_0 M_0 + V_0 M_1 + W_0 M_2.$$

In particular, $\alpha \sim M_1$, and by Theorem 4.1, (3.11), Theorem 3.3,

$$(5.1) \quad \alpha^n \sim M_n, \quad \alpha^n \cdot \pi \sim P_n$$

where the elements of P_n satisfy the conditions (4.3).

Let us start with the following trivial identities in $\mathfrak{F}(\alpha)$.

- I. $\alpha^{n+m} \cdot \pi = \pi \cdot \alpha^{n+m} = (\alpha^n \cdot \pi) \alpha^m = \alpha^m (\alpha^n \cdot \pi),$
- II. $(\pi \cdot \alpha^{n+m}) \pi = \pi (\alpha^{n+m} \cdot \pi) = (\alpha^m \cdot \pi) \cdot (\alpha^n \cdot \pi).$

⁶ It is perhaps worth noting that on account of the linearity of (1.2), (4.3) will hold for all values of n if it holds for $n = 0, 1, 2$; i. e. $(P)_n$ lies in \mathfrak{M} if P_0 lies in \mathfrak{M} .

The corresponding matrix identities in \mathfrak{M} are

$$\begin{aligned} \text{I}' . \quad & \mathbf{P}_{n+m} = \mathbf{P}_0 \cdot \mathbf{M}_{n+m} = \mathbf{P}_n \cdot \mathbf{M}_m = \mathbf{M}_m \cdot \mathbf{P}_n, \\ \text{II}' . \quad & \mathbf{P}_{n+m} \cdot \mathbf{P}_0 = \mathbf{P}_0 \cdot \mathbf{P}_{m+n} = \mathbf{P}_m \cdot \mathbf{P}_n. \end{aligned}$$

By equating corresponding elements on both sides of I' and II', we obtain a number of formulas involving $(U)_n, (V)_n, (W)_n, (X)_n, (Y)_n, (Z)_n$; for instance, from I' we obtain

$$\begin{aligned} (5.2) \quad U_{n+m} &= U_0 X_{n+m} + V_0 X_{n+m+1} + W_0 X_{n+m+2} \\ &= U_n X_m + V_n X_{m+1} + W_n X_{m+2} \\ &= X_m U_n + Y_m U_{n+1} + Z_m U_{n+2}. \end{aligned}$$

From II', we obtain

$$\begin{aligned} U_{n+m} U_0 + V_{n+m} U_1 + W_{n+m} U_2 &= U_0 U_{m+n} + V_0 U_{m+n+1} + W_0 U_{m+n+2} \\ &= U_m U_n + V_m U_{n+1} + W_m U_{n+2}. \end{aligned}$$

If we introduce the number

$$\pi' = N(\pi)/\pi = U'_0 + V'_0 \alpha + W'_0 \alpha^2,$$

we obtain another class of formulas. For by (4.13),

$$\text{Adj } \mathbf{P} = \mathbf{P}'_0 = U'_0 \mathbf{M}_0 + V'_0 \mathbf{M}_1 + W'_0 \mathbf{M}_2,$$

and if we let $\mathbf{P}'_n = \mathbf{M}_n \cdot \mathbf{P}'_0$, we find that

$$\text{Adj } \mathbf{P}_n = R^n \mathbf{P}'_n.$$

Hence,

$$V_{n+1} W_{n+2} - W_{n+1} V_{n+2} = R^n U'_{-n}, \quad W_{n+2} U_{n+1} - U_{n+2} W_{n+1} = R^n V'_n,$$

and so on.

The identity

$$\begin{aligned} \text{III. } (\alpha^m \cdot \pi') \cdot (\alpha^n \cdot \pi) &= (\alpha^m \cdot \pi) \cdot (\alpha^n \cdot \pi') = \pi \cdot (\alpha^{m+n} \cdot \pi') \\ &= \pi' \cdot (\alpha^{n+m} \cdot \pi) = N(\pi) \alpha^{n+m} \end{aligned}$$

gives us

$$\text{III}'. \quad \mathbf{P}'_m \cdot \mathbf{P}_n = \mathbf{P}_m \cdot \mathbf{P}'_n = \mathbf{P}_0 \cdot \mathbf{P}'_{m+n} = \mathbf{P}_{m+n} \cdot \mathbf{P}'_0 = N(\pi) \mathbf{M}_{n+m}.$$

From III', we obtain formulas of the type

$$\begin{aligned} U'_m U_n + V'_m U_{n+1} + W'_m U_{n+2} &= U_m U'_n + V_m U'_{n+1} + W_m U'_{n+2} \\ = U_0 U'_{m+n} + V_0 U'_{m+n+1} + W_0 U'_{m+n+2} &= U_{m+n} U'_0 + V_{m+n} U'_1 + W_{m+n} U'_2 \\ &= N(\pi) X_{n+m}, \quad (m, n = 0, \pm 1, \dots). \end{aligned}$$

6. **Extension of method.** We shall conclude by extending the method so as to apply to an important class of matrices not lying in \mathfrak{M} .

Let $(\mathbf{S})_n$ denote the sequence of matrices

$$\mathbf{S}_n = \begin{pmatrix} S_n, & S_{n+1}, & S_{n+2} \\ S_{n+1}, & S_{n+2}, & S_{n+3} \\ S_{n+2}, & S_{n+3}, & S_{n+4} \end{pmatrix}, \quad (n = 0, \pm 1, \dots)$$

where S_n is given by (2.3).

By the converse to Theorem 3.2, $\mathbf{S}_m = \mathbf{M}_m \cdot \mathbf{S}_0$, so that

$$(6.1) \quad \mathbf{M}_n \cdot \mathbf{S}_m = \mathbf{S}_{m+n}.$$

However, $\mathbf{M} \cdot \mathbf{S}_0 \neq \mathbf{S}_0 \cdot \mathbf{M}$, so that $(\mathbf{S})_n$ does not lie in \mathfrak{M} .

Define a new matrix \mathbf{T}_n by

$$(6.2) \quad \mathbf{T}_n = \mathbf{P}_0 \cdot \mathbf{S}_n.$$

If we write T_n for

$$U_0 S_n + V_0 S_{n+1} + W_0 S_{n+2}, \quad (n = 0, \pm 1, \dots)$$

we find from (6.2) that

$$\mathbf{T}_n = \begin{pmatrix} T_n, & T_{n+1}, & T_{n+2} \\ T_{n+1}, & T_{n+2}, & T_{n+3} \\ T_{n+2}, & T_{n+3}, & T_{n+4} \end{pmatrix}, \quad (n = 0, \pm 1, \dots).$$

From (6.2) and (6.1)

$$\mathbf{T}_{m+n} = \mathbf{P}_0 \cdot \mathbf{S}_{m+n} = \mathbf{P}_0 \cdot \mathbf{M}_n \cdot \mathbf{S}_m = \mathbf{P}_n \cdot \mathbf{S}_m,$$

giving the useful formula

$$(6.3) \quad T_{m+n} = U_n S_m + V_n S_{m+1} + W_n S_{m+2}.$$

Formula (6.3) applies to any sequence satisfying (1.2). For if

$$(T)_n \sim [T_0, T_1, T_2],$$

the three equations

$$T_i = U_0 S_i + V_0 S_{i+1} + W_0 S_{i+2}, \quad (i = 0, 1, 2)$$

will determine U_0, V_0, W_0 . The six remaining elements of $\mathbf{P}_0, U_1, \dots, W_2$ are then completely determined by the relations (4.3), and the demonstration given applies.

There is an interesting consequence of formula (6.3). We may use (4.3) to express (6.3) in the form

$$(6.31) \quad T_{m+n} = (W_{n+2} - PW_{n+1} + QW_n)S_m + (W_{n+1} - PW_n)S_{m+1} + W_n S_{m+2}.$$

On interchanging m and n in (6.31) and rearranging the terms, we obtain

$$(6.32) \quad T_{m+n} = (S_{n+2} - PS_{n+1} + QS_n)W_m + (S_{n+1} - PS_n)W_{m+1} + S_nW_{m+2}.$$

Since (6.32) may be derived from (6.31) by simply interchanging the S and the W , we have a parallelism between the expression for T_{m+n} in terms of S_m, S_{m+1}, S_{m+2} and in terms of W_m, W_{m+1}, W_{m+2} . There is a similar parallelism between the expression for T_{m+n} in terms of T_m, T_{m+1}, T_{m+2} and in terms of Z_m, Z_{m+1}, Z_{m+2} . For from (5.2), taking $(U)_n = (T)_n$,

$$T_{m+n} = X_n T_m + Y_n T_{m+1} + Z_n T_{m+2}.$$

On replacing X_n and Y_n by their expressions in terms of Z_n from (4.3),⁷ we obtain two formulas analogous to (6.31) and (6.32); namely,⁸

$$\begin{aligned} T_{m+n} &= (Z_{n+2} - PZ_{n+1} + QZ_n)T_m + (Z_{n+1} - PT_n)T_{m+1} + Z_nT_{m+2}, \\ T_{m+n} &= (T_{n+2} - PT_{n+1} + QT_n)Z_m + (T_{n+1} - PT_n)Z_{m+1} + T_nZ_{m+2}. \end{aligned}$$

⁷ Bell, p. 173 formula (12). The matrix M_n is of course a special form of P_n .

⁸ If we take $(T)_n = (Z)_n$, $n = n+1$, $m = m-1$, the last two formulas become equation (34) in section 7 of Bell, p. 179.

SOME ARITHMETICAL PROPERTIES OF SEQUENCES SATISFYING A LINEAR RECURSION RELATION.¹

BY MORGAN WARD.

1. Let

$$(U)_n: \quad U_0, U_1, U_2, \dots$$

denote a sequence of integers satisfying the recursion relation

$$(1.1) \quad \Omega_{N+1+n} = P_1 \Omega_{N+n} + P_2 \Omega_{N+n-1} + \dots + P_{N+1} \Omega_n$$

where P_1, \dots, P_{N+1} and the $N+1$ initial values U_0, \dots, U_N of $(U)_n$ are all fixed integers.

Let p denote a fixed prime, and assume furthermore that the characteristic function of (1.1)

$$F(x) = x^{N+1} - P_1 x^N - \dots - P_{N+1}$$

is irreducible modulo p .

Denote the $N+1$ roots of the equation $F(x) = 0$ by $\alpha = \alpha_0, \alpha_1, \dots, \alpha_N$ and let S_m denote $\alpha_0^m + \alpha_1^m + \dots + \alpha_N^m$. For convenience of printing, we shall occasionally write $\alpha(n)$ for α^n and $\{m\}$ for S_m .

In this paper, I give a number of congruences to the modulus p satisfied by particular solutions of (1.1) and by determinants relating to such solutions. The two main results are as follows:

If $(U)_n$ is any particular solution of (1.1), then²

$$(I) \quad U_{n+m} + U_{n+pm} + U_{n+p^2m} + \dots + U_{n+p^sm} \equiv U_n S_m \pmod{p}.$$

If $N+1$ is odd, and if $M(r_0, r_1, \dots, r_N)$ denotes the determinant

$$|\alpha_i^j|, \quad (i, j = 0, 1, \dots, N)$$

where r_0, r_1, \dots, r_N are any fixed integers, then

$$(II) \quad M(r_0, r_1, \dots, r_N) \equiv \sum_{(j)} (\pm)^j \{r_0 + p r_{j_1} + p^2 r_{j_2} + \dots + p^N r_{j_N}\} \pmod{p},$$

¹ Received October 1, 1930, and February 3, 1931.

² If μ is the exponent to which α belongs, modulo p , the relations $U_a \equiv U_b, S_a \equiv S_b \pmod{p}$ if $a \equiv b \pmod{\mu}$ may be used to reduce the subscripts of U and S to values less than μ .

where the summation is extended over all the $N!$ permutations (j) of the integers $1, 2, \dots, N$ and the sign $(\pm)^j$ is to be taken positive or negative according as the permutation is of even or odd parity.

For example, if $N+1 = 3$, we have

$$\begin{vmatrix} \alpha_0^{r_0}, & \alpha_0^{r_1}, & \alpha_0^{r_2} \\ \alpha_1^{r_0}, & \alpha_1^{r_1}, & \alpha_1^{r_2} \\ \alpha_2^{r_0}, & \alpha_2^{r_1}, & \alpha_2^{r_2} \end{vmatrix} \equiv S_{r_0+pr_1+p^2r_2} - S_{r_0+pr_2+p^2r_1} \pmod{p}.$$

The proofs of these formulas are given in the next two sections of the paper. The final section contains some special cases of the first formula and some properties of the determinant $M(r_0, r_1, \dots, r_N)$ regarded as a function of r_0, r_1, \dots, r_N .

2. With a proper choice of notation, we may assume that

$$(2.1) \quad \alpha_i \equiv \alpha^{p^i} \pmod{p}, \quad (i = 0, 1, \dots, N)$$

in the Galois Field³ of order p^{N+1} associated with the root α of $F(x) = 0$.

Since $F(x)$ is irreducible, the general term of $(U)_n$ may be represented as

$$U_n = A_0 \alpha_0^n + A_1 \alpha_1^n + \dots + A_N \alpha_N^n$$

where the constants A are independent of n . We shall take this formula as a definition of U_n when n is a negative integer. Thus

$$(2.2) \quad U_n \equiv \sum_{r=0}^N A_r \alpha^{p^r n} \pmod{p}, \quad S_m \equiv \sum_{s=0}^N \alpha^{p^s m} \pmod{p}.$$

To prove formula I, we observe that

$$\sum_{s=0}^N \alpha^{p^{r+s} m} \equiv S_m \pmod{p}$$

for any integer r . Hence

$$\sum_{s=0}^N U_{n+p^s m} \equiv \sum_{s=0}^N \sum_{r=0}^N A_r \alpha^{p^r(n+p^s m)} \equiv \sum_{r=0}^N A_r \alpha^{p^r n} \sum_{s=0}^N \alpha^{p^{r+s} m} \equiv U_n S_m \pmod{p}.$$

3. Formula II may be proved as follows. With the notation explained in the introduction,

$$M(r_0, r_1, \dots, r_N) = \sum_{(j)} (\pm)^j \alpha_0^{r_{j_0}} \alpha_1^{r_{j_1}} \dots \alpha_N^{r_{j_N}}.$$

Hence by (2.1),

$$(3.1) \quad M(r_0, r_1, \dots, r_N) \equiv \sum_{(j)} (\pm)^j \alpha(r_{j_0} + r_{j_1} p + \dots + r_{j_N} p^N) \pmod{p}.$$

³ For the properties of Galois Fields which are assumed, see Dickson, *Linear Groups*, Teubner, (1901).

The $(N+1)!$ permutations (j) of the integers $0, 1, \dots, N$ which occur in the subscripts of the r on the right hand side of (3.1) may be grouped into $N!$ classes

$$(3.2) \quad J_1, J_2, \dots, J_{N!}$$

where each class contains exactly $N+1$ cyclic permutations. Suppose that

$$(3.3) \quad j_0, j_1, \dots, j_{N-1}, j_N; \quad j_1, j_2, \dots, j_N, j_0; \quad \dots; \quad j_N, j_0, \dots, j_{N-2}, j_{N-1};$$

are the permutations of the class J . These permutations are either all even or all odd; for since $N+1$ is odd, each can be derived from its predecessor by an even number of transpositions.⁴ Accordingly, the sign of the general term $\alpha(r_{j_0} + r_{j_1} p + \dots + r_{j_N} p^N)$ in (3.1) is the same for all the permutations of a given class J .

Furthermore, since any one of the permutations (3.3) completely specifies the class J , we may choose our notation so that $j_0 = 0$. Make a similar change of notation for every other one of the classes (3.2). Then to each of the $N!$ permutations of the integers $1, 2, \dots, N$ there corresponds a unique class J , and the parity of this permutation determines the parity of all the permutations of J .

The congruence (3.1) can now be written as

$$(3.4) \quad M(r_0, r_1, \dots, r_N) \equiv \sum_{(j)} (\pm)^j \sum \alpha(r_0 + r_{j_1} p + \dots + r_{j_N} p^N) \pmod{p}$$

where the inner summation is taken over the $N+1$ permutations (3.3), while the outer summation (j) is taken over the $N!$ permutations of $1, 2, \dots, N$, the sign being plus or minus according as (j) is even or odd.

But since $\alpha(rp^{N+1}) \equiv \alpha(r) \pmod{p}$, the inner summation in (3.4) is congruent modulo p to

$$\begin{aligned} & \alpha(r_0 + r_{j_1} p + \dots + r_{j_N} p^N) + \alpha(p \cdot (r_0 + r_{j_1} p + \dots + r_{j_N} p^N)) + \dots \\ & \quad \dots + \alpha(p^N \cdot (r_0 + r_{j_1} p + \dots + r_{j_N} p^N)) \\ & \equiv \{r_0 + r_{j_1} p + \dots + r_{j_N} p^N\} \pmod{p}, \end{aligned}$$

by formula (2.2). On substituting this last expression in (3.4), we obtain formula II.

4. The following special cases of formula I are of interest. First, if we write S for U in I, we obtain a multiplication formula for the function S :

⁴ It is at precisely this point that an attempted proof of a similar result for the case when the degree of $F(x)$ is even will break down.

$$(4.1) \quad S_n S_m \equiv S_{n+m} + S_{n+pm} + \cdots + S_{n+p^m m} \pmod{p}.$$

Secondly, let $(Z^0)_n; (Z^{(1)})_n, \dots, (Z^{(N)})_n$ denote the particular solutions of (1.1) with the initial values

$$1, 0, 0, \dots, 0; \quad 0, 1, 0, \dots, 0; \quad \dots; \quad 0, 0, 0, \dots, 1.$$

Then if the Kronecker symbol δ_{ij} is defined as usual by

$$\delta_{ij} = 0, \quad i \neq j; \quad \delta_{ij} = 1, \quad i = j; \quad (i, j = 0, 1, \dots, N),$$

we have on taking $Z^{(i)}$ for U in I the curious formulas

$$Z_{j+m}^{(i)} + Z_{j+pm}^{(i)} + \cdots + Z_{j+p^m m}^{(i)} \equiv \delta_{ij} S_m \pmod{p}, \\ (i, j = 0, 1, \dots, N; m = 0, \pm 1, \dots).$$

The function M has a multiplication theorem analogous to that given for S_m in formula (4.1). If for brevity we write $R_{(k)}$ for $r_{k_0} + r_{k_1} p + \cdots + r_{k_N} p^N$, then

$$(4.2) \quad M(r_0, r_1, \dots, r_N) \cdot M(u_0, u_1, \dots, u_N) \\ \equiv \sum_{(k)} (\pm)^k M(R_{(k)} + u_0, u_1, \dots, u_N) \pmod{p},$$

where the summation (k) extends over all the $(N+1)!$ permutations of the integers $0, 1, \dots, N$ and the signs are determined as in II by the parity of (k) .

To prove (4.2), write $R_{(j)}$ for $r_0 + r_{j_1} p + \cdots + r_{j_N} p^N$. Then by formula II and formula (4.1)

$$(4.3) \quad M(r_0, r_1, \dots, r_N) \cdot M(u_0, u_1, \dots, u_N) \\ \equiv \sum_{(j)} \sum_{(k)} (\pm)^j (\pm)^k \{R_{(j)}\} \{u_0 + u_{l_1} p + \cdots + u_{l_N} p^N\} \\ \equiv \sum_{(j)} (\pm)^j \sum_{t=0}^N \sum_{(l)} (\pm)^k \{R_{(j)} + p^t u_0 + p^t u_{l_1} p + \cdots + p^t u_{l_N} p^N\} \\ \equiv \sum_{(j)} (\pm)^j \sum_{t=0}^N M(R_{(j)} + p^t u_0, p^t u_1, \dots, p^t u_N) \pmod{p}.$$

We now reverse the argument in section 3 by which we passed from the $(N+1)!$ permutations of $0, 1, 2, \dots, N$ to the $N!$ permutations of $1, 2, \dots, N$. Let $k_0 = j_t, k_1 = j_{t+1}, \dots, k_N = j_{t-1}$ so that $(k): k_0, k_1, \dots, k_N$ is a cyclic permutation of the subscripts $0, j_1, \dots, j_N$ of the r in $R_{(j)}$. Then (k) is a permutation of $0, 1, \dots, N$ which has the same parity as the permutation (j) of $1, 2, \dots, N$.

If we now write $R_{(k)}$ for $r_{k_0} + r_{k_1}p + \dots + r_{k_N}p^N$, then

$$\begin{aligned} (\pm)^j M(R_{(k)} + p^t u_0, p^t u_1, \dots, p^t u_N) \\ \equiv (\pm)^k M(p^t R_{(k)} + p^t u_0, p^t u_1, \dots, p^t u_N) \\ \equiv (\pm)^k M(R_{(k)} + u_0, u_1, \dots, u_N) \pmod{p}. \end{aligned}$$

On substituting this expression into (4.3), we obtain (4.2).

In conclusion, we may note that $M(0, 1, \dots, N)$ is the square root of the discriminant of $F(x)$. Denoting this discriminant by Δ , we have from II after some obvious simplifications,

$$\sqrt{\Delta} \equiv \sum_{(j)} (\pm)^j \{j_1 + j_2 p + \dots + j_N p^{N-1}\} \pmod{p}.$$

For $N+1 = 3$, this result assumes the simple form

$$\sqrt{\Delta} \equiv S_{1+2p} - S_{2+p} \pmod{p}.$$

PASADENA,
September, 1930.

THE DISTRIBUTION OF RESIDUES IN A SEQUENCE SATISFYING A LINEAR RECURSION RELATION*

BY
MORGAN WARD

I. INTRODUCTION

1. Statement of problem. Let

$$(W)_n: \quad W_0, W_1, \dots, W_n, \dots$$

denote a sequence of integers satisfying the linear difference equation of order $r=3$,

$$(1.1) \quad \Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + R\Omega_n, \quad R \neq 0,$$

where P, Q, R, W_0, W_1, W_2 are fixed integers.[†]

If m is a positive integer, and if

$$W_n \equiv A_n \pmod{m}, \quad 0 \leq A_n \leq m-1,$$

we shall call

$$(A)_n: \quad A_0, A_1, \dots, A_n, \dots$$

the *reduced sequence corresponding to $(W)_n$, modulo m* .

It is easily shown the $(A)_n$ is periodic; following Carmichael,[‡] we shall call its smallest period, τ , the *characteristic number* of $(W)_n$ modulo m .

The object of this memoir is to attack the following fundamental distribution problem:[§]

Given the numerical values of the integers $P, Q, R, W_0, W_1, W_2, m$ and τ , to determine the distribution of the residues $0, 1, 2, \dots, m-1$ among any τ terms of the reduced sequence $(A)_n$.

There are really two distinct problems involved here: the determination of the particular place a given residue occurs in $(A)_n$ and the determination of the number of times a given residue occurs in any τ terms of $(A)_n$. Both

* Presented to the Society, November 29, 1929; received by the editors in January, 1930.

† For references to investigations of (1.1) see Dickson's *History*, vol. 1, chapter 17. For a general discussion of the problems in number theory connected with (1.1), see Carmichael, American Mathematical Monthly, vol. 36 (1929), pp. 132-143.

‡ Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 344-345.

§ As far as I am aware, this problem has not been explicitly considered for difference equations of order greater than two. In a paper which has already appeared in these Transactions I have considered the problem of determining τ , given P, Q, R, W_0, W_1, W_2 and m .

problems may be readily solved in particular cases. Consider for example the difference equation $\Omega_{n+3} = \Omega_{n+2} + \Omega_{n+1} - \Omega_n$ with $W_0 = 0$, $W_1 = 1$, $W_2 = 2$. But the general solution of either problem presents considerable difficulties.*

I shall confine myself here almost entirely to the second, simpler, distribution problem for the special case when m is a prime p and the characteristic function of (1.1),

$$(1.2) \quad F(x) = x^3 - Px^2 + Qx - R,$$

is irreducible modulo p . A discussion of this case is a necessary preliminary to the more complicated cases when m is composite or when the characteristic function (1.2) is reducible modulo p .

2. Plan of paper and principal results. Let $k(i) = k_i$ denote the number of times the least positive residue i ($\bmod p$) occurs in the first τ terms

$$(A): \quad A_0, A_1, \dots, A_{\tau-1}$$

of any reduced sequence $(A)_n$ ($\bmod p$).† Regarding k_i as a function of i , we shall speak of it as the *distribution function for the cycle* (A) of $F(x)$ associated with $(A)_n$ and $(W)_n$.

If we know the distribution function for the cycle (A) , then we will know it for the cycle (B) if the three initial values B_0, B_1, B_2 of (B) happen to be three consecutive elements of (A) . It is thus important to be able to tell from the initial values of two sequences whether or not their cycles are distinct. This problem is dealt with in §§6 and 7, where it is reduced to the problem of determining whether or not any given three consecutive residues appear in a *fixed* cycle (K) of $F(x)$. The preliminary definitions and results needed there and in the body of the paper are developed in §§3, 4, and 5. In §8 I digress slightly to give some results connected with the first distribution problem.

In §9 I prove that the number of zeros that can occur in each cycle of $F(x)$ are not independent of one another, but must satisfy two simple diophantine equations. In §10, I apply this result to determine completely the number of zeros which can occur in any cycle of $F(x)$ when $\tau = (p^2 + p + 1)/3$. In §11 I prove that if $\tau = p^2 + p + 1$, then every residue occurs in every cycle at least once.

In §12 it is proved that the distribution problem is essentially the same for all difference equations (1.1) with the same characteristic number τ

* In connection with the first problem, probably the best known result is that if $W_0 = 3$, $W_1 = P$, $W_2 = P^2 - 2Q$ and p is a prime, then $W_n \equiv W_{np} \equiv W_{np^2} \pmod p$. In §8 of this paper I shall give several new results of a similar character.

† We shall omit the words "modulo p " when no confusion can arise.

modulo p , and that it can be reduced to the case when τ divides p^2+p+1 and is prime to 3.

In §13, I show that the distribution function $k(n)$ for any cycle (A) is known as soon as we know the least positive residues of k_i modulis p and 3. In particular, k_0 is known as soon as its residue modulo p is known.

In §15, I give an explicit formula which determines k_i modulo p as the residue of a summation taken over the solutions of a certain diophantine system. This system is discussed fully in §14, and a general method of solving it is given. I have been unable to determine the residue of k_i modulo 3 save in special cases.

In §16, I apply my results to various special cases, obtaining theorems like the following:

If $p=3N+1$, $3\tau=p^2+p+1$, and k_0 is the number of terms divisible by p in the first τ terms of $(S)_n$, where $S_0=3$, $S_1=P$, $S_2=P^2-2Q$, then k_0 is the least positive residue modulo p of $(2N+1)(1+3N!/(N!)^3)$.

Finally in §17, I give a method for obtaining an upper limit to the size of k_i for any (A) and τ .

3. Preliminary definitions. Triads. Let the roots of $F(x)=0$ in the Galois field of order p^3 associated with $F(x)$ be denoted by* α , α^p , α^{p^2} , and suppose that

$$\alpha^n + \alpha^{pn} + \alpha^{p^2n} \equiv S_n \pmod{p} \quad \begin{cases} 0 \leq S_n \leq p-1, \\ n = 0, \pm 1, \pm 2, \dots \end{cases}.$$

Then

$$S_1 \equiv P, \quad RS_{-1} \equiv Q, \quad \alpha^{1+p+p^2} \equiv R \pmod{p}.$$

We shall refer to the p numbers

$$0, 1, 2, \dots, p-1$$

which form a sub-field in the Galois field as *residues*. The characteristic number τ is simply the exponent to which α belongs in the Galois field; we shall also refer to it as the *period* of $F(x)$ (modulo p).

The τ residues $A_0, A_1, \dots, A_{\tau-1}$ of any reduced sequence $(A)_n$ will be said to form a *cycle belonging to $F(x)$* . The cycle (S) , where S_n is defined above, will be called the *principal cycle* of $F(x)$.

An ordered set of three residues (or more generally, of three rational integers) A', B', C' will be called a *triad*, and denoted by $[A', B', C']$. The τ triads

$$[A_0, A_1, A_2], [A_1, A_2, A_3], \dots, [A_{\tau-2}, A_{\tau-1}, A_0], [A_{\tau-1}, A_0, A_1]$$

will be called the *triads belonging to the cycle (A)* .

* For the properties of Galois fields which are assumed here, see Dickson, *Linear Groups*, Leipzig, 1901.

Two triads are equal when and only when they are identical modulo p ; two cycles are equal if one may be derived from the other by a cyclic permutation of its elements. It is clear that any cycle is completely specified by any one of its triads; furthermore, two given cycles have either all or none of their triads in common.

The cycles whose initial triads are $[1, 0, 0]$, $[0, 1, 0]$, and $[0, 0, 1]$ will be denoted by (X) , (Y) , and (Z) respectively.*

4. Multipliers and blocks. If L is any residue such that the cycles

$$LA_0, LA_1, \dots, LA_{\tau-1} \text{ and } A_0, A_1, \dots, A_{\tau-1}$$

are equal (modulo p), L is called a *multiplier* of (A) .

In the paper previously referred to, I have shown that every cycle of $F(x)$ has the same multipliers, and that there exists a unique “basic multiplier” M such that every other multiplier is congruent to some power of M .

It follows that if $e = \epsilon(M)$ denotes the exponent to which M belongs modulo p , then there are exactly e distinct multipliers. e moreover divides τ and the quotient divides $p^2 + p + 1$. If we write $\tau = \epsilon(M)\mu$, $\mu | p^2 + p + 1$, then μ is called the restricted period† of $F(x)$.

Let

$$et = p - 1, \quad \mu\kappa = p^2 + p + 1.$$

Then there are exactly t distinct cycles modulo p among the $p - 1$ cycles

$$XA_0, XA_1, \dots, XA_{\tau-1} \quad (X = 1, 2, \dots, p - 1).$$

These t cycles will be said to form a *block* of cycles. There are in all exactly κ distinct blocks of cycles; we shall denote them by the capital German letters $\mathfrak{B}_1, \mathfrak{B}_2, \dots, \mathfrak{B}_\kappa$.

In particular, it will be understood that \mathfrak{B}_1 is the block containing the principal cycle (S) .

The number of times a given residue appears in a given block is given by the following easily established theorem.

THEOREM 4.1. *If b_0 denotes the number of times the residue 0 appears in the first μ terms of any cycle of a given block \mathfrak{B} , then every residue other than zero appears in \mathfrak{B} exactly $\mu - b_0$ times, while the residue zero appears $(p - 1)b_0$ times.*

5. Illustration. In order to clarify the definitions of the preceding two sections, we give all the cycles of $F(x) = x^3 + 3x^2 + 4x + 1$ for $p = 7$, and a list of the notations introduced.

* For a number of algebraic properties of the associated sequences, see Bell, Tôhoku Mathematical Journal, vol. 24 (1924), pp. 169–184. The terms of the principal cycle (S) and (X) , (Y) , (Z) are connected by the simple relation $S_n \equiv X_n + Y_{n+1} + Z_{n+2} \pmod{p}$.

† This term is due to Carmichael, who uses it in a slightly more general sense. See Quarterly Journal paper, p. 354.

COMPLETE CYCLES, GROUPED BY BLOCKS

 \mathfrak{B}_1

$$\begin{cases} \{3, 4, 1, 6, 2, 4, 2, 4, 4, 5, 0, 4, 4, 0, 1, 0, 3, 4, 4, \\ 4, 3, 6, 1, 5, 3, 5, 3, 3, 2, 0, 3, 3, 0, 6, 0, 4, 3, 3. \end{cases}$$

$$\begin{cases} 6, 1, 2, 5, 4, 1, 4, 1, 1, 3, 0, 1, 1, 0, 2, 0, 6, 1, 1, \\ 1, 6, 5, 2, 3, 6, 3, 6, 6, 4, 0, 6, 6, 0, 5, 0, 1, 6, 6. \end{cases}$$

$$\begin{cases} 2, 5, 3, 4, 6, 5, 6, 5, 5, 1, 0, 5, 5, 0, 3, 0, 2, 5, 5, \\ 5, 2, 4, 3, 1, 2, 1, 2, 2, 6, 0, 2, 2, 0, 4, 0, 5, 2, 2. \end{cases}$$

 \mathfrak{B}_2

$$\begin{cases} 0, 0, 1, 4, 5, 3, 2, 5, 2, 0, 1, 2, 4, 0, 3, 1, 6, 3, 1, \\ 0, 0, 6, 3, 2, 4, 5, 2, 5, 0, 6, 5, 3, 0, 4, 6, 1, 4, 6. \end{cases}$$

$$\begin{cases} 0, 0, 2, 1, 3, 6, 4, 3, 4, 0, 2, 4, 1, 0, 6, 2, 5, 6, 2, \\ 0, 0, 5, 6, 4, 1, 3, 4, 3, 0, 5, 3, 6, 0, 1, 5, 2, 1, 5. \end{cases}$$

$$\begin{cases} 0, 0, 3, 5, 1, 2, 6, 1, 6, 0, 3, 6, 5, 0, 2, 3, 4, 2, 3, \\ 0, 0, 4, 2, 6, 5, 1, 6, 1, 0, 4, 1, 2, 0, 5, 4, 3, 5, 4. \end{cases}$$

 \mathfrak{B}_3

$$\begin{cases} 0, 1, 3, 1, 5, 6, 3, 4, 5, 1, 1, 2, 3, 3, 5, 5, 4, 5, 6, \\ 0, 6, 4, 6, 2, 1, 4, 3, 2, 6, 6, 5, 4, 4, 2, 2, 3, 2, 1. \end{cases}$$

$$\begin{cases} 0, 2, 6, 2, 3, 5, 6, 1, 3, 2, 2, 4, 6, 6, 3, 3, 1, 3, 5, \\ 0, 5, 1, 5, 4, 2, 1, 6, 4, 5, 5, 5, 3, 1, 4, 4, 6, 4, 2. \end{cases}$$

$$\begin{cases} 0, 3, 2, 3, 1, 4, 2, 5, 1, 3, 3, 6, 2, 2, 1, 1, 5, 1, 4, \\ 0, 4, 5, 4, 6, 3, 5, 2, 6, 4, 4, 1, 5, 5, 6, 2, 6, 3. \end{cases}$$

For this case, $p-1=6$, $p^2+p+1=57$, $M=6$, $e=2$, $t=3$, $\mu=19$, $\kappa=3$, $\tau=38$ and in \mathfrak{B}_1 , $b_0=3$.

LIST OF NOTATION

Characteristic number period of $F(x)$	Number of cycles in a block: t	Triad: $[U, V, W]$
Number of elements or triads in a cycle	Number of blocks: κ	Cycle: (A)
Restricted period of $F(x)$: μ	Connecting relations:	Block: \mathfrak{B}
Basic multiplier: M	$\mu\kappa=p^2+p+1$,	
	$et=p-1$,	
Exponent to which M belongs modulo p : $e=e(M)$.	$\tau=e\mu$.	

II. THE DISTRIBUTION OF TRIADS

6. Invariant of a cycle. Let us assume that we know the distribution functions of the cycles (U) , (V) , \dots , (W) and that we are given the initial values $A_0 = K$, $A_1 = L$, $A_2 = M$ of some cycle (A) . Then if the triad $[K, L, M]$ occurs in one of the cycles (U) , (V) , \dots , (W) , the distribution function of (A) is also known. We are thus led to consider the problem of determining to what cycle any given triad belongs. In this section we shall restrict ourselves to the simplest case, when we know beforehand that the triad belongs to a certain block.

First, if α, β, γ are the roots of

$$(6.1) \quad F(x) = x^3 - Px^2 + Qx - R = 0$$

and

$$W_n = \sum_{(\alpha)} (K_0 + K_1\alpha + K_2\alpha^2)\alpha^n \quad (n = 0, 1, \dots)$$

is the general term of any sequence $(W)_n$ satisfying (1.1), then it is easily shown that the determinant

$$D_n(W) = \begin{vmatrix} W_n, & W_{n+1}, & W_{n+2} \\ W_{n+1}, & W_{n+2}, & W_{n+3} \\ W_{n+2}, & W_{n+3}, & W_{n+4} \end{vmatrix}$$

has the value

$$(6.11) \quad D_n(W) = R^n \Delta N(w),$$

where R is the constant term of the characteristic equation (6.1), Δ is the discriminant of $F(x)$, and $N(w)$ the norm of the algebraic number $w = K_0 + K_1\alpha + K_2\alpha^2$.

Consequently, if $\epsilon(R)$ denotes the exponent to which R belongs modulo p , and if (A) is the cycle corresponding to $(W)_n$ modulo p , then the value of

$$J(A) \equiv [\Delta_n(A)]^{\epsilon(R)} \mod p$$

is independent of n . We shall call this residue the *invariant* of the cycle (A) .

By means of (1.1), we can express the determinant $\Delta_n(W)$ as a polynomial in W_n, W_{n+1}, W_{n+2} . If we define $\Lambda(K, L, M)$ for all values of its arguments to be the polynomial

$$\begin{aligned} \Lambda(K, L, M) = & -R^2 K^3 + 2QRK^2L - PRK^2M - (PR + Q^2)KL^2 \\ & + (PQ + 3R)KLM - QKM^2 + (PQ - R)L^3 - (P^2 + Q)L^2M \\ & + 2PLM^2 - M^3, \end{aligned}$$

then

$$(6.12) \quad \Delta_n(W) = \Lambda(W_n, W_{n+1}, W_{n+2}).$$

Thus if A_0, A_1, A_2 are the initial values of any cycle (A) , the invariant $J(A)$ is determined by the congruence

$$J(A) \equiv [\Lambda(A_0, A_1, A_2)]^{\epsilon(R)} \pmod{p}.$$

Now if L is any constant residue, $\Delta_n(L \cdot W) = L^3 \Delta_n(W)$. Hence if $(L \cdot A)$ denotes the cycle $LA_0, LA_1, \dots, LA_{r-1}$,

$$(6.2) \quad J(L \cdot A) \equiv L^{3\epsilon(R)} J(A) \pmod{p}.$$

In the work previously referred to, I have shown that either $\epsilon(M) = \epsilon(R)$ or $\epsilon(M) = 3\epsilon(R)$, where it will be recalled that $\epsilon(M)$ is the exponent to which the basic multiplier M belongs modulo p . If $p \equiv 2 \pmod{3}$, then $\epsilon(M)$ necessarily equals $\epsilon(R)$. Moreover, $L^{3\epsilon(M)} \equiv 1 \pmod{p}$ when and only when $L^{\epsilon(M)} \equiv 1 \pmod{p}$; hence, from (6.2) $J(L \cdot A) \equiv J(A) \pmod{p}$ when and only when L is a multiplier of (A) . A precisely similar result holds if $p \equiv 1 \pmod{3}$ and $\epsilon(M) = 3\epsilon(R)$.*

It follows that in these two cases if $(A^{(1)}), \dots, (A^{(t)})$ are the t distinct cycles of a given block \mathfrak{B} , the invariants $J(A^{(1)}), \dots, J(A^{(t)})$ are all incongruent to one another modulo p . We thus obtain the following theorem.

THEOREM 6.1. *If $p \equiv 2 \pmod{3}$ or $p \equiv 1 \pmod{3}$, and $\epsilon(M) = 3\epsilon(R)$, and if $[K, L, M]$ is any triad of the block \mathfrak{B} , then a necessary and sufficient condition that $[K, L, M]$ belong to the cycle (A) of \mathfrak{B} is that*

$$(6.3) \quad \{\Lambda(K, L, M)\}^{\epsilon(R)} \equiv J(A) \pmod{p}.$$

If $p \equiv 1 \pmod{3}$ and $\epsilon(M) = \epsilon(R)$ (which implies that $\epsilon(M) \not\equiv 0 \pmod{3}$), we cannot go quite so far. For if ω is a primitive cube root of unity modulo p , then

$$\Delta_n(\omega \cdot A) = \omega^3 \Delta_n(A) \equiv \Delta_n(A) \pmod{p}.$$

Consequently, since ω is not a multiplier, the three cycles (A) , $(\omega \cdot A)$, $(\omega^2 \cdot A)$ are distinct, and will have the same invariant. (6.3) must then be replaced by

$$\{\Lambda(K, L, M)\}^{\epsilon(R)} \equiv J(A) = J(\omega \cdot A) = J(\omega^2 \cdot A),$$

and for any given triad $[K, L, M]$ of the block \mathfrak{B} , we can ascertain merely that it must be in one of three cycles of \mathfrak{B} .

* If $p = 3^l N + 1$ sufficient conditions for $\epsilon(M) = 3\epsilon(R)$ are $\epsilon(R) \equiv 0 \pmod{3}$, $\not\equiv 0 \pmod{3^k}$; or R not a cubic residue of p .

7. Distribution of triads in cycles. Let

$$(K): \quad K_0, K_1, \dots, K_{r-1}$$

denote a fixed cycle of $F(x)$. We shall show that we can determine whether or not two triads $[A, B, C]$ and $[A', B', C']$ belong to the same cycle if we know all the triads which belong to (K) .

If L_0, L_1, L_2 are determined by the congruences

$$\begin{aligned} (7.1) \quad A &\equiv L_0 K_0 + L_1 K_1 + L_2 K_2, \\ B &\equiv L_0 K_1 + L_1 K_2 + L_2 K_3, \\ C &\equiv L_0 K_2 + L_1 K_3 + L_2 K_4, \end{aligned}$$

then a necessary and sufficient condition that $[A', B', C']$ should belong to the same cycle as $[A, B, C]$ is that for some value of m there should exist congruences of the form

$$\begin{aligned} (7.2) \quad A' &\equiv L_0 K_m + L_1 K_{m+1} + L_2 K_{m+2}, \\ B' &\equiv L_0 K_{m+1} + L_1 K_{m+2} + L_2 K_{m+3}, \\ C' &\equiv L_0 K_{m+2} + L_1 K_{m+3} + L_2 K_{m+4}. \end{aligned}$$

Now, by means of the difference equation (1.1), we can express K_{m+3} and K_{m+4} in (7.2) linearly in terms of K_m, K_{m+1}, K_{m+2} . Write A'', B'', C'' for K_m, K_{m+1}, K_{m+2} . Then if we introduce the abbreviations $[LU]_i$ ($U = X, Y, Z; i = 1, 2, 3$) for the sums $L_0 U_i + L_1 U_{i+1} + L_2 U_{i+2}$, the equations (7.2) give the following values for A'', B'', C'' :

$$(7.3) \quad A'' \equiv \frac{|A', [LY]_1, [LZ]_2|}{|[LX]_0, [LY]_1, [LZ]_2|}, \text{ etc.},$$

where $|A', [LY]_1, [LZ]_2|$ stands for the determinant

$$\begin{vmatrix} A', & [LY]_0, & [LZ]_0 \\ B', & [LY]_1, & [LZ]_1 \\ C', & [LY]_2, & [LZ]_2 \end{vmatrix},$$

and so on.

If we treat (7.1) in a similar manner, letting $\{KX\}_i$ stand for the sum $K_0 X_i + K_1 Y_i + K_2 Z_i$ ($i = 0, 1, 2, 3, 4$) we find that

$$(7.4) \quad L_0 \equiv \frac{|A, \{KX\}_2, \{KX\}_4|}{|\{KX\}_0, \{KX\}_2, \{KX\}_4|}, \text{ etc.},$$

where $|A, \{KX\}_2, \{KX\}_4|$ stands for the determinant

$$\begin{vmatrix} A, & \{KX\}_1, & \{KX\}_2 \\ B, & \{KX\}_2, & \{KX\}_3 \\ C, & \{KX\}_3, & \{KX\}_4 \end{vmatrix}$$

and so on.

We thus obtain the following theorem.

THEOREM 7.1. *A necessary and sufficient condition that the triads $[A, B, C]$ and $[A', B', C']$ should belong to the same cycle is that the triad $[A'', B'', C'']$ determined by (7.3) and (7.4) should belong to the cycle (K) .*

We have thus reduced the problem of determining to what cycle any triad belongs to the problem of determining whether or not a triad belongs to some fixed cycle, say the principal cycle of $F(x)$.

8. The distribution of zeros in a cycle. We shall assume in this section that the cycles of $F(x)$ have no multiplier other than the trivial multiplier unity which implies that τ divides $p^2 + p + 1$. The distribution of zeros in an arbitrary cycle (U) of $F(x)$ then depends in a remarkable manner upon the distribution of residues in the principal cycle (S) , as is shown by the following theorem:

THEOREM 8.1. *Let (U) denote a definite cycle of $F(x)$ in which it is known that*

$$(8.1) \quad U_a \equiv U_b \equiv 0 \pmod{p} \quad (a \neq b).$$

*Then a necessary and sufficient condition that $U_c \equiv 0 \pmod{p}$ is that**

$$(8.2) \quad S_{a+b+p+c} \equiv S_{a+b+p^2+c} \pmod{p}.$$

Let

$$(8.3) \quad U_n \equiv K_0 S_n + K_1 S_{n+1} + K_2 S_{n+2} \pmod{p}.$$

Then (8.1) gives

$$K_0 : K_1 : K_2 = \begin{vmatrix} S_{a+1}, & S_{a+2} \\ S_{b+1}, & S_{b+2} \end{vmatrix} : \begin{vmatrix} S_{a+2}, & S_a \\ S_{b+2}, & S_b \end{vmatrix} : \begin{vmatrix} S_a, & S_{a+1} \\ S_b, & S_{b+1} \end{vmatrix}.$$

Hence by (8.3)

$$U_n \equiv LD(a, b, n) \pmod{p},$$

where $D(a, b, n)$ denotes the determinant

$$\begin{vmatrix} S_a, & S_{a+1}, & S_{a+2} \\ S_b, & S_{b+1}, & S_{b+2} \\ S_n, & S_{n+1}, & S_{n+2} \end{vmatrix}$$

and L is a constant residue.

* In numerical cases the subscripts of the S are reduced modulo τ .

On expanding this determinant and substituting for S_a, S_b , etc.,

$$\alpha^a + \alpha^{pa} + \alpha^{p^2a}, \quad \alpha^b + \alpha^{pb} + \alpha^{p^2b} \text{ etc.,}$$

we find that

$$D(a, b, n) \equiv S_{a+b+p+n} - S_{a+b+p^2+n} \pmod{p},$$

so that

$$(8.31) \quad U_n \equiv L(S_{a+b+p+n} - S_{a+b+p^2+n}) \quad (n = 0, 1, \dots, r-1).$$

This proof would fail if

$$\begin{vmatrix} S_{a+1}, & S_{a+2} \\ S_{b+1}, & S_{b+2} \end{vmatrix}, \quad \begin{vmatrix} S_{a+2}, & S_a \\ S_{b+2}, & S_b \end{vmatrix}, \quad \begin{vmatrix} S_a, & S_{a+1} \\ S_b, & S_{b+1} \end{vmatrix}$$

should all be congruent to zero modulo p . But in this case

$$S_a \equiv MS_b, \quad S_{a+1} \equiv MS_{b+1}, \quad S_{a+2} \equiv MS_{b+2}$$

where M is a constant residue. Since the only multiplier of (S) is unity, $M=1$ and $a=b$ contrary to hypothesis.

The following two theorems are direct corollaries of Theorem 8.1.

THEOREM 8.11. *If (Z) denotes the cycle $0, 0, 1, \dots$, then a necessary and sufficient condition that $Z_n \equiv 0 \pmod{p}$ is that $S_{n+p} \equiv S_{n+p^2} \pmod{p}$.*

THEOREM 8.12. *If (Y) denotes the cycle $0, 1, 0, \dots$, then a necessary and sufficient condition that $Y_n \equiv 0 \pmod{p}$ is that $S_{n+2p} \equiv S_{n+2p^2} \pmod{p}$.*

We have several times used the fact that if (S) is the principal cycle, $S_n \equiv S_{np} \equiv S_{np^2} \pmod{p}$. The following limited converse of this result is a direct consequence of Theorem 8.1.

THEOREM 8.2. *Let (U) be any cycle of $F(x)$. If for any $m \neq 0$ it is known that $U_m \equiv U_{pm} \equiv U_{p^2m} \equiv 0 \pmod{p}$, then $U_n \equiv KS_n$ ($n = 0, 1, \dots, r-1$).*

The following congruences, which are all special cases of the easily established general formula

$$U_{n+m} + U_{n+pm} + U_{n+p^2m} \equiv U_n S_m \pmod{p},$$

give some curious arithmetical properties of cycles:

$$(8.4) \quad \begin{aligned} U_n + U_{pn} + U_{p^2n} &\equiv U_0 S_n, \\ U_0 + U_{(p-1)n} + U_{(p^2-1)n} &\equiv U_{-n} S_n, \\ S_{n+m} + S_{n+pm} + S_{n+p^2m} &\equiv S_n S_m, \\ X_n + X_{pn} + X_{p^2n} &\equiv S_n, \\ Y_n + Y_{pn} + Y_{p^2n} &\equiv 0, \\ Z_n + Z_{pn} + Z_{p^2n} &\equiv 0 \pmod{p}. \end{aligned}$$

From Theorem 8.2, we see that it is impossible for Y_n , Y_{pn} , Y_{p^2n} or Z_n , Z_{pn} , Z_{p^2n} to be all congruent to zero modulo p simultaneously. From the last two formulas of (8.4), we see that it is also impossible for Y_n and Y_{pn} or Z_n and Z_{pn} to be congruent to zero simultaneously. In the succeeding section we shall prove a much more precise result of this character, which will enable us to obtain valuable information about the number of zeros in any cycle.

9. Diophantine relations for the number of zeros in a cycle. If the cycles of $F(x)$ have no multiplier save unity, each block of cycles contains $p-1$ distinct cycles. Let $\mathfrak{B}_1, \mathfrak{B}_2, \dots, \mathfrak{B}_\tau$ be the separate blocks, and let $(p-1)b_i$ be the number of zeros in \mathfrak{B}_i , so that each cycle of \mathfrak{B}_i contains b_i zeros. Clearly, $\sum_{i=1}^\tau (p-1)b_i = p^2 - 1$; hence

$$(9.1) \quad b_1 + b_2 + \dots + b_\tau = p + 1.$$

In this section I shall establish the additional formula

$$(9.2) \quad b_1^2 + b_2^2 + \dots + b_\tau^2 = \tau + p.$$

THEOREM 9.1. *Let a, b be any two distinct numbers $\geq 0, < \tau$. Then there exists a cycle $U_0, U_1, \dots, U_{\tau-1}$ such that*

$$U_a \equiv U_b \equiv 0 \pmod{p}.$$

The τ residues

$$U_n \equiv \begin{vmatrix} S_n, & S_a, & S_b \\ S_{n+1}, & S_{a+1}, & S_{b+1} \\ S_{n+2}, & S_{a+2}, & S_{b+2} \end{vmatrix} \pmod{p}$$

clearly form a cycle satisfying the conditions of the theorem.

THEOREM 9.2. *Let (U) , (V) be any two cycles of $F(x)$, in which it is known that*

$$U_a \equiv U_b \equiv 0, \quad V_c \equiv V_d \equiv 0 \pmod{p}.$$

Then a sufficient condition that (U) and (V) should belong to the same block is that $a-b \equiv c-d \pmod{\tau}$.

Let $V_n = W_{n+a-c}$ ($n=0, 1, \dots, \tau-1$). Then $W_a \equiv W_b \equiv 0 \pmod{p}$. Hence if

$$U_n \equiv K_0 S_n + K_1 S_{n+1} + K_2 S_{n+2}, \quad W_n \equiv L_0 S_n + L_1 S_{n+1} + L_2 S_{n+2},$$

then

$$\begin{aligned} K_0 S_a + K_1 S_{a+1} + K_2 S_{a+2} &\equiv 0, & L_0 S_a + L_1 S_{a+1} + L_2 S_{a+2} &\equiv 0, \\ K_0 S_b + K_1 S_{b+1} + K_2 S_{b+2} &\equiv 0, & L_0 S_b + L_1 S_{b+1} + L_2 S_{b+2} &\equiv 0. \end{aligned}$$

Hence* $L_0:L_1:L_2 = K_0:K_1:K_2$, so that

$$V_{n+c-a} \equiv W_n \equiv MU_n \pmod{p} \quad (n = 0, 1, \dots, \tau - 1),$$

and (V) and (W) belong to the same block.

THEOREM 9.3. *If the cycle (U) has no multiplier save unity, and if $U_{a_1}, U_{a_2}, \dots, U_{a_b}$ are the b residues of (U) congruent to zero modulo p , then the $b(b-1)$ differences $a_i - a_j$ ($i, j = 1, \dots, b$; $i \neq j$) are all incongruent modulo τ .*

If $a_i - a_j \equiv a_k - a_l \pmod{\tau}$, then, by the previous theorem,

$$U_{a_i-a_k+n} \equiv MU_n \quad (n = 0, 1, \dots, \tau - 1).$$

Hence $M = 1$ and $a_i - a_k \equiv 0 \pmod{\tau}$; $i = k, j = l$.

THEOREM 9.4. *Let $(U^{(1)}), \dots, (U^{(\kappa)})$ be κ cycles belonging to the blocks $\mathfrak{B}_1, \dots, \mathfrak{B}_\kappa$, respectively, so that $(U^{(i)})$ contains exactly b_i zeros. Then*

$$(9.21) \quad \sum_{i=1}^k b_i(b_i - 1) = \tau - 1.$$

If $b_i < 2$, $b_i(b_i - 1) = 0$. If $b_i \geq 2$, then as in Theorem 9.3 the cycle $(U^{(i)})$ furnishes $b_i(b_i - 1)$ differences $a_i - a_j$ which are all incongruent modulo τ . But by Theorems 9.1 and 9.2, to each of the $\tau - 1$ distinct differences $a_k - a_l$ modulo τ there corresponds exactly one block such that for every cycle (U) of this block $U_{a_k} \equiv U_{a_l} \equiv 0 \pmod{p}$. Hence (9.21) follows.

Formula (9.2) now follows from (9.21) and (9.1) by addition.

10. Application to the case $\tau = (p^2 + p + 1)/3$. We shall now apply the formulas of §9 to the case when $p = 3N + 1$ and when the characteristic number τ equals $(p^2 + p + 1)/3$. There are then only three blocks of cycles and no multipliers, so that (9.1) and (9.2) become

$$(10) \quad \begin{aligned} b_1 + b_2 + b_3 &= p + 1, \\ b_1^2 + b_2^2 + b_3^2 &= (p^2 + 4p + 1)/3. \end{aligned}$$

Moreover, since \mathfrak{B}_1 contains the principal cycle (S) , $b_1 \equiv 0 \pmod{3}$; for $S_n \equiv 0 \pmod{p}$ implies that $S_{np} \equiv S_{n,p^2} \equiv 0 \pmod{p}$. Thus we have the additional restrictions

$$(10.1) \quad b_1 \equiv 0 \pmod{3}, \quad 0 \leq b_1, b_2, b_3 \leq p + 1.$$

The theory of the diophantine system (10) and (10.1) is a special case of a theory of simultaneous quadratic and linear representation given by Dr. Gordon Pall in a forthcoming paper. I am indebted to Dr. Pall for the following result:

* It is impossible for the ratios to be indeterminate; see the proof of Theorem 8.1.

The system (10), (10.1) always has a unique solution in positive integers. If (ξ, η) is that solution of $\xi^2 + 3\eta^2 = p$ satisfying the condition $\xi \equiv 2 \pmod{3}$, then the solution of (10) is given by

$$b_1 = N + \frac{2}{3}(\xi + 1), \quad b_2 = N + \eta - \frac{1}{3}(\xi - 2), \quad b_3 = N - \eta - \frac{1}{3}(\xi - 2).$$

It should be noted that b_2 and b_3 are both congruent to 1 modulo 3, and distinct.

In §17, we shall return to this case and obtain the values of b_1, b_2, b_3 by quite a different method.

The next simplest case is when $\tau = (p^2 + p + 1)/7$. Pall's theory allows us to reduce the solution of (9.1) and (9.2) to a single equation in six variables, but unfortunately this new equation has a large number of possible solutions.

11. Minimum number of residues of a cycle. I shall conclude this part of the paper by proving the following theorem:

THEOREM. *If the characteristic number τ equals $p^2 + p + 1$, then every residue appears in every cycle of $F(x)$ at least once.*

Under the hypothesis of the theorem, there are $p - 1$ cycles grouped in a single block \mathfrak{B} ; hence it is sufficient to prove that every residue appears in the cycle (S) at least once.

Consider the $(p - 1)^3 - 1$ triads which do not contain a particular residue K . If U, V, W stand for distinct residues, these triads may be grouped into five classes; namely,

$$\begin{aligned} m_1 &= (p - 1)(p - 2)(p - 3) \text{ triads of type } [U, V, W]; \\ m_2 &= (p - 1)(p - 2) \quad " \quad [U, V, U]; \\ m_3 &= (p - 1)(p - 2) \quad " \quad [U, U, V]; \\ m_4 &= (p - 1)(p - 2) \quad " \quad [U, V, V]; \\ m_5 &= (p - 2) \quad " \quad [U, U, U]. \end{aligned}$$

Let μ_i be the number of triads of type i which appear in (S) . To each triad of type 1 there correspond $p - 4$ distinct triads of type 1 in the block of cycles $L(S)$; namely, those for which

$$LU \not\equiv K, \quad LV \not\equiv K, \quad LW \not\equiv K \pmod{p} \quad (L = 1, 2, \dots, p - 1).$$

Therefore,

$$(p - 4)\mu_1 \leq m_1, \quad \text{or} \quad \mu_1 < (p - 1)(p - 2).$$

Similarly,

$$\mu_2 < p - 1; \quad \mu_3 < p - 1; \quad \mu_4 < p - 1; \quad \mu_5 < 1.$$

Accordingly, if the residue K does not appear in (S) ,

$$\tau = \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 < (p - 1)(p - 2) + 3(p - 1) + 1 = p^2,$$

giving a contradiction.

III. DETERMINATION OF DISTRIBUTION FUNCTION

12. Reduction to the case when τ is prime to 3 and divides $p^2 + p + 1$. We shall now show that it is sufficient to determine the distribution functions for difference equations whose characteristic number is prime to 3 and divides $p^2 + p + 1$.

Let $F(x)$ and $F'(x)$ be two irreducible cubics modulo p with the periods τ and τ' , where $F'(x)$ is so chosen that τ' divides τ . Write

$$(12.1) \quad \tau = \tau' k'.$$

Let the roots of $F(x) = 0$ and $F'(x) = 0$ be denoted by $\alpha, \beta, \gamma; \alpha', \beta', \gamma'$ respectively. We then have in the Galois field associated with $F(x)$ a congruence of the form

$$(12.2) \quad \alpha' \equiv \alpha^{k's} \pmod{p}.$$

s here is a fixed integer prime to τ depending on our choice of $F'(x)$.

Now let (U') be any cycle of $F'(x)$. Then

$$U'_n \equiv \sum_{(\alpha')} (K_0 + K_1 \alpha' + K_2 \alpha'^2) \alpha'^n \quad (n = 0, 1, \dots, \tau' - 1).$$

Hence by (12.2)

$$U'_n \equiv \sum_{(\alpha)} (L_0 + L_1 \alpha + L_2 \alpha^2) \alpha^{nk's}$$

where

$$(12.3) \quad \begin{aligned} L_0 &\equiv X_0 K_0 + X_{k's} K_1 + X_{2k's} K_2; \\ L_1 &\equiv Y_0 K_0 + Y_{k's} K_1 + Y_{2k's} K_2; \\ L_2 &\equiv Z_0 K_0 + Z_{k's} K_1 + Z_{2k's} K_2. \end{aligned}$$

L_0, L_1, L_2 cannot moreover all be congruent to zero modulo p , for if Δ and Δ' are the discriminants of $F(x)$ and $F'(x)$,

$$\begin{vmatrix} X_0, & X_{k's}, & X_{2k's} \\ Y_0, & Y_{k's}, & Y_{2k's} \\ Z_0, & Z_{k's}, & Z_{2k's} \end{vmatrix} \equiv \Delta'/\Delta \not\equiv 0 \pmod{p}.$$

Write

$$(12.31) \quad \begin{aligned} A &\equiv L_0 S_0 + L_1 S_1 + L_2 S_2, \\ B &\equiv L_0 S_1 + L_1 S_2 + L_2 S_3, \\ C &\equiv L_0 S_2 + L_1 S_3 + L_2 S_4. \end{aligned}$$

Then A, B, C are the initial values of the sequence (U) where

$$U_n \equiv \sum_{(\alpha)} (L_0 + L_1\alpha + L_2\alpha^2)\alpha^n \quad (n = 0, 1, \dots, \tau - 1)$$

and we have the formula

$$(12.4) \quad U'_n \equiv U_{nk's} \mod p \quad (n = 0, 1, \dots, \tau' - 1).$$

The process by which we obtained (U) from (U') fixed the initial elements of (U) ; if we remove this restriction, then if we are given (U) , τ' and s , by letting $[A, B, C]$ in (12.31) equal successively the triads $[U_0, U_1, U_2]$, $[U_1, U_2, U_3]$, \dots , $[U_{k'-1}, U_{k'}, U_{k'+1}]$, K_0, K_1, K_2 are obtained from (12.3), so that (U') is known, and (12.4) is replaced by the more general relation

$$(12.41) \quad U'_n \equiv U_{nk's+r} \quad (n = 0, 1, \dots, \tau' - 1; 0 \leq r < k').$$

Since ns in (12.4) or (12.41) runs through a complete residue system modulo τ' , the result we have obtained may be formulated as follows:

THEOREM 12.1. *Any cycle (U') of $F'(x)$ can be obtained from some cycle (U) of $F(x)$ by selecting from (U) terms whose subscripts lie in an arithmetical progression of constant difference k' , and arranging them in a suitable order.*

A cycle (U') obtained in this manner from some cycle (U) of $F(x)$ will be called a *derived cycle* of (U) . On taking $\tau' = \tau$, we obtain the following:

THEOREM 12.2. *If $F(x)$ and $F'(x)$ are two irreducible cubics modulo p with the same characteristic number τ , and if (U') is any cycle of $F'(x)$, then there exists a cycle (U) of $F(x)$ with the same distribution function as (U') .*

Thus in a certain sense the distribution function of a cycle is independent of the characteristic function to which the cycle belongs. For example, the distribution functions of the derived cycles (U') of (U) defined in (12.41) are independent of the value of s , provided only that s is prime to τ .

Now let us take* $\tau = e\mu$ where e denotes as usual the period modulo p of the basic multiplier, and take $\tau' = \mu$. We shall show that the distribution function of any cycle (U) of $F(x)$ is determined if we know the distribution function for a single one of its derived cycles (U') of period μ .

Let

$$a_0M, a_0M^2, \dots, a_0M^e;$$

$$a_1M, a_1M^2, \dots, a_1M^e;$$

.

$$a_{t-1}M, a_{t-1}M^2, \dots, a_{t-1}M^e$$

* It can be shown that $(e, \mu) = 1$ save when $p = 3^kN + 1$, $\epsilon(R) \equiv 0 \pmod{3^k}$. We shall exclude this case from consideration here.

represent the separation of the multiplicative group $\{1, 2, \dots, p-1\}$ of the $p-1$ non-zero residues of p into co-sets with respect to its cyclic sub-group $\{M\}$. Then if $k(n)$ is the distribution function of (U) , and $l(n)$ the distribution function of the first μ terms of (U) ,

$$k(a_i M^s) = [l(a_i M) + l(a_i M^2) + \dots + l(a_i M^\sigma)] \\ (i = 0, 1, \dots, \tau; s = 1, 2, \dots, e).$$

Now let $k'(n)$ be the distribution function of any derived cycle (U') of (U) with the period μ . From the properties of multipliers, it is evident that if $a \equiv b \pmod{\mu}$, then $U_a \equiv M^\sigma U_b \pmod{p}$, the exponent σ depending of course on our choice of U_a and U_b . Now the subscript $n\kappa's+r(\kappa'=e)$ of (U) in (12.41) runs through a complete residue system modulo μ , for $(e, \mu)=1$; hence to each term U_a' of (U') there corresponds a unique term U_b in the first μ terms of (U) such that

$$U_a' \equiv M^\sigma U_b \pmod{p}.$$

Consequently, U_a' and U_b always lie in the same co-set, and

$$k'(a_i M) + k'(a_i M^2) + \dots + k'(a_i M^\sigma) = l(a_i M) + l(a_i M^2) + \dots + l(a_i M^\sigma).$$

Thus we have the formula

$$k(a_i M^s) = [k'(a_i M) + k'(a_i M^2) + \dots + k'(a_i M^\sigma)] \\ (i = 0, 1, \dots, \tau; s = 0, 1, \dots, e).$$

In a similar manner, we find that

$$k(0) = ek'(0).$$

These two formulas express the distribution function of (U) in terms of the distribution function of any one of its derived cycles (U') of period μ . It can be readily shown that μ divides p^2+p+1 and is prime to 3.

If we assume that the period τ of $F(x)$ is p^2+p+1 while the period τ' of $F'(x)$ is a divisor of p^2+p+1 , we can deduce the following important result from Theorem 12.1.

THEOREM 12.3. *If τ divides p^2+p+1 , then no residue can appear in any cycle of period τ more times than it appears in any cycle of period p^2+p+1 .*

13. Reduction to determination of residues modulis P and 3. Consider an irreducible cubic $F(x) = x^3 - Px^2 + Qx - R$ with the period $\tau = p^2+p+1$, modulo p , so that its cycles are grouped into a single block \mathfrak{B} , and let $k_n = k(n)$ be the distribution function of the principal cycle (S) .

Then since

$$S_n \equiv S_{np} \equiv S_{np^2} \pmod{p},$$

we see that if $p = 3N + 2$, then

$$k_i \equiv 0 \quad (i \neq 3), \quad k_3 \equiv 1 \quad \text{mod } 3.$$

If $p = 3N + 1$, it is easily verified that $p\tau/3 \equiv \tau/3 \pmod{\tau}$. Furthermore, if ω denotes a primitive cube root of unity modulo p ,

$$S_0 \equiv 3, \quad S_{\tau/3} \equiv 3\omega, \quad S_{2\tau/3} \equiv 3\omega^2 \quad \text{mod } p.$$

Hence

$$\begin{aligned} k_i &\equiv 0 \quad \text{mod } 3 & (i \neq 3, 3\omega, 3\omega^2), \\ k_3 &\equiv k_{3\omega} \equiv k_{3\omega^2} \equiv 1 & \text{mod } 3. \end{aligned}$$

Consequently,

$$\begin{aligned} (13.1) \quad k_i &= 3l_i \quad (i \neq 3), \quad k_3 = 3l_3 + 1, \quad p = 3N + 2, \\ &k_i = 3l_i \quad (i \neq 3, 3\omega, 3\omega^2), \\ &k_{3\omega^a} = 3l_{3\omega^a} + 1 \quad (a = 0, 1, 2), \quad p = 3N + 1. \end{aligned}$$

Now all of the cubics

$$x^3 - S_n x^2 + S_{-\bar{n}} x - 1, \quad 0 < n < \tau \quad \left(n \neq \frac{\tau}{3}, \quad \frac{2\tau}{3} \text{ if } p = 3N + 1 \right)$$

are irreducible modulo p and have periods which divide τ ; thus l_i is the number of irreducible cubics modulo p among the p cubics

$$x^3 - ix^2 + ux - 1 \quad (u = 0, 1, \dots, p-1).$$

Hence

$$(13.2) \quad 0 \leq l_i \leq p-2,$$

for the cubics $x^3 - ix^2 + ix - 1$, $x^3 - ix^2 - (i+2)x - 1$ are obviously reducible for any p .

Consequently, for $p > 3$, k_i is completely determined if we know its residues modulis p and 3.

Since the other cycles of $F(x)$ are obtained simply by multiplying the cycle (S) by some constant residue, their distribution functions are merely permutations of the distribution function of (S) , so that (13.2) holds for all the cycles of $F(x)$.

Now let $F'(x)$ be any other irreducible cubic with the period τ' , a divisor of $p^2 + p + 1$, and let $k'(n)$ be the distribution function of some cycle (U') of $F'(x)$. If $k(n)$ is the distribution function of the cycle (U) of $F(x)$ from which (U') is derived in accordance with Theorem 12.1, then by Theorem 12.2,

$$k'(n) \leq k(n) \quad (n = 0, 1, \dots, p-1).$$

We thus have the following important result.

THEOREM 13.1. *If $k(n)$ is the distribution function of any cycle (U) whose characteristic number divides p^2+p+1 , then $k(n)$ is completely determined if we know its residues modulo p and modulo 3.*

Since by (9.1), $k(0) \leq p+1$, we merely need to know the residue of $k(0)$ modulo p .

14. Digression on diophantine systems. The diophantine system

$$(D) \quad r_1 + r_2 + r_3 = m, \quad r_1 + pr_2 + p^2r_3 = s\tau,$$

where the integers m, p, τ are given, plays such an important part in the developments which are to follow, that it is necessary to discuss its solution rather fully.

The parameters p and τ are defined as follows. Let κ be any fixed integer of the sequences 1, 3, 7, 13, 19, 21, 31, 39, ..., of all possible divisors of the form x^2+x+1 , and let p be a prime such that p^2+p+1 is exactly divisible by κ .

If $p=k\kappa+\rho$, $1 < \rho < \kappa$, then ρ is zero if $\kappa=1$ and unity if $\kappa=3$. In all other cases, ρ is a primitive cube root of unity modulo κ . p is thus restricted to certain linear forms $n\kappa+\rho$.

τ is defined to be the quotient obtained by dividing p^2+p+1 by κ . If $p^2+p+1=\sigma\kappa$, then

$$(14.1) \quad \tau = k(k\kappa+\rho) + (\rho+1)k + \sigma, \quad 0 < (\rho+1)k + \sigma < 2p.$$

Finally m is restricted to be less than p , and the solutions r_1, r_2, r_3 must all be ≥ 0 . There are no restrictions on s other than that it be an integer.

Since $p^3 \equiv 1 \pmod{\tau}$, if $r_1=u, r_2=v, r_3=w$, or for short (u, v, w) is a solution of (D), (v, w, u) and (w, u, v) are also solutions. We can accordingly restrict ourselves to finding those solutions of (D) for which $r_3 \leq r_1, r_2$.

Now

$$r_1 + pr_2 + p^2r_3 - r_3\kappa\tau = (k\kappa+\rho)(r_2 - r_3) + (r_1 - r_3) \equiv 0 \pmod{\tau}.$$

Thus if we let $r_2 - r_3 = s_1, r_1 - r_3 = s_2$, we obtain

$$(14.2) \quad (k\kappa+\rho)s_1 + s_2 = u\tau \quad (s_1, s_2, u \geq 0; \quad 0 \leq s_1, s_2 < p).$$

Moreover, it is easily shown that $0 \leq u < \kappa, s_1 + s_2 < p$, and

$$(14.21) \quad m \geq s_1 + s_2; \quad m \equiv s_1 + s_2 \pmod{3}.$$

The method for solving (D) is then as follows: For a given value of κ, ρ and σ are determined, so that τ is known as a function of k from (14.1). For

each value of u between 0 and $\kappa - 1$ we can determine from (14.2) a pair of values for s_1 and s_2 in terms of k . We reject all solutions of (14.2) for which $s_1 + s_2 \geq p$. (14.21) then gives the restrictions upon m , and the corresponding solution of (D) is

$$\left(\frac{m - s_1 + 2s_2}{3}, \frac{m + 2s_1 - s_2}{3}, \frac{m - s_1 - s_2}{3} \right).$$

The following theorems for the cases $\kappa = 1$ and $\kappa = 3$ will serve to illustrate the method.

THEOREM 14.1. *If $\kappa = 1$, there is no solution of (D) unless $m \equiv 0 \pmod{3}$. If $m = 3M$, there is the single solution (M, M, M) .*

We have $\rho = 0$, $p = k$, so that (14.5) becomes

$$ps_1 + s_2 = u(p^2 + p + 1); \quad u = 0 \text{ giving } s_1 = s_2 = 0, \quad m \equiv 0 \pmod{3}; \\ (r_1, r_2, r_3) = (M, M, M).$$

THEOREM 14.2. *If $\kappa = 3$, there is no solution of (D) unless $p \equiv 1, m \equiv 0 \pmod{3}$. If $m = 3M$, there is the single solution (M, M, M) .*

Since $p^2 + p + 1 \equiv 0 \pmod{3}$, $p \equiv 1 \pmod{3}$. Let $p = 3k + 1$. Then $\tau = k(3k + 1) + 2k + 1$, and (14.2) becomes

$$(3k + 1)s_1 + s_2 = uk(3k + 1) + u(2k + 1) \quad (u = 0, 1, 2).$$

Case (i) $u = 0$. We have $s_1 = s_2 = 0$, so that from (14.2), $m = 3M$, giving the solution (M, M, M) .

Case (ii) $u = 1$. Then $s_1 = k$, $s_2 = 2k + 1$ so that $s_1 + s_2 = p$ and there is no solution.

Case (iii) $u = 2$. From (14.5) $s_2 \equiv 4k + 2 \equiv k + 1 \pmod{p}$. Since $s_2 < p$, $s_2 = k + 1$ and consequently $s_1 = 2k + 1$. Hence $s_1 + s_2 > p$ and there is no solution.

In general, if $p \equiv 1 \pmod{3}$, we see from (14.2) and (14.21) that $m \equiv \tau \equiv 0 \pmod{3}$.

When $\kappa = 7$, which requires that p be of the form $7n + 2$ or $7n + 4$, we find by the same method the following solutions of (D).

SOLUTIONS FOR $p \equiv 2, 4 \pmod{7}$, $7\tau = p^2 + p + 1$

Form of p	Form of m	Restriction on m	Solution
$21L + 2$	$3M$	≥ 0	(M, M, M)
	$3M + 1$	$\geq 12L + 1$	$(M + 5L + 1, M - L, M - 4L)$
	$3M + 2$	$\geq 15L + 2$	$(M + L + 1, M + 4L + 1, M - 5L)$
	$3M$	$\geq 18L + 3$	$(M - 3L, M + 9L + 1, M - 6L - 1)$

SOLUTIONS FOR $p \equiv 2, 4 \pmod{7}$, $7\tau = p^2 + p + 1$ (continued)

Form of p	Form of m	Restriction on m	Solution
$21L+16$	$3M$	≥ 0	(M, M, M)
	$3M$	$\geq 12L+9$	$(M+5L+4, M-L-1, M-4L-3)$
	$3M$	$\geq 15L+12$	$(M+L+1, M+4L+3, M-5L-4)$
$21L+4$	$3M$	$\geq 18L+15$	$(M-3L-2, M+9L+7, M-6L-5)$
	$3M$	≥ 0	(M, M, M)
	$3M$	$\geq 12L+3$	$(M-L, M+5L+1, M-4L-1)$
$21L+11$	$3M$	$\geq 15L+3$	$(M+4L+1, M+L, M-5L-1)$
	$3M$	$\geq 18L+3$	$(M+9L+2, M-3L-1, M-6L-1)$
	$3M$	≥ 0	(M, M, M)
$21L+11$	$3M+1$	$\geq 12L+5$	$(M-L, M+5L+3, M-4L-2)$
	$3M+2$	$\geq 15L+8$	$(M+4L+3, M+L+1, M-5L-2)$
	$3M$	$\geq 18L+9$	$(M+9L+5, M-3L-2, M-6L-3)$

For other small values of k the explicit solution of (D) may be obtained in a similar manner without undue labor.

15. Determination of distribution function modulo p . Let $k(n) = k_n$ be the distribution function modulo p of any cycle (U) whose characteristic number τ divides $p^2 + p + 1$. We shall determine the residue of k_n modulo p .

Let i be any residue of p . Then by Fermat's theorem

$$(U_n - i)^{p-1} \equiv 1 \pmod{p}, \quad U_n \not\equiv i; \\ \equiv 0 \pmod{p}, \quad U_n = i.$$

Hence

$$\sum_{n=0}^{p-1} (U_n - i)^{p-1} \equiv \tau - k_i \pmod{p} \quad (i = 0, 1, \dots, p-1).$$

On expanding $(U_n - i)^{p-1}$ by the binomial theorem, we obtain after a few easy reductions

$$(15.1) \quad \tau - k_i \equiv \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} (i)^{-m} U_n^m \tau - k_0 \equiv \sum_{n=0}^{p-1} U_n^{p-1} \pmod{p}.$$

Suppose that

$$U_n \equiv A\alpha^n + B\beta^n + C\gamma^n,$$

where $A = K_0 + K_1\alpha + K_2\alpha^2$, etc., so that

$$N(u) = ABC \equiv N(K_0 + K_1\alpha + K_2\alpha^2) \pmod{p}.$$

Then by the multinomial theorem

$$U_n^m \equiv \sum_{(r)} \frac{m!}{r_1!r_2!r_3!} A^{r_1} B^{r_2} C^{r_3} \alpha^{n(r_1+pr_2+p^2r_3)} \pmod{p}.$$

Since

$$\begin{aligned} \sum_{n=0}^{p-1} \alpha^{nR} &\equiv 0 \pmod{p} \text{ if } \tau \text{ does not divide } R, \\ &\equiv \tau \pmod{p} \text{ if } \tau \text{ divides } R, \end{aligned}$$

we obtain, on substituting in (15.1), the fundamental formulas

$$\begin{aligned} k_i &\equiv -\tau \sum_{m=1}^{p-1} \sum_{(r)} \frac{m!}{r_1!r_2!r_3!} \frac{A^{r_1} B^{r_2} C^{r_3}}{i^m} \pmod{p}, \\ (15.2) \quad k_0 &\equiv \tau \left(1 + \sum_{(r)} \frac{A^{r_1} B^{r_2} C^{r_3}}{r_1!r_2!r_3!} \right) \pmod{p}, \end{aligned}$$

where in the expression for k_i the summation variables satisfy the conditions

$$(D) \quad r_1 + r_2 + r_3 = m, \quad r_1 + pr_2 + p^2r_3 \equiv 0 \pmod{\tau},$$

while in the expression for k_0 ,

$$r_1 + r_2 + r_3 = p - 1, \quad r_1 + pr_2 + p^2r_3 \equiv 0 \pmod{\tau}.$$

For the principal cycle (S), $A = B = C = 1$ and the formulas (15.2) assume the simpler form

$$\begin{aligned} (15.3) \quad k_i &\equiv \tau \sum_{m=1}^{p-1} \sum_{(r)} \frac{m!}{r_1!r_2!r_3!i^m} \pmod{p}, \\ k_0 &\equiv \tau \left(1 + \sum_{(r)} \frac{1}{r_1!r_2!r_3!} \right) \pmod{p}. \end{aligned}$$

The problem of determining the residue of k_i modulo 3 offers very serious difficulties, principally because $U_0, U_1, \dots, U_{\tau-1}$ do not satisfy a difference equation when taken modulo 3. The only cases in which I have succeeded in determining the residue are given in the formulas (13.1) for the distribution function of the principal cycle (S), and their obvious extension to the remaining cycles of the block \mathfrak{B}_1 to which (S) belongs.

16. Applications. By applying the results of §14 on the solutions of the diophantine equations (D) to formulas (15.2) and (15.3), we obtain a number of interesting special cases. Throughout this section, (U) denotes a fixed cycle of $F(x)$ whose general term is $U_n \equiv A\alpha^n + B\beta^n + C\gamma^n \pmod{p}$, $A = K_0 + K_1\alpha + K_2\alpha^2$ etc., and whose distribution function is $k(n)$.

From formulas (6.11), (6.13),

$$(16.1) \quad ABC \equiv \Lambda(U_0, U_1, U_2)/\Delta \pmod{p},$$

where Λ is the polynomial defined in formula (6.12), and Δ is the discriminant of $F(x)$.

If $p \equiv 2 \pmod{3}$ and $\tau = p^2 + p + 1$, then by Theorem 14.1 formulas (15.2) become

$$\begin{aligned} k_i &\equiv \sum_{n=1}^{(p-2)/3} \frac{(3n)!}{(n!)^3} \left(\frac{\Lambda(U_0, U_1, U_2)}{\Delta i^3} \right)^n \pmod{p}, \\ k_0 &\equiv 1 \pmod{p}. \end{aligned}$$

Since in this case the residues of k_i modulo 3 are known, these formulas determine the distribution function $k(n)$ completely.

If $p \equiv 1 \pmod{3}$ and $\tau = (p^2 + p + 1)/3$, then on writing $p = 3N + 1$, $\tau \equiv 2N + 1 \pmod{p}$, and by Theorem 14.2, formulas (15.2) become

$$\begin{aligned} (16.2) \quad k_i &\equiv N \sum_{n=1}^N \frac{(3n)!}{(n!)^3} \left(\frac{\Lambda(U_0, U_1, U_2)}{\Delta i^3} \right)^n \pmod{p}, \\ k_0 &\equiv (2N + 1) \left(1 + \frac{(\Lambda(U_0, U_1, U_2))^N}{(N!)^3} \right) \pmod{p}. \end{aligned}$$

These formulas will determine the distribution function $k(n)$ for any cycle (U) belonging to the block \mathfrak{B} , since the residues of k_i modulo 3 are known. For the other blocks, the residues of k_i modulo 3 are unknown.

Formula (16.2) has some important consequences. We have seen in §10 that if $k_0^{(1)}, k_0^{(2)}, k_0^{(3)}$ are the number of zeros in three cycles $(U^{(1)}), (U^{(2)}), (U^{(3)})$ belonging to the blocks $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$ respectively, then $h_0^{(1)}, h_0^{(2)}, h_0^{(3)}$ are all distinct from one another. Hence if (U) is allowed to range over all the cycles of $F(x)$, we see from (16.1), (16.2) that $(ABC)^N$ must take three distinct values modulo p .

Since $(ABC)^{3N} \equiv 1 \pmod{p}$, $(ABC)^N \equiv \omega^a \pmod{p}$ where ω is a primitive cube root of unity modulo p , and the exponent a of ω depends on the block to which (U) belongs. In particular, for (S) , $ABC = 1$ so that $a = 0$. We thus obtain from (16.1) and formulas (6.11), (6.12) the following simple criterion to decide whether or not two triads belong to the same block.

THEOREM 16.1. *If $[A', B', C']$ and $[A'', B'', C'']$ are any two triads of $F(x)$ and if $F(x)$ has the period $(p^2 + p + 1)/3$, then a necessary and sufficient condition that $[A', B', C']$ and $[A'', B'', C'']$ belong to the same block is that $\Lambda(A', B', C')$ and $\Lambda(A'', B'', C'')$ have the same cubic character modulo p .*

For the cycle $(Z): 0, 0, 1, \dots, ABC \equiv (-1/\Delta) \pmod{p}$. Hence (Z) lies in \mathfrak{B}_1 when and only when $\Delta^N \equiv 1 \pmod{p}$. But obviously (Z) lies in \mathfrak{B}_1 when and

only when the cycle (S) contains two consecutive zeros; we thus obtain the following interesting theorem:

THEOREM 16.2. *If $p \equiv 1 \pmod{3}$ and $F(x)$ is any irreducible cubic with the period $\tau = (p^2 + p + 1)/3 \pmod{p}$, then the sequence $(S)_n$ of $F(x)$ will contain pairs of consecutive elements divisible by p when and only when the discriminant of $F(x)$ is a cubic residue of p .*

Formulas (15.1) serve to determine the distribution function for all the cycles of \mathfrak{B}_1 , regardless of the value of τ , but if the period τ is less than $(p^2 + p + 1)/3$, they become increasingly complicated as τ is taken smaller. The table at the close of §14 allows us to give explicit formulas for the residues of $k(n)$ modulo p when $\tau = (p^2 + p + 1)/7$. The simplest of these results is contained in the following theorem.

THEOREM 16.3. *If $\tau = (p^2 + p + 1)/7$, $p \equiv 2 \pmod{3}$ and if b_0 denotes the number of zeros in the principal cycle (S) , then*

$$b_0 \equiv (9L + 1) \left(1 + \frac{3}{(12L + 1)!6L!3L!} \right) \pmod{p}$$

or

$$b_0 \equiv (15L + 8) \left(1 + \frac{3}{(6L + 3)!(12L + 6)!(3L + 1)!} \right) \pmod{p}$$

according as p is of the form $21L + 2$ or $21L + 11$.

17. Determination of upper limit to distribution function. On account of the great increase in complexity in the formulas (15.2) as τ is taken smaller, it is desirable to have an upper limit to the number of times a given residue can appear in a given cycle. The results I have obtained in this connection are incomplete in the same sense as those I have obtained to determine $k(n)$; it is necessary to know this upper limit modulis p and 3, whereas I have determined it only modulo p . They suffice nevertheless to give an upper limit to the number of times the residue zero can appear in any cycle, and the number of times any residue can appear in the principal cycle.

We have seen, in §13, that if (U') is any sequence of $F'(x)$ of period τ' , where $\tau'k' = \tau$, the period of $F(x)$, then the terms of (U') consist of the r th, $(k'+r)$ th, $(2k'+r)$ th, \dots , $((\tau'-1)k'+r)$ th terms of some definite sequence (U) of $F(x)$ written usually in a different order. We shall now regard (U) , τ , and r as given, but τ' as unknown, and endeavor to obtain an upper limit to $k'(n)$, the distribution function of (U') . Let us take U_r, U_{r+1}, U_{r+2} as the initial values of (U) , which amounts to replacing (U) by the cycle (W) , where

$$W_n = U_{n+r} \quad (n = 0, 1, \dots, \tau - 1).$$

This change does not affect the distribution function $k(n)$ of (U) . Then if m_i denotes the number of times the residue i appears in those terms of (U) whose indices are prime to τ , it is apparent that

$$(17.1) \quad k_i' \leq k_i - m_i \quad (i = 0, 1, \dots, p-1).$$

m_i is determined if we know its residues modulis p and 3, in particular, m_0 is determined if we know its residue modulo p . Moreover, it is easily shown that if (W) belongs to the block of the principal cycle, $m_i \equiv 0 \pmod{3}$. We shall now determine m_i modulo p .

By Fermat's theorem, we have the fundamental formula

$$\phi(\tau) - m_i \equiv \sum_{(n,\tau)=1} (W_n - i)^{p-1} \pmod{p},$$

where the summation extends over all the terms of (W) whose subscripts are prime to τ , and $\phi(\tau)$ denotes as usual the totient of τ .

On proceeding as in §17, we find that, if $i \neq 0$,

$$\sum_{(n,\tau)=1} (W_n - i)^{p-1} \equiv \sum_{(n,\tau)=1} \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3} \alpha^{(r_1 + pr_2 + p^2 r_3)n},$$

where $r_1 + r_2 + r_3 = m$ and $W_n \equiv A\alpha^n + B\beta^n + C\gamma^n \pmod{p}$.

Now if $\mu(n)$ denotes Möbius' function, it is easily shown that

$$\begin{aligned} \sum_{(n,\tau)=1} \alpha^{Rn} &\equiv \mu(\tau) \pmod{p}, & \tau \text{ does not divide } R, \\ &\equiv \phi(\tau) \pmod{p}, & \tau \text{ divides } R. \end{aligned}$$

Hence after a slight transformation, we find that

$$\begin{aligned} \phi(\tau) - m_i &\equiv \mu(\tau) \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3} \\ &\quad + (\phi(\tau) - \mu(\tau)) \sum_{m=0}^{p-1} \sum_{(r)} \frac{(i)^{-m} m!}{r_1! r_2! r_3!} A^{r_1} B^{r_2} C^{r_3}, \end{aligned}$$

where in the first summation $r_1 + r_2 + r_3 = m$, but in the second summation

$$(D) \quad r_1 + r_2 + p^2 r_3 \equiv 0 \pmod{\tau}, \quad r_1 + r_2 + r_3 = m.$$

By the multinomial theorem, the first sum is found to be congruent modulo p to $\mu(\tau) [W_0(W_0 - i)]^{p-1}$.

Referring back to the formulas (15.2), the second sum is congruent to $(\phi(\tau) - \mu(\tau))(1 - k_i/\tau)$. Thus using the fact that $\kappa\tau = p^2 + p + 1 \equiv 1 \pmod{p}$, we obtain

$$(17.2) \quad m_i \equiv \kappa(\phi(\tau) - \mu(\tau))k_i + \epsilon\mu(\tau) \pmod{p},$$

where $\epsilon = -1$, if $W_0 = 0$ or i , $\epsilon = 0$, otherwise.

In a similar manner, we find that

$$(17.3) \quad m_0 \equiv \kappa(\phi(\tau) - \mu(\tau))k_0 + \epsilon'\mu(\tau) \pmod{p},$$

where $\epsilon' = 1$, $W_0 = 0$, $\epsilon' = 0$ otherwise.

Thus if τ has a square factor, we have the simple formula*

$$m_i \equiv \kappa\phi(\tau)k_i \pmod{p} \quad (i = 0, 1, \dots, p-1).$$

For $\tau = p^2 + p + 1$ or $(p^2 + p + 1)/3$, these formulas give a practicable determination of m_i for any given p .

* It is perhaps worth noting that p never divides $\phi(\tau)$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

CONDITIONS FOR THE SOLUBILITY OF THE DIOPHANTINE EQUATION $x^2 - My^2 = -1$ *

BY
MORGAN WARD

1. In this paper I apply the theory of Lucas' functions† to determine conditions‡ under which the well known diophantine equation

$$(1) \quad x^2 - N^2 Dy^2 = -1$$

is soluble for given integers§ N and D .

I show first of all that it is sufficient to consider (1) in the case when N is an odd prime P and D is square-free and not divisible by P . Suppose that $N=P$. Clearly, a necessary condition that (1) be soluble is that the equation

$$(2) \quad x^2 - Dy^2 = -1$$

be soluble. If D is not a quadratic residue of P , this condition is also sufficient for the solubility of (1). However, if D is a quadratic residue of P , the following additional restriction must hold.

Let (u, v) be the least positive integral solution of (2), and suppose that P is of the form $2^{k+1}(2M+1)+1$ with $\mathbb{P}(D|P) = +1$. Then in order that (1) be soluble it is necessary and sufficient that

$$(3) \quad (u + vD^{1/2})^{(P-1)/2k} \equiv -1 \pmod{P}.$$

In case P is of the form $8M+5$, (3) may be replaced by the following condition. Let

$$P = (a + bi)(a - bi), \quad u + i = \epsilon\zeta \prod (\alpha + \beta i) \quad (a, \alpha \text{ odd})$$

be the decomposition of P and $u+i$ into primary factors in the field $\mathfrak{F}(i = (-1)^{1/2})$. Here ζ is equal to 1 or $1+i$ according as the norm of $u+i$ is odd or even, and ϵ is a unit chosen so that the integers α are all odd. Then a necessary and sufficient condition that (1) be soluble is that

$$(4) \quad \prod (a + bi | \alpha + \beta i) = (\epsilon\zeta | a + bi).$$

* Presented to the Society, April 11, 1931; received by the editors March 3, 1931.

† A recent paper by D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–448, gives references to the literature on these functions.

‡ Very few general conditions are known. See Dickson's *History*, vol. 2, chapter XII.

§ On considering (1) modulo 8, it is obvious that N must be odd and D or $D/2$ odd for a solution to exist. Furthermore, every odd prime factor of $N^2 D$ must be of the form $4n+1$.

¶ $(A | B)$ denotes as usual the quadratic character of A with respect to B .

If P is of the form $8M+1$, this condition is necessary, but not sufficient, for the solubility of (1).

For a given value of D , (4) gives an easily applied criterion for the solubility of (1). Its use is illustrated in the closing sections of the paper for the case $D=5$.

2. To prove these statements, consider equations (1) and (2), where we assume that (2) is soluble and that N is odd. If (u, v) is the least positive integral solution of (2), every other solution is given by the formula

$$r_n + D^{1/2}s_n = (u + vD^{1/2})^n \quad (n = \pm 1, \pm 3, \pm 5, \dots).$$

Hence a necessary and sufficient condition that (1) be soluble is that there exist an odd n such that

$$s_n \equiv 0 \pmod{N}.$$

Now let $\gamma = u + vD^{1/2}$, $\delta = u - vD^{1/2}$ so that $\gamma + \delta = 2u$, $\gamma - \delta = 2vD^{1/2}$, $\gamma\delta = -1$.

Then $r_n + s_nD^{1/2} = \gamma^n$, $r_n - s_nD^{1/2} = \delta^n$ so that $2r_n = V_n$, $s_n = vU_n$ where

$$V_n = \gamma^n + \delta^n, \quad U_n = \frac{\gamma^n - \delta^n}{\gamma - \delta}$$

are the Lucas functions associated with the quadratic equation

$$x^2 - 2ux - 1 = 0.$$

Thus if $N = md$, $v = v'd$, $(m, v') = 1$, $s_n \equiv 0 \pmod{N}$, when and only when $U_n \equiv 0 \pmod{m}$.

Now let $\mu(m)$ denote the least positive value of n such that $U_n \equiv 0 \pmod{m}$. We shall refer to this number as the rank of apparition of m in $(U)_n$. Its more important properties are as follows.*

- I. U_n is divisible by m when and only when n is divisible by $\mu(m)$.
- II. If a and b are co-prime, $\mu(ab)$ is the least common multiple of $\mu(a)$ and $\mu(b)$. Consequently
- III. If $m = p_1^{a_1} \cdots p_k^{a_k}$ is the decomposition of m into its prime factors, then $\mu(m)$ is the least common multiple of $\mu(p_1^{a_1}), \dots, \mu(p_k^{a_k})$.
- IV. If m is a prime p , and $(D|p)$ denotes the quadratic character of D with respect to p , then $\mu(p)$ divides $p - (D|p)$ and $\mu(p^a) = p^b\mu(p)$, $b \leq a - 1$.
- V. If m is odd, $\mu(m)$ is odd when and only when all of the V_n are prime to m .

The first property of $\mu(m)$ gives us immediately the following theorem.

* D. H. Lehmer paper cited.

THEOREM. *If (u, v) is the least positive integral solution of*

$$(2) \quad x^2 - Dy^2 = -1$$

and $N = md$, $v = v'd$; N odd and $(m, v') = 1$, then a necessary and sufficient condition that the equation

$$(1) \quad x^2 - N^2 Dy^2 = -1$$

be soluble is that the rank of apparition of m in the Lucas function $(U)_n$ associated with the quadratic equation $x^2 - 2ux - 1 = 0$ be odd.

3. The question of the solubility of (1) is thus reduced to the problem of determining the parity of $\mu(m)$ for any odd m . It follows from III and IV that if

$$m = p_1^{a_1} \cdots p_k^{a_k}$$

is the decomposition of m into its prime factors, $\mu(m)$ is odd when and only when $\mu(p_1), \dots, \mu(p_k)$ are all odd. Since if p divides D , $(D|p)=0$ and $\mu(p)$ divides p , we can assume that m is prime to D .

Thus it is sufficient to discuss the solubility of (1) when D is square-free, and N is a prime P of the form $4n+1$ not dividing vD . We shall therefore replace (1) by

$$(5) \quad x^2 - P^2 Dy^2 = -1, \quad (P, vD) = 1, \quad P \text{ a prime, } D \text{ square-free,}$$

where

$$(6) \quad P = 2^{k+1}(2M + 1) + 1, \quad k \geq 1.$$

From V we have immediately the following theorem.

THEOREM. *If $x^2 - Dy^2 = -1$ is soluble, and P is an odd prime, then at most one of the equations*

$$x^2 - P^2 Dy^2 = -1, \quad P^2 x^2 - Dy^2 = -1$$

is soluble.

Suppose that $(D|P) = -1$. Since $(P+1)/2$ is odd, we see from IV that $\mu(P)$ is odd when and only when $\mu(P)$ divides $(P+1)/2$; that is, when and only when

$$(7) \quad U_{(P+1)/2} \equiv 0 \pmod{P}.$$

Referring back to the equations in §2 defining U_n , we see that (7) holds when and only when the congruence

$$\gamma^{P+1} \equiv -1 \pmod{P}$$

holds in the Galois field of order P^2 associated with the root γ of $x^2 - 2ux - 1 = 0$. But

$$\gamma^{P+1} = (u + vD^{1/2})^{P+1} \equiv u^{P+1} + v^{P+1}D^{(P+1)/2} \equiv u^2 - Dv^2 \equiv -1 \pmod{P}.$$

We thus have established the following result:

THEOREM. *If P is a prime of the form $4n+1$ such that $(D|P) = -1$, the diophantine equation $x^2 - P^2Dy^2 = -1$ is soluble when and only when the diophantine equation $x^2 - Dy^2 = -1$ is soluble.*

4. The case when $(D|P) = +1$ is considerably more difficult. Since $(P-1)/2^{k+1}$ is odd, $\mu(P)$ is odd when and only when $\mu(P)$ divides $(P-1)/2^{k+1}$. This condition is easily shown to be equivalent to the criterion stated in §1,

$$(3) \quad (u + vD^{1/2})^{(P-1)/2k} \equiv -1 \pmod{P}.$$

It is now necessary to discuss separately the increasingly more complicated cases* $k = 1, 2, 3, 4, \dots$, corresponding to primes of the form $8n+5$, $16n+9$, $32n+17$, $64n+33$, \dots .

I shall confine myself here to the simplest case $k=1$ where the criterion (3) can be put into a much more manageable form.

Suppose then that

$$(8) \quad (u + vD^{1/2})^{(P-1)/2} \equiv -1 \pmod{P}, \text{ where } P = 8M + 5 \text{ and } (D|P) = +1.$$

(8) is equivalent to saying that the congruences

$$(8.1) \quad x^2 \equiv u + vD^{1/2}, \quad \bar{x}^2 \equiv u - vD^{1/2} \pmod{P}$$

have no solutions. Now let

$$x = \kappa + \lambda D^{1/2}, \quad \bar{x} = \kappa - \lambda D^{1/2}.$$

Then the congruences (8.1) are insoluble when and only when the congruences

$$\kappa^2 + \lambda^2 D \equiv u, \quad 2\kappa\lambda \equiv v, \quad u^2 - v^2 D \equiv -1 \pmod{P}$$

are insoluble. On eliminating λ and v , we obtain

$$(2\kappa^2 - u)^2 + 1 \equiv 0 \pmod{P}.$$

Hence if $w^2 \equiv -1 \pmod{P}$, $4\kappa^2 \equiv 2(u \pm w) \pmod{P}$. On recalling that P is of the form $8M+5$, we see that the congruences (8.1) are insoluble when and only when the congruence

$$z^2 \equiv u \pm w \pmod{P}$$

* For the case $k=2$, $D=2$, $u=v=1$, see a paper by Perott, *Sur l'équation $t^2 - Du^2 = -1$* , Crelle's Journal, vol. 102 (1888), pp. 185-223.

is soluble. Since $(u+w)(u-w) \equiv u^2 + 1 \equiv v^2D \pmod{P}$, $u+w$ and $u-w$ have the same quadratic character modulo P . Hence a necessary and sufficient condition that (8) should hold is that

$$(9) \quad \left(\frac{u+w}{P} \right) = +1 \text{ where } w^2 \equiv -1 \pmod{P}.$$

By passing into the field $\mathfrak{F}(i)$, $i^2 = -1$, we can apply the reciprocity law* to simplify the criterion (9). Suppose that

$$P = (a+bi)(a-bi), \text{ } a \text{ odd},$$

is the decomposition of P into primary factors in $\mathfrak{F}(i)$.

Since

$$(u+i|a-bi) = (u-i|a+bi) \text{ and } (u+i|a+bi) = (u-i|a+bi),$$

a necessary and sufficient condition that (9) should hold is that

$$(10) \quad (u+i|a+bi) = +1.$$

Let

$$u+i = \epsilon\zeta \prod (\alpha + \beta i)$$

be the decomposition of $u+i$ into primary factors in $\mathfrak{F}(i)$ where $\zeta = 1$ or $1+i$ according as the norm of $u+i = v^2D$ is even or odd and ϵ is a unit so chosen that the α are all odd. Then by the reciprocity law in $\mathfrak{F}(i)$,

$$(u+i|a+bi) = (\epsilon\zeta|a+bi) \prod (a+bi|\alpha+\beta i).$$

If P is a prime of the form $8n+1$ and $(D|P) = +1$, we see from (3) of the previous theorem that a necessary condition that $x^2 - P^2Dy^2 = -1$ be soluble is that

$$(u+vD^{1/2})^{(P-1)/2} \equiv 1 \pmod{P}.$$

On proceeding as in the previous case, we find that this condition is again equivalent to the criterion

$$(u+i|a+bi) = +1.$$

Hence we have the following theorem.

THEOREM. *Let (u, v) be the least positive integral solution of the diophantine equation*

$$(2) \quad x^2 - Dy^2 = -1$$

and let P be a prime of the form $4n+1$ such that $(D|P) = +1$, $(v, P) = 1$.

* Bachmann, *Kreistheilung*, Lecture 13.

Then if

$$P = (a + bi)(a - bi), u + i = \epsilon \zeta \prod (\alpha + \beta i)$$

(a, α odd; ϵ a unit; $\zeta = 1$ or $1+i$) are the decompositions of P and $u+i$ into primary factors in the field $\mathfrak{F}(i)$, a necessary condition that the diophantine equation

$$(5) \quad x^2 - P^2 Dy^2 = -1$$

be soluble is that

$$(4) \quad \prod (a + bi | \alpha + \beta i) = (\epsilon \zeta | a + bi).$$

If P is of the form $8M+5$, this condition is also sufficient for the solubility of (5).

5. We shall now apply our results to the case $D=5$. Here $u=2$, $v=1$ so that the norm of $u+i=5$, and $\alpha=1$, $\beta=-2$, $\zeta=1$, $\epsilon=i$. (4) becomes simply

$$(a + bi | 1 - 2i) = (i | a + bi) \begin{cases} = -1, P \equiv 5 \pmod{8}, \\ = +1, P \equiv 1 \pmod{8}. \end{cases}$$

We easily find that the square of any integer in $\mathfrak{F}(i)$ is congruent modulo $1 - 2i$ to 0 , ± 1 or $\pm 2i$; moreover since $P=a^2+b^2$ is a quadratic residue of 5 , we must have either $a \equiv 0$ or $b \equiv 0 \pmod{5}$. Hence

$$(a + bi | 1 - 2i) = +1 \begin{cases} b \equiv 0, a \equiv \pm 1, P \equiv 1 \pmod{5}, \\ a \equiv 0, b \equiv \pm 2, P \equiv 4 \pmod{5}, \end{cases}$$

$$(a + bi | 1 - 2i) = -1 \begin{cases} b \equiv 0, a \equiv \pm 2, P \equiv 4 \pmod{5}, \\ a \equiv 0, b \equiv \pm 1, P \equiv 1 \pmod{5}. \end{cases}$$

Now every odd prime save 5 must belong to one of the forms

$$40n + 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39.$$

Hence if P is of the form

$$40n + 3, 7, 11, 19, 23, 27, 31, 39,$$

the diophantine equation

$$(11) \quad x^2 - 5P^2 y^2 = -1$$

is insoluble, since $P \equiv 3 \pmod{4}$, while if P is of the form

$$40n + 13, 17, 33, 37,$$

(11) is soluble since P is then a non-residue of 5 .

There are left primes of the forms

$$40n + 21, 40n + 29 \text{ and } 40n + 1, 40n + 9$$

congruent to 5 and 1 modulo 8 respectively. For such primes, we have from the results just given the following remarkable theorem:

THEOREM. Let $P = a^2 + b^2$ be the representation of any prime of the forms $40n+1, 9, 21, 29$ as the sum of two squares, where a is assumed to be odd. Then a necessary condition that the diophantine equation

$$(11) \quad x^2 - 5P^2y^2 = -1$$

be soluble is given by the following table:

Residue of $P \pmod{40}$	Criterion for solubility
1	$b \equiv 0 \pmod{5}$
9	$a \equiv 0 \pmod{5}$
21	$a \equiv 0 \pmod{5}$
29	$b \equiv 0 \pmod{5}$.

In the last two cases, this criterion is also sufficient for the solubility of (11).

In the concluding table, we apply this theorem to all the primes of the four forms considered less than 1000. Soluble cases are marked with S, insoluble with I and doubtful with ?. In conjunction with our previous results, we see that for the 168 primes < 1000 , we are left in doubt as to the solubility of (11) only in the six cases $P = 89, 401, 521, 761, 769$ and 809 .

Table of Primes of the Form $40n+1, 9, 21, 29$ Less than a Thousand

$P = 40n+1$	$a^2+b^2,$ $a \text{ odd}$	$5P^2$		$P = 40n+9$	$a^2+b^2,$ $a \text{ odd}$	$5P^2$	
41	5^2+4^2	8405	I	89	5^2+8^2	39605	?
241	15^2+4^2	290405	I	409	3^2+20^2	836405	I
281	25^2+4^2	394805	I	449	7^2+20^2	1008005	I
401	1^2+20^2	804005	?	569	13^2+20^2	1618805	I
521	11^2+20^2	1357205	?	769	25^2+12^2	2956805	?
601	5^2+24^2	1806005	I	809	5^2+28^2	3272405	?
641	25^2+4^2	2054405	I	929	23^2+20^2	4315205	I
761	19^2+20^2	2895605	?				
881	25^2+16^2	3880805	I				
$P = 40n+21$				$P = 40n+29$			
61	5^2+6^2	18605	S	29	5^2+2^2	4205	I
101	1^2+10^2	51005	I	109	3^2+10^2	59405	S
181	9^2+10^2	163805	I	149	7^2+10^2	111005	S
421	15^2+14^2	886205	S	229	15^2+2^2	262205	I
461	19^2+10^2	1062605	I	269	13^2+10^2	361805	S
541	21^2+10^2	1463405	I	349	5^2+18^2	609005	I
661	25^2+6^2	2184605	S	389	17^2+10^2	756605	S
701	5^2+26^2	2457005	S	509	5^2+22^2	1294055	I
821	25^2+14^2	3370205	S	709	15^2+22^2	2513405	I
941	21^2+20^2	4427405	I	829	27^2+10^2	3436205	S

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

Chapter 6

1932

Annals of Mathematics

The Linear Form of Numbers Represented by a Homogeneous Polynomial in Any Number of Variables

Author(s): Morgan Ward

Source: *Annals of Mathematics*, Second Series, Vol. 33, No. 2 (Apr., 1932), pp. 324-326

Published by: [Annals of Mathematics](#)

Stable URL: <http://www.jstor.org/stable/1968334>

Accessed: 15/11/2014 00:25

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at
<http://www.jstor.org/page/info/about/policies/terms.jsp>

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



Annals of Mathematics is collaborating with JSTOR to digitize, preserve and extend access to *Annals of Mathematics*.

<http://www.jstor.org>

THE LINEAR FORM OF NUMBERS REPRESENTED
BY A HOMOGENEOUS POLYNOMIAL IN
ANY NUMBER OF VARIABLES.¹

BY MORGAN WARD.

1. In this paper I obtain the following necessary conditions that all of the numbers properly represented by a homogeneous polynomial in any number of variables may be of one or the other² of the linear forms

$$(1) \quad nz, \quad nz + a_1, \dots, \quad nz + a_r.$$

n here is any integer, and a_1, \dots, a_r are r distinct integers less than n and prime to it.³

THEOREM 1. *If all of the numbers properly represented by the homogeneous polynomial of degree N*

$$(2) \quad H = H(x_1, x_2, \dots, x_k) = \sum_{(s)} h_{(s)} x_1^{s_1} \cdot x_2^{s_2} \cdots x_k^{s_k}$$

(all the $h_{(s)}$ integers)

are of one or the other of the forms (1), and if

$$n = p_1^{b_1} \cdots p_L^{b_L}$$

is the resolution of n into its prime factors, then it is necessary that the least common multiple of the numbers

$$p_1^{b_1-1}(p_1 - 1), \dots, p_L^{b_L-1}(p_L - 1)$$

divide rN .

We shall denote this least common multiple by $\lambda(n)$.

THEOREM 2. *Under the hypotheses of Theorem 1, the r numbers a_1, \dots, a_r in (1) must form q complete co-sets of the group G_r of the N^{th} powers of the elements in the totient group of n .*

¹ Received January 21 and April 13, 1931.

² The form nz may be omitted without invalidating the theorems. Each of the other forms is assumed actually to occur.

³ The problem becomes rather unwieldy if we remove the restriction that the a_i be prime to n . The simplest case is when all the numbers representable by the form are divisible by n ; for polynomials in two variables, we have essentially the problem of determining all residual polynomials modulo n . See Dickson, *Introduction to the Theory of Numbers*, Chicago, (1929), Chapter II.

From Theorem 1, we see that⁴ $\lambda(n) \leq rN$. Since $\lambda(n)$ tends to infinity with n , we have the following corollary:

COROLLARY. *For a given r and N in (1) and (2), there are only a finite number of values of n satisfying the hypotheses of Theorem 1.*

Furthermore, we see from Theorem 2 that we must have

$$(3) \quad r = \tau,$$

where τ is the order of the group G_τ .

2. Theorem 2 is readily established as follows.

Assume that the hypotheses of Theorem 1 are satisfied. Then for each a_i we can find a set of co-prime integers c_1, c_2, \dots, c_k such that⁵

$$H(c_1, c_2, \dots, c_k) \equiv a_i \pmod{n}, \quad (a_i, n) = 1.$$

Let s denote any integer prime to n . Then it is possible to choose k integers z_1, z_2, \dots, z_k so that the numbers

$$d_1 = z_1 n + s c_1, \quad d_2 = z_2 n + s c_2, \quad \dots \quad d_r = z_r n + s c_r$$

are co-prime. The number $m = H(d_1, d_2, \dots, d_r)$ is accordingly properly represented by the form H . Hence since H is homogeneous of degree N ,

$$m \equiv s^N H(c_1, c_2, \dots, c_r) \equiv s^N a_i \not\equiv 0 \pmod{N}.$$

But m must be congruent modulo n to some one of the a_i ; therefore the numbers

$$(4) \quad s^N a_i, \quad (i = 1, 2, \dots, r), \quad (s, n) = 1,$$

are all congruent modulo n to one or the other of the numbers a_i in (1).

Now if $G_{\varphi(n)}$ denotes the totient group of n , the N th powers of all the elements of $G_{\varphi(n)}$ form a sub-group G_τ of order $\tau \leq \varphi(n)$. Hence for a given a_i , the numbers (4) are congruent modulo n to the τ numbers of some co-set of G_τ in $G_{\varphi(n)}$. Since the numbers a_i are all distinct and all in $G_{\varphi(n)}$, Theorem 2 follows.

The proof of Theorem 1 is now immediate. For if g is any element of G_τ , $g^\tau \equiv 1 \pmod{n}$. Hence since the elements of G_τ are congruent to the N th powers of the elements of $G_{\varphi(n)}$, $s^{N\tau} \equiv 1 \pmod{n}$, so that by (3)

⁴ That rN is actually the “best possible” maximum for $\lambda(n)$ is shown by the case $N = 3, r = 2, n = 7, a_1 = 1, a_2 = 6$. For $H = (x_1 + x_2 + \dots + x_k)^3$, we find that $\lambda(n) = rN = 6$.

⁵ We use when convenient the standard notation (a, b, \dots, c) for the greatest common divisor of the numbers a, b, \dots, c .

$$s^{rN} \equiv 1 \pmod{n}$$

for every integer s prime to n .

Accordingly, if $\lambda(n)$ is the least positive value of u such that $s^u \equiv 1 \pmod{n}$ for all integers s prime to n , $\lambda(n)$ divides rN .

But if $n = p_1^{b_1} \cdots p_L^{b_L}$ is the resolution of n into its prime factors, $\lambda(n)$ is precisely⁶ the L. C. M. of $p_1^{b_1-1}(p_1-1), \dots, p_L^{b_L-1}(p_L-1)$.

3. As an application of these theorems, let us consider the problem⁷ of obtaining primitive binary forms

$$H(x_1; x_2) = \sum_{s=0}^N h_s x_1^{N-s} x_2^s$$

of degree N such that the prime factors of all of the numbers properly represented by H are either divisors of n or of the form $nz \pm 1$ (so that n is necessarily even). Examples of such forms, due to Lehmer, place cited, are $x^8 + 16x^2y - 51xy^2 - y^3$ for $n = 14$ and $x^8 - 18x^2y + 69xy^2 - y^3$ for $n = 18$.

These forms are obviously included in the more general category of forms which properly represent only numbers of the types nz , $nz + a_1$, $nz + a_2$ with a_1, a_2 prime to n . Hence by Theorem 1 and equation (3), we must have $\lambda(n)$ a divisor of $2N$ and $\tau \leq 2$.

For example, suppose that $N = 3$. $\lambda(n) = 1$ has the solution $n = 2$; $\lambda(n) = 2$ the four solutions 3, 4, 6, 12 while $\lambda(n) = 6$ has the twelve solutions 7, 9, 14, 18, 21, 28, 36, 42, 63, 84, 126, 252. Of the even values of n , the cases $n = 2, 4$ and 6 are trivial since every prime save 2 is of the form $2k+1$ and $4k \pm 1$ and every prime save 2 and 3 is of the form $6k \pm 1$. On the other hand in the cases 12, 28, 36, 42, 84, 126 and 252, $\tau > 2$. Hence $n = 14$ and $n = 18$ are the only non-trivial values of n for which such cubic forms can exist. In a similar manner one can show that 22 is the only non-trivial value of n for which such quintic forms can exist, and that there are no non-trivial values of n for septic forms.

⁶ Dickson, Work cited, p. 15.

⁷ See D. H. Lehmer, An Extended Theory of Lucas' Functions. Annals, Vol. 31 (1930), p. 436. Dr. Lehmer has informed me that since the paper was written he has considerably extended his results on this problem.

ON THE BEHAVIOR OF NON-STATIC MODELS OF THE
UNIVERSE WHEN THE COSMOLOGICAL TERM
IS OMITTED

BY RICHARD C. TOLMAN AND MORGAN WARD

CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA

(Received January 22, 1932)

ABSTRACT

If the cosmological term in the equations of relativistic mechanics is set equal to zero, it has been shown by Einstein that a non-static model of the universe filled with a homogeneous distribution of incoherent matter would expand to a maximum volume and then start contracting. This, however, is a very special model of the universe filled with a highly simplified fluid, and subjected to changes which can be shown to be thermodynamically reversible; and it has recently been pointed out by one of the present authors that we can also expect a similar expansion to a maximum volume with much more general models of the universe allowing irreversible as well as reversible changes in the fluid filling the model. The present article gives a somewhat detailed analysis of the behavior of a wide class of non-static models of the universe when the cosmological term is set equal to zero, and shows that we may expect a continued succession of expansions and contractions without reference to the reversible or irreversible nature of the processes taking place in the fluid filling the model. The bearings of this finding on the problems of relativistic thermodynamics, which have already been treated by one of the present authors, are again noted.

§ 1. Introduction. Einstein's original equations connecting the distribution of matter and energy with the space-time metric of general relativity can be written in the form

$$-8\pi T_{\mu\nu} = G_{\mu\nu} - \frac{1}{2}Gg_{\mu\nu} \quad (1)$$

where $T_{\mu\nu}$ is the energy-momentum tensor, $G_{\mu\nu}$ is the contracted Riemann-Christoffel tensor, and $g_{\mu\nu}$ the fundamental metrical tensor. The choice of these equations as a starting point for relativistic mechanics has considerable justification. In empty space, they reduce to

$$G_{\mu\nu} = 0 \quad (2)$$

which has the support provided by the three well-known crucial tests of the general theory of relativity. In weak static gravitational fields, only one of the ten equations, that with $\mu=\nu=4$, is of importance and this can then be shown to reduce to Poisson's equation

$$4\pi\rho = \frac{\partial^2\psi}{\partial x^2} + \frac{\partial^2\psi}{\partial y^2} + \frac{\partial^2\psi}{\partial z^2} \quad (3)$$

where ρ is the density of matter and ψ the ordinary Newtonian gravitational potential. And finally, the energy-momentum tensor $T_{\mu\nu}$ is a quantity whose divergence we wish to have equal to zero on physical grounds while the

combination on the right-hand side of (1) is a quantity whose divergence is known to be identically equal to zero.

As is well-known the original equations given above were later modified by Einstein's addition of the so-called cosmological term to read

$$-8\pi T_{\mu\nu} = G_{\mu\nu} - \frac{1}{2}Gg_{\mu\nu} + \Lambda g_{\mu\nu} \quad (4)$$

where the cosmological constant Λ is a quantity independent of the spatial and temporal coordinates, which would have to be regarded as a new fundamental constant of nature.

At the time the reason for making such a change appeared to be twofold. In the first place, by adding the cosmological term there was obtained the most general possible function, of the gravitational potentials $g_{\mu\nu}$ and their first and second differential coefficients, the divergence of which is identically equal to zero. In the second place, without the cosmological term it was impossible to construct a static model of the universe containing a finite density of matter; but by adding the cosmological term it became possible to obtain Einstein's well known static model for the universe, with reasonable values for the density of matter and radius of the model, and no disagreement with the three observational tests of the theory, provided Λ was taken as a small positive quantity.

More recently, however, the arguments in favor of changing from the original form of the equations as given by (1) have seemed less strong. In the first place, we know that Λ must in any case be a very small quantity in order to agree with the three crucial tests of the theory of relativity, and we should certainly prefer to take it equal to zero merely in the interests of simplicity and definiteness. In the second place, if we do not set Λ equal to zero, we have to inquire into the significance and magnitude of this new fundamental constant of nature, and the results of such inquiry have so far not seemed very satisfactory. Finally, it now appears evident, both from theoretical and observational points of view,¹ that non-static models of the universe are to be preferred to static models, and it is entirely possible to construct satisfactory non-static models of the universe without introducing the cosmological term, a fact that has recently been specially pointed out and emphasized by Einstein himself.²

For these reasons it becomes a matter of some interest to consider the consequences of omitting the cosmological term from the equations of relativistic mechanics, even though in the interests of generality we must continue to keep in mind the possibility that Λ may not be exactly equal to zero.

§2. Purpose of the Present Article. The purpose of the present article is to consider the general behavior of non-static models of the universe, setting

¹ On the theoretical side, as pointed out by Tolman, Proc. Nat. Acad. **16**, 320 (1930), we cannot have a static universe if matter is changing over into radiation, and as pointed out by Eddington, Monthly Notices R.A.S. **90**, 668 (1930), we cannot regard the Einstein static universe as stable. On the observational side, the red shift in the light from the extra-galactic nebulae indicates a non-static universe as first appreciated by Lemaître, Ann. Societe Sci. Bruxelles **47**, Series A, 49 (1927).

² Einstein, Berl. Ber. (1931), p. 235.

the cosmological term equal to zero, and making only very general assumptions as to the nature of the fluid which fills the model, and as to the nature of the processes which occur in this fluid as the model expands or contracts.

In the article of Einstein referred to above, it was shown that on setting Λ equal to zero we must expect a non-static model of the universe, filled with incoherent matter exerting no pressure, to expand to a maximum volume and then to start contracting. This, however, was a very special model of the universe, filled with a highly simplified fluid, and subjected only to changes which can be shown to be thermodynamically reversible,³ and it might be questioned whether we could expect a similar behavior in the case of less simple fluids and models in which irreversible processes might take place. Nevertheless, it has been pointed out in a recent article by one of us⁴ that we can also expect such expansion to a maximum followed by contraction in the case of any model of the universe filled with a homogeneous distribution of fluid exerting a positive pressure, provided we set the cosmological term equal to zero. In the present article this behavior will be considered in more detail.

In the next section, §3, we shall give those mechanical equations governing the behavior of non-static universes which will be needed later. In §4, we shall then prove for any such non-static model of the universe, filled with a fluid which could exert only positive pressures, and having initially a finite volume and finite rate of expansion, that there would be a finite upper boundary beyond which the volume could not expand. Continuing in §5, we shall then show that the model would reach its maximum upper volume in a finite time and would then start contracting. And in §6, we shall show that the equations would thereafter require the contraction to continue to zero volume which would also be reached within a finite time. In §7, we shall then discuss this mathematical conclusion that the model would contract down to the exceptional point of zero volume, and show from a physical point of view that we might expect contraction to the lower limit to be followed by a renewed expansion. Finally in §8, we shall make some remarks concerning the possible application of these conclusions as to the behavior of highly idealized models, in interpreting the behavior of the actual universe.

§3. The Mechanics of the Non-Static Universe. An expression for the line element for a non-static model of the universe filled with a homogeneous distribution of fluid with properties which are independent of position but dependent on the time, can be derived⁵ and written in the form

$$ds^2 = -\frac{e^{g(t)}}{[1 + r^2/4R^2]^2} (dr^2 + r^2 d\theta^2 + r^2 \sin^2 \theta d\phi^2) + dt^2 \quad (5)$$

where r , θ and ϕ are the spatial coordinates, t is the time coordinate, R is a constant, and the dependence of the line element on the time is given by the exponent $g(t)$.

³ Tolman, Phys. Rev. 38, 1758 (1931). See 9.

⁴ Tolman, Phys. Rev. 39, 320 (1932).

⁵ Tolman, Proc. Nat. Acad. 16, 320 (1930).

For the proper pressure p_0 and proper macroscopic density ρ_{00} corresponding to this line element we can write in accordance with the principles of relativistic mechanics⁶

$$8\pi p_0 = -\frac{1}{R^2} e^{-g} - \frac{3}{4}\dot{g}^2 + \Lambda \quad (6a)$$

$$8\pi\rho_{00} = \frac{3}{R^2} e^{-g} + \frac{3}{4}\dot{g}^2 - \Lambda \quad (7a)$$

provided we retain the cosmological term, or

$$8\pi p_0 = -\frac{1}{R^2} e^{-g} - \ddot{g} - \frac{3}{4}\dot{g}^2 \quad (6b)$$

$$8\pi\rho_{00} = \frac{3}{R^2} e^{-g} + \frac{3}{4}\dot{g}^2 \quad (7b)$$

if we set the cosmological term equal to zero, as is of prime interest for the present article. The pressure and density are independent of position and dependent as shown on the exponent $g(t)$ and its time derivatives \dot{g} and \ddot{g} .

With the above choice of coordinates particles which are at rest with respect to r , θ and ϕ will not be subject to gravitational acceleration, so that we can regard the fluid as macroscopically at rest in these coordinates. As g changes with the time, however, the proper volume

$$\delta V_0 = \frac{r^2 \sin \theta e^{3g/2}}{[1 + r^2/4R^2]^3} \delta r \delta \theta \delta \phi \quad (8)$$

associated with a small range in coordinates $\delta r \delta \theta \delta \phi$, and the total integrated proper volume of the model⁷

$$V_0 = \pi^2 R^3 e^{3g/2} \quad (8a)$$

will change with the time. Hence we can describe the changes that take place in such a universe, as g increases or decreases, as expansions or contractions in the proper volume of the elements of fluid which fill the model, and in the total proper volume of the model.

Furthermore, in accordance with the expressions for pressure and density we can easily obtain the relation⁸

$$\frac{d}{dt} (\rho_{00} \delta V_0) + p_0 \frac{d}{dt} (\delta V_0) = 0 \quad (9)$$

which shows that the change in the energy content of any given small element of the fluid, as measured by a local observer using proper coordinates, will be found equal to the negative of the work performed on the surroundings.

⁶ Reference 5, Eqs. 34.

⁷ Tolman, Phys. Rev. 37, 1652 (1931). Eq. (28).

⁸ Tolman, Proc. Nat. Acad. 16, 409 (1930). Eq. (4).

§4. *The Upper Boundary of Expansion.* Let us now consider such a model of the universe filled with a mixture of matter and radiation which might exert a positive pressure

$$p_0 \geq 0 \quad (10)$$

but cannot withstand tension. And at some initial time $t=0$ let the model have a finite volume and finite rate of expansion corresponding to

$$g = g_0 \text{ and } \dot{g} = \dot{g}_0 \quad (11)$$

where g_0 is finite and \dot{g}_0 is finite and positive. We shall first show, with $\Lambda=0$, that there will be a finite upper volume beyond which the expansion cannot go, that is a finite upper boundary for the quantity g .

Combining equation (6b) with the inequality (10), we can write in general

$$\ddot{g} + \frac{3}{4}\dot{g}^2 + \frac{1}{R^2}e^{-g} \leq 0. \quad (12)$$

Furthermore, since \dot{g} will be positive as long as expansion continues we can multiply (12) by the positive quantity $2e^{3g/2}\dot{g}$ and write

$$2e^{3g/2}\ddot{g}\dot{g} + \frac{3}{2}e^{3g/2}\dot{g}^3 + \frac{2}{R^2}e^{g/2}\dot{g} \leq 0 \quad (13)$$

or

$$\frac{d}{dt}(e^{3g/2}\dot{g}^2) + \frac{4}{R^2}\frac{d}{dt}(e^{g/2}) \leq 0 \quad (14)$$

as an expression which will continue to hold as long as g continues to increase.

Integrating (14) between $t=0$ and any later time of interest $t=t$, and substituting the values for g and \dot{g} at time $t=0$ as given by (11), we obtain

$$e^{3g/2}\dot{g}^2 + \frac{4}{R^2}e^{g/2} \leq e^{3g_0/2}\dot{g}_0^2 + \frac{4}{R^2}e^{g_0/2} \quad (15)$$

or, taking the constant R as real for the models in which we shall be interested,

$$e^{g/2} \leq \frac{R^2}{4}e^{3g_0/2}\dot{g}_0^2 + e^{g_0/2} - \frac{R^2}{4}e^{3g/2}\dot{g}^2 \quad (16)$$

as an expression which will hold as long as g continues to increase. Since g_0 and \dot{g}_0 are, however, finite by hypothesis this shows that there is an upper finite boundary say γ which g cannot surpass. So that we can necessarily write

$$g \leq \gamma \quad (17)$$

where γ is finite.

§5. *Time Necessary to Reach the Maximum.* From the inequality (17) we can then evidently write

$$-\frac{1}{R^2}e^{-g} \leq -\frac{1}{R^2}e^{-\gamma} \quad (18)$$

and combining this with (12) we obtain

$$\ddot{g} \leq -\frac{1}{R^2} e^{-\gamma} - \frac{3}{4} g^2 \quad (19)$$

or

$$\frac{dg}{dt} \leq -\frac{1}{R^2} e^{-\gamma}. \quad (20)$$

And integrating this between $t=0$ and any later time of interest $t=t$, we obtain

$$\dot{g} \leq \dot{g}_0 - \frac{1}{R^2} e^{-\gamma} t \quad (21)$$

where \dot{g}_0 is the rate of increase in g at $t=0$.

In accordance with this expression, however, noting from (11) that \dot{g}_0 is positive, we see that at a finite time

$$t \leq R^2 e^\gamma g_0 \quad (22)$$

\dot{g} will become equal to zero, g will pass through a maximum, and the volume will start to decrease.

§6. *Time Necessary to Reach Zero Volume.* It will also be of interest to consider the behavior of the model after passing through its maximum volume. Since \dot{g} will then evidently be negative, we may this time multiply (12) by the negative quantity $2e^{3g/2}\dot{g}$, and integrating as in §4, obtain in correspondence with (15)

$$e^{3g/2}\dot{g}^2 + \frac{4}{R^2} e^{g/2} \geq e^{3g_m/2}\dot{g}_m^2 + \frac{4}{R^2} e^{g_m/2} \quad (23)$$

where g_m and \dot{g}_m are the values of the quantities indicated on passing through the maximum point at the time $t=t_m$. Since, however, the velocity will be zero when the model passes through its maximum volume, we may substitute

$$\dot{g}_m = 0 \quad (24)$$

and rewrite (23) in the form

$$e^{3g/2}g^2 \geq \frac{4}{R^2}(e^{g_m/2} - e^{g/2}) \quad (25)$$

and with \dot{g} negative this gives us

$$e^{3g/4} \frac{dg}{dt} \leq -\frac{2}{R}(e^{g_m/2} - e^{g/2})^{1/2} \quad (26)$$

provided we take the constant R not only as real but positive, which will be the case for a closed model with the positive "radius" $Re^{g/2}$.

Expression (26), however, can easily be integrated between $t=t_m$ and any later time of interest $t=t$ to give

$$-\frac{e^{g/4}}{2}(e^{\theta_m/2} - e^{g/2})^{1/2} + \frac{e^{\theta_m/2}}{2} \sin^{-1} \frac{e^{g/4}}{e^{\theta_m/4}} - \frac{\pi}{4} e^{\theta_m/2} \leq -\frac{(t - t_m)}{2R} \quad (27)$$

or on rearranging

$$(t - t_m) \leq R \left[e^{g/4}(e^{\theta_m/2} - e^{g/2})^{1/2} - e^{\theta_m/2} \sin^{-1} \frac{e^{g/4}}{e^{\theta_m/4}} + \frac{\pi}{2} e^{\theta_m/2} \right]. \quad (28)$$

And in accordance with this result, it is evident that $e^{g/4}$ will reach the value zero or g the value minus infinity at a finite time after the maximum

$$(t - t_m) \leq \frac{\pi}{2} R e^{\theta_m/2}. \quad (29)$$

We have thus shown not only that the model, starting with a finite volume and finite rate of expansion, would reach a finite maximum volume within a finite time, but continuing beyond the maximum would go on down to zero volume within a finite time later. In addition it will be noted, by comparing equations (6a) and (6b) and examining the method of analysis which has been employed, that these results would also hold if the cosmological constant Λ were taken as a negative quantity, as well as for the case which we have treated with the cosmological term set equal to zero.

§7. Behavior of the Model on Reaching Zero Volume. As a result of the preceding section we have seen that our equations lead to the conclusion that the proper volume of the model would decrease to the value zero within a finite time after passing the maximum. We must now inquire into the physical significance of this result, and into the further behavior of the model after reaching this exceptional point.

In accordance with the inequality (26) we may write

$$\dot{g} \leq -\frac{2}{R e^{3g/4}}(e^{\theta_m/2} - e^{g/2})^{1/2} \quad (30)$$

as an expression which holds at any time after passage of the maximum, so that on reaching zero volume with $g = -\infty$ we shall have

$$\dot{g} = -\infty. \quad (31)$$

Furthermore, in accordance with our general expression (12) we can write

$$\ddot{g} \leq -\frac{1}{R^2} e^{-g} - \frac{3}{4} \dot{g}^2 \quad (32)$$

so that we shall also have

$$\ddot{g} = -\infty \quad (33)$$

on reaching zero volume. The exceptional point $g = -\infty$ is thus reached with the velocity \dot{g} and the acceleration \ddot{g} both equal to minus infinity.

The conditions for an analytical minimum are thus unsatisfied and the analysis fails to describe the passage through the exceptional point of zero

volume. From a mathematical point of view, however, it is evident that our differential equations of motion (6b, 7b) can be satisfied if we have a renewed expansion taking place at this point, and from a physical point of view as previously emphasized by one of us⁹ it is evident that contraction to zero volume could only be followed by renewed expansion. Furthermore, as noted in a similar connection by Einstein,¹⁰ it is possible that the idealization upon which our considerations have been based should be regarded as failing in the neighborhood of zero volume¹¹ so that the analysis fails to give a correct description of the behavior at the lower limit of volume. It hence appears reasonable to conclude for models of the kind we are discussing that the contraction to zero volume or more generally to the lower limit of volume would result in a sudden reversal in the direction of the velocity \dot{g} , followed by a renewed expansion of similar character to the previous one.

§8. *Conclusion.* The main results of the foregoing analysis may now be summarized and a few remarks made concerning their significance.

It has previously been shown that the line element for any non-static model of the universe containing a uniform distribution of fluid can be written in the general form

$$ds^2 = -\frac{e^{g(t)}}{[1 + r^2/4R^2]^2} (dr^2 + r^2 d\theta^2 + r^2 \sin^2 \theta d\phi^2) + dt^2 \quad (34)$$

where R is a constant and the dependence of the line element on the time is given by the exponent $g(t)$. The "radius" for such a model is $Re^{g/2}$, and the changes that take place in the model, as g increases or decreases, can be described as expansions or contractions in the proper volume of the elements of the material filling the model, and in the total proper volume of the model as a whole.

Let us now consider the special case of a "closed" model with R real¹² and positive, filled with a perfect fluid which could not withstand tension, and having at some initial time a finite volume and finite rate of expansion. Applying the equations of relativistic mechanics with the cosmological term omitted, it has then been rigorously shown that such a model would expand to a finite maximum volume which would be reached within a finite time, and would then contract to zero volume which would also be reached within a finite time later. Furthermore, although the mathematical analysis fails to carry us through the exceptional point of zero volume, it has been shown plausible on physical grounds to expect that contraction to the lower limit would be followed by renewed expansion, thus leading to a continued succession of somewhat similar expansions and contractions.

⁹ Tolman, Phys. Rev. 38, 1758 (1931). See §7.

¹⁰ Reference 2.

¹¹ The assumptions that the material filling the model has a perfectly homogeneous distribution, and that this material is a perfect fluid incapable of shearing stresses, may fail at very small volumes.

¹² It should be emphasized that these conclusions apply to "closed" models with R real. The theoretical possibility for "hyperbolic" models with R imaginary has recently been pointed out by Heckmann, Göttingen Nachrichten II, 126 (1931).

This result applies of course in the first instance only to the class of simplified cosmological models that we have considered. Nevertheless, in view of the fairly general nature of the assumptions that were necessary, the result may at least be taken as indicating a possibility that the actual universe or parts thereof might also exhibit such a continued succession of expansions and contractions.

Furthermore, it may again be pointed out, as was emphasized in a previous article,¹³ that this result has been obtained solely by applying the principles of relativistic mechanics, without the necessity for any assumption as to the thermodynamic nature of the processes which take place in the fluid in the model as a consequence of the expansion and contraction. We are hence led to the conclusion that the continued series of expansions and contractions would recur even though the processes taking place in the fluid might be thermodynamically irreversible in character.¹⁴

This latter conclusion is of particular interest since the classical thermodynamics would have led us to expect that the continued occurrence of irreversible processes would result in a condition of maximum entropy where further change would be impossible. As shown in detail in the article mentioned, however, relativistic thermodynamics would permit a continued succession of irreversible expansions and contractions without the entropy ever reaching an unsurpassable maximum.

¹³ Reference 4.

¹⁴ If the processes taking place in the fluid are thermodynamically reversible we may expect a series of identical expansions and contractions as previously studied in detail (Ref. 9). When the processes are thermodynamically irreversible, however, we may expect a series of non-identical expansions and contractions of gradually increasing amplitude as studied in the article mentioned. (Ref. 4).

Chapter 7

1933



A Type of Multiplicative Diophantine System

Author(s): Morgan Ward

Source: *American Journal of Mathematics*, Vol. 55, No. 1 (1933), pp. 67-76

Published by: [The Johns Hopkins University Press](#)

Stable URL: <http://www.jstor.org/stable/2371110>

Accessed: 04/12/2014 20:26

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at

<http://www.jstor.org/page/info/about/policies/terms.jsp>

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



The Johns Hopkins University Press is collaborating with JSTOR to digitize, preserve and extend access to *American Journal of Mathematics*.

<http://www.jstor.org>

A TYPE OF MULTIPLICATIVE DIOPHANTINE SYSTEM.

By MORGAN WARD.

1. Consider the system of M equations in the $K + L$ unknowns $x_1, \dots, x_K, y_1, \dots, y_L$

$$(S) \quad A_i x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_K^{a_{iK}} = B_i y_1^{b_{i1}} y_2^{b_{i2}} \cdots y_L^{b_{iL}}, \quad (i = 1, 2, \dots, M).$$

The exponents a, b are assumed to be positive integers or zero, while the constants A, B are positive integers.

The problem of determining all the real positive * solutions of (S) is a trivial one; for if we let

$$z_1 = \log x_1, \dots, z_K = \log x_K, w_1 = \log y_1, \dots, w_L = \log y_L, e_i = \log(A_i/B_i), \quad (i = 1, \dots, M),$$

then on taking the logarithm of both sides of each equation in (S) we obtain the linear system

$$(E) \quad a_{i1}z_1 + \cdots + a_{iK}z_K - b_{i1}w_1 - \cdots - b_{iL}w_L = e_i, \quad (i = 1, \dots, M).$$

The solution of (S) is thus effectively reduced to a mere inspection of the matrix of the coefficients of (E).

On the other hand, the problem of determining all positive integral solutions of (S) is distinctly non-trivial, and offers several interesting and unexpected features.† To give an idea of the difficulties involved, if we seek to replace (S) by the linear system (E), we must add the restrictions that z_1, \dots, w_L be non-negative, and that e^{z_1}, \dots, e^{w_L} be rational integers. But to select from the totality of solutions of (E) the particular solutions which meet these restrictions appears to be as difficult as to solve the original system (S).

For a direct attack upon this problem, the reader may consult the paper of Bell's already referred to. The method I develop here is indirect. It is, however, strictly arithmetical, being based upon the fundamental theorem of rational arithmetic—unique decomposition into prime factors. It accordingly would not be applicable if we were attempting to find all solutions of (S) in an arbitrary domain of integrality.‡

* The negative solutions may be immediately obtained from the positive on considering the parity of the a and b .

† E. T. Bell, "Reciprocal arrays and diophantine analysis," this JOURNAL, Vol. 55 (1933), pp. 50-66. In this paper a general non-tentative method for solving the system (M) is developed.

‡ van der Waerden, *Algebra*, Part I, Berlin (1931), p. 39.

The essentials of the method are as follows. We consider along with (S) a more special system (M) obtained on setting all the constants A and B equal to unity:

$$(M) \quad x_1^{a_{i1}}x_2^{a_{i2}} \cdots x_K^{a_{iK}} = y_1^{b_{i1}}y_2^{b_{i2}} \cdots y_L^{b_{iL}}, \quad (i = 1, 2, \dots, M).$$

We then show that there exists a correspondence between the solutions of (M) in positive integers x and y and the solutions of the linear system

$$(A) \quad a_{i1}z_1 + a_{i2}z_2 + \cdots + a_{iK}z_K = b_{i1}w_1 + b_{i2}w_2 + \cdots + b_{iL}w_L, \quad (i = 1, 2, \dots, M),$$

in non-negative integers z and w . This correspondence is of a dual character, so that any theorem about the solutions of (A) yields a theorem about the solutions of (M) and vice-versa. Since the broad outlines of the theory of the solution of (A) are known,* we obtain without effort considerable information about the solutions of (M). A slight extension of the method allows us finally to discuss the general system (S).

2. We must first lay down a few definitions. The systems (M) and (A) will be said to be *associated*. By a solution of (S) or (M) we shall mean a solution in positive integers, and by a solution of (A) a solution in non-negative integers. To avoid trivialities, we shall furthermore assume that (S) actually has solutions.

We shall find it convenient to represent a solution $\xi_1, \xi_2, \dots, \xi_K, \eta_1, \eta_2, \dots, \eta_L$ of any one of the three systems (S), (M) or (A) under consideration as a one-rowed matrix,[†]

$$[\xi; \eta] = [\xi_1, \xi_2, \dots, \xi_K, \eta_1, \eta_2, \dots, \eta_L].$$

If

$$[\xi'; \eta'] = [\xi'_1, \xi'_2, \dots, \xi'_K, \eta'_1, \eta'_2, \dots, \eta'_L]$$

is a second such solution, then the matrix

$$[\xi + \xi'; \eta + \eta'] = [\xi_1 + \xi'_1, \dots, \eta_L + \eta'_L]$$

is called the sum of the solutions $[\xi; \eta]$, $[\xi'; \eta']$ and expressed as usual by the notation

$$[\xi + \xi'; \eta + \eta'] = [\xi; \eta] + [\xi'; \eta'].$$

In like manner, the product of two solutions is expressed by

$$[\xi\xi'; \eta\eta'] = [\xi; \eta] \cdot [\xi'; \eta'],$$

* See for example, Grace and Young, *Algebra of Invariants*, Cambridge (1903), pp. 102-106.

† Bell, *Algebraic Arithmetic*, pp. 15-16.

and the identity of any two solutions by

$$[\xi; \eta] = [\xi'; \eta'].$$

Finally, if t is any integer,

$$\begin{aligned} t[\xi; \eta] &= [t\xi_1, \dots, t\eta_L], \\ [\xi; \eta]^t &= [\xi_1^t, \dots, \eta_L^t]. \end{aligned}$$

We shall on occasion denote matrices of solutions by German capitals. It is immediately evident that

*the product of a solution of (S) and a solution of (M) is a solution of (S);
the product of two solutions of (M) is a solution of (M);
the sum of two solutions of (A) is a solution of (A).*

The solution $x_1 = x_2 = \dots = x_K = y_1 = y_2 = \dots = y_L = 1$ of (M) will be called the trivial solution of (M) and denoted by

$$\mathfrak{J} = [1; 1].$$

The trivial solution of (A) is defined in an analogous manner as

$$\mathfrak{D} = [0; 0].$$

A solution of (A) is said to be irreducible if it cannot be expressed as the sum of two non-trivial solutions *; similarly, a solution of (M) is said to be irreducible if it cannot be expressed as the product of two non-trivial solutions. Lastly, a solution of (S) is said to be irreducible if it cannot be expressed as the product of a solution of (S) and a non-trivial solution of (M).

The Greek letters α and β appearing as sub-scripts or super-scripts will have the ranges $1, 2, \dots, K$ and $1, 2, \dots, L$ respectively. Thus we write $x_\alpha = P^{u_\alpha}$ for $x_1 = P^{u_1}, x_2 = P^{u_2}, \dots, x_K = P^{u_K}$,

$$\sum_{(\beta)} v_\beta \text{ for } v_1 + v_2 + \dots + v_L, \quad \prod_{(\alpha)} P^{u_\alpha} \text{ for } P^{u_1} P^{u_2} \dots P^{u_K},$$

and so on.

3. We shall first give some properties of the system (M).

THEOREM 3.1. *Every primitive solution of (M) is of the form*

$$x_\alpha = P^{u_\alpha}, \quad y_\beta = P^{v_\beta}$$

where P is a prime, and $[u; v]$ is a primitive solution of (A).

* Grace and Young, p. 102.

Proof. Assume that (M) has a primitive solution $[\xi; \eta]$. Then there exists a prime P dividing at least one of the numbers ξ, η . Write

$$\xi_a = P^{ua} \xi'^a, \quad \eta_\beta = P^{vb} \eta'^\beta$$

where the ξ', η' are prime to P . Substituting these numbers in (M), we obtain

$$\prod_{(a)} P^{a_i a u a} \prod_{(a)} \xi'^{a_i a} = \prod_{(\beta)} P^{b_i \beta v \beta} \prod_{(\beta)} \eta'^{b_i \beta}, \quad (i = 1, \dots, M).$$

Therefore

$$(3.1) \quad \prod_{(a)} P^{a_i a u a} = \prod_{(\beta)} P^{b_i \beta v \beta}, \quad \prod_{(a)} \xi'^{a_i a} = \prod_{(\beta)} \eta'^{b_i \beta}, \quad (i = 1, \dots, M),$$

and $[P^u; P^v]$, $[\xi'; \eta']$ are solutions of (M). Since the first is non-trivial, the second must be trivial, and

$$[\xi; \eta] = [P^u; P^v].$$

$[u; v]$ must be a primitive solution of (A). For from the first set of equations in (3.1)

$$\sum_{(a)} a_i a u_a = \sum_{(\beta)} b_i \beta v_\beta, \quad (i = 1, \dots, M),$$

so that $[u; v]$ is a solution of (A). But if it were the sum of two non-trivial solutions of (A), $[P^u; P^v]$ would be the product of two non-trivial solutions of (M).

COROLLARY. *Both the systems (A) and (M) have non-trivial solutions, or both have only trivial solutions.*

The primitive solution $[P^u; P^v]$ of (M) will be said to be of type $[u; v]$. There are an infinite number of primitive solutions of (M) of a given type; namely, one for each rational prime P . However the number of types of primitive solutions of (M) is finite, for the number of primitive solutions of (A) is known to be finite.*

Suppose that (A) has in all the R distinct primitive solutions

$$\mathbf{u}_i = [\xi_i; \eta_i], \quad (i = 1, 2, \dots, R).$$

THEOREM 3.2. *Every solution of (M) is of the form*

$$(3.2) \quad \begin{aligned} x_a &= T_1^{\xi_1 a} T_2^{\xi_2 a} \cdots T_R^{\xi_R a} \\ y_\beta &= T_1^{\eta_1 \beta} T_2^{\eta_2 \beta} \cdots T_R^{\eta_R \beta} \end{aligned}$$

where the parameters T_1, T_2, \dots, T_R are positive integers. Conversely, every such expression is a solution of (M).

* Grace and Young, p. 103.

Proof. From the proof of theorem 3.1, it is evident that any solution $[\lambda; \mu]$ of (M) is of the form

$$\prod_{\sigma=1}^S [P_\sigma^{u_{\sigma 1}}, P_\sigma^{u_{\sigma 2}}, \dots, P_\sigma^{u_{\sigma K}}; P_\sigma^{v_{\sigma 1}}, P_\sigma^{v_{\sigma 2}}, \dots, P_\sigma^{v_{\sigma L}}],$$

where P_1, P_2, \dots, P_S are the distinct primes dividing $\lambda_1 \lambda_2 \dots \lambda_K \mu_1 \mu_2 \dots \mu_L$, and the $[u_\sigma; v_\sigma]$ are solutions of (A). Now *

$$[u_\sigma; v_\sigma] = k_1^{(\sigma)} \mathbf{U}_1 + k_2^{(\sigma)} \mathbf{U}_2 + \dots + k_R^{(\sigma)} \mathbf{U}_R$$

where the $k^{(\sigma)}$ are non-negative integers. Therefore

$$P_\sigma^{u_{\sigma a}} = \prod_{\tau=1}^R P_\sigma^{k_\tau^{(\sigma)} \xi_{\tau a}}, \quad P_\sigma^{v_{\sigma \beta}} = \prod_{\tau=1}^R P_\sigma^{k_\tau^{(\sigma)} \eta_{\tau \beta}}.$$

Accordingly,

$$\begin{aligned} \lambda_a &= \prod_{(\sigma)} P_\sigma^{u_{\sigma a}} = \prod_{(\sigma)} \prod_{(\tau)} P_\sigma^{k_\tau^{(\sigma)} \xi_{\tau a}} = \prod_{(\tau)} \prod_{(\sigma)} P_\sigma^{k_\tau^{(\sigma)} \xi_{\tau a}} = \prod_{(\tau)} T_\tau^{\xi_{\tau a}}, \\ \mu_\beta &= \prod_{(\sigma)} P_\sigma^{v_{\sigma \beta}} = \prod_{(\sigma)} \prod_{(\tau)} P_\sigma^{k_\tau^{(\sigma)} \eta_{\tau \beta}} = \prod_{(\tau)} \prod_{(\sigma)} P_\sigma^{k_\tau^{(\sigma)} \eta_{\tau \beta}} = \prod_{(\tau)} T_\tau^{\eta_{\tau \beta}}, \end{aligned}$$

where

$$T_\tau = \prod_{(\sigma)} P_\sigma^{k_\tau^{(\sigma)}} = P_1^{k_\tau^{(1)}} P_2^{k_\tau^{(2)}} \dots P_S^{k_\tau^{(s)}}, \quad (\tau = 1, 2, \dots, R),$$

so that the T are positive integers. The converse of the theorem is obvious from the relations just given.

4. Since for each fixed value of α there must be at least one value of τ for which $\xi_{\tau \alpha} \neq 0$, and for each fixed value of β one value of τ for which $\eta_{\tau \beta} \neq 0$, none of the parameters T in (3.2) can be equal to unity for all solutions of (M) unless all solutions of (M) are trivial. In other words, *the number of primitive solutions of (A) gives the minimum number of parameters T necessary to express every solution of (M) in the form (3.2)*.

The question naturally arises whether we can determine this number *a priori* without actually exhibiting all the primitive solutions of (A). In general, this appears to be impossible, but there are certain fairly general special systems (M) for which such a determination can be made. We give in this connection the following two theorems.

THEOREM 4.2. *The total number of parameters T necessary to express all solutions of the system*

$$(M') \quad x_1^{a_1} x_2^{a_2} \dots x_K^{a_K} = y_{11} y_{12} \dots y_{1L_1} = \dots = y_{n1} y_{n2} \dots y_{nL_n}$$

is given by the formula

$$\sum_{\alpha=1}^K \prod_{\tau=1}^n \binom{L_\tau + a_\alpha - 1}{a_\alpha}.$$

* Grace and Young, pp. 104, 103.

Here $\binom{m}{n}$ denotes as usual the number of combinations of m things taken n at a time.

THEOREM 4.2. *The total number of parameters T necessary to express all solutions of the system*

(M'') $(x_{11}x_{12}\cdots x_{1K_1})^{a_1} = (x_{21}x_{22}\cdots x_{2K_2})^{a_2} = \cdots = (x_{n1}x_{n2}\cdots x_{nK_n})^{a_n}$
is given by the formula

$$\prod_{\tau=1}^n \binom{a'_\tau + K_\tau - 1}{a'_\tau},$$

where $a'_\tau = a/a_\tau$, ($\tau = 1, 2, \dots, n$), and a is the least common multiple of integers a_1, a_2, \dots, a_n .

To illustrate these theorems,* consider the three systems

- (i) $x^2y^3z^3 = uv = wrst,$
- (ii) $x^3y^3z^3 = u^2v^2 = wrst,$
- (iii) $x^9 = y^5 = u^4v^4 = wrst.$

For the first system, we apply theorem 4.1 with $K = 3$, $a_1 = 2$, $a_2 = a_3 = 3$, $n = 2$, $L_1 = 2$, $L_2 = 4$,

$$\sum_{\tau=1}^3 \prod_{a=1}^2 \binom{L_\tau + a_a - 1}{a_a} = \sum_{a=1}^2 \binom{a_a + 1}{a_a} \binom{a_a + 3}{a_a} = \binom{3}{2} \binom{2}{2} + 2 \binom{4}{3} \binom{6}{3} = 190$$

For the second system, we apply theorem 4.2 with $n = 3$, $a_1 = 3$, $a_2 = 2$, $a_3 = 1$, $K_1 = 3$, $K_2 = 2$, $K_3 = 4$, $a = 6$, $a'_1 = 2$, $a'_2 = 3$, $a'_3 = 6$,

$$\prod_{\tau=1}^3 \binom{a'_\tau + K_\tau - 1}{a'_\tau} = \binom{4}{2} \binom{4}{3} \binom{9}{6} = 2,016.$$

For the third system, which involves only five algebraically independent variables, theorem 4.2 gives

$$\prod_{\tau=1}^4 \binom{K_\tau + a'_\tau - 1}{a'_\tau} = \binom{20}{20} \binom{36}{36} \binom{46}{45} \binom{183}{180} = \binom{46}{1} \binom{183}{3} = 46,217,626.$$

From these illustrations it is clear that even for rather simple looking

* In the last section of the paper will be found a simple system for which a verification of the theorems is feasible. If we take in (M') $a_1 = a_2 = \cdots = a_k = 1$ or in (M'') $a_1 = a_2 = \cdots = a_n = 1$, we find that the total number of parameters necessary to express all solutions of the system

$x_{11}x_{12}\cdots x_{1k_1} = x_{21}x_{22}\cdots x_{2k_2} = \cdots = x_{n1}x_{n2}\cdots x_{nk_n}$
is $\sum_{a=1}^{k_1} \prod_{\tau=a}^n \binom{K_\tau}{1} = \prod_{\tau=1}^n \binom{K_\tau}{1} = k_1 \cdot k_2 \cdots k_n$, a result obtained by Bell in the paper already cited by an entirely different argument.

systems, the number of parameters may be extraordinarily large, and that the actual exhibition of the solutions of a given system in the form (3.2) is usually impracticable.

The proof of theorem 4.1 is as follows. Consider the additive system associated with (M') ,

$$(A') \quad a_1 z_1 + \cdots + a_K z_K = w_{11} + \cdots + W_{1L_1} = \cdots = w_{n1} + \cdots + w_{nL_n}.$$

We have seen that the number of parameters T necessary for the solution of (M') is the number of primitive solutions of (A') .

There exist solutions of (A') with one of the z equal to one and all the remaining z equal to unity, and every such solution is primitive. Let us consider those solutions in which $z_a = 1$ and $z_1 = z_2 = \cdots = z_{a-1} = z_{a+1} = \cdots = z_K = 0$.

For such a solution we must have from (A') n relations of the type

$$(4.1) \quad a_\alpha = w_1 + w_2 + \cdots + w_L$$

where the w are non-negative integers. But the total number of ways that we can choose such numbers w to satisfy (4.1) equals the coefficient of t^{a_α} in the product $(1 + t + t^2 + \cdots)^L$, which is $\binom{L + a_\alpha - 1}{a_\alpha}$.

Therefore the total number of solutions under consideration is

$$\prod_{\tau=1}^n \binom{L_\tau + a_\alpha - 1}{a_\alpha}.$$

On taking $\alpha = 1, 2, \dots, K$ it follows that there are at least

$$\sum_{\alpha=1}^k \prod_{\tau=1}^n \binom{L_\tau + a_\alpha - 1}{a_\alpha} \text{ primitive solutions of } (A').$$

To show that there are exactly this number, it suffices to show that no solution of (A') not of the special form considered can be primitive.

Let the values of z in such a solution be $\eta_1, \eta_2, \dots, \eta_K$ where $\eta_i \neq 0$ and let $N = a_1 \eta_1 + a_2 \eta_2 + \cdots + a_K \eta_K$, $M = a_i$. Then by our hypothesis, $N > M$.

It follows as for (4.1) that the values of w in any one of the sums in (A') must form a partition of N into L or fewer parts. But for every such partition of N ,

$$N = \gamma_1 + \gamma_2 + \cdots + \gamma_{L'},$$

where $\gamma_1 \geq \gamma_2 \geq \cdots \geq \gamma_{L'} > 0$, ($L' \leq L$) we can find a partition of M

$$M = \theta_1 + \theta_2 + \cdots + \theta_{K'}$$

such that $K' \leq L'$, $\theta_j \leq \gamma_j$, ($j = 1, 2, \dots, K'$).

Therefore by assigning the proper w to the γ and θ , we exhibit our solution as the sum of a primitive solution of (A') and a non-trivial solution of (A') associated with a certain set of partitions of $N - M$.

The proof of theorem 4.2 follows similar lines. With an obvious extension of our matrix notation, let

$$[\xi^{(1)}; \xi^{(2)}; \dots; \xi^{(n)}]$$

be a solution of the additive system associated with (M''),

$$(A'') \quad a_1(z_{11} + \dots + z_{1K_1}) = \dots = a_n(z_{n1} + \dots + z_{nK_n})$$

and let

$$N_\tau = \xi_1^{(\tau)} + \xi_2^{(\tau)} + \dots + \xi_{K_\tau}^{(\tau)}, \quad (\tau = 1, 2, \dots, n).$$

Then

$$(4.2) \quad a_1 N_1 = a_2 N_2 = \dots = a_n N_n = N, \text{ say.}$$

Now for integral N_1, \dots, N_n the least positive value of N which can satisfy a relation of the form (4.2) is the least common multiple of a_1, a_2, \dots, a_n . Denote this number by a , and let

$$a'_\tau = a/a_\tau, \quad (\tau = 1, 2, \dots, n).$$

Then if

$$(4.3) \quad a'_\tau = \eta_1^{(\tau)} + \eta_2^{(\tau)} + \dots + \eta_{K_\tau}^{(\tau)}$$

is a partition of a'_τ into K_τ parts, zero counting as a part,

$$[\eta^{(1)}; \eta^{(2)}; \dots; \eta^{(n)}]$$

will be a primitive solution of (A''). There are $\binom{a'_\tau + K_\tau - 1}{a'_\tau}$ distinct ways of selecting non-negative $\eta^{(\tau)}$ to satisfy (4.3), and hence in all

$$\prod^{\infty} \binom{a'_\tau + K_\tau - 1}{a'_\tau}$$

such primitive solutions. The proof that there are no other primitive solutions is almost exactly the same as for Theorem 4.1.

5. The results of section three allow us to complete the discussion of the general system (S).

Let P_1, P_2, \dots, P_H be the distinct prime factors of the $2M$ integers A_1, \dots, B_M so that

$$A_i = P_1^{c_{i1}} P_2^{c_{i2}} \cdots P_H^{c_{iH}}, \quad B_i = P_1^{d_{i1}} P_2^{d_{i2}} \cdots P_H^{d_{iH}}, \quad (i = 1, \dots, M)$$

where the c and d are non-negative integers, and for a fixed k at least one of the $2M$ numbers $c_{1k}, c_{2k}, \dots, c_{Mk}, d_{1k}, d_{2k}, \dots, d_{Mk}$ is positive.

Consider the system

$$(M^{(k)}) \quad P_k c_{ik} x_1^{a_{i1}} \cdots x_K^{a_{iK}} = P_k d_{ik} y_1^{b_1} \cdots y_L^{b_L}, \quad (i = 1, \dots, M)$$

and the associated additive system

$$(A^{(k)}) \quad c_{ik} + a_{i1}z_1 + \cdots + a_{iK}z_K = d_{ik} + b_{i1}w_1 + \cdots + b_{iL}w_L, \quad (i = 1, \dots, M).$$

Then if a primitive solution of $(A^{(k)})$ is defined as one which cannot be expressed as the sum of a solution of $(A^{(k)})$ and a non-trivial solution of (A) , it follows as in the proof of theorem 3.1 that every primitive solution of $(M^{(k)})$ is of the form $[P_k^\lambda; P_k^\mu]$ where $[\lambda; \mu]$ is a primitive solution of $(A^{(k)})$.

Consider in connection with $(A^{(k)})$ the additive system

$$(B^{(k)}) \quad c_{ik}z_0 + a_{i1}z_1 + \cdots + a_{iK}z_K = d_{ik}w_0 + b_{i1}w_1 + \cdots + b_{iL}w_L, \quad (i = 1, \dots, M).$$

Then the number of primitive solutions of $(B^{(k)})$ is finite. If among these primitive solutions there are l_0 with $z_0 = w_0 = 1$, l_1 with $z_0 = 0$, $w_0 = 1$ and l_2 with $z_0 = 1$, $w_0 = 0$ then $(A^{(k)})$ and hence $(M^{(k)})$ has exactly $v_k = l_0 + l_1 l_2$ primitive solutions. If $l_0 + l_1 l_2 = 0$, $(M^{(k)})$ has no primitive solutions, and hence no solutions whatever. We shall see in a moment that this would entail (S) having no solutions contrary to our hypothesis. Hence $v_k > 0$ and the primitive solutions of $(M^{(k)})$ may be exhibited, since the primitive solutions of $(B^{(k)})$ can be found by trial in a finite number of steps.*

If we denote such a primitive solution of $(M^{(k)})$ by $[\xi^{(k)}; \eta^{(k)}]$, then

$$(5.1) \quad [\xi; \eta] = [\xi^{(1)}; \eta^{(1)}] \cdot [\xi^{(2)}; \eta^{(2)}] \cdots [\xi^{(H)}; \eta^{(H)}]$$

is a primitive solution of (S), and there are in all exactly $v = v_1 v_2 \cdots v_H$ such solutions. Conversely, if (S) has solutions, and hence primitive solutions, a decomposition such as (5.1) is possible, so that each $(M^{(k)})$ must have primitive solutions. We summarize our results in the following theorem.

THEOREM 5.1. *If (S) has solutions, every solution is of the form*

$$(5.2) \quad \begin{aligned} x_\alpha &= C_\alpha T_1^{\xi_{1\alpha}} T_2^{\xi_{2\alpha}} \cdots T_s^{\xi_{s\alpha}} \\ y_\beta &= D_\beta T_1^{\eta_{1\beta}} T_2^{\eta_{2\beta}} \cdots T_s^{\eta_{s\beta}} \end{aligned}$$

where the T , ξ and η are as in Theorem 3.2, and the pairs of integers C_α, D_β may assume at most v sets of values, where v is given in the discussion above.

6. We have not treated here the important problem of what restrictions

* Grace and Young, p. 104.

it is necessary to impose upon the parameters T so that the formulas (5.1) shall give the solutions of (S) once and once only.* This question is bound up in a highly interesting manner with the co-primality of sets of the parameters and their restriction to be numbers of a special form; e. g. square free. I hope to give some results connected with this problem subsequently.

I conclude by solving by the additive method the system used by Bell to illustrate his general process of solution,†

$$(iv) \quad x_1x_2^2 = y_1y_2 = z_1z_2.$$

The additive dual of (iv) is

$$(6.1) \quad X_1 + 2X_2 = Y_1 + Y_2 = Z_1 + Z_2.$$

By inspection we can write down the following thirteen primitive solutions of (6.1):

$$\begin{aligned} \mathbf{U}_1 &= [1, 0; 1, 0; 1, 0], & \mathbf{U}_7 &= [0, 1; 0, 2; 2, 0], \\ \mathbf{U}_2 &= [1, 0; 1, 0; 0, 1], & \mathbf{U}_8 &= [0, 1; 0, 2; 0, 2], \\ \mathbf{U}_3 &= [1, 0; 0, 1; 1, 0], & \mathbf{U}_9 &= [0, 1; 1, 1; 2, 0], \\ \mathbf{U}_4 &= [1, 0; 0, 1; 0, 1], & \mathbf{U}_{10} &= [0, 1; 1, 1; 0, 2], \\ \mathbf{U}_5 &= [0, 1; 2, 0; 2, 0], & \mathbf{U}_{11} &= [0, 1; 2, 0; 1, 1], \\ \mathbf{U}_6 &= [0, 1; 2, 0; 0, 2], & \mathbf{U}_{12} &= [0, 1; 0, 2; 1, 1], \\ \mathbf{U}_{13} &= [0, 1; 1, 1; 1, 1]. \end{aligned}$$

By theorem (4.1), the solution of (iv) will contain $\binom{2}{1}\binom{2}{1} + \binom{3}{2}\binom{3}{2} = 13$ parameters.

Hence $\mathbf{U}_1, \dots, \mathbf{U}_{13}$ are all the primitive solutions of (6.1), so that by theorem (3.2) the solution of (iv) is

$$\begin{aligned} x_1 &= T_1T_2T_3T_4, & x_2 &= T_5T_6T_7T_8T_9T_{10}T_{11}T_{12}T_{13}, \\ y_1 &= T_1T_2T_5^2T_6^2T_9T_{10}T_{11}^2T_{13}, & y_2 &= T_3T_4T_7^2T_8^2T_9T_{10}T_{12}^2T_{13}, \\ z_1 &= T_1T_3T_5^2T_7^2T_9^2T_{11}T_{12}T_{13}, & z_2 &= T_2T_4T_6^2T_8^2T_{10}^2T_{11}T_{12}T_{13}. \end{aligned}$$

On making the change of variables

$$\begin{aligned} T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8, T_9, T_{10}, T_{11}, T_{12}, T_{13} &\text{ into} \\ \phi_1, \phi_2, \phi_3, \phi_4, \psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6, \psi_7, \psi_8, \psi_9, \psi_{10}, \psi_{11}, \psi_{12}, \psi_{13}, \psi_{14} \end{aligned}$$

this solution agrees with that obtained by Bell.

The additive method gives no information about the co-primeness of the parameters T , and it is to some extent tentative. In compensation, it is usually shorter than the multiplicative method.

* See Elliott, *Quarterly Journal of Mathematics*, Vol. 34 (1903), pp. 348-377 for a discussion of the similar problem for (A) in the case $M = 1$, with considerable detail for the sub-case $K + L = 3$.

† Paper cited, § 15.

Hence

$$\rho \geq p_1 + \dots + p_r.$$

The limit given here is therefore always as good as Vranceanu's. That it is sometimes better is seen from the following system whose species is two:

$$\begin{aligned}\omega^1 &= dx^5 + x^1dx^2, \quad \omega^2 = dx^6 - x^3dx^1 + x^2dx^4, \\ \omega'^1 &= dx^1dx^2, \quad \omega'^2 = dx^1dx^3 + dx^2dx^4.\end{aligned}$$

We have $p_1 = 1$, $p_2 = 0$, $p_1 + p_2 = 1$, whereas $\rho = 2$.

Had the equations been written in the opposite order, we should have found $p_1 = 2$, $p_2 = 0$, $p_1 + p_2 = 2$. This illustrates the fact that $p_1 + \dots + p_r$, unlike the rank, is not an invariant.

¹ Species is defined in the author's paper "Pfaffian Systems of Species One," *Trans. Amer. Math. Soc.*, 35, 356-71 (1933).

² Cf. Goursat, E., *Problème de Pfaff*, Paris, 291 (1922).

³ Cartan, E., *Invariants Intégraux*, Paris, 59 (1922).

⁴ Vranceanu, G., *Comptes Rendus*, Paris, 196, 1859-61 (1933).

A PROPERTY OF RECURRING SERIES

BY MORGAN WARD

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA

Communicated September 6, 1933

1. If

$$(U): \quad U_1, U_2, \dots, U_n, \dots$$

denotes a sequence of rational numbers satisfying a linear difference equation of order k with rational coefficients, then if a group of k consecutive terms of (U) ever repeats itself, all the roots of the polynomial associated with the difference equation are roots of unity, and the sequence (U) is periodic.¹ I show here that the like occurs, generally speaking, if one term of the sequence repeats itself at regular intervals a sufficient number of times. More precisely, I shall show that

If in any particular rational solution (U) of the difference equation

$$\Omega_{n+k} = P_1\Omega_{n+k-1} + P_2\Omega_{n+k-2} + \dots + P_k\Omega_n, \quad P_i \text{ rational}, \quad i = 1, \dots, k, \quad (1)$$

we have

$$U_a = U_{a+b} = U_{a+2b} = \dots = U_{a+kb} \neq 0, \quad (2)$$

where a, b are fixed positive integers, and if the associated polynomial

$$x^k - P_1 x^{k-1} - P_2 x^{k-2} - \dots - P_k \quad (3)$$

is irreducible in the field of rationals, then the polynomial is cyclotomic, and every solution of the difference equation is periodic.

2. The necessity for the restrictive hypotheses of the theorem is shown by the following two examples.

For the difference equation $\Omega_{n+3} = \Omega_{n+2} + 4\Omega_{n+1} - 4\Omega_n$ the associated polynomial $x^3 - x^2 - 4x + 4$ factors into $(x - 1)(x - 2)(x + 2)$. Therefore, if c is any rational number $\neq 0$, the particular solution $U_n = 2^n + (-2)^n + c 1^n$ has all terms with odd subscripts equal to c .

On the other hand, for the difference equation $\Omega_{n+4} = \Omega_{n+2} + \Omega_n$, the associated polynomial $x^4 - x^2 - 1$ is irreducible and not cyclotomic, while any particular solution (U) with $U_2 = U_4 = 0$ has all terms with even subscripts equal to zero.

3. The theorem itself may be proved as follows. Let $\alpha_1, \alpha_2, \dots, \alpha_k$ be the roots of the polynomial (2). Then U_n is of the form

$$U_n = A_1 \alpha_1^n + A_2 \alpha_2^n + \dots + A_k \alpha_k^n$$

where the A_i are fixed non-vanishing algebraic numbers. If the common rational value of $U_a, U_{a+b}, \dots, U_{a+kb}$ in (2) is denoted by c , we have then $k + 1$ homogeneous linear equations in $A_1 \alpha_1^a, \dots, A_k \alpha_k^a$ and c :

$$(A_1 \alpha_1^a) \alpha_1^{rb} + (A_2 \alpha_2^a) \alpha_2^{rb} + \dots + (A_k \alpha_k^a) \alpha_k^{rb} - c = 0, r = 0, 1, \dots, k. \quad (4)$$

Since $c \neq 0$, the determinant of this system must vanish. But this determinant is of Vandermonde's type; we obtain, therefore

$$V(\alpha_1^b, \alpha_2^b, \dots, \alpha_k^b, 1) = \prod_{i \neq j} (\alpha_i^b - \alpha_j^b) \prod (\alpha_i^b - 1) = 0.$$

Hence for some i, j , we must have either $\alpha_i^b = 1$ or $\alpha_i^b = \alpha_j^b$.

In the first case, $\alpha_1^b = \alpha_2^b = \dots = \alpha_k^b = 1$ for (3) was assumed irreducible. Therefore every root of (3) is a root of unity, and the theorem follows.

In the second case, on appealing again to the irreducibility of (3), we see that the b^{th} powers of the roots of (3) can be grouped into m sets of l equal powers each, say

$$\alpha_{rl+1}^b = \alpha_{rl+2}^b = \dots = \alpha_{rl+l}^b = \xi_{r+1}, r = 0, 1, \dots, m-1, ml = k,$$

where $\xi_1, \xi_2, \dots, \xi_m$ are distinct algebraic numbers.

If $m = 1$, ξ_1 is rational, and on comparing U_a and U_{a+b} , we see that ξ_1 is unity, giving the first case again. The assumption that $m > 1$ leads to a contradiction. For then we obtain from (4) the equations

$$(A_1 \alpha_1^a + \dots + A_l \alpha_l^a) \xi_1^r + (A_{l+1} \alpha_{l+1}^a + \dots + A_m \alpha_m^a) \xi_2^r + \dots - c = 0, \\ r = 0, 1, \dots, m.$$

Since $c \neq 0$, we infer as before that

$$V(\xi_1, \xi_2, \dots, \xi_m, 1) = \prod_{i \neq j} (\xi_i - \xi_j) \prod (\xi_i - 1) = 0.$$

This last relation is impossible, for the ξ are all distinct and all irrational.

¹ See E. T. Bell, these PROCEEDINGS, 16, 750-752 (1930). Such a repetition will certainly occur if the difference equation has rational integral coefficients and the sequence (U) is bounded provided that U_1, U_2, \dots, U_k are integers, a result which is due to Laguerre.

INTENSITIES IN ATOMIC SPECTRA

By M. H. JOHNSON, JR.*

DEPARTMENT OF PHYSICS OF NEW YORK UNIVERSITY

Communicated August 8, 1933

Introductory.—In the theory of complex spectra a number of methods have been developed for calculating the relative energies of the states arising from an electronic configuration. In these methods various schemes of coupling together the orbital and spin angular momenta play an important rôle. Thus a common procedure is to find the matrix of the energy in LS coupling and to obtain the eigenvalues as the roots of the corresponding secular determinant. The advantage of this and other schemes is principally due to the fact that the total angular momentum J , which is an integral of the motion, is given specified values. The energy matrix then takes on an especially simple form (factored according to J values). There is a further advantage in that the energy as well as other dynamical quantities can often be calculated rather simply in definite coupling schemes. The particular choice of coupling may be dictated by convenience for the calculation and occasionally by physical consideration, for the actual states of an atom sometimes very nearly correspond to definite coupling arrangement among the angular momentum vectors.

In this paper we are concerned with the matrix of the electric moment whose components determine the intensity of the lines radiated by the atom. The problem naturally divides into two parts: I, the determination of the electric moment in a definite coupling scheme; II, the electric moment matrix in intermediate coupling. The procedure for determining the latter from the former is quite straightforward and will be illustrated by an example.

Intensities in a Definite Coupling Scheme.—Let us suppose the atomic states are obtained by coupling the vectors $l_1 \dots l_N s_1 \dots s_N$ together

THE CANCELLATION LAW IN THE THEORY OF CONGRUENCES TO A DOUBLE MODULUS*

BY
MORGAN WARD

1. Let m be an integer greater than unity and $f(x)$ a fixed polynomial with integral coefficients.† If the leading coefficient of $f(x)$ is prime to m , then the quotient and remainder obtained on dividing any other polynomial by $f(x)$ have integral coefficients modulo m . Hence, as is well known, all polynomials may be separated into a finite number of residue classes $\mathfrak{A}, \mathfrak{B}, \dots, \mathfrak{U}, \dots$ which form a commutative ring‡ with respect to the operations of addition and multiplication (modulis $m, f(x)$). I propose here to determine what inferences can be drawn concerning the ring elements \mathfrak{U} and \mathfrak{B} from the ring equality $\mathfrak{A}\mathfrak{U} = \mathfrak{A}\mathfrak{B}$ when $\mathfrak{A} \neq 0$. Since $\mathfrak{A}\mathfrak{U} = \mathfrak{A}\mathfrak{B}$ is equivalent to $\mathfrak{A}(\mathfrak{U} - \mathfrak{B}) = 0$, we may assume that $\mathfrak{B} = 0$. Stated in terms of congruences our problem is then equivalent to the following one:

Suppose that $f(x) = c_0x^k + c_1x^{k-1} + \dots + c_k$ is a fixed polynomial with integral coefficients c_0, \dots, c_k and that m is an integer prime to c_0 . Let $A(x)$ be a given polynomial such that

$$A(x) \not\equiv 0 \quad (\text{mod } m, f(x)).$$

To determine all polynomials $U(x)$ such that

$$(1.1) \quad A(x)U(x) \equiv 0 \quad (\text{mod } m, f(x)).$$

The problem is essentially a generalization of the problem of solving

$$au \equiv 0 \quad (\text{mod } m)$$

for given integers a and m . Nevertheless it does not seem to have been considered heretofore save in very special cases.

I shall first of all show that it is sufficient to consider the case when m is a power of a prime p , say $m = p^n$, and when $f(x)$ is congruent modulo p to a power of an irreducible polynomial $\phi(x) \pmod{p}$;

$$f(x) = B(x) \equiv \{\phi(x)\}^s \quad (\text{mod } p).$$

* Presented to the Society, August 31, 1932; received by the editors May 24, 1932.

† We shall restrict the term polynomial in what follows to mean a polynomial with integral coefficients.

‡ van der Waerden, *Moderne Algebra*, Berlin, 1930, vol. I, p. 37; Haupt, *Einführung in die Algebra*, Leipzig, 1929, vol. I, chapter V.

This reduction corresponds to the fact that the ring associated with the moduli m and $f(x)$ is the direct sum of rings of the type associated with the moduli p^N and $B(x)$.

In this simpler case I shall show that there exists a positive integer λ and a set (S) of λ polynomials

$$A_0(x), A_1(x), \dots, A_{\lambda-1}(x)$$

where λ and (S) depend only upon $A(x)$ and $B(x)$ and are independent of N , such that

$$A(x)U(x) \equiv 0 \quad (\text{mod } p^N, B(x))$$

when and only when

$$\begin{aligned} U(x) &= p^{N-\lambda}(Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \dots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)) \text{ if } N = \lambda \\ &= Q_{\lambda-N}(x)A_{\lambda-N}(x) + pQ_{\lambda-N+1}(x)A_{\lambda-N+1}(x) + \dots + p^{N-1}Q_{\lambda-1}(x)A_{\lambda-1}(x) \\ &\qquad\qquad\qquad \text{if } N \leq \lambda, \end{aligned}$$

the polynomials $Q(x)$ being completely arbitrary, save for a restriction upon their degrees which we shall give later.

In the ring associated with the double modulus $p^N, B(x)$, our results are equivalent to the theorem that the ideal to which every element U of the ring belongs which satisfies the relation

$$AU = 0$$

has a basis of the form

$$p^{N-\lambda}U_0, p^{N-\lambda+1}U_1, \dots, p^{N-1}U_{\lambda-1} \quad \text{if } N \geq \lambda$$

or of the form

$$U_{\lambda-N}, pU_{\lambda-N+1}, \dots, p^{N-1}U_{\lambda-1} \quad \text{if } N \leq \lambda,$$

where λ and $U_0, \dots, U_{\lambda-1}$ depend only upon A , p and $B(x)$ and are independent of N .

2. Suppose that

$$m = p_1^{n_1} \cdots p_r^{n_r}$$

is the decomposition of m into its prime factors. Then it is readily seen that a necessary and sufficient condition that the congruence (1.1) hold is that the r congruences

$$(2.1) \quad A(x)U(x) \equiv 0 \quad (\text{mod } p_i^{n_i}, f(x)), i = 1, \dots, r,$$

hold. Furthermore, if we know the general solution $U^{(i)}(x)$ of each of the congruences (2.1), the general solution of the congruence (1.1) can be written

down immediately by means of the Chinese remainder theorem.* Hence it is sufficient to discuss the case when $m = p^N$, p a prime.

Let

$$f(x) \equiv c_0 \{ \phi_1(x) \}^{\beta_1} \cdots \{ \phi_s(x) \}^{\beta_s} \pmod{p}, \quad (c_0, p) = 1,$$

be the decomposition of $f(x)$ into primary irreducible polynomials modulo p . Then by Schönemann's second theorem† there exists a decomposition of $f(x)$ modulo p^N of the type

$$f(x) \equiv c'_0 B_1(x) \cdots B_s(x) \pmod{p^N}, \quad (c'_0, p) = 1,$$

where the polynomials $B_i(x)$ are primary, and

$$(2.2) \quad B_i(x) \equiv \{ \phi_i(x) \}^{\beta_i} \pmod{p}, \quad i = 1, \dots, s.$$

Since $\text{Res}\{B_i(x), B_j(x)\}$ is prime to p if $i \neq j$, it easily follows that (1.1) holds with $m = p^N$ when and only when the s congruences

$$A(x)U(x) \equiv 0 \pmod{p^N, B_i(x)}, \quad i = 1, \dots, s,$$

hold. If the solutions of these congruences are known, then the solution of the congruence (1.1) may be written down by the procedure of the Chinese remainder theorem.

It is sufficient then to study the congruence

$$(2.3) \quad A(x)U(x) \equiv 0 \pmod{p^N, B(x)}$$

where

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad B(x) = x^m + b_1x^{m-1} + \cdots + b_m$$

are given polynomials, p is a prime number, N a positive integer, and $U(x)$ is to be determined. Furthermore

$$(2.4) \quad B(x) \equiv \{ \phi(x) \}^\beta \pmod{p}$$

where $\phi(x)$ is a primary irreducible polynomial modulo p and β a positive integer. We shall not need to use this last fact in what immediately follows. Finally, we lose no generality by requiring that $U(x)$ be of lesser degree than $B(x)$.

3. The first problem is to determine for a given N the highest power of p which divides every $U(x)$ satisfying (2.3). We shall show that there exists an integer λ depending only upon $A(x)$ and $B(x)$ such that if $N > \lambda$, every solution of (2.3) is divisible by $p^{N-\lambda}$, while if $N \leq \lambda$, there exist solutions of

* Dickson, *Introduction to the Theory of Numbers*, Chicago, 1929, p. 10.

† For an account of Schönemann's theorems, see Fricke, *Algebra*, Braunschweig, 1928, vol. II, chapter 2.

(2.3) which are not divisible by p . If $N > \lambda$, we may therefore write $U(x) = p^{N-\lambda}W(x)$ and thus reduce (2.3) to a congruence of the same form with $N = \lambda$. We shall see in the next section that the discussion of (2.3) when $N \leq \lambda$ presents no difficulties whatsoever.

Let

$$E = E \begin{pmatrix} a_0, a_1, \dots, a_n \\ 1, b_1, \dots, b_m \end{pmatrix}$$

denote the $(m+n)$ -rowed Sylvester eliminant of the polynomials $A(x)$ and $B(x)$, and let

$$\mathcal{E} = (e_{ij}) \quad (i, j = 1, \dots, m+n)$$

denote the transpose of the matrix of the determinant E .

Suppose that

$$E = p^L E' \text{ where } L \geq 0, \quad (p, E') = 1.$$

The congruence (2.3) is equivalent to an identity in x of the form

$$A(x)U(x) + B(x)V(x) = p^N W(x)$$

where the polynomial $V(x)$ is at most of degree $n-1$ and the polynomial $W(x)$ at most of degree $m+n-1$. If we denote the $m+n$ unknown coefficients of $U(x)$ and $V(x)$ in order by z_1, z_2, \dots, z_{m+n} and the coefficients of $W(x)$ by w_1, w_2, \dots, w_{m+n} , then this identity is easily seen to be equivalent to the system of $m+n$ linear equations

$$(3.1) \quad \sum_{j=1}^t e_{ij} z_j = p^N w_i \quad (i = 1, \dots, t)$$

where for brevity we have written t for $m+n$. The determinant of this system is E ; hence

$$E z_j = p^N \sum_{i=1}^t \bar{e}_{ji} w_i \quad (j = 1, \dots, t),$$

\bar{e}_{ji} denoting the co-factor of e_{ij} in E . Suppose that p^D is the highest power of p dividing all of the first minors $\pm \bar{e}_{ji}$ of E . Then on writing $p^L E'$ for E , we see that

$$E' z_j = p^{N+D-L} \sum_{i=1}^t e'_{ji} w_i \quad (j = 1, \dots, t)$$

where $p^D e'_{ji} = \bar{e}_{ji}$. At least one of the numbers e'_{ji} is not divisible by p ; suppose that it is e'_{kl} . Then on taking w_l equal to 1 and the remaining w equal to 0,

we obtain a solution of (3.1) such that every z is divisible by p^{N+D-L} and at least one z , namely z_k , is not divisible by any higher power of p . It follows that the highest power of p dividing all solutions of (3.1) is p^{N+D-L} .

The integer p^{L-D} is simply the first elementary divisor of the matrix \mathcal{E} corresponding to the prime factor p . Writing λ for $L-D$, we have the following result:

The least value of N such that every solution $U(x)$ of (2.3) of degree less than $B(x)$ should be divisible by p^r is $T+\lambda$, where p^λ is the first elementary divisor corresponding to the prime p of the matrix of the eliminant of $A(x)$ and $B(x)$.

Consequently, if $N \leq \lambda$, there exist solutions of (2.3) which are not divisible by p , while if $N > \lambda$, every solution is divisible by $p^{N-\lambda}$. Since $\lambda=0$ only when $L=D=0$, we must have $U(x) \equiv 0 \pmod{p^N}$ if the resultant of $A(x)$ and $B(x)$ is prime to p . In the ring associated with p^N and $B(x)$, the corresponding case is when $\mathfrak{A}\mathfrak{U}=0$ and \mathfrak{A} is a unit of the ring.

4. We can now complete the discussion of the congruence (2.3). If $N > \lambda$, set $U(x) = p^{N-\lambda}W(x)$ thus obtaining the congruence for $W(x)$

$$(4.1) \quad A(x)W(x) \equiv 0 \pmod{p^\lambda, B(x)}.$$

Among the polynomials $W(x)$ which satisfy (4.1) are some not divisible by p . Let $T(x)$ be such a one of lowest possible degree. Then the leading coefficient of $T(x)$ must be prime to p ; for if not, by Schönemann's first theorem* there would exist a polynomial of the form $c+pQ(x)$ where c is prime to p such that $T(x)(c+pQ(x))$ would be congruent modulo p^λ to a polynomial $T'(x)$ of lower degree than $T(x)$. Then, since $\text{Res}\{c+pQ(x), B(x)\}$ is prime to p , we would have $A(x)T'(x) \equiv 0 \pmod{p^\lambda, B(x)}$ contradicting our assumption about the degree of $T(x)$. On multiplying $T(x)$ by a constant prime to p , we obtain a polynomial $A_0(x)$ with leading coefficient unity and of minimal degree satisfying (4.1). This polynomial is unique modulo p^λ ; for the difference of two such polynomials would be of lesser degree than either. Moreover if $W(x)$ is any solution of (4.1), the quotient and remainder obtained on dividing $W(x)$ by $A_0(x)$ have integral coefficients and the remainder being of lower degree than $A_0(x)$ must be divisible by p . Hence

$$W(x) = Q_0(x)A_0(x) + pW_1(x)$$

where $W_1(x)$ is of lesser degree than $A_0(x)$. On substituting this expression in (4.1), we obtain a congruence of the same form for $W_1(x)$:

$$A(x)W_1(x) \equiv 0 \pmod{p^{\lambda-1}, B(x)}.$$

* Fricke, loc. cit., p. 59.

We now repeat the previous argument. Every solution of this congruence must be of the form

$$W_1(x) = Q_1(x)A_1(x) + pW_2(x)$$

where $A_1(x)$ is a solution of minimal degree in x with leading coefficient unity uniquely determined modulo $p^{\lambda-1}$, while $W_2(x)$ is of lesser degree than $A_1(x)$.

We find on continuing in this manner that the general solution of (4.1) is of the form

$$W(x) = Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \cdots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)$$

where the polynomial $A_i(x)$ is uniquely determined modulo $p^{\lambda-i}$.

We shall show in the next section that two consecutive polynomials $A_r(x)$ and $A_{r+1}(x)$ are equal only when all the polynomials $A_r(x), A_{r+1}(x), A_{r+2}(x), \dots, A_{\lambda-1}(x)$ are equal, a circumstance which may occur for special choice of $A(x)$ and $B(x)$. If the degrees of $A_i(x)$ and $Q_i(x)$ are α_i and γ_i respectively, then it is clear that

$$\alpha_i - \alpha_{i+1} > \gamma_{i+1} \geq 0 \quad (i = 0, 1, \dots, r-1).$$

The modification when the initial value of N is less than λ is obvious, and will be left to the reader. The results stated in the beginning of the paper are thus established.

5. We shall conclude by showing how the polynomials $A_{\lambda-1}(x), A_{\lambda-2}(x), \dots, A_0(x)$ may be determined. We first observe that since

$$(5.1) \quad A(x)A_i(x) \equiv 0 \quad (\text{mod } p^{\lambda-i}, B(x))$$

we have $A(x)A_i(x) \equiv 0 \pmod{p^{\lambda-i-1}, B(x)}$. Therefore by the fundamental property of $A_{i+1}(x)$,

$$(5.2) \quad A_i(x) \equiv 0 \quad (\text{mod } p, A_{i+1}(x)) \quad (i = 0, \dots, \lambda-1).$$

We have seen in §2 that we may assume that $B(x)$ is of the form $\{\phi(x)\}^\beta + pV(x)$ where $\phi(x)$ is primary and irreducible modulo p . If we construct a Schönenmann decomposition of $A(x)$ modulo p^N , it is easily seen that we may assume that $A(x)$ is of the same form; thus

$$(5.3) \quad B(x) = \{\phi(x)\}^\beta + pV(x), \quad A(x) = \{\phi(x)\}^\alpha + pR(x)$$

where $\alpha < \beta$, and the degrees of $V(x)$ and $R(x)$ are less than those of $B(x)$ and $A(x)$ respectively. Hence

$$A(x)\{\phi(x)\}^{\beta-\alpha} \equiv pR(x)\{\phi(x)\}^{\beta-\alpha} - pV(x) \quad (\text{mod } B(x)).$$

If p^M is the highest power of p dividing the right side of this last congruence, we have

$$A(x)\{\phi(x)\}^{\beta-\alpha} \equiv 0 \quad (\text{mod } p^M, B(x)), \quad \not\equiv 0 \quad (\text{mod } p^{M+1}, B(x))$$

and we may take

$$A_{\lambda-1}(x) = A_{\lambda-2}(x) = \dots = A_{\lambda-M}(x), \quad A_{\lambda-M}(x) \equiv \{\phi(x)\}^{\beta-\alpha} \pmod{p^M}.$$

Let i denote an integer $\leq \lambda - M$. Then

$$(5.4) \quad A(x)A_i(x) \equiv p^{\lambda-i}S_i(x) \pmod{B(x)},$$

where $S_i(x)$ is of lesser degree than $B(x)$.

We may assume that $S_i(x)$ is not divisible by p and is of lesser degree than $A(x)$. For since $A_i(x)$ is determined only modulo $p^{\lambda-i}$, if $S_i(x) = pS'_i(x)$ we have

$$A(x)(A_i(x) + p^{\lambda-i}) \equiv p^{\lambda-i}(A(x) + pS'_i(x)) \pmod{B(x)}$$

and by (5.3), the polynomial multiplying $p^{\lambda-i}$ on the right is not divisible by p . In the same way, if $S_i(x) = Q(x)A(x) + S''_i(x)$ where $S''_i(x)$ is of lesser degree than $A(x)$, then $Q(x)$ is necessarily of lesser degree than $A_i(x)$ so that $A_i(x) + p^{\lambda-i}Q(x)$ is a primary polynomial such that

$$A(x)(A_i(x) + p^{\lambda-i}Q(x)) \equiv p^{\lambda-i}S''_i(x) \pmod{B(x)}.$$

If $A_i(x)$ is known, we can determine $A_{i-1}(x)$. For, by (5.2),

$$A_{i-1}(x) = Q(x)A_i(x) + pR(x)$$

where $Q(x)$ must be primary, and $R(x)$ of lesser degree than $A_i(x)$. By (5.4),

$$A(x)A_{i-1}(x) \equiv p^{\lambda-i}Q(x)S_i(x) + pR(x)A(x) \pmod{B(x)}.$$

Take $R(x) = p^{\lambda-i-1}$. Then

$$A(x)A_{i-1}(x) \equiv 0 \pmod{p^{\lambda-i+1}, B(x)}$$

when and only when

$$Q(x)S_i(x) + A(x) \equiv 0 \pmod{p, B(x)},$$

that is, when and only when

$$Q(x)S_i(x) + \{\phi(x)\}^\alpha \equiv 0 \pmod{p, \{\phi(x)\}^\beta}.$$

Since $S_i(x)$ is known and is of lesser degree than $\{\phi(x)\}^\alpha$ and not divisible by p , there exists a primary polynomial $Q(x)$ uniquely determined modulo p which satisfies this congruence. $A_{i-1}(x)$ is now uniquely determined modulo $p^{\lambda-i+1}$ and may be modified so as to satisfy the conditions corresponding to those imposed upon $A_i(x)$ in (5.4).

The remaining polynomials $A_{\lambda-M-1}(x), \dots, A_1(x), A_0(x)$ can therefore be calculated step by step, and our solution is completed.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

THE ARITHMETICAL THEORY OF LINEAR RECURRING SERIES*

BY
MORGAN WARD

I. INTRODUCTION. THE DIFFERENCE EQUATION OF ORDER ONE

1. Let m be an integer greater than one, and let

$$(u): \quad u_0, u_1, u_2, \dots, u_n, \dots$$

be an arithmetical series† of order k ; that is, a particular solution of the linear difference equation

$$(1.1) \quad \Omega_{n+k} = c_1\Omega_{n+k-1} + c_2\Omega_{n+k-2} + \dots + c_k\Omega_n$$

where c_1, c_2, \dots, c_k and the k initial values u_0, u_1, \dots, u_{k-1} of (u) are given integers. Then if a_n is the least positive residue of u_n modulo m , we may associate with (u) a second sequence

$$(a): \quad a_0, a_1, a_2, \dots, a_n, \dots$$

which we call the reduced sequence corresponding to (u) modulo m .

It is easily seen that after a finite number of terms, the sequence (a) repeats itself periodically, and that any one of its periods is a multiple of a certain least period which is called the *characteristic number* of (u) (or (a)) modulo m .‡ The number of non-repeating terms in (a) is called the *numeric* of (u) modulo m ; if it is zero, (u) is said to be *purely periodic*§ modulo m . If all the terms of (u) after a certain point are divisible by m , so that the repeating part of (a) consists of the single residue zero, (u) is said to be a *null sequence* modulo m .

Three important problems immediately suggest themselves: first, to determine the characteristic number and numeric of the sequence (u) as

* Presented to the Society, August 31, 1932; received by the editors September 6, 1932.

† The literature prior to 1917 is summarized in Dickson's *History*, vol. I, chapter XVII. Among the more recent papers, D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), pp. 419–449, treats the case $k=2$, and the author, these Transactions, vol. 33 (1931), pp. 153–165, the case $k=3$. For general k , see R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372. Certain of Carmichael's results were extended by the use of ideals by H. T. Engstrom, these Transactions, vol. 33 (1931), pp. 210–218. I shall refer to these papers by the authors' name and page number. For the bearing of the problem upon elementary number theory, see R. D. Carmichael, American Mathematical Monthly, vol. 36 (1929), pp. 132–143.

‡ This term is due to Carmichael, p. 345.

§ This is always the case if m is prime to c_k in (1.1).

functions of the $2k+1$ integers $c_1, \dots, c_k, u_0, \dots, u_{k-1}$ and m^* ; secondly, given (1.1) and m , to determine least upper bounds for the characteristic number and numeric of any solution of (1.1); and thirdly, given m and k , to determine the least upper bounds for the characteristic number and numeric of any arithmetical series of order k . The bearing of these problems upon the arithmetical properties of such series is evident; nevertheless none of them has as yet been completely solved.†

2. The course of the investigation may best be explained by considering the special case of a difference equation of order one,

$$(2.1) \quad \Omega_{n+1} = c\Omega_n.$$

Any solution (u) of (2.1) is of the form

$$u_n = u_0 c^n$$

where u_0 is an integer. It is possible to express this solution as the sum of two other solutions $v_n = v_0 c^n$, and $w_n = w_0 c^n$ where for the modulus m , (v) is a null sequence with the same numeric as (u), and (w) is a purely periodic sequence with the same characteristic number. The numbers v_0 and w_0 may be determined as soon as u_0 is known.

It readily follows that the numeric and characteristic number of the sequence (u) modulo m are respectively the least values of n such that

$$(2.2) \quad v_0 c^n \equiv 0 \pmod{m}, \quad w_0(c^n - 1) \equiv 0 \pmod{m}.$$

In the special case when m is a prime p and w_0 is not divisible by p , the least value of n for which the second of these congruences is satisfied is simply the exponent to which c belongs modulo p . A complete solution of our fundamental problems is thus at present out of the question even for a difference equation of order one. Nevertheless it is of considerable interest to reduce the general problem to its basic constituents. A short analysis discloses that in order to determine the minimal values of n in (2.2) it is sufficient to know

- (i) the decomposition of m, v_0, w_0 and c into their prime factors;
- (ii) the least value of n such that

$$c^n \equiv 1 \pmod{p}$$

for every prime factor p of m ;

- (iii) if λ is the least value of n satisfying (ii), the highest power of p dividing $c^\lambda - 1$.

* Compare Carmichael, pp. 345, 346.

† Compare Engstrom, p. 218.

Furthermore, (i) alone suffices for the determination of the numeric of (u) , and (i) and (ii) alone for the determination of the characteristic number of (u) for all square-free integers m . (ii) is the unsolved problem of determining the exponent to which a given integer belongs for a given prime modulus, while (iii) is equivalent to the (unsolved) problem of the quotients of Fermat: to find the highest power of p dividing $c^{p-1} - 1$.

Let us pass now to the general case of a difference equation of order k . Let

$$F(x) = x^k - c_1x^{k-1} - \cdots - c_k$$

denote the polynomial associated with the difference equation (1.1), and (u) as before any solution of (1.1). Then we can associate with (1.1) and m two congruences analogous to (2.2):

$$V(x)x^n \equiv 0 \pmod{m, F(x)}, \quad W(x)(x^n - 1) \equiv 0 \pmod{m, F(x)},$$

where $V(x)$ and $W(x)$ are two polynomials whose coefficients may be determined as soon as the k initial values of (u) are known. The numeric and characteristic number of (u) modulo m are respectively the least values of n such that the first and second of these congruences are satisfied.

The central result of this investigation is that these minimal values of n may be determined in general provided that we know the following:

- [i] (a) the decomposition of m into its prime factors;
- (b) the Schönemann decompositions* of $F(x)$, $V(x)$ and $W(x)$ modulo p^N , where p is a prime factor of m ;
- [ii] for every prime factor p of m and every irreducible polynomial factor $\phi(x)$ of $F(x)$ to the modulus p , the least value of n such that

$$x^n \equiv 1 \pmod{p, \phi(x)};$$

- [iii] if λ is the least value of n satisfying [ii], the polynomial $L(x)$ defined by

$$x^\lambda - 1 \equiv pL(x) \pmod{p^2, \phi^2(x)}.$$

We have then a complete analogy with the case of a difference equation of order one. Corresponding to (ii), [ii] is the unsolved problem of determining the period of a mark in a Galois field, while [iii] is a kind of generalization of the problem of the quotients of Fermat.†

The methods employed are elementary in the sense that no use is made either of the theory of ideals or the “fundamental theorem of algebra.” Instead free use is made of polynomial congruences to single and double moduli in the spirit of Kronecker’s theory of algebraic fields. The difficulties in the algebraic treatment due to discriminantal divisors are thereby evaded.‡

* See Fricke’s *Algebra*, vol. 2, Braunschweig, 1928, chapter 2, and §7 of the present paper.

† Compare Ward, p. 161.

‡ Compare Engstrom, p. 211.

3. We shall adopt the following terminology in this paper. The term polynomial is restricted to mean a polynomial with integral coefficients; if the leading coefficient of the polynomial is unity, it will be said to be primary. We designate polynomials by $A(x)$, $B(x)$, \dots , $U(x)$, $V(x)$, \dots , $\theta(x)$, $\phi(x)$, \dots . A polynomial is said to be divisible by an integer m when and only when all of its coefficients are divisible by m . The notations $\text{Res } \{A(x), B(x)\}$ and (a, b, \dots) will be used for the resultant of two polynomials $A(x)$ and $B(x)$ and the greatest common divisor of two or more integers a, b, \dots .

If (a) is the reduced sequence corresponding to the solution (u) of (1.1) modulo m , and if μ is a period of (a) , we shall say that (u) admits the period μ (mod m , $F(x)$) where it will be recalled that $F(x) = x^k - \dots - c_k$ is the polynomial associated with the difference equation (1.1). In like manner, we shall refer to the characteristic number of (u) as its characteristic number (mod m , $F(x)$) whenever it is necessary to bring m and $F(x)$ in evidence. The notation

$$(u) \equiv (v), (u) \equiv (a) \pmod{m}, 0 \leq a < m,$$

is self-explanatory.

The following convenient definition was introduced by H. T. Engstrom*: A number π is said to be a general period of the difference equation (1.1) for the modulus m if every sequence of rational integers (u) satisfying (1.1) has the period π . Let τ be the least such general period for the modulus m . Then it is easily seen that every other general period is a multiple of τ , and that the characteristic number of any particular sequence (u) is a divisor of τ . We shall call τ the principal period of the difference equation (1.1) (mod m , $F(x)$). It possesses the following important property:

THEOREM 3.1. *There exist solutions of (1.1) whose characteristic number modulo m is the principal period of (1.1).*

Let (u) and (w) be any two solutions of (1.1). Then if we can determine integers b_1, b_2, \dots, b_k such that

$$u_n \equiv b_1 w_n + b_2 w_{n+1} + \dots + b_k w_{n+k-1} \pmod{m}, n = 0, 1, \dots,$$

the characteristic number of (w) will be a period of (u) . Owing to the linearity of (1.1) these congruences will hold for every n provided that they hold for $n=0, 1, 2, \dots, k-1$. But a sufficient condition that the k congruences

$$\begin{array}{rcl} b_1 w_0 + \dots + b_k w_{k-1} & \equiv & u_0, \\ \vdots & & \vdots \\ b_1 w_{k-1} + \dots + b_k w_{2k-1} & \equiv & u_{k-1} \end{array} \quad (\text{mod } m)$$

* Engstrom, p. 210.

have integral solutions b_1, \dots, b_k is that their determinant be prime to m . For that particular sequence (w) with the initial values $w_0 = w_1 = \dots = w_{k-2} = 0, w_{k-1} = 1$, this determinant has the value $(-1)^k$.

Hence the characteristic number of (w) is a general period of (1.1). But the characteristic number of (w) must divide the principal period. Hence it is equal to it.

Thus the principal period is the least upper bound of the characteristic numbers of all solutions of (1.1), and the determination of the characteristic number of (w) gives the solution of the second fundamental problem mentioned in the introduction.

COROLLARY. *If (u) is any solution of (1.1) and if $\Delta(u)$ denotes the determinant*

$$\Delta(u) = \begin{vmatrix} u_0, & u_1, \dots, u_{k-1} \\ u_1, & u_2, \dots, u_k \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ u_{k-1}, & u_k, \dots, u_{2k-1} \end{vmatrix},$$

then if $\Delta(u)$ is prime to m , the characteristic number of (u) is the principal period of (1.1).

As an application of this corollary, consider the solution (s) of (1.1) with the initial values $s_0 = k, s_1 = c_1, s_2 = c_1^2 + 2c_2$ and so on, so that if the discriminant of $F(x)$ does not vanish, s_n is the familiar sum of the n th powers of the roots of $F(x) = 0$. It is well known that $\Delta(s)$ equals the discriminant of $F(x)$. Hence *the characteristic number of (s) is the principal period of (1.1) provided that m is prime to the discriminant of $F(x)$.*

II. THE RELATIONSHIP WITH THE RING ASSOCIATED WITH THE DOUBLE MODULUS

4. We begin by considering the solutions of (1.1) from a group-theoretic stand-point. If we regard any two solutions (u) and (v) of (1.1) as one-rowed matrices we may define their “sum” to be the sequence $(u+v)$:

$$(u) + (v) = (u + v).$$

The set of all solutions of (1.1) form an infinite Abelian group with respect to the operation of vector addition just defined, the identity element of the group being the sequence

$$(0): \quad 0, 0, \dots, 0, \dots.$$

Denote this group by \mathfrak{U} and the corresponding finite group of the reduced sequences (a) by \mathfrak{A} . The relationship between these two groups may be conveniently symbolized by writing

$$\mathfrak{U} \equiv \mathfrak{A} \pmod{m}.$$

Now the method of attack upon the fundamental problems mentioned in the introduction is *to set up an isomorphism between the group \mathfrak{A} and the ring of residue classes associated with the double modulus m and $F(x)$* . The problems considered are thus transformed into problems belonging to the theory of congruences to a double modulus which admit of perfectly definite answers.

To set up this isomorphism, it is necessary to define the “product” of two sequences (u) and (v) . How this may be done will be explained in §6; for the present, we will confine ourselves to developing the idea of addition of sequences.

THEOREM 4.1. *Every sequence (u) may be uniquely represented modulo m as the sum of a null sequence and a purely periodic sequence with the same numeric and characteristic number.*

Let λ and μ be respectively the numeric and characteristic number of (u) modulo m , and suppose that $\lambda \equiv -r \pmod{\mu}$, where $0 \leq r < \mu$, so that $\lambda + r = q\mu$.

Set $v_n = u_{\lambda+r+n}$, $w_n = u_n - v_n$ ($n = 0, 1, \dots$).

Then (v) is a purely periodic sequence with the characteristic number μ modulo m , and

$$(u) = (v) + (w).$$

(w) is a null sequence modulo m with the numeric λ . For if $n \geq 0$,

$$\begin{aligned} w_{n+\lambda} &= u_{n+\lambda} - v_{n+\lambda} = u_{n+\lambda} - u_{q\mu+n+\lambda} \equiv 0, \\ w_{\lambda-1} &= u_{\lambda-1} - v_{\lambda-1} = u_{\lambda-1} - u_{q\mu+\lambda-1} \not\equiv 0 \end{aligned} \pmod{m}.$$

Such a representation of (u) is unique modulo m ; for if there were a second one

$$(u) = (v') + (w')$$

we would have $(w - w') = (v' - v)$, so that $(w - w')$ would be a purely periodic null sequence. Hence $(w - w') \equiv (0) \pmod{m}$, $(w) \equiv (w')$, $(v) \equiv (v') \pmod{m}$.

It is evident that the set of all null sequences of \mathfrak{A} and the set of all purely periodic sequences of \mathfrak{A} are both sub-groups of \mathfrak{A} . If we denote these sub-groups by \mathfrak{N} and \mathfrak{P} , we have from Theorem 4.1

THEOREM 4.2. *The group \mathfrak{A} is the direct sum of \mathfrak{N} and \mathfrak{P} , where \mathfrak{N} is the group of all null sequences of \mathfrak{A} , and \mathfrak{P} is the group of all purely periodic sequences of \mathfrak{A} .*

5. If we form from the first n terms of any solution (u) of (1.1) a polynomial of degree $n-1$ in the indeterminate x

$$U_n(x) = u_0x^{n-1} + u_1x^{n-2} + \cdots + u_{n-1},$$

it is easily verified that we have identically in x

$$\begin{aligned} F(x)U_n(x) &= x^n \{ u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + \cdots + (u_{k-1} - c_1u_{k-2} \\ &\quad - \cdots - c_{k-1}u_0) \} - \{ u_nx^{k-1} + (u_{n+1} - c_1u_n)x^{k-2} + \cdots \\ &\quad + (u_{n+k-1} - c_1u_{n+k-2} - \cdots - c_{k-1}u_n) \}. \end{aligned}$$

Denote the two polynomials in brackets by $U(x)$ and $U^{(n)}(x)$ respectively. Then on considering the identity modulo m , we obtain the congruence

$$(5.1) \quad x^n U(x) - U^{(n)}(x) \equiv 0 \pmod{m, F(x)}.$$

Assume first that (u) is purely periodic modulo m and admits the period n . Then $U^{(n)}(x) \equiv U(x) \pmod{m}$, so that (5.1) becomes

$$(x^n - 1)U(x) \equiv 0 \pmod{m, F(x)}.$$

Conversely if for some n this latter congruence holds, (u) is purely periodic modulo m and admits the period n .

Secondly, assume that (u) is a null sequence modulo m of numeric $\leq n$. Then $U^{(n)}(x) \equiv 0 \pmod{m}$ and (5.1) becomes

$$x^n U(x) \equiv 0 \pmod{m, F(x)}.$$

Conversely if for some n this latter congruence holds, (u) is a null sequence of numeric $\leq n$. We have thus established the following two basic theorems:

FUNDAMENTAL THEOREM ON PURELY PERIODIC SEQUENCES. *If (u) is any solution of the difference equation (1.1), then a necessary and sufficient condition that (u) should be purely periodic and admit the period n ($\text{mod } m, F(x)$) is that*

$$(5.2) \quad (x^n - 1)U(x) \equiv 0 \pmod{m, F(x)},$$

where

$$(5.3) \quad U(x) = u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + \cdots + (u_{k-1} - c_1u_{k-2} - \cdots - c_{k-1})$$

is a polynomial of degree $k-1$ in x whose coefficients are determined entirely by the k initial values of (u) and the coefficients of (1.1), while $F(x)$ is the polynomial associated with (1.1).

We shall call the polynomial $U(x)$ which completely determines the k initial values of (u) and hence (u) itself, the *generator* of (u) .

FUNDAMENTAL THEOREM ON NULL SEQUENCES. *If $U(x)$ is the generator of the sequence (u) , then a necessary and sufficient condition that (u) should be a null sequence with numeric less than or equal to n is that*

$$(5.4) \quad x^n U(x) \equiv 0 \pmod{m, F(x)}.$$

We have the following important corollaries to these theorems.

COROLLARY 1. *If (u) is a purely periodic sequence modulo m , its characteristic number is the least value of n for which the congruence (5.2) is satisfied.*

COROLLARY 2. *If (u) is a null sequence modulo m , its numeric is the least value of n for which the congruence (5.4) is satisfied.*

The generator of the sequence (w) with the initial values $0, 0, \dots, 0, 1$ is unity. Hence we have from Theorem 3.1

COROLLARY 3. *The principal period of (1.1) modulo m is the least value of n such that*

$$x^n \equiv 1 \pmod{m, F(x)}.$$

6. We are now ready to establish the isomorphism between the ring of residue classes associated with the double modulus $m, F(x)$ and the group of reduced sequences defined in §4. The ring may be represented by the set of m^k polynomials

$$L(x) = l_0 x^{k-1} + l_1 x^{k-2} + \dots + l_{k-1} \quad (0 \leq l_i < m).$$

On identifying $U(x)$ of (5.3) modulo m with $L(x)$ we obtain the congruences

$$(6.1) \quad u_r - c_1 u_{r-1} - c_2 u_{r-2} - \dots - c_r u_0 \equiv l_r \pmod{m}, \quad r = 0, \dots, k-1.$$

These congruences have a unique solution

$$u_i \equiv a_i \pmod{m}, \quad 0 \leq a_i < m; \quad i = 0, \dots, k-1.$$

We associate with $L(x)$ the reduced sequence (a) whose initial values are a_0, \dots, a_{k-1} , and write

$$(a) \sim L(x).$$

Since the congruences (6.1) are solvable for the l_r for any m , given (a) , we can determine a unique $L(x)$. The correspondence is therefore a reciprocal one.

Suppose that

$$(b) \sim M(x).$$

Then evidently

$$(a + b) \sim L(x) + M(x).$$

If $L(x) \cdot M(x) \equiv N(x) \pmod{m, F(x)}$, we define the reduced sequence (c) associated with $N(x)$ to be the *product* of the sequences (a) and (b) . The exact dependence of the elements of (c) upon those of (a) and (b) need not detain us here. If we write $(a) \cdot (b)$ for the product of the sequences (a) and (b) , we have then

$$(a) \cdot (b) \sim L(x) \cdot M(x).$$

It is easily verified that the set \mathfrak{A} with the two operations of addition and multiplication just defined satisfies the postulates for a ring*; hence we have the following result:

THEOREM 6.1. *The set \mathfrak{A} of reduced sequences modulo m forms a commutative ring with respect to the operations of addition and multiplication of sequences defined above which is simply isomorphic with the ring \mathfrak{R} of residue classes associated with the double modulus $m, F(x)$.*

If

$$(a): \quad a_0, a_1, a_2, \dots$$

is any sequence of \mathfrak{A} , the corresponding element of the ring \mathfrak{R} is

$$L(x) = l_0x^{k-1} + l_1x^{k-2} + \dots + l_{k-1}$$

where

$$l_r \equiv a_r - c_1a_{r-1} - c_2a_{r-2} - \dots - c_ra_0 \pmod{m}, \quad r = 0, \dots, k-1.$$

To examine the nature of this correspondence further, we need the following lemma.

LEMMA. *If (u) is a solution of the difference equation (1.1), and if $\Delta(u)$ denotes the determinant*

$$\Delta(u) = \begin{vmatrix} u_0, & u_1, & \dots, & u_{k-1} \\ u_1, & u_2, & \dots, & u_k \\ \vdots & \vdots & & \vdots \\ u_{k-1}, & u_k, & \dots, & u_{2k-1} \end{vmatrix}$$

and $U(x)$ the polynomial

$$U(x) = u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + (u_2 - c_1u_1 - c_2u_0)x^{k-3} + \dots + (u_{k-1} - c_1u_{k-2} - \dots - c_{k-1}u_0),$$

then $(-1)^k\Delta(u)$ is equal to the resultant of $U(x)$ and $F(x)$, where $F(x)$ is the polynomial associated with the difference equation (1.1).

* van der Waerden, *Algebra*, Berlin, 1930, vol. 1, p. 37.

The nature of the proof is sufficiently indicated by the special case $k=3$. The resultant of $U(x)$ and $F(x)$ may then be expressed as the five-rowed eliminant

$$E = \begin{vmatrix} u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0, & 0, & 0 \\ 0, & u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0, & 0 \\ 0, & 0, & u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0 \\ 1, & -c_1, & -c_2, & -c_3, & 0 \\ 0, & 1, & -c_1, & -c_2, & -c_3 \end{vmatrix}.$$

Now perform upon E the operations

$$\text{row } 1 - u_0 \text{ row } 4 - u_1 \text{ row } 5, \quad \text{row } 2 - u_0 \text{ row } 5.$$

The first two elements in the first three rows of E become zero, so that E reduces to the third-order determinant

$$E = - \begin{vmatrix} u_2, & c_2u_1 + c_3u_0, & c_3u_1 \\ u_1, & u_2 - c_1u_1, & c_3u_0 \\ u_0, & u_1 - c_1u_0, & u_2 - c_1u_1 - c_2u_0 \end{vmatrix}.$$

From the difference equation,

$$u_3 = c_1u_2 + c_2u_1 + c_3u_0, \quad u_4 = c_1u_3 + c_2u_2 + c_3u_1.$$

Hence performing upon E successively the operations

$$\text{col } 2 + c_1 \text{ col } 1, \quad \text{col } 3 + c_2 \text{ col } 1 + c_1 \text{ col } 2,$$

we obtain

$$E = - \begin{vmatrix} u_2, & u_3, & c_3u_1 \\ u_1, & u_2, & c_3u_0 \\ u_0, & u_1, & u_2 - c_1u_1 - c_2u_0 \end{vmatrix} = - \begin{vmatrix} u_2, & u_3, & u_4 \\ u_1, & u_2, & u_3 \\ u_0, & u_1, & u_2 \end{vmatrix} = (-1)^3 \Delta(u).$$

THEOREM 6.2. *To the units of the ring \mathfrak{R} correspond those sequences of \mathfrak{A} whose characteristic number is the principal period of the difference equation (1.1) modulo m , while to the identity element 1 of \mathfrak{R} there corresponds the sequence (w) with the initial values $0, 0, \dots, 0, 1$.*

For the units of \mathfrak{R} are represented by those polynomials $L(x)$ such that the resultant of $L(x)$ and $F(x)$ is prime to m . But if $L(x) = U(x)$ is the generator of the sequence (u) , we have just seen that $\Delta(u)$ is numerically

equal to the resultant of $L(x)$ and $F(x)$. By the corollary to Theorem 3.1, the characteristic number of all sequences (u) with $\Delta(u)$ prime to m is the same, and equal to the principal period of (1.1) modulo m . The latter part of the theorem follows from the fact that for the sequence $(w): 0, 0, \dots, 0, 1, \dots$ we have $W(x) = 1$.

III. SIMPLIFICATION OF THE FORM OF THE MODULUS AND ASSOCIATED POLYNOMIAL

7. If $m = p_1^{n_1} \cdots p_r^{n_r}$ is the decomposition of m into its prime factors, then it is easy to see that the ring associated with the double modulus m , $F(x)$ is the direct sum of the r rings associated with the double moduli $p_i^{n_i}, F(x)$. We have of course a similar dissection of the ring \mathfrak{A} into a sum of simpler rings. The following important theorem gives the corresponding reduction of the problem of determining the characteristic number and numeric of any sequence modulo m to the case when m is a power of a prime.

THEOREM 7.1. *If*

$$m = p_1^{n_1} \cdots p_r^{n_r}$$

is the decomposition of m into its prime factors, then the characteristic number of any sequence modulo m is the least common multiple of its characteristic numbers modulis $p_i^{n_i}$ ($i = 1, \dots, r$) while its numeric is the maximum of its numerics modulis $p_i^{n_i}$.

It is sufficient to show that if $m = a \cdot b$ where a and b are relatively prime, then the characteristic number of (u) modulo m is the least common multiple of its characteristic numbers modulo a and modulo b , while its numeric modulo m is the greatest of its numerics modulo a and modulo b .

Let

$$(u) \equiv (v) + (w) \pmod{m}$$

be the unique decomposition of (u) into a null sequence (v) and a purely periodic sequence (w) . Then since a and b divide m ,

$$(u) \equiv (v) + (w) \pmod{a}, \text{ and } (u) \equiv (v) + (w) \pmod{b}.$$

Furthermore (v) is a null sequence modulis a and b and (w) is a purely periodic sequence modulis a and b .

In view of Theorem 4.1, it is sufficient to prove the result for the numeric of (v) and the characteristic number of (w) .

Consider first (v) , and let $V(x)$ be its generator, ν_m, ν_a and ν_b its numerics modulis m, a and b respectively, and τ the greatest of ν_a and ν_b . Then by the fundamental theorem of §5,

$$\begin{aligned} x^{r_m} V(x) &\equiv 0 \pmod{m, F(x)}, \quad x^{r_a} V(x) \equiv 0 \pmod{a, F(x)}, \\ x^{r_b} V(x) &\equiv 0 \pmod{b, F(x)}. \end{aligned}$$

Thus $x^{r_m} V(x) \equiv 0 \pmod{a, F(x)}$ (and $\pmod{b, F(x)}$) so that $r_m \geq \tau$. But since a and b are relatively prime,

$$x^{\tau} V(x) \equiv 0 \pmod{ab, F(x)}$$

so that $\tau \geq r_m$. Hence $\tau = r_m$.

The proof for the characteristic number of (w) is similar and will be left to the reader.*

We shall assume hereafter that $m = p^N$, p a prime, N a given integer.

Now suppose that

$$F(x) \equiv \{\phi_1(x)\}^{t_1} \cdot \{\phi_2(x)\}^{t_2} \cdots \{\phi_s(x)\}^{t_s} \pmod{p}$$

is the unique decomposition of $F(x)$ modulo p into a product of powers of primary irreducible polynomials $\phi(x)$. Then by Schönemann's second theorem† there exists a decomposition of $F(x)$ modulo p^N of the form

$$(7.1) \quad F(x) \equiv F_1(x) \cdot F_2(x) \cdots F_s(x) \pmod{p^N}$$

where

$$F_i(x) \equiv \{\phi_i(x)\}^{t_i} \pmod{p}, \quad i = 1, 2, \dots, s,$$

and the polynomials $F_i(x)$ are primary. We shall refer to (7.1) as a Schönemann decomposition of $F(x)$ (modulo p^N).

Corresponding to this decomposition of $F(x)$, we have a decomposition of the ring associated with the double modulus $p^N, F(x)$ into the direct sum of the s rings associated with the moduli $p^N, F_i(x)$. If $U(x)$ is any element of this ring, and

$$U(x) \equiv U^{(i)}(x) \pmod{p^N, F_i(x)}, \quad i = 1, \dots, s,$$

where $U^{(i)}(x)$ is of degree less than $F_i(x)$, then $U(x)$ may be uniquely represented as

$$U(x) \equiv B^{(1)}(x)U^{(1)}(x) + B^{(2)}(x)U^{(2)}(x) + \cdots + B^{(s)}(x)U^{(s)}(x) \pmod{p^N, F(x)}$$

where the $B^{(i)}(x)$ are of degree less than $F(x)$ and

$$\begin{aligned} B^{(i)}(x) &\equiv 1 \pmod{p^N, F_i(x)}, \\ &\equiv 0 \pmod{p^N, F_j(x)}, \quad j \neq i; 1 \leq j \leq s; i = 1, \dots, s. \end{aligned}$$

* See Ward, p. 155, Theorem 3.11.

† See Fricke, work cited, §11.

If (u) is the sequence generated by $U(x)$, $(u^{(i)})$ and $(b^{(i)})$ the sequences generated by $U^{(i)}(x)$ and $B^{(i)}(x)$, the analogous decomposition of (u) is

$$(u) \equiv (b^{(1)}) \cdot (u^{(1)}) + (b^{(2)}) \cdot (u^{(2)}) + \cdots + (b^{(s)}) \cdot (u^{(s)}) \pmod{p^N}.$$

The corresponding theorem for the characteristic numbers and numeric of (u) is as follows:

THEOREM 7.2. *Suppose that (7.1) is a Schönemann decomposition of $F(x)$ modulo p^N , and that $U(x)$ is a polynomial of degree $\leq k-1$ in x generating a sequence (u) . Furthermore suppose that*

$$U(x) \equiv U^{(i)}(x) \pmod{p^N, F_i(x)}$$

where $U^{(i)}(x)$ is a polynomial of degree less than $F_i(x)$, and the generator of a sequence $(u^{(i)})$ which is a solution of the difference equation whose associated polynomial is $F_i(x)$.

Then the characteristic number of (u) ($\text{mod } p^N, F(x)$) is the least common multiple of the characteristic numbers of $(u^{(i)})$ ($\text{mod } p^N, F_i(x)$) and the numeric of (u) is the maximum of the numerics of the $(u^{(i)})$.

Suppose that

$$(u) \equiv (v) + (w) \pmod{p^N} \text{ and } U(x) \equiv V(x) + W(x) \pmod{p^N, F(x)}$$

are the decompositions of (u) into a null sequence (v) and a purely periodic sequence (w) , and the corresponding decomposition of the generator $U(x)$ of (u) . Furthermore, suppose that

$$U(x) \equiv U^{(i)}(x), V(x) \equiv V^{(i)}(x), W(x) \equiv W^{(i)}(x) \pmod{p^N, F_i(x)}$$

where the polynomials on the right side of the congruences are of lesser degree than $F_i(x)$, and that $(u^{(i)})$, $(v^{(i)})$ and $(w^{(i)})$ are the solutions of the difference equation associated with $F_i(x)$ with the generators $U^{(i)}(x)$, $V^{(i)}(x)$ and $W^{(i)}(x)$ respectively. Then we may write

$$(7.2) \quad \begin{aligned} (u^{(i)}) &\equiv (v^{(i)}) + (w^{(i)}) \pmod{p^N}, \\ U^{(i)}(x) &\equiv V^{(i)}(x) + W^{(i)}(x) \pmod{p^N, F_i(x)}. \end{aligned}$$

I assert that (7.2) gives the decomposition of $(u^{(i)})$ into its purely periodic and null components; for if τ and λ are the numeric and characteristic number of (u) , we have by the theorems of §§4 and 5

$$x^\tau V(x) \equiv 0, \quad x^\lambda W(x) \equiv W(x) \pmod{p^N, F(x)}.$$

Hence

$$(7.3) \quad x^\tau V^{(i)}(x) \equiv 0, \quad x^\lambda W^{(i)}(x) \equiv W^{(i)}(x) \pmod{p^N, F_i(x)}$$

so that by the theorems of §5, $(v^{(i)})$ is a null sequence and $(w^{(i)})$ is a purely

periodic sequence. By Theorem 4.1, the numeric of $(v^{(i)})$ and the characteristic number of $(w^{(i)})$ are the numeric and the characteristic number of $(u^{(i)})$. Call this latter number λ_i ; and let μ be the least common multiple of $\lambda_1, \lambda_2, \dots, \lambda_s$. From the second congruence in (7.3), $(w^{(i)})$, and hence $(u^{(i)})$, admits the period λ (mod $p^N, F_i(x)$). Hence λ_i divides λ so that μ divides λ . But clearly

$$(x^\mu - 1)W^{(i)}(x) \equiv 0 \quad (\text{mod } p^N, F_i(x))$$

so that

$$(x^\mu - 1)W(x) \equiv 0 \quad (\text{mod } p^N, F_i(x)), i=1, \dots, s.$$

Since the resultant of any two distinct $F_i(x)$ is prime to p , these last congruences imply that

$$(x^\mu - 1)W(x) \equiv 0 \quad (\text{mod } p^N, F(x)).$$

Hence by the fundamental theorem again, λ divides μ so that λ equals μ .

The proof of the result for the numerics is similar and will be omitted here.

8. In the present section, we shall solve completely the problem of determining the null component and the purely periodic component of any sequence (mod $p^N, F(x)$).

Let us assume that the coefficient c_k in (1.1) is divisible by p . Then in the Schönemann decomposition (7.1) one of the $F_i(x)$ must be of the form $x^{t_i} + pV(x)$; let us suppose that it is $F_1(x)$, so that

$$F_1(x) = x^{t_1} + pV(x).$$

The exponent t_1 is simply the number of consecutive coefficients $c_k, c_{k-1}, c_{k-2}, \dots$ which are divisible by p . Let

$$F'(x) = F_2(x) \cdot F_3(x) \cdots F_s(x),$$

so that $\text{Res} \{F_1(x), F'(x)\}$ is prime to p .

By the fundamental theorem of §5, the sequence (u) is a null sequence modulo p^N when and only when the congruence

$$x^n U(x) \equiv 0 \quad (\text{mod } p^N, F(x))$$

is solvable, $U(x)$ denoting as usual the generator of (u) . But this congruence is solvable when and only when the two congruences

$$x^n U(x) \equiv 0 \quad (\text{mod } p^N, F_1(x)), \quad x^n U(x) \equiv 0 \quad (\text{mod } p^N, F'(x))$$

are solvable. The first of these congruences is solvable for any $U(x)$, for we may take $n=Nt_1$. The second is solvable when and only when $U(x) \equiv 0$ (mod $p^N, F'(x)$) for $\text{Res} \{x, F'(x)\}$ is prime to p . We have thus established the following theorem.

THEOREM 8.1. *If in the Schönemann decomposition modulo p^N of the polynomial $F(x)$ associated with the difference equation (1.1),*

$$(7.1) \quad F(x) \equiv F_1(x) \cdot F_2(x) \cdots F_s(x) \pmod{p^N},$$

we have $F_1(x) = x^{t_1} + pV(x)$, then a necessary and sufficient condition that a given solution (u) of (1.1) be a null sequence modulo p^N is that its generator $U(x)$ satisfy the relation

$$U(x) \equiv 0 \pmod{p^N, F_2(x) \cdots F_s(x)}.$$

In this case its numeric is the least value of n such that

$$(8.1) \quad x^n U(x) \equiv 0 \pmod{p^N, F_1(x)}.$$

We can prove the following result in very much the same manner.

THEOREM 8.2. *With the hypotheses of Theorem 8.1, a necessary and sufficient condition that a given solution (u) of (1.1) be purely periodic modulo p^N is that its generator $U(x)$ satisfy the relation*

$$U(x) \equiv 0 \pmod{p^N, F_1(x)}.$$

The decomposition of (u) into its purely periodic and null components is now easily effected. For since $\text{Res} \{F_1(x), F'(x)\}$ is prime to p , we can determine two polynomials $S_1(x), S_2(x)$ such that

$$S_1(x)F_1(x) + S_2(x)F'(x) \equiv U(x) \pmod{p^N, F(x)}.$$

Suppose that

$$S_2(x)F'(x) \equiv V(x), \quad S_1(x)F_1(x) \equiv W(x) \pmod{p^N, F(x)}$$

where the degrees of $V(x)$ and $W(x)$ do not exceed $k-1$, and let (v) and (w) be the sequences generated by $V(x)$ and $W(x)$ respectively. Then

$$U(x) \equiv V(x) + W(x) \pmod{p^N, F(x)}, \quad (u) \equiv (v) + (w) \pmod{p^N},$$

and (v) is a null sequence and (w) a purely periodic sequence modulo p^N .

IV. THE DETERMINATION OF THE NUMERIC

9. If (u) is a null sequence modulo p^N , we have just seen that its generator is of the form

$$U(x) \equiv U'(x) \cdot F_2(x) \cdots F_s(x) \pmod{p^N}$$

and that its numeric is the least value of n such that

$$x^n U'(x) \equiv 0 \pmod{p^N, F_1(x)}.$$

$F_1(x)$ it will be recalled is of the form $x^{t_1} + pV(x)$. It may happen that $V(x)$ is also divisible by p . To conserve generality, we therefore assume that

$$F_1(x) = x^{t_1} - p^{\alpha} \theta(x); \quad \theta(x) \not\equiv 0 \pmod{p}; \quad \theta(x) \text{ of degree less than } t_1.$$

By Schönemann's theorems,* $U'(x)$ has a decomposition modulo p^N of the form

$$U'(x) \equiv p^M G_1(x) U''(x) \pmod{p^N}$$

where

$$M \geq 0, \quad G_1(x) = x^{\alpha_1} + p^{\beta_1} \xi_1(x);$$

$$\text{Res } \{G_1(x), U''(x)\} \text{ prime to } p; \quad \xi_1(x) \not\equiv 0 \pmod{p}.$$

It follows immediately that the numeric of (u) is the least value of n such that

$$(9.1) \quad x^n G_1(x) \equiv 0 \pmod{p^{N-M}, F_1(x)}.$$

This minimal value may always be calculated in view of the following two theorems:

THEOREM 9.1. Suppose that a set of polynomials $U(x)$, $G(x)$, $\xi(x)$ are defined recursively by

$$\begin{aligned} U_{r-1}(x) &\equiv G_r(x) \bar{U}_{r-1}(x) \pmod{p^{L_{r-1}}}, \quad r = 1, 2, \dots, \\ x^{t_1-\alpha_r} G_r(x) &\equiv p^{\rho_r} U_r(x) \pmod{F_1(x)}, \\ G_r(x) &= x^{\alpha_r} + p^{\beta_r} \xi_r(x), \\ L_r &= N - M - (\rho_1 + \rho_2 + \dots + \rho_r), \end{aligned}$$

where $U_r(x)$ is not divisible by p , $\bar{U}_{r-1}(x)$ is not divisible by x modulo p , and $\xi_r(x)$ is a polynomial of degree less than α_r , not divisible by p , while $U_0(x) = G_1(x) U''(x)$, $\bar{U}_0(x) = U''(x)$. Then the numbers ρ are all positive, and after a finite number of steps, say l , we will either have

$$N \leq M + \rho_1 + \rho_2 + \dots + \rho_l \text{ or } \text{Res } \{U_l(x), F_1(x)\} \text{ prime to } p.$$

Let l now denote the first time one of these alternatives occurs. Then in the first case, the numeric of (u) is $lt_1 - (\alpha_1 + \alpha_2 + \dots + \alpha_l)$ and in the second case, the numeric is $lt_1 - (\alpha_1 + \alpha_2 + \dots + \alpha_l) + \nu_l$, where ν_l is the least value of n such that

$$(9.2) \quad x^n \equiv 0 \pmod{p^{L_l}, F_1(x)}.$$

* Fricke, work cited, p. 59, p. 65.

THEOREM 9.2. Suppose that a set of polynomials $\theta_r(x)$, $\bar{\theta}_r(x)$ are defined recursively by

$$\begin{aligned}\theta_r(x) &\equiv (x^{\tau_r} + p^{\sigma_r} \phi_r(x)) \bar{\theta}_r(x) \pmod{p^{L_k}}, \\ x^{\tau_1 - \tau_r} \theta_r(x) &\equiv p^{\sigma_r} \theta_{r+1}(x) \pmod{F_1(x)}, r = 1, 2, \dots,\end{aligned}$$

where $\theta_r(x)$ is not divisible by p , and $\bar{\theta}_r(x)$ is not divisible by x modulo p , $\phi_r(x)$ is a polynomial of degree less than τ_r not divisible by p , while τ_r is the number of consecutive coefficients of the zeroth, first, second, \dots powers of x in $\theta_r(x)$ which are divisible by p . Then after a finite number of steps, say h , we will either have $L_1 \leq \sigma_1 + \sigma_2 + \dots + \sigma_h$ or $\tau_h = 0$ and $\text{Res } \{\theta_h(x), F_1(x)\}$ prime to p .

Let h denote the first time one of these alternatives occurs. Then in the first case, the least value of n for which the congruence (9.2) is satisfied is $\bar{\tau}_h = ht_1 - (\tau_1 + \tau_2 + \dots + \tau_h)$. In the second case it is $q_h \bar{\tau}_h$, where q_h is the integer next greater than or equal to L_1 divided by $\sigma_1 + \sigma_2 + \dots + \sigma_h$.

The proofs of these theorems are by induction, and are perfectly straightforward though rather lengthy. They will be omitted here, as the important result is that the numeric may be calculated if we merely know the Schönemann decompositions of $U(x)$ and $F(x)$ quite independently of the calculation of the characteristic number.

The following results are immediate corollaries of Theorems 9.1 and 9.2.

COROLLARY 1. If

$$\begin{aligned}F(x) &\equiv F_1(x) \cdots F_s(x) \pmod{p^N}, \\ F_1(x) &\equiv x^{t_1} - p^{\sigma_1} \theta_1(x) \quad (\theta_1(x) \not\equiv 0 \pmod{p})\end{aligned}$$

is the Schönemann decomposition of the polynomial $F(x) \pmod{p^N}$ associated with the difference equation (1.1), the least upper bound of the numerics of all solutions of (1.1) modulo p^N is qt_1 , where q is the integer next greater than or equal to N/σ_1 .

COROLLARY 2.* The least upper bound for the numerics of all difference equations (1.1) modulo p^N whose t_1 last coefficients are divisible by p is Nt_1 .

COROLLARY 3. The least upper bound for the numeric of all difference equations (1.1) of order k modulo p^N is Nk .

V. THE DETERMINATION OF THE CHARACTERISTIC NUMBER

10. In this division of the paper we shall reduce the problem of determining the characteristic number of any solution of (1.1) to its constituents in the sense explained in the introduction. In view of the results of §7, we may

* Due to Engstrom, p. 218, Theorem 9.

assume that $m = p^N$ where p is a prime, and that the associated polynomial $F(x)$ is of the form

$$(10.1) \quad F(x) = \{\phi(x)\}^a - p\theta(x)$$

where it will be recalled that $\phi(x)$ is primary and irreducible modulo p , while $\theta(x)$ is of lesser degree than $F(x)$.

The results of §8 allow us to assume that (u) is purely periodic. Hence by the fundamental theorem of §5, the characteristic number of (u) is the least value of n such that

$$(10.2) \quad (x^n - 1)U(x) \equiv 0 \pmod{p^N, F(x)},$$

where $U(x)$ is the generator of (u) .

The following easily established theorem* justifies us in assuming that $U(x)$ is not divisible by p .

THEOREM 10.1. *If (u) is any solution of the difference equation (1.1), the form of $F(x)$ being unrestricted, and if the integer d is a common factor of the k initial values of (u) , then the characteristic number of (u) to any modulus m is the characteristic number of $d^{-1}(u)$ modulo (m/l) , where l is the greatest common divisor of m and d .*

Suppose that λ is the characteristic number of (u) $(\text{mod } p^N, F(x))$, so that

$$(10.21) \quad (x^\lambda - 1)U(x) \equiv 0 \pmod{p^N, F(x)}$$

and let p^K be the first elementary divisor of the matrix of the eliminant of $U(x)$ and $F(x)$ corresponding to the prime p . Then I have shown elsewhere† that (10.21) implies that

$$x^\lambda - 1 \equiv 0 \pmod{p^{N-K}, F(x)}.$$

Thus λ is a multiple of the principal period of (1.1) modulo p^{N-K} .

THEOREM 10.2. *If the first elementary divisor of the matrix of the eliminant of $U(x)$ and $F(x)$ corresponding to the prime p is p^K , then the characteristic number of (u) $(\text{mod } p^N, F(x))$, $N > K$, is a multiple of the principal period of (1.1) modulo p^{N-K} .*

This theorem is of some practical importance, as it gives us a lower limit to the characteristic number of any sequence. The extension to composite m and $F(x)$ unrestricted is obvious in view of the results of §7.

* Ward, p. 157, Theorem 5.2.

† These Transactions, vol. 35 (1933), p. 258.

Since $U(x)$ in (10.2) is not congruent to zero modulo p , we may assume that

$$U(x) \equiv \{\phi(x)\}^b \psi(x) \pmod{p}, \quad a > b \geq 0,$$

where $\text{Res } \{\psi(x), \phi(x)\}$ is prime to p . Then by Schönemann's second theorem,[†] we have

$$U(x) \equiv U^*(x)V(x) \pmod{p^N}$$

where

$$(10.3) \quad U^*(x) = \{\phi(x)\}^b + p\xi(x), \quad \xi(x) \text{ of lower degree than } U^*(x),$$

and $V(x) \equiv \psi(x) \pmod{p}$.

It follows that *the characteristic number of (u) is the least value of n such that*

$$(10.4) \quad (x^n - 1)U^*(x) \equiv 0 \pmod{p^N, F(x)}.$$

To avoid circumlocutions, we shall refer to this number as the characteristic number of the congruence (10.4).

If $N = 1$, we may replace (10.4) by

$$(10.5) \quad x^n - 1 \equiv 0 \pmod{p, \{\phi(x)\}^{a-b}}.$$

Suppose that the polynomial $\phi(x)$ is of degree t in x . Then the characteristic number of

$$x^n - 1 \equiv 0 \pmod{p, \phi(x)}$$

is a well known quantity in the Galois field theory[‡]; for it is simply the exponent to which belongs the mark associated with a root of $\phi(x) = 0$ in the Galois field of order p^t . We shall regard this number as known to us[§]; it is a divisor of $p^t - 1$ and hence prime to p and at most equal to $p^t - 1$. Let us denote it by λ . Then there exist polynomials $\phi(x)$ of degree t for which the corresponding λ equals $p^t - 1$; in other words, $p^t - 1$ is not only an upper bound for λ , but it is the least upper bound for λ .

We have then

$$(10.6) \quad x^\lambda - 1 = \psi(x)\phi(x) + p\xi(x),$$

where $\psi(x)$ and $\xi(x)$ are polynomials and $\xi(x)$ is of lower degree than $\phi(x)$. Since the discriminant of $x^\lambda - 1$ is prime to p ,

$$(10.7) \quad \psi(x) \not\equiv 0 \pmod{p, \phi(x)}.$$

[†] Fricke, work cited, pp. 65–66.

[‡] See Dickson, *Linear Groups*, Teubner, 1901, Part I.

[§] Compare the remarks in §2 of the introduction.

From (10.6),

$$x^{r\lambda} \equiv 1 + r\psi(x)\phi(x) \pmod{p, \phi^2(x)}.$$

Hence the characteristic number of

$$x^n \equiv 1 \pmod{p, \phi^2(x)}$$

is $p\lambda$. But since

$$x^{p\lambda} \equiv 1 + \{\psi(x)\}^p \{\phi(x)\}^p \pmod{p},$$

$p\lambda$ is also the characteristic number of (10.5) if $2 \leq a - b \leq p$.

Proceeding in this manner, we obtain the following result:

THEOREM 10.3. *If $U(x)$ is the generator of a purely periodic solution (u) of the difference equation (1.1) whose associated polynomial is of the form*

$$F(x) \equiv \{\phi(x)\}^a \pmod{p}, \text{ while } U(x) \equiv \{\phi(x)\}^b V(x) \pmod{p},$$

where $\text{Res}\{V(x), \phi(x)\}$ is prime to p and $\phi(x)$ is irreducible modulo p , then the characteristic number of (u) modulo p is $p^q\lambda$ where the integer q is such that

$$p^{q-1} < a - b \leq p^q$$

and λ is the least value of n such that

$$x^n \equiv 1 \pmod{p, \phi(x)}.$$

THEOREM 10.4. *Under the hypothesis of Theorem 10.3, the principal period of (1.1) modulo p is $p^r\lambda$ where the integer r is determined by the condition*

$$p^{r-1} < a \leq p^r$$

and the least upper bound for the principal period is $p^r(p^t - 1)$, where t is the degree of the polynomial $\phi(x)$ in x .

We leave the formulation of the corresponding theorems when $F(x)$ is unrestricted in form and m any square-free integer to the reader.

11. We are now in a position to attack (10.4) in the general case when N is greater than one. We have, with the notation of Theorem 10.4,

$$(11.1) \quad x^{p^r\lambda} - 1 \equiv p^\sigma V(x) \pmod{F(x)}$$

where σ is a positive integer, and $V(x)$ is of lesser degree than $F(x)$. If $V(x) = 0$, we shall think of σ as arbitrarily large. If $V(x) \not\equiv 0$, the value of σ is fixed by the condition $V(x) \not\equiv 0 \pmod{p}$. Then

$$(11.2) \quad U^*(x)V(x) \equiv p^\rho W(x) \pmod{F(x)}$$

where ρ is a positive integer or zero, and $W(x)$ is of lesser degree than $F(x)$. If $W(x) = 0$, we assign an arbitrarily large value to ρ . Otherwise, the value of ρ is fixed by the condition $W(x) \not\equiv 0 \pmod{p}$.

ρ may be equally well defined as the largest whole number M such that

$$U(x)V(x) \equiv 0 \pmod{p^M, F(x)}.$$

Unless $V(x)$ divides $F(x)$ (when $U(x)$ may be taken so that $W(x)=0$), ρ has a definite upper bound† depending only on $V(x)$, $F(x)$ and p .

From (11.1), we deduce that

$$x^{\lambda p^{r+t}} \equiv (1 + p^\sigma V(x))^{p^t} \equiv 1 + p^{\sigma+t}V(x) + \frac{p^{2\sigma+t}(p^t - 1)}{1 \cdot 2}V^2(x) + \dots \pmod{F(x)}.$$

Hence from (11.2),

$$U^*(x)(x^{\lambda p^{r+t}} - 1) \equiv p^{\sigma+\rho+t}W(x) + p^{2\sigma+\rho+t}W(x)\frac{(p^t - 1)}{1 \cdot 2}V(x) + \dots \pmod{F(x)},$$

$$U^*(x)(x^{\lambda p^{r+t}} - 1) \equiv p^{\sigma+\rho+t}W(x) \pmod{p^{\rho+\sigma+t+1}, F(x)},$$

save possibly in the case $p=2$, $\sigma=1$, which we shall exclude. From this last congruence, we deduce the following theorems:

THEOREM 11.1. *If p is an odd prime, $N > 1$, the characteristic number of the congruence (10.4) is $p^r\lambda$ if $N \leq \rho + \sigma$ and $\lambda p^{r+N-\rho-\sigma}$ if $N \geq \rho + \sigma$, where ρ and σ are determined by the congruences (11.1) and (11.2).*

THEOREM 11.2. *If p is an odd prime, the least upper bound for the characteristic number of the congruence (10.4) for all choices of $U^*(x)$ is $p^r\lambda$ if $N \leq \rho$ and $\lambda p^{r+N-\rho}$ if $N \geq \rho$, where ρ is determined by the congruence (11.2).*

The fundamental problem of finding the characteristic number of any linear recursive sequence to any modulus m has thus finally reduced to determining the exponents σ and ρ in (11.1) and (11.2). We shall first seek to determine ρ in the case when p is odd and the exponent a in (10.1) is greater than unity.

If u is an indeterminate, and if we let

$$H(u) = u - \frac{u^2}{2} + \dots - \frac{u^{p-1}}{p-1},$$

$$K(u) = -\frac{u}{2} + \left(1 + \frac{1}{2}\right)\frac{u^2}{3} - \left(1 + \frac{1}{2} + \frac{1}{3}\right)\frac{u^3}{4} + \dots$$

$$+ \left(1 + \frac{1}{2} + \dots + \frac{1}{p-2}\right)\frac{u^{p-1}}{p-1},$$

$$L(u) = 1 - u + u^2 - \dots + u^{p-1},$$

$$H^{(r)}(x) = H((\phi\psi)^{p^r}), K^{(r)}(x) = K((\phi\psi)^{p^r}), L^{(r)}(x) = L((\phi\psi)^{p^r}),$$

† These Transactions, vol. 35 (1933), p. 258.

and, for uniformity of notation,

$$H^{(-1)}(x) = \zeta(x),$$

then it follows by induction on r from (10.6) that for any positive integral value of r ,

$$x^{p^r} \equiv 1 + p\Theta_1(x) + p^2\Theta_2(x) + \{\psi(x)\}^{p^r}\{\phi(x)\}^{p^r} \pmod{p^3},$$

where

$$(11.3) \quad \Theta_1(x) = H^{(r-1)}(x), \quad \Theta_2(x) = K^{(r-1)}(x) + H^{(r-2)}(x)L^{(r-1)}(x).$$

Now by (10.1),

$$\phi^{p^r} = \phi^a \cdot \phi^{p^r-a} = \phi^{p^r-a}(F + p\theta) \equiv p\theta\phi^{p^r-a} \pmod{F(x)}.$$

Therefore

$$(11.4) \quad x^{p^r} \equiv 1 + p(\theta\psi^{p^r}\phi^{p^r-a} + \Theta_1) + p^2\Theta_2 \pmod{p^3, F(x)}.$$

On comparing (11.4) and (11.1), we have

$$(11.41) \quad p^{\sigma-1}V(x) \equiv \theta\psi^{p^r}\phi^{p^r-a} + \Theta_1 + p\Theta_2 \pmod{p^2, F(x)}.$$

Therefore a necessary and sufficient condition that σ be greater than one is that $\theta\psi^{p^r}\phi^{p^r-a} + \Theta_1 \equiv 0 \pmod{p, F(x)}$. This congruence is equivalent to

$$(11.5) \quad \theta\psi^{p^r}\phi^{p^r-a} + \psi^{p^{r-1}}\phi^{p^{r-1}} - \frac{1}{2}\psi^{2p^{r-1}}\phi^{2p^{r-1}} + \dots \equiv 0 \pmod{p, \{\phi(x)\}^a},$$

which may be looked upon as a condition upon $\theta(x)$.

If $p^r-a > p^{r-1}$ or $\theta(x) \equiv 0 \pmod{p}$, the congruence has no solutions. For if it had a solution, we would have

$$\psi^{p^{r-1}} \equiv 0 \pmod{p, \phi(x)}$$

contradicting (10.7). If $p^r-a \leq p^{r-1}$ and $\theta(x) \not\equiv 0 \pmod{p}$, (11.5) implies that

$$\theta(x) \equiv 0 \pmod{p, \{\phi(x)\}^c}, \text{ where } c = p^{r-1} - p^r + a.$$

If $\theta(x) \equiv 0 \pmod{p, \{\phi(x)\}^{c+1}}$, we again obtain a contradiction of (10.7). Hence

$$\theta(x) \equiv \kappa(x) \{\phi(x)\}^c \pmod{p}, \quad \kappa(x) \not\equiv 0 \pmod{p, \phi(x)}.$$

On substituting in (11.5), we find that

$$(11.6) \quad \kappa\psi^{p^r-p^{r-1}} + 1 \equiv 0 \pmod{p, \{\phi(x)\}^{p^{r-1}}}.$$

This criterion can be greatly simplified. For if $y = x^{p^{r-1}}$,

$$\{\psi(x)\}^{p^r-p^{r-1}} \equiv \{\psi(y)\}^{p-1}, \quad \{\phi(x)\}^{p^{r-1}} \equiv \phi(y) \pmod{p}.$$

Hence (11.6) is equivalent to

$$\kappa(x) \{ \psi(y) \}^{p-1} + 1 \equiv 0 \quad (\text{mod } p, \phi(y)).$$

Since $\psi(y) \not\equiv 0 \pmod{p, \phi(y)}$, there exists a polynomial $\vartheta(y)$ of degree less than $\phi(y)$ such that

$$\vartheta(y) \{ \psi(y) \}^{p-1} + 1 \equiv 0 \quad (\text{mod } p, \phi(y)).$$

Hence $\kappa(x) \equiv \vartheta(y) \pmod{p, \phi(y)}$, so that we may take

$$\kappa(x) = \vartheta(x^{p-1}),$$

where

$$(11.7) \quad \vartheta(x) \{ \psi(x) \}^{p-1} + 1 \equiv 0 \quad (\text{mod } p, \phi(x)).$$

If we let

$$\theta_1(x) = \vartheta(x^{p-1}) \{ \phi(x) \}^c, \quad F_1(x) = \{ \phi(x) \}^a - p\theta_1(x),$$

the results we have obtained may be summarized in the following theorem:

THEOREM 11.3. *If p is an odd prime, $a > 1$, the exponent σ in (11.1) is generally unity. It is always unity if $p^r - a > p^{r-1}$, or if $\theta(x) \equiv 0 \pmod{p}$ or if $p^r - a > p^{r-1}$, $\theta(x) \not\equiv 0 \pmod{p, \phi(x)}$. It is greater than unity only when $F(x) \equiv F_1(x) \pmod{p^2}$ where the polynomial $F_1(x)$ has been defined above.*

The further study of the exceptional case when $F(x) \equiv F_1(x) \pmod{p^2}$ would take us too far afield and will not be embarked upon here. The theorems of §13 on the determination of ρ when $a = 1$ will give the reader an idea of the considerations which apply. We do however gain additional insight into the close relationship between recurring series and higher congruences if we seek to determine the polynomial $\psi(x)$ in (11.7) which must be known $(\text{mod } p, \phi(x))$ for $F_1(x)$ to be well defined. It will be recalled that $\psi(x)$ was originally defined as the quotient obtained on dividing $x^\lambda - 1$ by $\phi(x)$. Hence if

$$x^\lambda - 1 \equiv pL(x) \pmod{p^2, \phi^2(x)}, \quad L(x) \text{ of lesser degree than } \phi^2(x),$$

$\psi(x)$ satisfies the congruence

$$\psi(x) \equiv L(x) \quad (\text{mod } p, \phi(x)).$$

It is sufficient then for our purpose to determine $L(x)$.

Now if we set

$$\phi^2(x) = x^l - d_1x^{l-1} - \cdots - d_l,$$

$$x^n \equiv \sum_{k=1}^l w_{n,k} x^{l-k} \quad (\text{mod } \phi^2(x)),$$

$$w_{n,l+1} = 0 \quad (n = 0, 1, 2, \dots),$$

then it is easily verified that the constants $w_{n,k}$ satisfy the following relations:

$$\begin{aligned} w_{n+1,k} &= w_{n,k+1} + d_k w_{n,1} \quad (k = 1, \dots, l; n = 0, 1, 2, \dots), \\ w_{n,k} &= \delta_{n,l-k} \end{aligned} \quad (n < l)$$

where $\delta_{n,l-k}$ is the Kronecker δ . It follows without much difficulty that $w_{0,k}, w_{1,k}, w_{2,k}, \dots$ is a particular solution of the difference equation

$$(11.8) \quad \Omega_{n+l} = d_1 \Omega_{n+l-1} + \dots + d_l \Omega_n.$$

For convenience denote the sequence $w_{0,l-1}, w_{1,l-1}, w_{2,l-1}, \dots$ whose initial values are $0, 0, \dots, 0, 1$ simply by (w) . Then we may write for a fixed k

$$w_{n,k} = \sum_{j=1}^l c_{kj} w_{n+l-j}$$

where the c_{kj} are integers determined by the l equations

$$\sum_{j=1}^l c_{kj} w_{n+l-j} = \delta_{n,l-k} \quad (n = 0, 1, \dots, l-1).$$

Thus if

$$W_j(x) = \sum_{k=1}^l c_{kj} x^{l-k},$$

$W_j(x)$ is a polynomial of degree $l-1$ in x with integral coefficients, which we may regard as known to us. Then

$$\begin{aligned} x^n &= \sum_{k=1}^l w_{n,k} x^{l-k} = \sum_{k=1}^l \sum_{j=1}^l c_{kj} w_{n+l-j} x^{l-k} \\ &= \sum_{j=1}^l w_{n+l-j} W_j(x). \end{aligned}$$

Hence

$$pL(x) \equiv w_{\lambda+l-1} W_1(x) + w_{\lambda+l-2} W_2(x) + \dots + w_\lambda W_l(x) + 1 \pmod{\phi^2(x)}$$

so that $L(x)$ is determined if we know the residues modulo p^2 of the l terms $w_{\lambda+l-1}, w_{\lambda+l-2}, \dots, w_\lambda$ of the solution $0, 0, \dots, 0, 1, d_1, \dots$ of (11.8). There seems to be no way of obtaining these residues short of calculating the whole sequence (w) modulo p^2 step by step out to $\lambda+l$ terms. Such a calculation will at the same time determine λ after at most p^t-1 terms have been found.

12. We are now in a position to study the value of ρ in (11.2) in the general case when $\sigma = 1$. We have from (10.3) and (11.41)

$$(12.1) \quad U^*(x)V(x) \equiv \theta\psi^{p^r}\phi^{p^{r-a+b}} + \phi^b\Theta_1 + p(\xi\psi^{p^r}\phi^{p^{r-a}} + \xi\Theta_1 + \phi^b\Theta_2) \pmod{p^2, F(x)}.$$

Hence ρ is greater than zero when and only when

$$\theta\psi^{p^r}\phi^{p^{r-a+b}} + \phi^b\Theta_1 \equiv 0 \pmod{p, F(x)};$$

that is, when and only when

$$(12.2) \quad \theta\psi^{p^{r-a+b}} + \phi^{p^{r-1}+b}\psi^{p^{r-1}}(1 - \frac{1}{2}\phi^{p^{r-1}}\psi^{p^{r-1}} + \dots) \equiv 0 \pmod{p, \{\phi(x)\}^a}.$$

If $p^r - a + b \geq a$, $p^{r-1} + b \geq a$, (12.2) is satisfied for any choice of $\theta(x)$. In the contrary case, it is either insolvable or imposes a condition upon $\theta(x)$. We find in fact that there are no solutions in any one of the five following cases:

- (i) $p^r - a + b \geq a$, $p^{r-1} + b < a$;
- (ii) $p^r - a + b < a$, $p^{r-1} + b < a$, $p^r - a > p^{r-1}$;
- (iii) $\theta(x) \equiv 0 \pmod{p}$, $p^{r-1} + b < a$;
- (iv) $p^r - a + b < a$, $p^{r-1} + b < a$, $p^{r-1} \geq p^r - a$,
 $\theta(x) \not\equiv \kappa(x)\{\phi(x)\}^{p^{r-1}-p^r+a} \pmod{p}$,

where $\kappa(x)\{\psi(x)\}^{p^r-p^{r-1}} + 1 \equiv 0 \pmod{p, \{\phi(x)\}^{2a-p^r-b}}$;

$$(v) \quad p^r - a + b < a, p^{r-1} + b \geq a, \theta(x) \not\equiv 0 \pmod{p, \{\phi(x)\}^{2a-p^r-b}}.$$

Thus generally speaking, if $\sigma = 1$, $\rho = 0$ unless $b \geq a - p^{r-1}$, $b \geq 2a - p^r$. Passing to this case, we have from (10.1), (11.21) and (12.1)

$$\begin{aligned} U^*(x)V(x) \equiv & p\{\theta^2\psi^{p^r}\phi^d + \theta\psi^{p^{r-1}}\phi^e(1 - \frac{1}{2}\psi^{p^{r-1}}\phi^{p^{r-1}} + \dots) + \xi\psi^{p^r}\phi^{p^{r-a}} \\ & + \xi\psi^{p^{r-1}}\phi^{p^{r-1}}(1 - \frac{1}{2}\psi^{p^{r-1}}\phi^{p^{r-1}} + \dots) \\ & + \phi^{b+p^{r-1}}\psi^{p^{r-1}}(-\frac{1}{2} + \frac{1}{2}\phi^{p^{r-1}}\psi^{p^{r-1}} - \dots) \\ & + \phi^{b+p^{r-2}}\psi^{p^{r-2}}(1 - \frac{1}{2}\psi^{p^{r-2}}\phi^{p^{r-2}} + \dots)\} \pmod{p^2, F(x)}, \end{aligned}$$

where the last group of terms within the bracket must be replaced by $\phi^b\xi(x)(1 - \psi\phi + \dots)$ if $r = 1$, and the exponents d and e in the first two groups of terms are ≥ 0 and have the values $p^r - 2a + b$, $p^{r-1} + b - a$.

Hence $\rho = 1$ unless the expression in brackets above is congruent to zero ($\pmod{p, F(x)}$) or

$$(12.3) \quad \begin{aligned} & \theta^2\psi^{p^r}\phi^d + \theta\psi^{p^{r-1}}\phi^e + \xi\psi^{p^r}\phi^{p^{r-a}} + \xi\psi^{p^{r-1}}\phi^{p^{r-1}} + \phi^{b+p^{r-1}}\psi^{p^{r-1}} + \phi^{b+p^{r-2}}\psi^{p^{r-2}} \\ & + \phi^{b+2p^{r-2}}E + \xi\phi^{2p^{r-1}}F + \phi^{b+2p^{r-1}}G + \theta\phi^{e+p^{r-1}}H \equiv 0 \pmod{p, \phi^a}, \end{aligned}$$

where E, F, G, H denote polynomials in x which are not congruent to zero ($\text{mod } p, \phi(x)$) with integral coefficients modulo p . The terms $\phi^{b+2p^{r-2}}E + \phi^{b+p^{r-2}}\psi^{p^{r-2}}$ must be replaced by $\phi^b\zeta + \phi^{b+1}\zeta E$ if $r=1$.

It is not difficult to show that the lowest exponent of ϕ occurring in (12.3) is either d or e so that (12.3) imposes a condition upon $\theta(x)$ of the type appearing under (12.2),

$$\theta(x) \equiv \{\phi(x)\}^g \pmod{p}.$$

The exponent g here depends upon the relative magnitudes of $a, b, p^r, p^{r-1}, p^{r-2}$ but may be shown to be positive. We may therefore state the following theorem:

THEOREM 12.1. *If p is an odd prime, $F(x) = \{\phi(x)\}^a + p\theta(x)$, $a > 1$, $\theta(x) \not\equiv 0 \pmod{p, \phi(x)}$, then p in (11.2) is unity if $p^r + b \geq 2a$, $p^{r-1} + b \geq a$ and zero otherwise. If $\theta(x) \equiv 0 \pmod{p}$, p is zero if $p^{r-1} + b < a$, and if $p^{r-1} + b \geq a$ it is unity unless both $p^r - a$ and p^{r-1} are $\leq b + p^{r-2}$ and $\theta(x)$ satisfies a special condition. If $\theta(x) \equiv 0 \pmod{p, \phi(x)} \not\equiv 0 \pmod{p}$, the same results usually apply unless $F(x)$ is of a special form similar to that of $F_1(x)$ in Theorem 11.4.*

13. We shall conclude by discussing the case when the exponent a in (10.1) is unity so that

$$(13.1) \quad F(x) = \phi(x) - p\theta(x).$$

A necessary condition for this to hold is that p should not divide the discriminant of $F(x)$. Hence if this discriminant is not zero, the results of this section will apply to the powers of all primes save a finite number.

If the sequence (u) is not divisible by p , $\text{Res} \{U(x), F(x)\}$ is necessarily prime to p , so that the characteristic number of (u) modulo p^N is the principal period of (1.1), and hence the characteristic number of the congruence

$$x^n \equiv 1 \pmod{p^N, F(x)}.$$

With the notation of §10, let λ be the characteristic number of the congruence

$$x^n \equiv 1 \pmod{p, \phi(x)},$$

so that we have identically in x

$$(13.2) \quad \begin{aligned} x^\lambda - 1 &= \psi(x)\phi(x) + p\zeta(x), \\ \psi(x) &\not\equiv 0 \end{aligned} \pmod{p, \phi(x)}.$$

We shall now establish the following comprehensive theorem:

THEOREM 13.1. *Let p be an odd prime, $\phi(x)$ an irreducible polynomial modulo p , and suppose that the polynomial $F(x)$ associated with the difference equation (1.1) is of the form (13.1). Furthermore, let*

$$F_2(x) = \phi(x) - p\theta_1(x)$$

where $\xi(x) = \theta_1(x)$ is a solution of the congruence

$$\psi(x)\xi(x) + \zeta(x) \equiv 0 \quad (\text{mod } p, \phi(x)),$$

$\psi(x)$ and $\zeta(x)$ being given† by (13.2).

Then if $F(x) \not\equiv F_2(x) \pmod{p^2}$, the characteristic number modulo p^N of any solution of (1.1) which is not divisible by p is $p^{N-1}\lambda$, where λ is the least value of n such that

$$x^n \equiv 1 \quad (\text{mod } p, \phi(x)).$$

On the other hand, if $F(x) \equiv F_2(x) \pmod{p^2}$, there exists a set of polynomials $F_2(x), F_3(x), \dots, F_T(x), \dots$, depending only upon $p, \phi(x), \psi(x)$ and $\zeta(x)$, such that if $F(x) \equiv F_T(x) \pmod{p^T}$, $\not\equiv F_{T+1}(x) \pmod{p^{T+1}}$, the characteristic number is λ or $p^{N-T}\lambda$ according as $N \leq T$ or $N \geq T$.

We have

$$x^\lambda - 1 = \psi(x)F(x) + p(\theta(x)\psi(x) + \zeta(x)).$$

Suppose first that $\theta(x)\psi(x) + \zeta(x) \not\equiv 0 \pmod{p, \phi(x)}$. Then

$$x^\lambda \equiv 1 + pK(x) \quad (\text{mod } F(x))$$

where $K(x)$ is of lesser degree than $F(x)$ and not divisible by p . On raising this last congruence to the p^r th power, we obtain

$$(13.3) \quad x^{p^r\lambda} \equiv 1 + p^{r+1}K(x) + \frac{p^r(p^r-1)}{1 \cdot 2} p^2 K(x) + \dots \quad (\text{mod } F(x)).$$

Hence if p is an odd prime,

$$x^{p^r\lambda} \equiv 1 + p^{r+1}K(x) \quad (\text{mod } p^{r+2}, F(x)).$$

But clearly

$$x^{p^{r+1}\lambda} \equiv 1 \quad (\text{mod } p^{r+2}, F(x)).$$

Since the characteristic number of (13.1) for $N=r+2$ is a multiple of its characteristic number for $N=r+1$, it is exactly equal to $p^{N-1}\lambda$.

Now let us assume that

† They may be determined sufficiently to define $F_2(x)$ by the procedure sketched in §11.

$$\psi(x)\theta(x) + \zeta(x) \equiv 0 \pmod{p, \phi(x)}.$$

This congruence has a unique solution modulo p of degree less than $\phi(x)$. Let us denote it by $\theta_1(x)$, and set

$$F_2(x) = \phi(x) - p\theta_1(x).$$

Then if $F(x) \not\equiv F_2(x) \pmod{p^2}$, $\theta(x) \not\equiv \theta_1(x) \pmod{p}$. Consequently $\psi(x)\theta(x) + \zeta(x) \not\equiv 0 \pmod{p, \phi(x)}$ and the argument just given is applicable. Assume then that

$$F(x) \equiv F_2(x) \pmod{p^2}.$$

Consider the polynomials

$$F_1(x), F_2(x), F_3(x), \dots, F_k(x), \dots$$

defined by the recursive relations†

$$(13.4) \quad \begin{aligned} F_k(x) &= \phi(x) - p\Theta_{k-1}(x), \quad \Theta_k(x) = \Theta_{k-1}(x) + p^{k-1}\theta_k(x), \quad \Theta_0(x) = 0, \\ \psi(x)\Theta_{k-1}(x) + \zeta(x) &\equiv p^{k-1}r_k(x) \pmod{p^k, F_k(x)}, \\ \psi(x)\theta_k(x) + r_k(x) &\equiv 0 \pmod{p, \phi(x)}, \quad k = 1, 2, 3, \dots. \end{aligned}$$

These relations are consistent with one another; for if $k = 1$ they give $F_1(x) = \phi(x)$ and for $k = 2$ they give the polynomial $F_2(x)$ defined above. If we assume that they are consistent for $k = 1, 2, 3, \dots, s$ it easily follows that they are consistent for $k = s+1$.

Now suppose that

$$F(x) \equiv F_T(x) \pmod{p^T}, \not\equiv F_{T+1}(x) \pmod{p^{T+1}}, \quad T \geq 2.$$

Then

$$x^\lambda - 1 \equiv 0 \pmod{p^T, F(x)}, \not\equiv 0 \pmod{p^{T+1}, F(x)}.$$

For by (13.2) and the relations (13.4),

$$\begin{aligned} x^\lambda - 1 &= \psi(x)\phi(x) + p\zeta(x) = \psi(x)\{F_T(x) + p\Theta_{T-1}(x)\} + p\zeta(x) \\ &= \psi(x)F_T(x) + p(\psi(x)\Theta_{T-1}(x) + \zeta(x)) \\ &\equiv p(\psi(x)\Theta_{T-1}(x) + \zeta(x)) \pmod{F_T(x)} \\ &\equiv p \cdot p^{T-1}r_{T-1}(x) \pmod{p^T, F_T(x)} \\ &\equiv 0 \pmod{p^T, F_T(x)}, \quad \equiv 0 \pmod{p^{T+1}, F(x)}. \end{aligned}$$

In like manner it can be shown that

$$x^\lambda - 1 \not\equiv 0 \pmod{p^{T+1}, F(x)}.$$

† The $\Theta(x)$ here have no connection with those of §11.

Hence we have

$$x^\lambda \equiv 1 + p^T K(x) \pmod{F(x)},$$

where $K(x) \not\equiv 0 \pmod{p, F(x)}$. On raising this congruence to the appropriate power, we find that whether p be even or odd the characteristic number is $p^{N-T}\lambda$ or λ according as $N \geq T$ or $N \leq T$.

The case $p=2$, $T=1$ demands separate treatment. If $\theta(x)\psi(x)+\xi(x) \equiv K(x) \not\equiv 0 \pmod{2, \phi(x)}$, we obtain from (12.3), on putting $p=2$,

$$x^{2^r\lambda} = 1 + 2^{r+1}K(x)(1 + (2^r - 1)K(x) + \dots) \equiv 1 + 2^{r+1}K(x)(1 - K(x)) \pmod{2^{r+2}, F(x)}.$$

If $K(x) \not\equiv 1 \pmod{2}$, the previous argument for p odd is applicable. But in case $K(x) \equiv 1 \pmod{2}$, the characteristic number is a divisor of $2^r\lambda$.

Since $K(x)$ is of lesser degree than $F(x)$, the most general assumption is that

$$K(x) + 1 = 2^s L(x) \text{ where } L(x) \not\equiv 0 \pmod{2}.$$

Then

$$(13.5) \quad \begin{aligned} x^\lambda &\equiv -1 + 2^{s+1}L(x) \pmod{F(x)}, \\ x^{2\lambda} &\equiv 1 \pmod{2^{s+2}, F(x)}. \end{aligned}$$

Hence if $N=1$, the characteristic number is λ , while if $s+2 \geq N > 1$, the characteristic number is 2λ . On raising (13.5) to a power of 2, we find that if $N \geq s+2$, the characteristic number is $2^{N-s-1}\lambda$.

These results determine the characteristic number in the excluded case of (11.1) when $\sigma=1$ and $p=2$ for all $F(x)$ of the form $\phi(x)-2\theta(x)$. The further discussion of the characteristic number for powers of 2 demands a special treatment which will be given elsewhere.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

Type I'. $D(\rho) = 0$ has one real root and two complex roots. Corresponding to the real root ρ_1 there is a single real fixed point P_1 and a single real fixed line p_1 , where, by Theorem VII, p_1 does not pass through P_1 . If now we choose P_1 as the vertex $(1, 0, 0)$ and the line p_1 as the side $x_1=0$ of our triangle of reference, the collineation assumes the canonical form

$$\begin{aligned} \tau x'_1 &= \rho_1 x_1 \\ \tau x'_2 &= a_{22}x_2 + a_{23}x_3 \\ \tau x'_3 &= a_{32}x_2 + a_{33}x_3, \end{aligned}$$

where the quadratic

$$F(\rho) = \rho^2 - (a_{22} + a_{33})\rho + a_{22}a_{33} - a_{23}a_{32} = 0,$$

has imaginary roots, i.e.,

$$(a_{22} - a_{33})^2 + 4a_{23}a_{32} < 0.$$

A CORRECTION

Professor Morgan Ward has kindly called my attention to an unintentional misstatement of Theorem I of my note "*On a Certain Transformation of Infinite Series*" in the April number of this MONTHLY (vol. 40, p. 226). It should read as follows:

If $\lim_{n \rightarrow \infty} n u_n = l$ exists, then the two series (U) and (V) both diverge, if $l \neq 0$. If $l = 0$, the convergence of one implies that of the other, and the two series have the same sum.

J. A. SHOHAT

QUESTIONS, DISCUSSIONS, AND NOTES

EDITED BY R. E. GILMAN, Brown University, Providence, Rhode Island

The department of Questions and Discussions in the Monthly is open to all forms of activity in collegiate mathematics, including the teaching of mathematics, except for specific problems, especially new problems which are reserved for the department of Problems and Solutions.

A CERTAIN CLASS OF TRIGONOMETRIC INTEGRALS

By MORGAN WARD, California Institute of Technology

1. In the December issue of the MONTHLY¹ Professor Uhler has raised some questions about the functions defined by the indefinite integrals

$$\int \frac{\cos(\cot \theta)}{\sin} \frac{\cos \theta}{\sin} d\theta$$

¹ American Mathematical Monthly, vol. 39 (1932), p. 589.

which I propose to answer here. Let us define four functions of the real variable θ :

$$\begin{aligned} K_1(\theta) &= \int_0^\theta \cos(\tan \phi) \cos \phi d\phi, & K_2(\theta) &= \int_0^\theta \cos(\tan \phi) \sin \phi d\phi, \\ K_3(\theta) &= \int_0^\theta \sin(\tan \phi) \cos \phi d\phi, & K_4(\theta) &= \int_0^\theta \sin(\tan \phi) \sin \phi d\phi. \end{aligned}$$

The integrals under discussion are immediately expressible in terms of these functions; for example,

$$\int \cos(\cot \theta) \sin \theta d\theta = \text{const.} - K_1\left(\frac{\pi}{2} - \theta\right).$$

We shall show that the functions $K(\theta)$ are not expressible in finite terms by any simple known functions. However, in the range $-\pi/2 < \theta < \pi/2$, they are representable by convergent series of which

$$\begin{aligned} (1.1) \quad K_1(\theta) &= \sin \frac{\theta}{2} \cos \frac{\theta}{2} - \frac{1}{6} \cos \frac{3\theta}{2} \left(2 \sin \frac{\theta}{2}\right)^3 - \frac{1}{8} \sin 2\theta \left(2 \sin \frac{\theta}{2}\right)^4 \\ &\quad + \frac{1}{30} \cos \frac{5\theta}{2} \left(2 \sin \frac{\theta}{2}\right)^5 - \frac{1}{36} \sin 3\theta \left(2 \sin \frac{\theta}{2}\right)^6 \\ &\quad + \frac{2}{45} \cos \frac{7\theta}{2} \left(2 \sin \frac{\theta}{2}\right)^7 + \frac{1}{30} \sin 4\theta \left(2 \sin \frac{\theta}{2}\right)^8 + \dots \end{aligned}$$

may be quoted as typical. I shall give recursion formulas by which the numerical coefficients in these series may be calculated, and an estimate of the error terms. It turns out that the convergence is fairly good in the range $-\pi/4 \leq \theta \leq \pi/4$.

There also exist asymptotic expansions giving the behavior of the functions near $\pi/2$ and $-\pi/2$ which limitations of space forbid my developing here.

2. We begin by observing that from our defining relations, it follows that¹

$$\begin{aligned} K_1(\theta + \pi) &= -K_1(\theta); & K_2(\theta + \pi) &= 2K_2\left(\frac{\pi}{2}\right) - K_2(\theta); \\ K_3(\theta + \pi) &= 2K_3\left(\frac{\pi}{2}\right) - K_3(\theta); & K_4(\theta + \pi) &= -K_4(\theta). \end{aligned}$$

We may therefore assume that $-\pi/2 \leq \theta \leq \pi/2$.

If we let

$$P(\theta) = K_1(\theta) + iK_2(\theta), \quad Q(\theta) = K_3(\theta) + iK_4(\theta),$$

we obtain immediately from (1.1) the integral formulas

¹ The constants $K_2(\pi/2)$, $K_3(\pi/2)$ may be expressed as infinite integrals by writing $\tan \phi = x$, and these integrals may be evaluated in terms of Bessel functions, and related expressions.

$$P(\theta) + iQ(\theta) = \int_0^\theta \cos(\tan \phi) e^{i\phi} d\phi + i \int_0^\theta \sin(\tan \phi) e^{i\phi} d\phi = \int_0^\theta e^{i(\tan \phi + \phi)} d\phi,$$

$$P(\theta) - iQ(\theta) = \int_0^\theta \cos(\tan \phi) e^{i\phi} d\phi - i \int_0^\theta \sin(\tan \phi) e^{i\phi} d\phi = \int_0^\theta e^{-i(\tan \phi - \phi)} d\phi.$$

We shall now introduce two functions of a complex variable in terms of which these last integrals are easily expressible.

3. Let Z denote a complex variable. Consider the two functions

$$(3.1) \quad F(Z) = \int_1^Z \exp\left(\frac{1-z^2}{1+z^2}\right) dz, \quad G(Z) = \int_1^Z \exp\left(\frac{z^2-1}{z^2+1}\right) dz.$$

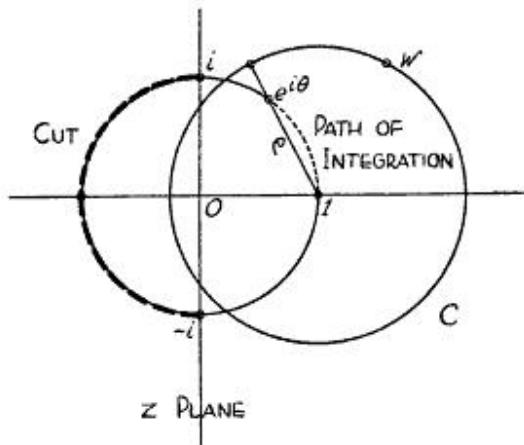
Then if we join the points $z=i$ and $z=-i$ by a cut which it is convenient to take along the left half of the unit circle (see figure), the reader may verify that

(a) The functions $F(Z)$ and $G(Z)$ are one-valued and analytic at all points Z of the cut z -plane save the point at infinity where each has a pole of order one, and their value at any point Z is independent of the path of integration joining 1 and Z .

(b) In particular, both functions are one-valued and analytic in the interior of a circle of radius $\sqrt{2}$ about the point $Z=1$.

(c) Both functions have essential singularities and logarithmic branch points at $z=i$ and $z=-i$, but remain finite as we approach these points along the right half of the unit circle.

(d) Upon a circle C with centre 1 and radius $\rho < \sqrt{2}$,



$$|F(Z)| \leq \rho \exp \frac{\sqrt{\rho^4 + 4} + \rho^2}{2(2 - \rho^2)}, \quad |G(Z)| \leq \rho \exp \frac{\sqrt{\rho^4 + 4} - \rho^2}{2(2 - \rho^2)}.$$

4. Now let $Z = e^{i\theta}$, $-\pi/2 < \theta < \pi/2$, be a point on the right half of the unit circle. Then if in the integrals (3.1) we choose for our path of integration the arc of the unit circle from 0 to θ , we obtain on writing $e^{i\phi}$ for z and reducing,

$$F(e^{i\theta}) = i \int_0^\theta e^{-i(\tan\phi - \phi)} d\phi, \quad G(e^{i\theta}) = i \int_0^\theta e^{i(\tan\phi + \phi)} d\phi.$$

On combining these results with the formulas of sections 1 and 2, we find that

$$(4.1) \quad \begin{aligned} K_1(\theta) &= \text{Real part of } \frac{F(e^{i\theta}) + G(e^{i\theta})}{2i}, \\ K_2(\theta) &= \text{Imaginary part of } \frac{F(e^{i\theta}) + G(e^{i\theta})}{2i}, \\ K_3(\theta) &= \text{Real part of } \frac{F(e^{i\theta}) - G(e^{i\theta})}{2}, \\ K_4(\theta) &= \text{Imaginary part of } \frac{F(e^{i\theta}) - G(e^{i\theta})}{2}. \end{aligned}$$

It is clear from these formulas that the function-theoretic nature of the $K(\theta)$ is determined by that of $F(Z)$ and $G(Z)$.

5. The nature of the functions $F(Z)$ and $G(Z)$ may be best seen from the differential equations which they satisfy. From formula (3.1)¹

$$\frac{dF}{dz} = \exp \frac{1-z^2}{1+z^2}; \quad \frac{dG}{dz} = \exp \frac{z^2-1}{z^2+1}.$$

Hence differentiating logarithmically, we see that

$$(5.1) \quad (z^2 + 1)^2 \frac{d^2F}{dz^2} + 4z \frac{dF}{dz} = 0; \quad (z^2 + 1)^2 \frac{d^2G}{dz^2} - 4z \frac{dG}{dz} = 0.$$

Consider the differential equation for $F(z)$. If we make the substitution $w = z^2/(z^2 + 1)$, this differential equation becomes

$$(5.3) \quad w(1-w) \frac{d^2F}{dw^2} - (2w^2 - w - \frac{1}{2}) \frac{dF}{dw} = 0.$$

The equation has 0 and 1 for regular points and ∞ for an irregular point. Now drawing upon the results of the theory of second order linear differential equations,² we see that if (5.3) is regarded as obtained by confluence from a differential equation with only regular points, the initial equation must have had five or more regular points. By actual trial, we find it is impossible to derive (5.3) from a differential with exactly five regular points. But all of the elementary functions of mathematical physics may be derived as solutions of confluent

¹ For convenience in printing, we hereafter write z for Z .

² See for example Whittaker and Watson, *Modern Analysis* Chap. X; or Ince, *Ordinary Differential Equations*, Chap. XX.

forms of such an equation. Hence $F(z)$ cannot be expressed in finite form by means of such functions.

Neither can $F(z)$ be expressed by means of elliptic integrals of the first or second kinds, for such integrals have no essential singularity in any part of the plane. A precisely similar argument holds for $G(z)$.

6. We are thus driven to seek series representations of $F(z)$ and $G(z)$ in the range in which we are interested. One such series is immediately obvious; namely an expansion about the point $z=1$ in ascending powers of $z-1$.

We have by Taylor's theorem

$$F(z) = \sum_{n=0}^{\infty} \frac{F^{(n)}(1)}{n!}(z-1)^n, \quad G(z) = \sum_{n=0}^{\infty} \frac{G^{(n)}(1)}{n!}(z-1)^n,$$

the radius of convergence of both series being $\sqrt{2}$ in accordance with section 3, (b), (c). On writing $z=e^{i\theta}$, we find that $z-1=2e^{(\pi+\theta)i/2}\sin(\theta/2)$. Hence

$$(6.1) \quad \begin{aligned} F(e^{i\theta}) &= \sum_{n=0}^{\infty} \frac{F^{(n)}(1)}{n!} e^{ni/2(\pi+\theta)} \left(2 \sin \frac{\theta}{2}\right)^n, & -\frac{\pi}{2} < \theta < \frac{\pi}{2}. \\ G(e^{i\theta}) &= \sum_{n=0}^{\infty} \frac{G^{(n)}(1)}{n!} e^{ni/2(\pi+\theta)} \left(2 \sin \frac{\theta}{2}\right)^n, \end{aligned}$$

Since $F(z)$ and $G(z)$ are real when z is real and greater than -1 , the constants $F^{(n)}(1)$ and $G^{(n)}(1)$ in (6.1) are all real. Hence on combining these formulas with (4.1), we find that

$$(6.2) K_1(\theta) = \frac{1}{2} \sum_{n=0}^{\infty} \frac{F^{(n)}(1) + G^{(n)}(1)}{n!} \sin \frac{n}{2}(\pi + \theta) \left(2 \sin \frac{\theta}{2}\right)^n, \quad -\frac{\pi}{2} < \theta < \frac{\pi}{2},$$

with similar formulas for $K_2(\theta)$, $K_3(\theta)$ and $K_4(\theta)$.

To calculate the constants $F^{(n)}(1)$ and $G^{(n)}(1)$, we differentiate the equations (5.1) $n+2$ times and set $z=1$. We thus obtain the recursion formulas

$$(6.3) \quad \begin{aligned} F^{(n+4)}(1) &= -(2n+5)F^{(n+3)}(1) - (n+2)(2n+3)F^{(n+2)}(1) \\ &\quad - (n+2)(n+1)nF^{(n+1)}(1) - \frac{(n+2)(n+1)n(n-1)}{4}F^{(n)}(1); \\ G^{(n+4)}(1) &= -(2n+3)G^{(n+3)}(1) - (n+2)(2n+1)G^{(n+2)}(1) \\ &\quad - (n+2)(n+1)nG^{(n+1)}(1) - \frac{(n+2)(n+1)n(n-1)}{4}G^{(n)}(1). \end{aligned}$$

On setting $n=-2, -1, 0, 1, \dots$ in these formulas, we find from (5.2) that¹

¹ These coefficients have been checked from (3.1) by expanding $\exp \pm (z^2-1)/(z^2+1)$ in ascending powers of $z-1$ up to the terms of order $(z-1)^7$, and integrating term by term.

$F^{(0)}(1) = 0; F^{(1)}(1) = 1; F^{(2)}(1) = -1; F^{(3)}(1) = 2; F^{(4)}(1) = -4; F^{(5)}(1) = 4;$
 $F^{(6)}(1) = 34; F^{(7)}(1) = -374; F^{(8)}(1) = 2498.$

$G^{(0)}(1) = 0; G^{(1)}(1) = 1; G^{(2)}(1) = 1; G^{(3)}(1) = 0; G^{(4)}(1) = -2; G^{(5)}(1) = 4;$
 $G^{(6)}(1) = 6; G^{(7)}(1) = -74; G^{(8)}(1) = 190.$

On substituting these values in the first nine terms of (6.2), we obtain the series for $K_1(\theta)$ given in section 1.

7. Let $z = e^{i\theta}$ be a fixed point on the unit circle to the right of the y axis, and C a circle of radius $\rho < \sqrt{2}$ about the point $z = 1$ including the point $e^{i\theta}$. Then

$$(7.1) \quad F(e^{i\theta}) = \frac{1}{2\pi i} \int_C \frac{F(w)dw}{w - z},$$

where w denotes a complex current co-ordinate upon the circle C .

From the identity

$$\frac{1}{w - z} = \frac{1}{w - 1} + \frac{z - 1}{(w - 1)^2} + \cdots + \frac{(z - 1)^n}{(w - 1)^{n+1}} + \frac{(z - 1)^{n+1}}{(w - 1)^{n+1}(w - z)},$$

we obtain

$$F(z) = c_0 + c_1(z - 1) + \cdots + c_n(z - 1)^n + \mathfrak{R}_n$$

where $c_k = F^{(k)}(1)/k!$ ($k = 0, \dots, n$) and

$$(7.2) \quad \mathfrak{R}_n = \frac{(z - 1)^{n+1}}{2\pi i} \int_C \frac{F(w)dw}{(w - 1)^{n+1}(w - z)}.$$

Now

$$|z - 1| = 2 \sin \frac{|\theta|}{2}, \quad |w - 1| = \rho, \quad |w - z| \geq \rho - |z - 1| = \rho - 2 \sin \frac{|\theta|}{2}$$

and by 3 (d),

$$|F(w)| \leq \rho \exp \frac{\sqrt{\rho^4 + 4} + \rho^2}{2(2 - \rho^2)}.$$

Hence from (7.2),

$$|\mathfrak{R}_n| \leq \left(\frac{2 \sin \frac{|\theta|}{2}}{\rho} \right)^{n+1} \frac{\rho^2}{\rho - 2 \sin \frac{|\theta|}{2}} \exp \frac{\sqrt{\rho^4 + 4} + \rho^2}{2(2 - \rho^2)}.$$

The inequality for the remainder in the series for $G(z)$ is precisely the same, save that the numerator of the exponential is replaced by $\sqrt{\rho^2 + 4} - \rho^2$.

A somewhat better inequality when n is large may be obtained by integrating the right side of (7.2) by parts before obtaining the dominant. It gives

$$|\mathfrak{R}_n| \leq \frac{1}{n} \left(\frac{2 \sin \frac{|\theta|}{2}}{\rho} \right)^{n+1} \frac{2\rho^2 \left(\rho + \sin \frac{|\theta|}{2} \right)}{\left(\rho - 2 \sin \frac{|\theta|}{2} \right)^2} \exp \frac{\sqrt{\rho^4 + 4} + \rho^2}{2(2 - \rho^2)}.$$

If we take $\rho^2 = 3/2$, $\theta = \pi/4$ in the first inequality, we obtain

$$|\mathfrak{R}_n| < (\frac{5}{8})^{n+1} \times 51.08 = .0042 \text{ for } n = 19.$$

The second inequality gives

$$|\mathfrak{R}_n| < \frac{1}{n} \left(\frac{5}{8} \right)^{n+1} 438 = .0019 \text{ for } n = 19.$$

If θ is quite small, we may take $\rho = 1$, obtaining

$$|\mathfrak{R}_n| < \left(2 \sin \frac{|\theta|}{2} \right)^{n+1} \frac{e^{(\sqrt{5}+1)/2}}{1 - 2 \sin \frac{|\theta|}{2}} \text{ for } F(z)$$

and

$$|\mathfrak{R}_n| < \left(2 \sin \frac{|\theta|}{2} \right)^{n+1} \frac{e^{(\sqrt{5}-1)/2}}{1 - 2 \sin \frac{|\theta|}{2}} \text{ for } G(z).$$

HOMOGENEOUS LINEAR DIFFERENTIAL EQUATIONS OF THE SECOND ORDER

By T. C. BENTON, Pennsylvania State College

1. *Introduction.* After teaching the subject of linear differential equations to sophomore students a number of times, it has seemed to the author that the customary methods of assuming the correct answers and then verifying them are highly unsatisfactory from a pedagogical viewpoint. The student always asks how the form of solution used was obtained in the first place. Also the latter student is left with the feeling, that except for a lucky guess, there is no way to obtain the solution of similar problems. It is the purpose of this development of the subject to present a method in which every step is forced—a method in which there is no guesswork at all. The actual work is all of well known character but the fact that the general methods of the higher theory of differential equations work out in such a simple way for the elementary cases seems worthy of attention.

2. *General Theory* of the solution of:

$$(A) \quad \frac{d^2y}{dx^2} + P \frac{dy}{dx} + Qy = 0,$$

P, Q being functions of x or constants.

Chapter 8

1934

THE REPRESENTATION OF STIRLING'S NUMBERS AND STIRLING'S POLYNOMIALS AS SUMS OF FACTORIALS.

By MORGAN WARD.

1. I give here a new representation of the Stirling numbers and the associated Stirling polynomials * as sums of factorials, and use the formulas to deduce various arithmetical and algebraic properties of the numbers. My fundamental formula for the Stirling polynomial † $\psi_{p-1}(x)$ reads as follows:

$$(3.31) \quad \psi_{p-1}(x) = \frac{(-1)^{p-1}}{(p+1)!} \left[H_p^{p-1} - \frac{x+2}{p+2} H_p^{p-2} + \frac{(x+2)(x+3)}{(p+2)(p+3)} H_p^{p-3} - \cdots + (-1)^{p-1} \frac{(x+2)(x+3) \cdots (x+p)}{(p+2)(p+3) \cdots 2p} H_p^0 \right].$$

The constants H_p^r appearing here are positive integers defined recursively by

$$(4.1) \quad H^r_{p+1} = (2p+1-r)H_p^r + (p-r+1)H_p^{r-1},$$

with the initial values

$$(4.11) \quad H_0^0 = 1, \quad H_{p+1}^0 = 1 \cdot 3 \cdot 5 \cdots (2p+1), \quad H_{p+1}^p = 1.$$

Nielsen ‡ has expressed the Stirling polynomial $\psi_{p-1}(x)$ in the form

$$\psi_{p-1}(x) = \sigma_{p-1,0}x^{p-1} + \sigma_{p-1,1}x^{p-2} + \cdots + \sigma_{p-1,p-2}x + \sigma_{p-1,p-1}.$$

Unfortunately, the numbers $\sigma_{p,r}$ are not integers, and the recursion formulas for them are very complicated, so that it is difficult both to ascertain their form, § and to obtain properties of the Stirling polynomial from such a representation. In contrast, the numbers H_p^r are integers of comparatively simple

* We use here freely the notation and formulas for the Stirling numbers given by Nielsen in his well known *Handbuch der Theorie der Gammafunction* (Leipzig, 1906), Chapter V. We shall refer to this source as Nielsen, *Handbuch*, giving page reference. A recent paper by C. Tweedie, *Proceedings of the Edinburgh Mathematical Society*, vol. 37 (1918), pp. 2-25, contains many interesting new results on these numbers. Since this paper was in press, C. Jordan (*Tohoku Journal*, vol. 37 (1933), pp. 254-278) has given an expression for the Stirling number as a sum of factorials. See especially pp. 264-265 of his paper, where his numbers \bar{C}_{mt} are my H_m^t .

† Nielsen, *Handbuch*, p. 72.

‡ *Handbuch*, pp. 72-73. See also *Annali di Matematica*, III, vol. 10, pp. 309-316.

§ Nielsen, *Annali di Matematica*, III, vol. 10, p. 313; Tweedie, paper cited, Section 11.

form, while (3.31) leads directly to interesting congruential properties of the Stirling polynomials and Stirling numbers.

To give an example of such congruences, let P be any prime greater than $2p$, and r any positive integer. Then if C_n^p denotes the Stirling number,

$$\begin{aligned} C_{n+1}^p &\equiv 1 \pmod{P^r}, & \text{if } n+2 \equiv 0 \pmod{P^r}, \\ C_{n+1}^p &\equiv 2^{p+1} - 1 \pmod{P^r}, & \text{if } n+3 \equiv 0 \pmod{P^r}. \end{aligned}$$

As a numerical illustration, take $p = 3$, $P = 7$, $r = 1$. Then from Glaisher's table * of C_n^p , $C_5^3 = 225$, $C_4^3 = 50$, and

$$225 \equiv 1 \pmod{7}, \quad 50 \equiv 2^4 - 1 \pmod{7}.$$

2. We begin with the Stirling numbers of the first kind defined by

$$x(x+1)\cdots(x+n-1) = C_n^0 x^n + C_n^1 x^{n-1} + \cdots + C_n^p x^{n-p} + \cdots + C_n^{n-1} x.$$

We call n the rank of C_n^p and p its order. We have the immediate relations

$$(2.1) \quad C_{n+1}^p = C_n^p + nC_n^{p-1},$$

$$(2.2) \quad C_n^0 = 1, \quad C_n^{n-1} = (n-1)!, \quad (n = 1, 2, \dots; p = 0, 1, \dots, n-1).$$

We now define C_n^p for all integral values of n and p , positive or negative, by the recursion formula (2.1) with the initial values (2.2). Then it is readily shown that

$$(2.3) \quad C_n^{n+r-1} = 0, \quad (n = 0, 1, \dots; r = 1, 2, \dots).$$

Furthermore, if

$$F_p(z) = \sum_{n=0}^{\infty} C_n^p z^n$$

is the generating function for the Stirling numbers

$$C_0^p, C_1^p, C_2^p, \dots$$

of fixed order p , then an easy induction shows us that

$$(2.4) \quad F_p(z) = [z^{p+1}/(1-z)^{2p+1}]H_p(z), \quad (p = 0, 1, 2, \dots)$$

where $H_p(z)$ is a polynomial in z of degree $p-1$ with positive integral coefficients, and, by convention, we take

$$(2.41) \quad H_0(z) = 1.$$

* *Quarterly Journal*, vol. 31 (1900), pp. 26-28. This Table extends as far as $n = 20$. C_n^p is denoted in Glaisher's notation by $S_p(1, 2, \dots, n-1)$.

The polynomials $H_p(z)$ appearing in (2.4) satisfy the recursion relation

$$(2.5) \quad H_{p+1}(z) = (pz + p + 1)H_p(z) + (1 - z)z(d/dz)H_p(z)$$

which with (2.41) determines them completely.

3. We next put the polynomial $H_p(z)$ in the form

$$(3.1) \quad H_p(z) = H_p^0 - H_p^1(1 - z) \\ + H_p^2(1 - z)^2 - \cdots + (-1)^{p-1} H_p^{p-1}(1 - z)^{p-1}.$$

Before studying the constants H_p^r , we shall deduce our main formulas. On substituting (3.1) into (2.4) and then expanding in ascending powers of z , we find that

$$F_p(z) = z^{p+1} \sum_{r=0}^{p-1} \sum_{s=0}^{\infty} (-1)^r H_p^r \frac{(s+1)(s+2) \cdots (s+2p-r)}{1 \cdot 2 \cdot 3 \cdots (2p-r)} z^s.$$

Therefore by comparing the coefficient of z^n on both sides of this expression, we find that

$$C_n^p = \sum_{r=0}^{p-1} (-1)^r H_p^r (n-p)(n+1-p) \cdots (n+p-r-1)/(2p-r)!.$$

On replacing n by $n+1$ in this expression and removing the common factor $(-1)^{p-1}(n+1)n \cdots (n+1-p)/(p+1)!$ from the right side, we obtain finally the formula

$$(3.2) \quad C_{n+1}^p = \frac{(n+1)!(-1)^{p-1}}{(n-p)!(p+1)!} \\ \times \left[H_p^{p-1} - \frac{n+2}{p+2} H_p^{p-2} + \frac{(n+2)(n+3)}{(p+2)(p+3)} H_p^{p-3} \right. \\ \left. - \cdots + (-1)^{p-1} \frac{(n+2)(n+3) \cdots (n+p)}{(p+2)(p+3) \cdots (2p)} H_p^0 \right].$$

Now *

$$C_{n+1}^p = [(n+1)!/(n-p)!] \psi_{p-1}(n)$$

where $\psi_{p-1}(x)$ is the Stirling polynomial of order $p-1$. Hence

$$\psi_{p-1}(n) = \frac{(-1)^{p-1}}{(p+1)!} \left[H_p^{p-1} - \cdots + (-1)^{p-1} \frac{(n+2) \cdots (n+p)}{(p+2) \cdots 2p} H_p^0 \right].$$

Since this formula holds for all positive integral values of n , we deduce that

* Nielsen, *Handbuch*, p. 14, formula (15).

$$(3.21) \quad \psi_{p-1}(x) = \frac{(-1)^{p-1}}{(p+1)!} \left[H_p^{p-1} - \frac{x+2}{p+2} H_p^{p-2} + \frac{(x+2)(x+3)}{(p+2)(p+3)} H_p^{p-3} - \dots + (-1)^{p-1} \frac{(x+2)(x+3)\dots(x+p)}{(p+2)(p+3)\dots 2p} H_p^0 \right]$$

for all values of the variable x .

We may use this result to obtain a formula similar to (3.2) for the Stirling numbers \mathfrak{C}_n^s of the second kind * defined by the expansion

$$1/x(x+1)\dots(x+n-1) = \sum_{s=0}^{\infty} (-1)^s \mathfrak{C}_n^s / x^{n+s}.$$

For †

$$\mathfrak{C}_n^p = [(-1)^{p-1}(n+p-1)/(n-2)!] \psi_{p-1}(-n),$$

so that by (3.21),

$$(3.3) \quad \mathfrak{C}_n^p = \frac{(n+p-1)!}{(n-2)!(p+1)!} \left[H_p^{p-1} + \frac{n-2}{p+2} H_p^{p-2} + \frac{(n-2)(n-3)}{(p+2)(p+3)} H_p^{p-3} + \dots + \frac{(n-2)(n-3)\dots(n-p)}{(p+2)(p+3)\dots 2p} H_p^0 \right].$$

These formulas have immediate arithmetical consequences. For suppose that P denotes a fixed prime greater than $2p$, and r any positive integer. Then we deduce from (3.21) that

$$\begin{aligned} \psi_{p-1}(n) &\equiv [(-1)^{p-1}/(p+1)!] H_p^{p-1} \pmod{P^r} & \text{if } n+2 \equiv 0 \pmod{P^r}, \\ \psi_{p-1}(n) &\equiv [(-1)^{p-1}/(p+1)!] \{H_p^{p-1} + [1/(p+2)] H_p^{p-2}\} \pmod{P^r} & \text{if } n+3 \equiv 0 \pmod{P^r}, \end{aligned}$$

and so on. There are analogous congruences for the Stirling numbers deducible from (3.2) and (3.3); namely,

$$(3.4) \quad \begin{aligned} C_{n+1}^p &\equiv H_p^{p-1} \pmod{P^r} & \text{if } n+2 \equiv 0 \pmod{P^r}, \\ C_{n+1}^p &\equiv (p+2)H_p^{p-1} + H_p^{p-2} \pmod{P^r} & \text{if } n+3 \equiv 0 \pmod{P^r}, \\ \mathfrak{C}_n^p &\equiv H_p^{p-1} \pmod{P^r} & \text{if } n-2 \equiv 0 \pmod{P^r}, \\ \mathfrak{C}_n^p &\equiv (p+2)H_p^{p-1} + H_p^{p-2} \pmod{P^r} & \text{if } n-3 \equiv 0 \pmod{P^r}, \end{aligned}$$

and so on.

* Nielsen, *Handbuch*, p. 68.

† Nielsen, *Handbuch*, p. 74.

We may note in passing an interesting consequence of the form of the generating function $F_p(z)$ given in (2.4). For if

$$\Delta C_n^p = C_n^p - C_{n-1}^p \Sigma C_n^p = C_0^p + C_1^p + \cdots + C_n^p$$

denote the usual operations of the calculus of finite differences applied to the rank of the Stirling number C_n^p , the generating functions of the numbers ΔC_n^p and ΣC_n^p are $(1-z)F_p(z)$ and $(1-z)^{-1} F_p(z)$ respectively. But with $H_p(z)$ in the form (3.1), each of these functions may be immediately expanded in ascending powers of z . We obtain in this manner the formulas

$$(3.5) \quad \begin{aligned} \Delta C_{n+1}^p &= (-1)^{p-1} \binom{n}{p} \\ &\times \left[H_p^{p-1} - \frac{n+1}{p+1} H_p^{p-2} + \frac{(n+1)(n+2)}{(p+1)(p+2)} H_p^{p-3} - \cdots \right], \\ \Sigma C_{n+1}^p &= (-1)^{p-1} \binom{n+2}{p+2} \\ &\times \left[H_p^{p-1} - \frac{n+3}{p+3} H_p^{p-2} + \frac{(n+3)(n+4)}{(p+3)(p+4)} H_p^{p-3} - \cdots \right], \end{aligned}$$

and it is easy to write down analogous formulas for the higher differences and summations of C_{n+1}^p . The method by which we obtained the congruences (3.4) yields then an unlimited number of congruences involving sums and differences of Stirling numbers of the same order.

If we compare (3.5) (i) with (2.1), we see that

$$\begin{aligned} nC_n^{p-1} &= (-1)^{p-1} \binom{n}{p} \\ &\times \left[H_p^{p-1} - \frac{n+1}{p+1} H_p^{p-2} + \frac{(n+1)(n+2)}{(p+1)(p+2)} H_p^{p-3} - \cdots \right]. \end{aligned}$$

On the other hand, if we put $n = n-1$, $p = p-1$ in (3.2), we find that

$$\begin{aligned} C_n^{p-1} &= (-1)^{p-2} \binom{n}{p} \\ &\times \left[H_{p-1}^{p-2} - \frac{n+1}{p+1} H_{p-1}^{p-3} + \frac{(n+1)(n+2)}{(p+1)(p+2)} H_{p-1}^{p-4} - \cdots \right]. \end{aligned}$$

Therefore, for all integral values of n , we have the fundamental formula

$$(3.6) \quad \begin{aligned} &\left[H_p^{p-1} - \frac{n+1}{p+1} H_p^{p-2} + \frac{(n+1)(n+2)}{(p+1)(p+2)} H_p^{p-3} \right. \\ &\left. - \cdots + (-1)^{p-1} \frac{(n+1)(n+2) \cdots (n+p-2)}{(p+1)(p+2) \cdots (2p-2)} H_p^{p-1} \right] = -n \\ &\left[H_{p-1}^{p-2} - \frac{n+1}{p+1} H_{p-1}^{p-3} + \frac{(n+1)(n+2)}{(p+1)(p+2)} H_{p-1}^{p-4} \right. \\ &\left. - \cdots + (-1)^{p-2} \frac{(n+1)(n+2) \cdots (n+p-3)}{(p+1)(p+2) \cdots (2p-3)} H_{p-1}^{p-2} \right]. \end{aligned}$$

We may if we please replace n here by a continuous variable x as in formula (3.21).

In particular, if we let $n = p$, we have

$$H_p^{p-1} - H_p^{p-2} + H_p^{p-3} - \cdots = -(H_{p-1}^{p-2} - H_{p-1}^{p-3} + H_{p-2}^{p-3} - \cdots).$$

From this result and the fact that $H_1^0 = 1$, we deduce that

$$(3.7) \quad H_p^0 - H_p^1 + H_p^2 - \cdots + (-1)^{p-1} H_p^{p-1} = p!,$$

a formula which affords a convenient check when computing the numerical values of the integers H_p^r .

4. We now proceed with the study of the numbers H_p^r . If we assume that (3.1) holds for all positive integral values of p , we obtain by substituting in (2.5) and comparing the coefficients of the various powers of $1-z$, the recursion relations

$$(4.1) \quad \begin{aligned} H_{p+1}^0 &= (2p+1)H_p^0, \quad H_{p+1}^p = H_p^{p-1} \quad \text{and} \\ H_{p+1}^r &= (2p+1-r)H_p^r + (p-r+1)H_p^{r-1}. \end{aligned}$$

Since $H_0^0 = 1$, we deduce from the first two relations that

$$(4.12) \quad H_{p+1}^0 = 1 \cdot 3 \cdot 5 \cdots 2p+1, \quad H_{p+1}^p = 1, \quad (p = 0, 1, \dots).$$

The first few numbers H_p^r are given in the following table: *

p	$r = 0$	1	2	3	4	5	6	7	8	9
1	1									
2	3	1								
3	15	10	1							
4	105	105	25	1						
5	945	1260	490	56	1					
6	10895	17825	9450	1918	119	1				
7	135135	270270	190575	56980	6825	246	1			
8	2027025	4729725	4099095	1636635	802995	22985	501	1		
9	34459425	91891800	94594500	47507480	12122110	1487200	74816	1012	1	
10	654729075	1964187225	2343240900	1422280860	466876410	81431350	6914908	235092	2085	1

Here the number in the p -th row and r -th column is H_p^r ; thus $H_4^2 = 25$.

We next extend the definition of H_p^r to all integral values of p and r by (4.1) and (4.12). By a brief induction, we find that

$$(4.13) \quad H_p^{-r} = 0 \quad (r \geq 1; p = 0, 1, 2, \dots)$$

$$(4.14) \quad H_p^{p+r} = 0 \quad (r = 0, p = 1, 2, 3, \dots; r \geq 1, p = r, r+1, \dots).$$

* The table has been checked by the use of formula (3.7).

Now replace r by $p - r$ in (4.1). We obtain

$$(4.2) \quad H_{p+r}^{p-r} = (p+r+1)H_{p+r}^{p-r} + (r+1)H_{p+r-1}^{p-r-1}.$$

Let the generating function of the numbers

$$H_0^{-r}, H_1^{-r}, H_2^{-r}, \dots, H_p^{-r}, \dots$$

be denoted by $\mathcal{H}_r(x)$, so that

$$(4.3) \quad \mathcal{H}_r(x) = \sum_{p=0}^{\infty} H_p^{-r} x^p = \sum_{p=r}^{\infty} H_p^{-r} x^p$$

since by (4.13), $H_0^{-r} = H_1^{-r} = \dots = H_{r-1}^{-r} = 0$.

On replacing r by $r + 1$ in (4.3), changing the summation variable from p to $p + 1$, and reducing by (4.2), we obtain the formula

$$(4.4) \quad (1 - (r+1)x)\mathcal{H}_{r+1}(x) = (r+1)x\mathcal{H}_r(x) + x^2(d/dx)\mathcal{H}_r(x), \quad (r = 0, 1, 2, \dots).$$

Since by (4.14), $H_p^p = 0$ and $H_0^0 = 1$, we have

$$(4.41) \quad \mathcal{H}_0(x) = 1.$$

These two formulas serve then to define the functions $\mathcal{H}_r(x)$ completely, and $\mathcal{H}_r(x)$ is seen to be a rational function of x . It is easy to determine its form. For by direct calculation from (4.4), we find that

$$(4.5) \quad \begin{aligned} \mathcal{H}_1(x) &= \frac{x}{1-x}, \quad \mathcal{H}_2(x) = \frac{x^2[3-2x]}{(1-x)^2(1-2x)}, \\ \mathcal{H}_3(x) &= \frac{x^3[15-45x+40x^2-12x^3]}{(1-x)^3(1-2x)^2(1-3x)}, \\ \mathcal{H}_4(x) &= \frac{x^4[105-840x+2625x^2-4130x^3+3500x^4-1560x^5+288x^6]}{(1-x)^4(1-2x)^3(1-3x)^2(1-4x)}. \end{aligned}$$

We are therefore led to infer that the generating function $\mathcal{H}_r(x)$ is of the form

$$(4.51) \quad \mathcal{H}_r(x) = x^r \Phi_r(x) / (1-x)^r (1-2x)^{r-1} \cdots (1-rx)$$

where $\Phi_r(x)$ is a polynomial in x with integral coefficients of degree $r(r-1)/2$. The proof is a straightforward induction from (4.41) and (4.4) and will be omitted here.*

If we put the right-hand side of (4.51) into partial fractions, we see that $\mathcal{H}_r(x)$ may be written as

* The relationship between $\Phi_{r+1}(x)$ and $\Phi_r(x)$ deduced in the course of the induction is unfortunately too complicated to be of much service.

$$\begin{aligned} \mathcal{H}_r(x) = A_0 + \frac{B_1}{1-rx} + \frac{C_1}{1-(r-1)x} + \frac{C_2}{(1-(r-1)x)^2} \\ + \cdots + \frac{U_1}{1-x} + \cdots + \frac{U_r}{(1-x)^r}, \end{aligned}$$

where the numbers A_0, \dots, U_r are all rational. If we now expand the right-hand side of this expression in ascending powers of x and collect the coefficient of x^p , we find that H_p^{p-r} is of the form

$$H_p^{p-r} = b_0 r^p + (c_0 + c_1 p)(r-1)^p + \cdots + (u_0 + u_1 p + u_2 p^2 + \cdots + u_{r-1} p^{r-1})$$

where the numbers b_0, \dots, u_{r-1} are again all rational. We can however assert more than this. For if we apply the process just described to the expressions in (4.5), we find that *

$$\begin{aligned} H_p^{p-1} &= 1, \quad H_p^{p-2} = [2^{p+1} - (p+3)], \\ (4.6) \quad H_p^{p-3} &= \frac{1}{2}[3^{p+2} - (2p+10)2^{p+1} + (p^2+7p+13)], \\ H_p^{p-4} &= \frac{1}{6}[4^{p+3} - (3p+21)3^{p+2} \\ &\quad + (3p^2+33p+96)2^{p+1} - (p^3+12p^2+50p+73)]. \end{aligned}$$

We infer therefore that H_p^{p-r} is actually of the form

$$(4.61) \quad H_p^{p-r} = [1/(r-1)!] \sum_{l=0}^{r-1} (-1)^l \theta_l(p) (r-l)^{p+r-1-l}$$

where $\theta_l(p)$ is a polynomial in p of degree l with positive integral coefficients, and $\theta_0(p) = 1$. I cannot however prove this statement.†

5. We conclude by giving a method for calculating the polynomials $\theta_l(p)$ in (4.61) recursively. We begin by assuming that

$$(5.1) \quad H_p^{p-(r+1)} = (1/r!) \sum_{l=0}^r (-1)^l \Theta_l(p) (r+1-l)^{p+r-1-l},$$

where $\Theta_l(p)$ is a polynomial of the same form as $\theta_l(p)$. On setting $p = p+1$ in (5.1), we find that

$$H_{p+1}^{p-r} = (1/r!) \sum_{l=0}^r (-1)^l \Theta_l(p+1) (r+1-l)^{p+r-1-l}.$$

* All of these formulas have been checked numerically, and are believed to be correct. The two congruences mentioned in the introduction are obtained by substituting for H_p^{p-1} and H_p^{p-2} from (4.6) into (3.4).

† As additional support for it, I have found that

$$\begin{aligned} H_p^{p-5} &= (1/24)[5p^{14} - (4p+36)4p^{13} + (6p^2+90p+354)3p^{11} \\ &\quad - (4p^3+72p^2+452p+992)2p + (p^4+18p^3+125p^2+400p+501)]. \end{aligned}$$

If we now substitute these expressions for H_{p+1}^{p-r} , H_p^{p-r} , $H_p^{p-(r+1)}$ into (4.2) and express the fact that the resulting expression must be an identity in p , we obtain the formula

$$(5.2) \quad l\Theta_l(p+1) - (r+1)(\Theta_l(p+1) - \Theta_l(p)) \\ = r(p+r+1)\theta_{l-1}(p), \quad (r \geq l \geq 1),$$

which determines $\Theta_l(p)$ if $\theta_{l-1}(p)$ is known.

If we attempt to determine $\Theta_l(p)$ by writing it as a polynomial in p with undetermined coefficients, we find that we can express the coefficients only as determinants in the coefficients of $\theta_{l-1}(p)$. We therefore assume instead that $\theta_{l-1}(p)$ and $\Theta_l(p)$ are expressed as sums of factorials:

$$(5.3) \quad \begin{aligned} \theta_{l-1}(p) &= y_0 + y_1 p + y_2 p(p+1) + \cdots + y_{l-1} p(p+1) \cdots (p+l-2), \\ \Theta_l(p) &= x_0 + x_1 p + x_2 p(p+1) + \cdots + x_l p(p+1) \cdots (p+l-1), \end{aligned}$$

and seek to determine the x in terms of the y . Needless to say, the x and y are all integers, when and only when all the coefficients in the ordinary polynomial expressions for $\theta_{l-1}(p)$ and $\Theta_l(p)$ are integers.

If for convenience we set

$$x_{l+1} = y_{l+1} = y_l = y_{-1} = 0,$$

we obtain on substituting from (5.3) into (5.2) the difference relation

$$(5.4) \quad lx_s - (s+1)(r+1)x_{s+1} = r(y_{s-1} + (r-2s)y_s - (s+1)(r-s)y_{s+1}), \\ (s = 0, 1, \dots, l).$$

As a numerical verification of this formula, take $r = 3$ and $l = 2$ so that we have to do with H_p^{p-4} and H_p^{p-3} . From the formulas (4.6), we have $\Theta_2(p) = 3p^2 + 33p + 96$, $\theta_1(p) = 2p + 10$, so that $x_0 = 96$, $x_1 = 30$, $x_2 = 3$, $y_0 = 10$, $y_1 = 2$. The formula (5.6) with $s = 0, 1, 2$ then gives

$$\begin{aligned} 2x_0 - 4x_1 &= 3(3y_0 - 3y_1); \quad 2x_1 - 8x_2 = 3(y_0 + y_1); \quad 2x_2 = 3y_1; \\ \text{or} \quad 192 - 120 &= 3(30 - 6); \quad 60 - 24 = 3(10 + 2); \quad 6 = 6. \end{aligned}$$

Since (5.4) is effectively a linear difference equation of the first order for x_s , the explicit form of x_s may be written down, but the general result is too complicated to be of interest.

QUESTIONS, DISCUSSIONS, AND NOTES

EDITED BY R. E. GILMAN, Brown University, Providence, Rhode Island

The department of Questions and Discussions in the Monthly is open to all forms of activity in collegiate mathematics, including the teaching of mathematics, except for specific problems, especially new problems, which are reserved for the department of Problems and Solutions.

ON THE VANISHING OF THE SUM OF THE N TH POWERS
OF THE ROOTS OF A CUBIC EQUATION

By MORGAN WARD, California Institute of Technology

1. Suppose that

$$(1.1) \quad x^3 - Px^2 + Qx - R = 0,$$

P, Q, R rational integers, is a cubic equation with three distinct non-vanishing roots. Then it is a fundamental problem of considerable arithmetical interest to determine whether or not a given rational integer A may be represented as a sum of n th powers of the roots of (1.1), and—granted that such a representation is possible—to find out in how many ways it can occur.

More precisely, if $\alpha_1, \alpha_2, \alpha_3$ are the roots of (1.1) and if $S_n = \alpha_1^n + \alpha_2^n + \alpha_3^n$ is the sum of their n th powers, we wish to solve the diophantine equation

$$(1.2) \quad S_x = A$$

in positive integers x , given P, Q, R and A .

The great difficulty of this general problem is at once apparent. For if we restrict the roots of (1.1) to be rational integers, then the special case $A = 0$ is the Fermat problem, and Fermat's conjecture is equivalent to asserting that the diophantine equation

$$(1.3) \quad S_x = 0$$

can have only the solutions $x = 1$ and $x = 2$ if the roots of (1.1) are rational integers.

2. A simpler preliminary problem is to ascertain whether or not (1.2) and (1.3) can have an infinite number of solutions. In case all of the roots of (1.1) are real, the answer is apparent; *for any A , there are only a finite number of values of x satisfying (1.2)*. For since the roots α are distinct, and $|\alpha_1\alpha_2\alpha_3| = |R| \geq 1$, the magnitude of the arithmetically largest root of (1.1) is greater than one, and since S_n is clearly of the same order as the n th power of this root, $|S_n|$ tends to infinity with n .¹

In case two of the roots of (1.1) are complex, nothing general seems to be known as to the number of solutions of (1.2). However, in the special case when $R = \pm 1$, Siegel² has shown by the use of Thue's theorem that (1.3) *can have*

¹ A trivial exception occurs if we have $\alpha_1 = -\alpha_2 > |\alpha_3|$, as then $S_{2n+1} = \alpha_3^{2n+1}$. Hence if $\alpha_3 = \pm 1$, $S_x = \pm 1$ will have an infinite number of solutions.

² Tohoku Journal, Vol. 20 (1921), p. 29.

only a finite number of solutions unless (1.1) is of the form $(x \pm 1)(x^2 + 1)$ or $(x \pm 1)(x^2 \pm x + 1)$.¹

3. We can set ourselves the still more modest task of finding values of x for which (1.2) and (1.3) are insoluble—a common enough type of procedure in other problems in diophantine analysis.

For example, let p be a prime number, and r a positive integer. Then

$$S_{p^{r-1}} \equiv S_{p^{r-1}}^p \equiv (\alpha_1^{p^{r-1}} + \alpha_2^{p^{r-1}} + \alpha_3^{p^{r-1}})^p = \alpha_1^{p^r} + \alpha_2^{p^r} + \alpha_3^{p^r} \pmod{p}.$$

Since $S_1 = P$, we see that²

$$S_{p^r} \equiv P \pmod{p}, \quad (r = 0, 1, 2, \dots).$$

Accordingly, if (1.2) has a solution for x a power of a prime p , we have the restriction $A \equiv P \pmod{p}$. In particular, (1.3) can have a solution in such a case only if $P \equiv 0 \pmod{p}$. Therefore if $P \not\equiv 0$, for a given cubic equation (1.1), S_x can vanish for only a finite number of values of x which are primes or powers of primes.

If $P = 0$, we obtain a restriction on the value of A in (1.2), but no restriction upon x in (1.3). In this case, I shall conclude by proving the following theorem, the main point of novelty in the paper.

4. THEOREM. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of an irreducible cubic equation

$$(4.1) \quad x^3 + Qx - R = 0,$$

Q, R rational integers. Then if R is greater in absolute value than two, and prime to Q , the sum of the n th powers of the roots of (4.1), $S_n = \alpha_1^n + \alpha_2^n + \alpha_3^n$, can never vanish if n is even, or if n is a prime.

PROOF. By hypothesis, α_1, α_2 and α_3 are distinct and not zero, and

$$(4.2) \quad \alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = Q, \quad \alpha_1\alpha_2\alpha_3 = R,$$

$$(4.3) \quad |R| \geq 3, \quad (R, Q) = 1.$$

Consider first the case when (1) has only one real root. Denote it by α_1 . Then we may write

$$(4.4) \quad \alpha_2 = re^{i\theta}, \quad \alpha_3 = re^{-i\theta}, \quad r > 0, \quad 0 < \theta < 2\pi.$$

By (4.2), $\alpha_1 = -re^{i\theta} - re^{-i\theta} = -2r \cos \theta$. Therefore

$$\begin{aligned} S_n &= \alpha_1^n + \alpha_2^n + \alpha_3^n = (-2r \cos \theta)^n + (re^{i\theta})^n + (re^{-i\theta})^n \\ &= 2r^n \left\{ \cos n\theta + (-1)^n 2^{n-1} (\cos \theta)^n \right\}. \end{aligned}$$

¹ We may if we please regard $S_0, S_1, S_2, \dots, S_n, \dots$ as a sequence (S) giving that particular solution of the difference equation $\Omega_{n+2} = P\Omega_{n+1} - Q\Omega_n + R\Omega_0$ with the initial values $S_0 = 3$, $S_1 = P$, $S_2 = P^2 - 2Q$, and ask more generally about the solutions of the diophantine equations $U_x = A$, $U_x = 0$ for any particular rational integral solution $U_0, U_1, U_2, \dots, U_n, \dots$ of the difference equation. Siegel in the paper referred to studies the U_n as coefficients in the infinite series $\sum_{n=0}^{\infty} U_n t^n$. The two theorems just stated carry over to the general sequence (U).

² Lucas, *Theorie des Nombres*, p. 422.

Hence $S_n = 0$ when and only when

$$\cos n\theta + (-1)^n 2^{n-1} (\cos \theta)^n = 0.$$

Now by a familiar formula of elementary trigonometry,

$$\cos n\theta = (\cos \theta)^n \left\{ 1 - \binom{n}{2} \tan^2 \theta + \binom{n}{4} \tan^4 \theta - \binom{n}{6} \tan^6 \theta + \dots \right\},$$

the last term in the bracket being

$$(-1)^{(n/2)} \tan^n \theta \quad \text{or} \quad (-1)^{(n-1)/2} \binom{n}{n-1} \tan^{n-1} \theta$$

according as n is even or odd. Hence S_n vanishes when and only when $z = \tan^2 \theta$ is a root of the algebraic equation

$$(4.5) \quad F(z) = 1 + (-1)^n 2^{n-1} - \binom{n}{2} z + \binom{n}{4} z^2 - \binom{n}{6} z^3 + \dots = 0.$$

From (4.4) we see that $i \tan \theta = (\alpha_2 - \alpha_3)/(\alpha_2 + \alpha_3)$, or

$$(4.6) \quad \tan^2 \theta = - \left(\frac{\alpha_2 - \alpha_3}{\alpha_2 + \alpha_3} \right)^2.$$

Next, assume that (1) has three real roots. Then two of them must be of the same sign. Denote the remaining root by α_1 . If in the pair α_2, α_3 , the root of greatest magnitude is α_2 , we may write

$$(4.41) \quad \alpha_2 = \pm r e^\theta, \quad \alpha_3 = \pm r e^{-\theta}, \quad r > 0, \quad \theta > 0$$

where the upper sign is taken if α_2 and α_3 are both positive, and the lower sign if α_2 and α_3 are both negative. As in the first case, $\alpha_1 = -2r \cosh \theta$ and proceeding exactly as before, we find that S_n vanishes when and only when $z = -\tanh^2 \theta$ is a root of the algebraic equation (4.5), where

$$(4.61) \quad \tanh^2 \theta = \left(\frac{\alpha_2 - \alpha_3}{\alpha_2 + \alpha_3} \right)^2.$$

Now if n is even $= 2k$, the leading coefficient of (4.5) becomes unity on multiplying through by $(-1)^k$, and the remaining coefficients are obviously rational integers. If n is an odd prime p , the leading coefficient of $F(z)$ is $(-1)^{(p-1)/2} p$ and the integers

$$\binom{p}{2}, \binom{p}{4}, \binom{p}{6}, \dots$$

are all divisible by p . Furthermore the constant term $1 - 2^{p-1}$ of $F(z)$ is divisible by p by Fermat's theorem. Therefore on dividing $F(z)$ by $(-1)^{(p-1)/2} p$, we obtain again an equation with leading coefficient unity and rational integral coefficients. But any root of such an equation is an algebraic integer. Hence

referring to (4.6) and (4.61), we can state the result: *If S_n vanishes for n even or n an odd prime, it is necessary that $\xi = -(\alpha_2 - \alpha_3)/(\alpha_2 + \alpha_3)$ be an algebraic integer.*

5. We finally show that the quantity ξ cannot be an algebraic integer by proving that the irreducible canonical equation with leading coefficient unity which it satisfies has non-integral coefficients.

First, since $(\alpha_2 - \alpha_3)^2 = (\alpha_2 + \alpha_3)^2 - 4\alpha_2\alpha_3$ we obtain from (4.2) (iii) and (i) $\xi = 1 - 4R/\alpha_1^3$. Thus ξ is a root of the cubic equation

$$\Phi(z) = \left(z - 1 + \frac{4R}{\alpha_1^3}\right)\left(z - 1 + \frac{4R}{\alpha_2^3}\right)\left(z - 1 + \frac{4R}{\alpha_3^3}\right) = 0.$$

On multiplying out the right side of this expression and simplifying by the use of the relations (4.2) and (4.1), we obtain

$$\Phi(z) = z^3 + \left(9 + \frac{4Q^3}{R^2}\right)z^2 + \left(27 - \frac{8Q^3}{R^2}\right)z + 27 + \frac{4Q^3}{R^2} = 0.$$

This equation has rational integral coefficients when and only when $4Q^3 \equiv 0 \pmod{R^2}$ and hence never if $|R| > 2$, and $(R, Q) = 1$. It only remains to show that it is irreducible. If it were reducible, it would have at least one rational root, so that for $1 \leq i \leq 3$, we would have $1 - 4R/\alpha_i^3$ rational, $\alpha_i^3 = R - Q\alpha_i$ rational, or α_i rational, contradicting the assumed irreducibility of (4.1).

Note added in proof. Our analysis shows also that if $S_n = 0$, n cannot be prime to R . For both $n\xi^2$ and $R^4\xi^2$ are algebraic integers.

ON THE GENERAL EQUATION OF THE PARABOLA

H. W. BAILEY, University of Illinois

Consider the general equation of the second degree

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0.$$

While it is apparent that the various elements used in sketching this curve: directrices, foci, semi-axes, etc., are functions of the constants A, \dots, F , yet the explicit expression in terms of these constants is so complicated algebraically as to be worthless practically. For example, the eccentricity appears as a root of the quartic equation

$$Je^4 - (I^2 + 4J)e^2 + (I^2 + 4J) = 0,$$

where $I = A + C$, $J = B^2 - AC$. However, in the case of the parabola such expression is possible in very simple form. The purpose of this note is to give these explicit formulas when we take the equation of the parabola in the form

$$A^2x^2 + 2ACxy + C^2y^2 + 2Dx + 2Ey + F = 0.$$

Let the equation of the directrix and the coordinates of the focus be $\alpha x - \beta y - \gamma = 0$ and (m, n) respectively. Using the general definition of a conic, the equation of this parabola may also be written

NOTE ON THE PERIOD OF A MARK IN
A FINITE FIELD

BY MORGAN WARD

1. *Introduction.* If p is a fixed prime, and

$$F(x) = x^k - c_1x^{k-1} - \cdots - c_k,$$

where c_1, \dots, c_k are rational integers, is a polynomial which is irreducible modulo p , the period of a mark α associated with the polynomial $F(x)$ in the finite field \mathcal{J} of order p^k is fundamental not only in the theory of finite fields,* but also in many allied arithmetical investigations involving recurring series.†

Our information about the actual value of this period is disappointingly meagre beyond the well known facts that it is a divisor of $p^k - 1$ and that there actually exist polynomials $F(x)$ for which the period equals $p^k - 1$. I prove here the following additional result.

THEOREM. *Let τ denote the period of a mark α associated with the irreducible polynomial $F(x)$ modulo p in the finite field \mathcal{J} of order p^k , and let ω be the least positive value of n such that α^n is congruent to a rational integer modulo p .‡ Then $\tau = \delta\theta\omega$, where θ is the exponent to which norm α belongs modulo p , while δ is an integer dividing the greatest common divisor of k and $p-1$, and multiplying the greatest common divisor of θ and the integer $\sigma = (p^k - 1)/(\omega(p-1))$.*

* See, for example, Dickson, *Linear Groups*, 1901, Chapters 1–3.

† If $\Omega_{n+k} = c_1\Omega_{n+k-1} + \cdots + c_k\Omega_n$ is the difference equation associated with the polynomial $F(x)$, the period of α is the period modulo p of every sequence of rational integers satisfying the difference equation. (See Ward, *Transactions of this Society*, vol. 35 (1933), pp. 600–628, and the references given there.) The period of α is also the rank of apparition of the prime p for the number $\Delta_n = \pm \text{Res}\{x^n - 1, F(x)\}$ studied recently by D. H. Lehmer and others. (*Annals of Mathematics*, (2), vol. 34 (1933), pp. 461–479.)

‡ In the case $k=2$, ω is the rank of apparition of the prime p for the Lucas function U_n associated with the polynomial $x^2 - c_1x - c_2$ (D. H. Lehmer, *Annals of Mathematics*, (2), vol. 31 (1930), p. 422). In the general case, ω has been termed the restricted period of $F(x)$ modulo p (R. D. Carmichael, *Quarterly Journal of Mathematics*, vol. 48 (1920), p. 354).

2. *Proof of the Theorem.* We write as usual $a|b$ for a divides b , and (a, b) for the greatest common divisor of a and b . Denote the roots of $F(x)=0$ in the finite field \mathcal{F} by $\alpha, \alpha^p, \dots, \alpha^{p^{k-1}}$. Then

$$\text{norm } \alpha \equiv \alpha^q \pmod{p},$$

where $q = 1 + p + p^2 + \dots + p^{k-1}$.

As in the theorem, let ω denote the least positive value of n such that α^n is congruent to a rational integer modulo p . Then every other such n is readily seen to be divisible by ω . In particular,

$$\sigma = q/\omega = (p^k - 1)/(\omega(p - 1))$$

is a rational integer, and

$$\text{norm } \alpha \equiv M^\sigma \pmod{p},$$

where $\alpha^\omega \equiv M \pmod{p}$, $(1 \leq M \leq p - 1)$.

Let λ be the exponent to which M belongs modulo p , θ the exponent to which norm α belongs modulo p , and τ the period of α in \mathcal{F} . Then

$$(1) \quad \tau = \delta\theta\omega,$$

where $\delta = (\lambda, \sigma)$.

For since $\alpha^{\lambda\omega} \equiv M^\lambda \equiv 1 \pmod{p}$, $\tau|\lambda\omega$, and since α^τ is congruent to a rational integer modulo p , $\omega|\tau$. Therefore, $\tau = \nu\omega$, where $\nu|\lambda$. Then $\alpha^\tau = \alpha^{\nu\omega} \equiv M^\nu \equiv 1 \pmod{p}$, so that $\nu|\lambda$. Hence $\nu = \lambda$, $\tau = \lambda\omega$.

Now write $\lambda = \delta\lambda'$, $\sigma = \delta\sigma'$, where $(\lambda, \sigma) = \delta$, $(\lambda', \sigma') = 1$. Then $(\text{norm } \alpha)^{\lambda'} \equiv M^{\lambda'\sigma} = M^{\lambda\sigma'} \equiv 1 \pmod{p}$, so that $\theta|\lambda'$. Moreover, we have $M^{\theta\sigma} \equiv (\text{norm } \alpha)^\theta \equiv 1 \pmod{p}$, so that $\lambda|\theta\sigma$, $\lambda'\delta|\theta\delta\sigma'$, $\lambda'|\theta\sigma'$, $\lambda'|\theta$. Therefore $\lambda' = \theta$ and $\lambda = \delta\lambda' = \delta\theta$, $\tau = \lambda\omega = \delta\theta\omega$. Finally,

$$(2) \quad (\theta, \sigma)|\delta| \mid (k, p - 1).$$

For since $\theta|\lambda$, $(\theta, \sigma)|(\lambda, \sigma) = \delta$, and since

$$q = ((p - 1 + 1)^k - 1)/(p - 1) \equiv k(p - 1),$$

we have $(q, p - 1) = (k, p - 1)$. Therefore, since $\delta|\lambda|p - 1$ and $\delta|\sigma|q, \delta|(q, p - 1)$, it follows that $\delta|(k, p - 1)$. Equations (1) and (2) give us our theorem.

3. *Conclusion.* To illustrate the theorem, consider the Fibonaci sequence F_n defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$. Let p be a prime number. Then $F_p \equiv 0 \pmod{p}$ if and only if $p \equiv 0 \pmod{5}$ or $p \equiv 4 \pmod{5}$. This is a well-known result in number theory.

nacci series 0, 1, 1, 2, 3, 5, 8, 13, . . . giving the values of the Lucas function U_n associated with the polynomial $x^2 - x - 1$. This polynomial is irreducible modulo 13, so that the period of the Fibonacci series modulo 13 gives the period of the mark α associated with $x^2 - x - 1$ in the finite field of order 13^2 . We have $\omega = 7$, norm $\alpha = -1$, $\theta = 2$, $k = 2$, $\sigma = 2$, $p-1 = 12$. Hence (2) becomes $(2, 2) \mid \delta \mid (2, 12)$, so that $\delta = 2$. Hence the period is 28, which is easily verified directly. It seems quite difficult to determine the exact value of δ in all cases.*

CALIFORNIA INSTITUTE OF TECHNOLOGY

ON A PROBLEM OF KNASTER AND ZARANKIEWICZ†

BY J. H. ROBERTS

Knaster and Zarankiewicz have proposed the following problem:‡ “Does every continuum A contain a subcontinuum B such that $A - B$ is connected?” Knaster has shown,§ by an example in 3-space, that the answer is in the negative. In the present paper an example is given of a *plane* continuum M such that every non-degenerate proper subcontinuum of M disconnects M .

The point sets considered in this paper all lie in a plane.

DEFINITION OF $F(C; X, Y; \epsilon)$. Let C be any simple closed curve, X and Y distinct points of C , and ϵ any positive number. There exists a finite set of points A_1, A_2, \dots, A_n , ($n > 2$), such that (a) $A_1 + A_2 + \dots + A_n$ contains $X + Y$, (b) A_1, A_2, \dots, A_n lie on C in the order $A_1 A_2 \dots A_n A_1$, and (c) A_i and A_{i+1} (subscripts are to be reduced modulo n) are the end points of an arc t_i of diameter $< \epsilon$ which is a subset of C not containing A_{i+2} . There exists a set of mutually exclusive arc segments v_1, v_2, \dots, v_n lying within C such that $v_i + t_i$ is a simple closed curve w_i of diameter $< \epsilon$. Let J denote the simple closed curve

* See the discussion at the close of my paper, Transactions of this Society, vol. 33 (1931), p. 165.

† Presented to the Society, December 1, 1933.

‡ Fundamenta Mathematicae, vol. 8 (1926), Problem 42, p. 376.

§ B. Knaster, *Sur un continu que tout sous-continu divise*, Proceedings of the Polish Mathematical Congress, 1929, p. 59.

Note on an arithmetical property of recurring series.

Von

Morgan Ward in Pasadena.

1. In 1921, Siegel¹⁾ proved by the use of Thue's theorem a result equivalent to the following:

"If the sequence

$$(U) \quad U_0, U_1, U_2, \dots$$

is a rational solution of the difference equation

(1.1) $\Omega_{n+3} = P\Omega_{n+2} - Q\Omega_{n+1} + \Omega_n, \quad P, Q$ rational integers,
then only a finite number of terms of the sequence can vanish unless
the polynomial

$$(1.2) \quad F(x) = x^3 - Px^2 + Qx \pm 1$$

associated with (1.1) is of one or the other of the forms

$$(x \pm 1)(x^2 + 1) \quad \text{or} \quad (x \pm 1)(x^2 \pm x + 1)^n.$$

I wish to show here that as a simple consequence of the fundamental results of Delaunay²⁾ and Nagell³⁾ concerning the solution of the cubic diophantine equation

$$(1.3) \quad \Phi(u, v) = A u^3 + B u^2 v + C u v^2 + D v^3 = 1,$$

$$A, B, C, D$$
 rational integers,

that in general at most three terms of the sequence (U) can vanish provided that the discriminant of the associated polynomial is negative⁴⁾.

2. For let us assume that the polynomial $F(x)$ is irreducible in the field of rationals, has a negative discriminant, and that the sequence (U) contains $N \geq 1$ vanishing terms. Without affecting N , we may assume that the constant term of $F(x)$ is +1, and that the first non-vanishing term of (U) is U_0 , and that U_1 and U_2 are co-prime integers.

If (X), (Y), (Z) denote those particular solutions of (1.1) with the initial values 1, 0, 0; 0, 1, 0; 0, 0, 1 respectively, then it is easily shown that $U_n = U_0 X_n + U_1 Y_n + U_2 Z_n, \quad \alpha^n = X_n + Y_n \alpha + Z_n \alpha^2, \quad n = 0, 1, \dots$

¹⁾ Tohoku Journal 20 (1921), S. 26–31.

²⁾ Compt. Rend. 171 (1920), S. 136.

³⁾ Math. Zeitschr. 28 (1928), S. 10–29.

⁴⁾ If the discriminant of $F(x)$ is positive, so that all the roots of $F(x) = 0$ are real, the finiteness of the number of zeros in the sequence (U) is trivial, and extends to the case when P, Q, U_0, U_1, U_2 are real numbers and the constant term of $F(x)$ is not unity.

where α is any root of $F(x) = 0$. Since $U_0 = 0$, $(U_1, U_2) = 1$, $U_n = 0$ when and only when $Y_n = U_2 T_n$, $Z_n = -U_1 T_n$, T_n an integer. Thus $U_n = 0$ when and only when the norm of the algebraic integer $X_n + T_n(U_2\alpha - U_1\alpha^2)$ is unity; that is when and only when

$$(2.1) \quad A X_n^3 + B X_n^2 T_n + C X_n T_n^2 + D T_n^3 = 1$$

where

$$A = 1, \quad C = Q U_2^2 + (3 - P Q) U_1 U_2 + (Q^2 - 2 P) U_1^2,$$

$$B = P U_2 + (2 Q - P^2) U_1, \quad D = U_2^3 - P U_2^2 U_1 + Q U_2 U_1^2 - U_1^3.$$

Hence $u = X_n$, $v = T_n$ is a solution of the diophantine equation (1.2).

Owing to our hypotheses upon $F(x)$, the form $\Phi(u, v)$ is irreducible and has a negative discriminant. Therefore, by Nagell's main theorem⁵⁾, the diophantine equation has at most three integral solutions unless the form $\Phi(u, v)$ is equivalent to $u^3 + u v^2 + v^3$ or $u^3 - u^2 v + u v^2 + v^3$, when it has exactly four solutions, or to $u^3 - u^2 v + v^3$ when it has exactly five solutions.

Since $F(x)$ is irreducible, we cannot have $X_n = X_{n'}$, $T_n = T_{n'}$ unless $n = n'$. Hence the sequence (U) has in general at most three vanishing terms, and never more than five if the discriminant of $F(x)$ is negative.

3. It is possible to obtain a result analogous to Siegel's for the quartic difference equation

$$(3.1) \quad \Omega_{n+4} = P \Omega_{n+3} - Q \Omega_{n+2} + R \Omega_{n+1} \pm \Omega_n, \quad P, Q, R \text{ rational integers}$$

by a similar use of Thue's theorem; namely,

"If the sequence

$$(V) \quad V_0, V_1, V_2, \dots$$

is a rational solution of the difference equation (3.1), and if a is a fixed positive integer, then there are only a finite number of pairs of terms

$$V_{n_1}, V_{n_1+a}; V_{n_2}, V_{n_2+a}; V_{n_3}, V_{n_3+a}; \dots \quad n_1 < n_2 < n_3 < \dots$$

of the sequence (V) can vanish, provided that the associated polynomial

$$(3.2) \quad G(x) = x^4 - P x^3 + Q x^2 - R x \pm 1$$

is irreducible, and that its roots cannot be obtained by solving a chain of quadratic equations".

We may assume that V_0, V_a is the first pair of terms of (V) to vanish, and that V_1, V_2, V_3 are co-prime rational integers.

⁵⁾ Math. Zeitschr. 28 (1928), S. 10.

AN ARITHMETICAL PROPERTY OF RECURRING SERIES OF THE SECOND ORDER*

BY MORGAN WARD

1. *Statement of Property.* Let us denote by

$$(W_n) : \quad W_0, W_1, W_2, \dots, W_n, \dots,$$

a sequence of rational integers satisfying the difference equation

$$(1) \quad \Omega_{n+2} = P\Omega_{n+1} - Q\Omega_n, \quad (P, Q \text{ rational integers}),$$

and let p be an odd prime dividing neither Q nor $P^2 - 4Q = (\alpha - \beta)^2$, the discriminant of the polynomial

$$(2) \quad x^2 - Px + Q = (x - \alpha)(x - \beta)$$

associated with (1).†

We write as usual $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, $V_n = \alpha^n + \beta^n$ for the two Lucas functions built upon the roots α and β of (2).

The distribution of the multiples of p in the corresponding sequences $(U)_n$ and $(V)_n$ is well known: namely, *multiples of p always occur in $(U)_n$* ; more specifically, $U_n \equiv 0 \pmod{p}$ when and only when $n \equiv 0 \pmod{\tau}$, where τ is the restricted period‡ of $(U)_n$ modulo p . In the sequence $(V)_n$, *multiples of p occur when and only when τ is even*. In this case, $V_n \equiv 0 \pmod{p}$ when and only when $n \equiv 0 \pmod{\tau/2}$, $n \not\equiv 0 \pmod{\tau}$.

For the sequences $(U)_n$ and $(V)_n$ then, we know not only when multiples of p will occur, but where multiples of p will occur. Under the assumption that τ is odd, I propose to obtain a criterion which reduces the problem of determining *when* multiples of p will appear in *any* sequence $(W)_n$ (specified only by its two initial values W_0 and W_1) to the more fundamental (unsolved) problem of determining the characteristic number‡ and restricted period‡ of the Lucas functions associated with any given quadratic polynomial of the form (2).

* Presented to the Society, June 20, 1934.

† The excluded values of p are evidently trivial for the theorem that follows.

‡ For definitions of these terms, see my *Note on the period of a mark in a finite field*, this Bulletin, vol. 40 (1934), pp. 279–281.

In fact, let P' and Q' be rational integers satisfying the congruences

$$(3) \quad \begin{aligned} P' &\equiv W_0 \pmod{p}, \\ (4Q - P^2)Q' &\equiv W_1^2 - W_0W_1P + W_0^2Q \pmod{p}, \end{aligned}$$

and let $U'_n = (\alpha'^n - \beta'^n)/(\alpha' - \beta')$ be the Lucas function associated with the polynomial $x^2 - P'x + Q' = (x - \alpha')(x - \beta')$. Then a necessary and sufficient condition that the sequence $(W)_n$ should contain multiples of p is that the restricted period of U'_n modulo p should be an even divisor of 2τ .

2. *Illustration.* As a numerical illustration, take $P = 1$, $Q = -1$, $p = 89$, $W_0 = 1$, $W_1 = 4$. The sequence $(U)_n$ is then the familiar Fibonacci series

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \dots$$

so that $\tau = 11$. The congruences (3) become $P' \equiv 1 \pmod{89}$, $-5Q' \equiv 11 \pmod{89}$, so that we may take $P' = 1$, $Q' = -20$. The Lucas sequence $(U')_n$ for $\Omega_{n+2} = \Omega_{n+1} + 20\Omega_n$ runs $0, 1, 1, 21, 41, 461, 1281, 10501, \dots$ and by actual computation we find that $U'_{22} \equiv 69 \pmod{89}$. Hence the restricted period of $(U')_n$ modulo 89 is not an even divisor of $2\tau = 22$, and we conclude that all elements of the sequence $1, 4, 5, 9, 14, 23, 37, \dots$ are prime to 89, as may be easily verified.

3. *A Preliminary Identity.* My proof of this result is based upon a well known identity in the theory of partitions discovered by Euler,* which we formulate as follows.

Let q be any complex number,

$$[n] \left\{ \begin{array}{l} = (q^n - 1)/(q - 1), q \neq 1, \\ = \lim_{q \rightarrow 1} (q^n - 1)/(q - 1) = n, q = 1. \end{array} \right.$$

Writing $[n]!$ for $[1][2]\dots[n]$, $[0]! = 1$, we see that the basic bi-

* *Introductio in Analysisin Infinitorum*, 1748, Chapter VII; Netto, *Combinatorik*, 2d ed., 1927, p. 143.

nomial coefficient* $(n; r)$ is defined by $(n; r) = [n]! / \{[n-r]![r]!\}$. This expression, as Gauss showed,† is a polynomial in q which reduces to the ordinary binomial coefficient when $q=1$. The identity in question may now be written as follows:

$$(4) \quad \sum_{r=0}^{\tau} (\tau; r) q^{r(r+1)/2} z^r = (1 + qz)(1 + q^2z) \cdots (1 + q^{\tau}z).$$

4. *Proof.* The general term of the sequence $(W)_n$ may be expressed in the form

$$W_n = W_0 U_{n+1} + (W_1 - PW_0) U_n.$$

Thus the restricted period of $(W)_n$ modulo p is a divisor of the restricted period τ modulo p of the Lucas function U_n . Therefore the sequence $(W)_n$ will contain terms divisible by p when and only when the rational integer

$$(5) \quad \mathfrak{W} = \prod_{n=1}^{\tau} W_n$$

is divisible by p .

Now W_n can also be expressed in the form $W_n = A\alpha^n + B\beta^n$, where the constants A and B are determined by

$$(6) \quad W_0 = A + B, \quad W_1 = A\alpha + B\beta.$$

If we let‡ $\beta/\alpha = q$, $B/A = z$, we may write $W_n = A\alpha^n(1 + q^n z)$. Therefore by (5) and (4),

$$(7) \quad \begin{aligned} \mathfrak{W} &= \prod_{n=1}^{\tau} A\alpha^n(1 + q^n z) = A^{\tau} \alpha^{\tau(\tau+1)/2} \prod_{n=1}^{\tau} (1 + q^n z) \\ &= A^{\tau} \alpha^{\tau(\tau+1)/2} \sum_{r=0}^{\tau} (\tau; r) q^{r(r+1)/2} z^r. \end{aligned}$$

* This terminology is due to F. H. Jackson who in recent years has made an extensive study of the basic numbers $[n]$. (See, for example, Proceedings of the London Mathematical Society, (2), vol. 1 (1903–04), pp. 63–68; Proceedings of the Royal Society, (A), vol. 76 (1905), pp. 127–144.)

† *Summatio quarundam Serierum Singularium*, 1808; Works, vol. 2, p. 16.

‡ If A and B are rational integers modulo p , they cannot both be congruent to zero, and we take for A that one which is incongruent to zero modulo p . We have $\alpha \not\equiv 0 \pmod{p}$, since p was assumed prime to Q .

Now $[n] = (q^n - 1)/(q - 1) = (\alpha^n - \beta^n)/[(\alpha - \beta)\alpha^{n-1}] = \alpha^{-n+1}U_n$. Hence

$$(n; r) = U_n U_{n-1} \cdots U_{n-r+1} / (U_1 U_2 \cdots U_r \alpha^{-(n-r)r}).$$

But the first $\tau - 1$ of the numbers U_1, U_2, \dots, U_τ are prime to p , while U_τ is divisible by p . Hence $(\tau; r) \equiv 0 \pmod{p}$ unless $r=0$ or $r=\tau$, when it equals one. We therefore obtain from (7) the congruence

$$\mathfrak{W} \equiv A^\tau \alpha^{\tau(\tau+1)/2} (1 + q^{\tau(\tau+1)/2} z^\tau) \equiv A^\tau \alpha^{\tau(\tau+1)/2} + B^\tau \beta^{\tau(\tau+1)/2} \pmod{p}.$$

Now $\alpha^n = U_n \alpha - Q U_{n-1}, \beta^n = U_n \beta - Q U_{n-1}$. Therefore since τ is odd,*

$$\begin{aligned} \alpha^{\tau(\tau+1)/2} &\equiv (U_\tau \alpha - Q U_{\tau-1})^{(\tau+1)/2} \equiv (-Q U_{\tau-1})^{(\tau+1)/2} \pmod{p}, \\ \beta^{\tau(\tau+1)/2} &\equiv (-Q U_{\tau-1})^{(\tau+1)/2} \pmod{p}, \end{aligned}$$

and

$$(8) \quad \mathfrak{W} \equiv (-Q U_{\tau-1})^{(\tau+1)/2} (A^\tau + B^\tau) \pmod{p}.$$

Hence $\mathfrak{W} \equiv 0 \pmod{p}$ when and only when $A^\tau + B^\tau \equiv 0 \pmod{p}$.

Finally, write α', β' for A, B . Then $A^n + B^n = V'_n$, the Lucas function associated with the quadratic polynomial $x^2 - P'x + Q' = (x - \alpha')(x - \beta')$.

On referring back to (6) and recalling that p is prime to $P^2 - 4Q$, we find that we may assign to P' and Q' the rational integral values specified by the congruences (3). Our theorem now follows immediately from the laws of apparition for multiples of p in the Lucas functions stated in section 1 as applied to the sequence $(V')_n$.

CALIFORNIA INSTITUTE OF TECHNOLOGY

* It is at precisely this point that the assumption that τ is odd becomes vital. For if we assume that τ is even, we obtain in place of (8) the barren result $\mathfrak{W} = (U_{\tau+1})^{\tau/2} (A^\tau \alpha^{\tau/2} + B^\tau \beta^{\tau/2}) \pmod{p}$.

NOTE ON THE ITERATION OF FUNCTIONS
OF ONE VARIABLE*

BY MORGAN WARD

1. *Introduction.* Let $E(x)$ be a real-valued function of the real variable x for some specified range, and let

$$E_0(x) = x, E_1(x) = E(x), \dots, E_{n+1}(x) = E(E_n(x)), \dots$$

represent its successive iterations. The interpolation problem of defining $E_n(x)$ for non-integral values of n was discussed some time ago by A. A. Bennett,† who reduced it formally to the solution of the functional equation

$$(1) \quad \psi(x + 1) = E(\psi(x)).$$

For if $\psi(x)$ satisfies (1) and if n is any positive integer,

$$(2) \quad \psi(x + n) = E_n(\psi(x)).$$

Hence on writing $\psi^{-1}(x)$ for x , where $\psi^{-1}(x)$ denotes an inverse of the function $\psi(x)$, we obtain the formula

$$(3) \quad E_n(x) = \psi(\psi^{-1}(x) + n),$$

defining $E_n(x)$ for a continuous range of values of n .

In this note, I propose to give an entirely elementary explicit solution to this problem of interpolation for all functions $E(x)$ subject to the following three conditions:‡

- (a). $E(x)$ is a real, continuous, single-valued function of the real variable x in the range $a \leq x < \infty$.
- (b). $E(x) > x$ for all $x \geq a$.
- (c). $E(x') > E(x)$ if $x' > x \geq a$.

We may remark that the functional equation (1) is merely another form of a famous equation studied by Abel,§

* Presented to the Society, June 20, 1934.

† In two papers in the Annals of Mathematics, (2), vol. 17 (1915–16), pp. 74–75 and pp. 23–60. This second paper contains references to the earlier literature. A. Korkine (Bulletin des Sciences Mathématiques, (2), vol. 6 (1882), pp. 228–242) seems to have been the first to consider this problem.

‡ These conditions are all satisfied by $E(x) = e^x$, the particular case discussed by Bennett in the first paper cited.

§ Works, vol. II, *Posthumous Papers*, 1881, pp. 36–39.

$$(4) \quad \phi(x) + 1 = \phi(f(x)),$$

as Abel himself showed.* Here $f(x)$ is a given function, and $\phi(x)$ is to be determined. This equation has been extensively investigated of late by modern function-theoretic methods.†

2. *A Simplification.* As a preliminary simplification, we may assume that the constant a in condition (a) is zero, and that $E(0) = 1$. For if $E(a) \neq 0$, the function $E'(x) = E^2(x+a)/E^2(a)$ satisfies conditions (a), (b), (c) with $a=0$, while $E'(0) = 1$, and $E(x) = \pm E(a)(E'(x-a))^{1/2}$. On the other hand, if $E(a) = 0$, then $E_2(a) = E(0) > 0$ by (b). Hence $E''(x) = E_2(x+a)/E_2(a)$ will satisfy (a), (b), (c) with $a=0$, $E''(0) = 1$. Since $E(x)$ is continuous and monotonic increasing, it has a unique inverse $E_{-1}(x)$. Thus, if $E''(x)$ is given, $E(x) = E_{-1}(E_2(a)E''(x-a))$.

From (b) and (c), it follows that for any positive integer n , $E_n(x') > E_n(x)$ if $x' > x$. Since $E_n(x)$ is furthermore continuous by (a), it has a unique inverse which we shall denote by $E_{-n}(x)$. If we write $y = E_n(x)$, then by (b), $y \geq E_n(0)$, so that $E_{-n}(x)$ is defined only for $x \geq E_n(0)$. It is easily verified, however, that for any $x \geq 0$,

$$(5) \quad E_n(E_m(x)) = E_{n+m}(x)$$

for all integral values of n and m , positive or negative, for which the functions are defined.

3. *Solution of (1).* We shall next give a solution of the functional equation (1). Let $[x]$ denote as usual the greatest integer in x so that

$$(6) \quad 0 = E_0(0) \leq x - [x] < E_1(0) = 1.$$

Then

$$\psi(x) = E_{[x]}(x - [x])$$

is a monotonic increasing continuous solution of (1). For

$$\begin{aligned} \psi(x+1) &= E_{[x+1]}(x+1 - [x+1]) = E_{[x]+1}(x - [x]) \\ &= E(E_{[x]}(x - [x])) = E(\psi(x)), \end{aligned}$$

* Write (1) in the form $x+1 = \psi^{-1}(E(\psi(x)))$. Then on substituting $\psi^{-1}(x)$ for x , we obtain $\psi^{-1}(x)+1 = \psi^{-1}(E(x))$.

† See, for example, Picard, *Leçons sur Quelques Equations Fonctionnelles*, 1928, Chapter 4. For more recent papers, see the Zentralblatt für Mathematik under the index *Funktionentheorie: Iterationen*.

and if $x' \geq x + 1$,

$$\begin{aligned}\psi(x') &= E_{\lfloor x' \rfloor}(x' - \lfloor x' \rfloor) \geq E_{\lfloor x' \rfloor}(0) \\ &= E_{\lfloor x' \rfloor - 1}(1) \geq E_{\lfloor x \rfloor}(1) > E_{\lfloor x \rfloor}(x - \lfloor x \rfloor) = \psi(x),\end{aligned}$$

while if $x + 1 > x' > x$,

$$\begin{aligned}\psi(x') &= E_{\lfloor x' \rfloor}(x' - \lfloor x' \rfloor) = E_{\lfloor x \rfloor}(x' - \lfloor x \rfloor) \\ &> E_{\lfloor x \rfloor}(x - \lfloor x \rfloor) = \psi(x).\end{aligned}$$

The continuity of $\psi(x)$ is obvious if x is not an integer n . Also if $x = n$, $\epsilon > 0$, it is clear that $\lim_{\epsilon \rightarrow 0} \psi(n + \epsilon) = \psi(n)$. On setting $x = n - \epsilon$, $\epsilon > 0$, we have $\lim_{\epsilon \rightarrow 0} \psi(n - \epsilon) = \lim_{\epsilon \rightarrow 0} E_{n-1}(1 - \epsilon) = E_{n-1}(1) = E_n(0) = \psi(n)$.

It follows that $\psi(x)$ has a unique inverse $\psi^{-1}(x)$. To determine it, let x be given, and let the positive integer k be determined by the inequality

$$(7) \quad E_k(0) \leq x < E_k(1).$$

Then

$$\psi^{-1}(x) = E_{-k}(x) + k.$$

For first of all, $\psi^{-1}(x)$ is defined and continuous for all $x \geq 0$. Secondly, from (7), $0 \leq E_{-k}(x) < 1$ so that $k = [\psi^{-1}(x)]$, the greatest integer in $\psi^{-1}(x)$. Therefore

$$\psi(\psi^{-1}(x)) = E_k(\psi^{-1}(x) - k) = E_k(E_{-k}(x)) = E_0(x) = x.$$

Thirdly, since $E_{\lfloor x \rfloor}(0) \leq \psi(x) < E_{\lfloor x \rfloor}(1)$,

$$\begin{aligned}\psi^{-1}(\psi(x)) &= E_{-[\lfloor x \rfloor]}(\psi(x) + \lfloor x \rfloor) + \lfloor x \rfloor \\ &= E_{-[\lfloor x \rfloor]}(E_{\lfloor x \rfloor}(x - \lfloor x \rfloor)) + \lfloor x \rfloor = x.\end{aligned}$$

We obtain then, on substituting in (3), the final result of this note:

$$(8) \quad \begin{aligned}E_n(x) &= E_{[n+k+E_{-k}(x)]}(n + k + E_{-k}(x) - [n + k + E_{-k}(x)]) \\ &= E_{[n+k+E_{-k}(x)]}(n + E_{-k}(x) - [n + E_{-k}(x)]).\end{aligned}$$

Here the integer k is determined by the inequality (7) and the formula is valid for all real values of $n \geq 0$. The equation (5) may now be shown to hold for non-integral values of m and n .

In particular, if $R(x) > 0$,

$$t^x = \Gamma(x+1) \sum_{n=0}^{\infty} (-)^n \binom{x}{n} L_n(t).$$

6. Let

$$w(x) = x^{-1}\pi^x = \int_0^\pi t^{x-1} dt.$$

Then, if $f_n = \cos(nE)$, we have

$$\begin{aligned} f_m f_n w(x) &= \int_0^\pi t^{x-1} \cos(mt) \cos(nt) dt = C_{m,n}(x), \\ C_{m,n}(1) &= \int_0^\pi \cos(mt) \cos(nt) dt = 0 \quad m \neq n \\ &= (\pi/2) \quad m = n > 0 \\ &= \pi \quad m = n = 0. \end{aligned}$$

Let

$$C_n(x) = \int_0^\pi t^{x-1} \cos nt dt = \pi^x \sum_{s=0}^{\infty} (-)^s \frac{(n\pi)^{2s}}{(2s)!(x+2s)}$$

then the coefficients in an expansion

$$g(x) = \sum_{n=0}^{\infty} c_n C_n(x)$$

are given by the rule

$$\epsilon_n c_n = \lim_{x \rightarrow 0} f_n g(x), \quad \epsilon_n = \pi/2, \quad n > 0, \quad \epsilon_0 = \pi.$$

In particular

$$\begin{aligned} \pi C_m(x+y) &= C_0(x)C_m(1+y) + 2 \sum_{n=1}^{\infty} C_n(x)C_{m+n}(1+y) \\ &= \sum_{n=-\infty}^{\infty} C_n(x)C_{m+n}(1+y). \end{aligned}$$

This is easily confirmed with the aid of Parseval's theorem.

QUESTIONS, DISCUSSIONS AND NOTES

EDITED BY R. E. GILMAN, Brown University, Providence, Rhode Island

The department of Questions, Discussions, and Notes in the Monthly is open to all forms of activity in collegiate mathematics, including the teaching of mathematics, except for specific problems, especially new problems, which are reserved for the department of Problems and Solutions.

THE NUMERICAL EVALUATION OF A CLASS OF TRIGONOMETRIC SERIES

By MORGAN WARD, California Institute of Technology

1. In a recent problem arising in the design of an X-ray tube, it was necessary to sum two slowly convergent trigonometric series

$$\sum_1^{\infty} n^{-3/2} \cos 2n\pi x, \quad \sum_1^{\infty} n^{-3/2} \sin 2n\pi x, \quad 0 \leq x \leq 1,$$

to a fair degree of accuracy. It was thought that the method devised to transform these series into more rapidly converging ones might be useful to others confronted with a similar task.

2. Let us consider quite generally a trigonometric series of the form

$$(2.1) \quad F(x) = \sum_1^{\infty} \phi(n) e^{2n\pi i x},$$

where $\phi(n)$ is real and such that the series converges in the interval $0 \leq x \leq 1$.

Let $\Delta\phi(n)$, $\Delta^2\phi(n)$ and so on, represent the successive differences $\phi(n+1) - \phi(n)$, $\Delta\phi(n+1) - \Delta\phi(n)$, of $\phi(n)$; and let us write for brevity $\Delta^r\phi(a)$ for the value of the r th difference of $\phi(n)$ when n equals a . We then have the following

THEOREM. *If a is any positive integer, and if the $(s+1)$ th difference of $\phi(n)$ is of invariable sign for all positive integral values of n greater than a , then*

$$(2.2) \quad F(x) = \sum_1^a \phi(n) e^{2n\pi i x} + \sum_{r=0}^{s-1} \Delta^r \phi(a+1) \left(\frac{\csc \pi x}{2} \right)^{r+1} e^{2\pi i ax + \pi i(r+1)(x+1/2)} + R,$$

where

$$(2.3) \quad |R| \leq 2 \left(\frac{\csc \pi x}{2} \right)^{s+1} |\Delta^s \phi(a+1)|.$$

If we consider the real and imaginary parts of $F(x)$ separately, we can announce two precisely similar theorems where the exponentials appearing in (2.2) are replaced by the corresponding cosine and sine terms.

As regards our hypothesis about the sign of the $(s+1)$ th difference of $\phi(n)$, we may remark that if $\phi(t)$ may be considered as a function of the continuous variable t for all values of $t \geq a$, and if the $(s+1)$ th derivative of $\phi(t)$ exists and is of invariable sign for $t \geq a$, then the $(s+1)$ th difference of $\phi(n)$ is also of invariable sign for $n > a$. These conditions will be satisfied for example for any positive integers a and s if $\phi(n) = n^{-\beta}$, $\beta > 1$.

To demonstrate the utility of our result for practical computation, take $\phi(n) = n^{-3/2}$, $a = 5$, and $s = 2$. Then we have

$$\sum_1^{\infty} n^{-3/2} \cos 2n\pi x = \sum_1^5 n^{-3/2} \cos 2n\pi x - \frac{\csc \pi x}{2} 6^{-3/2} \sin 11\pi x$$

$$-\left(\frac{\csc \pi x}{2}\right)^2 \Delta 6^{-3/2} \cos 12\pi x + R,$$

where

$$|R| \leq 2 \left(\frac{\csc \pi x}{2}\right)^3 \Delta^2 6^{-3/2} \leq 2 \left(\frac{\csc \pi x}{2}\right)^3 (.0023).$$

Thus in the range $1/6 \leq x \leq 5/6$ where $1/2 \leq (\csc \pi x)/2 \leq 1$, $|R| < .005$. A comparable degree of accuracy from the series itself would require several hundred terms.

3. The above theorem may be proved as follows. Let

$$(3.1) \quad F_{(a)}(x) = \sum_{n=1}^{\infty} \phi(n) e^{2n\pi i x}$$

be the remainder of the series (2.1) after a terms, so that

$$(3.2) \quad F(x) = \sum_{n=1}^a \phi(n) e^{2n\pi i x} + F_{(a)}(x).$$

Then if s is any positive integer,

$$(3.3) \quad \begin{aligned} (1 - e^{2\pi i x})^{s+1} F_{(a)}(x) &= \sum_{r=0}^s (1 - e^{2\pi i x})^{s-r} \Delta^r \phi(a+1) e^{2\pi i (a+r+1)x} \\ &\quad + \sum_{n=a+1}^{\infty} \Delta^{s+1} \phi(n) e^{2\pi i (n+s+1)x}. \end{aligned}$$

For this formula is easily seen to be true when $s=0$. Assume that it is true when $s=k-1$:

$$\begin{aligned} (1 - e^{2\pi i x})^k F_{(a)}(x) &= \sum_{r=0}^{k-1} (1 - e^{2\pi i x})^{k-1-r} \Delta^r \phi(a+1) e^{2\pi i (a+r+1)x} \\ &\quad + \sum_{n=a+1}^{\infty} \Delta^k \phi(n) e^{2\pi i (n+k)x}. \end{aligned}$$

Multiply this expression by $1 - e^{2\pi i x}$. Then

$$\begin{aligned} (1 - e^{2\pi i x})^{k+1} F_{(a)}(x) &= \sum_{r=0}^{k-1} (1 - e^{2\pi i x})^{k-r} \Delta^r \phi(a+1) e^{2\pi i (a+r+1)x} \\ &\quad + \Delta^k \phi(a+1) e^{2\pi i (a+k+1)x} + \sum_{n=a+2}^{\infty} \Delta^k \phi(n) e^{2\pi i (n+k)x} - \sum_{n=a+1}^{\infty} \Delta^k \phi(n) e^{2\pi i (n+k+1)x}. \end{aligned}$$

The term $\Delta^k \phi(a+1) e^{2\pi i (a+k+1)}$ can be incorporated into the first summation, on changing its upper index from $k-1$ to k . In the second summation, we replace n by $n+1$, and then combine the resulting expression with the third summation. On recalling that by definition, $\Delta^k \phi(n+1) - \Delta^k \phi(n) = \Delta^{k+1} \phi(n)$, we obtain in this manner (3.3) with $s=k$. Hence (3.3) is true when $s=0$, and if it is true for $s=k-1$, it is true for $s=k$. Therefore, by induction, it is true generally.

Now assume that $\Delta^{s+1} \phi(n)$ is of invariable sign. Then in (3.3)

$$\begin{aligned}
 & \left| \sum_{n=a+1}^{\infty} \Delta^{s+1} \phi(n) e^{2\pi i(n+s+1)x} \right| \leq \sum_{n=a+1}^{\infty} |\Delta^{s+1} \phi(n) e^{2\pi i(n+s+1)x}| \\
 & = \pm \sum_{n=a+1}^{\infty} \Delta^{s+1} \phi(n) = \pm \sum_{n=a+1}^{\infty} \Delta^s \phi(n+1) - \Delta^s \phi(n) = |\Delta^s \phi(a+1)|, \text{ or} \\
 (3.4) \quad & \left| \sum_{n=a+1}^{\infty} \Delta^{s+1} \phi(n) e^{2\pi i(n+s+1)x} \right| \leq |\Delta^s \phi(a+1)|.
 \end{aligned}$$

Finally, $1 - e^{2\pi i x}$ may be written $2 \sin \pi x e^{\pi i(x-1/2)}$. Therefore, if we divide both sides of (3.3) by $(1 - e^{2\pi i x})^{s+1}$, we obtain

$$\begin{aligned}
 F_{(a)}(x) &= \sum_{r=0}^s \Delta^r \phi(a+1) \left(\frac{\csc \pi x}{2} \right)^{r+1} e^{2\pi i a x + \pi i(r+1)(x+1/2)} \\
 &\quad + \left(\frac{\csc \pi x}{2} \right)^{s+1} \sum_{n=a+1}^{\infty} \Delta^{s+1} \phi(n) e^{2\pi i n x + \pi i(s+1)(x+1/2)}.
 \end{aligned}$$

It follows then from (3.4) that

$$(3.5) \quad F_{(a)}(x) = \sum_{r=0}^{s-1} \Delta^r \phi(a+1) \left(\frac{\csc \pi x}{2} \right)^{r+1} e^{2\pi i a x + \pi i(r+1)(x+1/2)} + R,$$

where

$$|R| < 2 \left(\frac{\csc \pi x}{2} \right)^{s+1} |\Delta^s \phi(a+1)|.$$

On combining (3.2) and (3.5), we obtain the result stated in the theorem.

AN APPLICATION OF STIRLING'S NUMBERS

By H. J. GOLDSTEIN, New York City

1. J. Ginsburg has called attention in the February, 1928, issue of this MONTHLY, to the varied history of the Stirling numbers. These numbers, while perhaps as interesting and useful as the allied Bernoulli numbers, have received relatively little attention. Their properties have, however, been discussed at considerable length by N. Nielsen¹ and C. Tweedie.² We shall consider an elementary application, and derive, *en passant*, a relation among the numbers themselves. The latter is probably not new, but does not appear in the works cited, or in others consulted by the author.

The Stirling numbers of the first and second species, designated respectively by C_n^r and Γ_n^r ($n > 0, r \geq 0$) are the coefficients in the expansions

¹ *Theorie der Gamma Funktion* (1904), pp. 66–78; and *Recherches sur les Nombres et les Polynomes de Stirling*, *Annali di Matematica*, vol. 10 (1904), pp. 287–318.

² *Proc. Edinburgh Math. Soc.*, vol. 37 (1919), pp. 11–25.

Chapter 9

1935

AN ENUMERATIVE PROBLEM IN THE ARITHMETIC OF LINEAR RECURRING SERIES*

BY
MORGAN WARD

1. Let m be a fixed positive integer greater than one and let

$$(1.1) \quad \Omega_{n+k} = c_1\Omega_{n+k-1} + c_2\Omega_{n+k-2} + \cdots + c_k\Omega_n$$

be a linear difference equation of order k with rational integral coefficients c_1, c_2, \dots, c_k . If

$$(U): \quad U_0, U_1, U_2, \dots, U_n, \dots$$

is any sequence of rational integers satisfying (1.1), then after a certain point the sequence becomes periodic when considered modulo m . Its least period is called the characteristic number of the sequence (U) modulo m .

In a recent paper in these Transactions†, I have considered the problem of determining this characteristic number given m, c_1, c_2, \dots, c_k and the k initial values U_0, U_1, \dots, U_{k-1} of the sequence (U) , and I have reduced it to certain basic problems in the theory of higher congruences.‡

In the present paper, I am concerned with the following problem which I shall similarly reduce to a problem in the theory of higher congruences:

Given any positive integer s : to find the number of distinct sequences (U) modulo m whose characteristic number is exactly equal to s .

2. I obtain here the following results.

(i) *It suffices to determine the total number of purely periodic sequences (U) modulo m whose characteristic number is at most equal to s . (§3.)*

(ii) *It suffices to confine ourselves to the case when $m = p^N$ is a power of a prime p , and when the polynomial*

$$(2.1) \quad f(x) = x^k - c_1x^{k-1} - c_2x^{k-2} - \cdots - c_k$$

of degree k associated with the difference equation (1.1) is of the form

$$f(x) = B(x) \equiv \{\phi(x)\}^a \pmod{p}$$

where $\phi(x)$ is irreducible modulo p and a is a positive integer. (§4.)

* Presented to the Society, December 27, 1934; received by the editors August 1, 1934.

† Vol. 35 (1933), pp. 600–628. I shall refer to this paper as Trans I.

‡ Notably, to finding the least value of n such that $A(x)(x^n - 1) \equiv 0 \pmod{p^N, B(x)}$ for any prime p and any assigned polynomials $A(x)$ and $B(x)$.

(iii) *The problem thus delimited is equivalent to determining the total number of distinct polynomials $U(x)$ of degree $\leq k-1$ modulo p^N such that*

$$(2.2) \quad U(x)A(x) \equiv 0 \quad (\text{mod } p^N, B(x)),$$

where

$$A(x) \equiv x^s - 1 \quad (\text{mod } p^N, B(x)).$$

This number can be immediately written down provided that we know the elementary divisors corresponding to the prime p of the matrix \mathcal{E} of the Sylvester eliminant of $A(x)$ and $B(x)$. (§5.)

In another paper in these Transactions* I have made a detailed study of the congruence (2.2) and shown that if $N \leq \lambda$ (where p^λ is the first elementary divisor of the matrix \mathcal{E} of (iii) corresponding to the prime p) there exists a unique polynomial $U(x) \equiv A_{\lambda-N}(x)$, modulo p^N , satisfying (2.2) of minimal degree in x and leading coefficient unity. Let the degree of $A_{\lambda-N}(x)$ be $\alpha_{\lambda-N}$ ($N = 1, 2, \dots, \lambda$), and let

$$\sigma_N = \alpha_{\lambda-1} + \alpha_{\lambda-2} + \dots + \alpha_{\lambda-N} \quad (N = 1, 2, \dots, \lambda).$$

Then

(iv) *The total number of distinct polynomials modulo p^N of degree $\leq k-1$ satisfying (2.1) is*

$$p^{Nk-\sigma_N} \text{ if } N \leq \lambda \text{ and } p^{\lambda k-\sigma_\lambda} \text{ if } N \geq \lambda.$$

(§6.) In this latter case, the number is therefore independent of N .

3. In the sections which follow, we shall use the German capital \mathfrak{M} for the double modulus $m, f(x)$, writing

$$A(x) \equiv 0 \quad (\mathfrak{M}) \text{ for } A(x) \equiv 0 \quad (\text{mod } m, f(x)).$$

We shall otherwise use the same notation and terminology as in Trans I. In particular, the sequence (U) will be said to be “purely periodic” modulo m if it contains no non-repeating residues when considered modulo m . From Theorem 4.1, Trans I, it suffices to enumerate all the purely periodic sequences (U) with fixed characteristic number s . For if the number of such sequences be denoted by $\psi(s)$, the total number of sequences with characteristic number s may be obtained by multiplying $\psi(s)$ by a factor which is independent of s . (Trans I, part IV.)

By the fundamental theorem on page 606 of Trans I, the enumerative problem for purely periodic sequences is equivalent to the following problem in the theory of congruences to a double modulus:

* Vol. 35 (1933), pp. 254–260. I shall refer to this paper as Trans II.

To determine the total number of distinct polynomials $U(x)$ modulo m of degree $\leq k-1$ such that

$$(3.1) \quad U(x)(x^S - 1) \equiv 0 \pmod{m},$$

$$(3.2) \quad U(x)(x^R - 1) \not\equiv 0 \pmod{m} \quad (1 \leq R < S).$$

We can omit the restriction (3.2). For assume that (3.1) holds, and also that

$$(3.3) \quad U(x)(x^R - 1) \equiv 0 \pmod{m}.$$

Then it is easily seen that for any integers L and M ,

$$U(x)(x^{LS+MR} - 1) \equiv 0 \pmod{m}.$$

Choose L and M so that $LS+MR=D$, the greatest common divisor of S and R . Then

$$U(x)(x^D - 1) \equiv 0 \pmod{m}.$$

That is, if (3.3) holds, it must hold for some integer $R=D$ which is a divisor of S . We may therefore replace condition (3.2) by

$$(3.21) \quad U(x)(x^R - 1) \not\equiv 0 \pmod{m}, \quad R \text{ any proper divisor of } S.$$

Furthermore, if (3.3) holds, there is a smallest value of R for which it holds dividing all other such R .

If $\phi(s)$ is the total number of polynomials $U(x)$ satisfying (3.1) and $\psi(s)$ the total number of polynomials satisfying both (3.1) and (3.21), it is clear then that

$$\phi(s) = \sum_{R|S} \psi(R).$$

Therefore by Dedekind's inversion formula,

$$\psi(S) = \sum_{D|S} \mu(D)\phi(S/D).$$

The summation here extends over all divisors D of S and $\mu(D)$ denotes Möbius' function. It suffices therefore to determine $\phi(s)$.

4. For the moment, write $u(s; m; f(x))$ for the function $\phi(s)$ defined above. Then first of all, it is readily shown as in Trans I, part III, that if $m=ab$, $(a, b)=1$, then

$$u(s; m; f(x)) = u(s; a; f(x)) \cdot u(s; b; f(x)).$$

That is, $u(s; m; f(x))$ is a multiplicative function of m . We can assume therefore that

$$(4.1) \quad m = p^N, \quad p \text{ a prime, } N \geq 1.$$

Secondly, it is readily shown that if

$$f(x) \equiv f_1(x) \cdot f_2(x) \pmod{m}, \text{ Res } \{f_1(x), f_2(x)\} \text{ prime to } m,$$

then

$$u(s; m; f(x)) = u(s; m; f_1(x))u(s; m; f_2(x)).$$

Since $m = p^N$, we have by Schönemann's second theorem* a decomposition of $f(x)$ modulo p^N of the form

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

where $f_i(x)$ is primary and congruent to $\{\phi_i(x)\}^{a_i}$, modulo p , for $i = 1, \dots, r$, while the polynomials $\phi_1(x), \phi_2(x), \dots, \phi_r(x)$ are distinct and irreducible modulo p .

Since

$$\text{Res } \{f_i(x), f_j(x)\} \not\equiv 0 \pmod{p} \quad (i, j = 1, \dots, r; i \neq j),$$

we can assume that

$$f(x) = B(x) \equiv \{\phi(x)\}^a \pmod{p},$$

$\phi(x)$ irreducible modulo p .

5. Let

$$B(x) = x^m + b_1x^{m-1} + \cdots + b_m.$$

Then we have reduced our problem to determining the total number of polynomials $U(x)$ of degree $\leq m-1$, distinct modulo p^N , such that

$$(5.1) \quad U(x)A(x) \equiv 0 \pmod{p^N, B(x)},$$

where p is a prime, while

$$(5.2) \quad A(x) \equiv x^s - 1 \pmod{p^N, B(x)}.$$

In Trans I, pp. 622–623, I have shown how to determine a polynomial $A(x)$ satisfying (5.2) of degree less than $B(x)$ under the assumption that we know that solution of the difference equation associated with $B(x)$ with the m initial values $0, 0, \dots, 0, 1$. But here we shall not make any assumption about the degree of $A(x)$. Indeed, we shall show that the number of such polynomials $U(x)$ can be theoretically determined without restricting the form of the polynomial $A(x)$ in any way.

For let

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n.$$

* Fricke, *Algebra*, vol. 2, Braunschweig, 1928, chapter 2.

The congruence (5.1) may be written in the equivalent form

$$(5.3) \quad A(x)U(x) + B(x)V(x) \equiv 0 \pmod{p^N},$$

where $U(x) = u_0x^{m-1} + \dots + u_{m-1}$, $V(x) = v_0x^{n-1} + \dots + v_{n-1}$ are to be determined.

Let $\mathcal{E} = (e_{ij})$ denote the transpose of the matrix corresponding to the Sylvester eliminant of $A(x)$ and $B(x)$. Then if we let

$$z_{i+1} = u_i \quad (i = 0, 1, \dots, m-1), \quad z_{i+m} = v_{i-m} \quad (i = m, m+1, \dots, m+n-1),$$

(5.3) is equivalent to the set of $n+m$ congruences

$$(5.4) \quad \sum_{j=1}^{m+n} e_{ij} z_j \equiv 0 \pmod{p^N} \quad (i = 1, 2, \dots, m+n).$$

It is clear then that the number of distinct polynomials $U(x)$ satisfying the conditions of (5.1) equals the number of distinct solutions z_1, z_2, \dots, z_{m+n} modulo p^N of the system (5.4).

This number was determined by H. J. S. Smith in a classical memoir.* Namely, let $p^{\lambda_1}, p^{\lambda_2}, \dots, p^{\lambda_k}$ be the successive elementary divisors of the matrix \mathcal{E} corresponding to the prime p . Then if r is so chosen that $\lambda_{r-1} > N \geq \lambda_r$, the number of distinct incongruent solutions of (5.4) is $p^{rN+\lambda_r+\lambda_{r+1}+\dots+\lambda_k}$.

6. We can express the number of solutions of the congruence (5.1) in quite a different manner by using some of the results obtained in my paper Trans II.

Let us assume that $N \geq \lambda$, where p^λ now denotes the first elementary divisor of the matrix \mathcal{E} defined in §5 corresponding to p . Then (Trans II, p. 255) $U(x)$ must be of the form

$$(6) \quad U(x) = p^{N-\lambda}(Q_0(x)A_0(x) + pQ_1(x)A_1(x) + \dots + p^{\lambda-1}Q_{\lambda-1}(x)A_{\lambda-1}(x)),$$

where $A_r(x)$ is the unique polynomial of minimal degree and leading coefficient unity such that

$$A_r(x)A(x) \equiv 0 \pmod{p^{\lambda-r}, B(x)}.$$

Let the degree of this polynomial be denoted by α_r .

The procedure by which the polynomials $Q_0(x), Q_1(x), \dots$ are determined is then as follows:

Let $U(x) = p^{N-\lambda}V_0(x)$. Then $A(x)V_0(x) \equiv 0 \pmod{p^\lambda, B(x)}$ and, as proved in Trans II, $V_0(x) = Q_0(x)A_0(x) + V_1(x)$ where $V_1(x)$ is of lesser degree than

* On systems of linear indeterminate equations and congruences, Collected Papers, vol. 1, Oxford, 1894, p. 399.

$A_0(x)$. Then $V_0(x)$ is of degree $\leq m-1$, $A_0(x)$ is of degree α_0 , and $V_1(x)$ of degree $\leq \alpha_0-1$. Hence $Q_0(x)$ is of degree $\leq m-\alpha_0-1$, so that we can write

$$Q_0(x) = q_1 x^{m-\alpha_0-1} + q_2 x^{m-\alpha_0-2} + \cdots + q_{m-\alpha_0}$$

where $0 \leq q_j < p^\lambda$ ($j = 1, 2, \dots, m-\alpha_0$).

Therefore, there are $p^{\lambda(m-\alpha_0)}$ possible polynomials $Q_0(x)$ for a given $U(x)$.

Next, we have

$$A(x)V_1(x) \equiv 0 \quad (\text{mod } p^{\lambda-1}, B(x)),$$

$V_1(x) = Q_1(x)A_1(x) + pV_2(x)$ where $V_2(x)$ is of lesser degree than $A_1(x)$. Then $V_1(x)$ is of degree α_0-1 , $A_1(x)$ of degree α_1 , and $V_2(x)$ of degree $\leq \alpha_1-1$. Therefore $Q_1(x)$ is of degree $\leq \alpha_0-\alpha_1-1$, and reasoning as before, we see that there are $p^{(\lambda-1)(\alpha_0-\alpha_1)}$ possible polynomials $Q_1(x)$ for a given $U(x)$.

Continuing in this manner, we see that there are $p^{(\lambda-r)(\alpha_r-\alpha_{r-1})}$ possible polynomials $Q_r(x)$ ($0 \leq r \leq \lambda-1$; $\alpha_{-1}=m$). Therefore *there are in all*

$$p^{\lambda(m-\alpha_0)} \cdot p^{(\lambda-1)(\alpha_0-\alpha_1)} \cdot p^{(\lambda-2)(\alpha_1-\alpha_2)} \cdots \cdots p^{\alpha_{\lambda-2}-\alpha_{\lambda-1}} = p^{\lambda m - (\alpha_0+\alpha_1+\cdots+\alpha_{\lambda-1})}$$

polynomials $U(x)$ satisfying the congruence (5.1); for it easily is seen that each choice of $Q_0(x), \dots, Q_{\lambda-1}(x)$ in formula (6.1) leads to a distinct polynomial $U(x)$.

If we assume that $N \leq \lambda$, we have

$$U(x)A(x) \equiv 0 \quad (\text{mod } p^N, B(x)),$$

$$U(x) = Q_{\lambda-N}(x)A_{\lambda-N}(x) + pV_{\lambda-N+1}(x),$$

$$V_{\lambda-N+1}(x) = Q_{\lambda-N+1}(x)A_{\lambda-N+1}(x) + pV_{\lambda-N+2}(x),$$

and so on.

On determining the degrees of the polynomials $Q_{\lambda-N}(x), Q_{\lambda-N+1}(x), \dots$, we find that in this case *there are $p^{N m - (\alpha_{\lambda-N}+\alpha_{\lambda-N+1}+\cdots+\alpha_{\lambda-1})}$ possible polynomials $U(x)$.*

On writing σ_N for $\alpha_{\lambda-1}+\alpha_{\lambda-2}+\cdots+\alpha_{\lambda-N}$ and k for m , we obtain the final result stated in the second section of this paper.

INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

A DETERMINATION OF ALL POSSIBLE SYSTEMS OF STRICT IMPLICATION.

By MORGAN WARD.

1°. It is known that the postulates chosen by C. I. Lewis for his "system of strict implication" † are not categorical, since three distinct types of such a system have been shown to exist.‡ I shall prove here that the three types already discovered are the only ones possible. The inclusion of an additional modal postulate ‡ will therefore make the system categorical, and allow it to be exhibited as a four-valued truth-value system. The corresponding entscheidung problem may then be solved by the matrix method.

2°. In what follows, the decimal numeration 11.01-20.01 refers to *Symbolic Logic*, Chapter VI. We shall modify Lewis' notation as follows. We use + instead of v to denote logical addition, p' for $\sim p$ and p^* for $\sim \diamond p$. We shall refer to the system of strict implication as (the system) Σ .

TABLE I.
The System Σ .

Primitive Ideas	Postulates
$p, p', \diamond p, pq, p = q.$	11. 1 $pq \cdot \prec \cdot qp$
	11. 2 $pq \cdot \prec \cdot p$
Definitions	11. 3 $p \cdot \prec \cdot pp$
11. 01 $p + q \cdot = \cdot (p'q')'$.	11. 4 $(pq)r \cdot \prec \cdot p(qr)$
11. 02 $p \prec q \cdot = \cdot (pq)^*$	11. 5 $p \cdot \prec \cdot (p')'$.
11. 03 $p = q \cdot = \cdot : p \prec q \cdot q \prec p$	11. 6 $p \prec q \cdot q \prec r : \prec \cdot p \prec r$
	11. 7 $p \cdot p \prec q : \prec q$
	19. 01 $\diamond pq \cdot \prec \cdot \diamond p$
	20. 01 $(\exists p, q) : (p \prec q)' \cdot (p \prec q')'$.

It is also assumed that the system is closed with respect to the unary operations $p' \diamond p$ and the binary operation pq . The equality relation $=$ of the primitive ideas has the usual properties.§ In the present abstract treatment, 11. 03 may be looked upon as a condition upon the relation \prec .

† It is assumed that the reader is familiar with the contents of Chapters VI and VII of C. I. Lewis and C. H. Langford's book, *Symbolic Logic* (New York, 1932), where a detailed account is given both of the system of strict implication and the matrix method as applied to truth-value systems. We shall refer to this book as *Symbolic Logic*.

‡ *Symbolic Logic*, Appendix II.

§ As given, for example, in E. V. Huntington's paper, "Postulates for the algebra of logic," *Transactions of the American Mathematical Society*, vol. 35 (1933), pp. 279-280.

3°. THEOREM.† *The system Σ is a Boolean algebra in which $p + q$ and pq are the operations of addition and multiplication, and p' is the negation of p .*

The following set of postulates for a Boolean algebra is given by Huntington in his Transactions paper, page 280. We presuppose a class K of elements p, q, r, \dots a unary operation p' , a binary operation $+$ and an equality relation $=$ which we identify with the corresponding entities of Σ

$H_0[20.1, 20.11]$ *K contains at least two distinct elements.*

$H_1[11.01]$ *If p and q are in the class K , then $p + q$ is in the class K .*

$H_2[13.11]$ *$p + q = q + p$.*

$H_3[13.4]$ *$(p + q) + r = p + (q + r)$.*

$H_4[13.31]$ *$p + p = p$.*

$H_5[18.2]$ *$(p' + q')' + (p' + q)' = p$.*

Def. $H_6[11.01, 12.3]$ *$pq = (p'q')'$.*

The numbers in square brackets refer to the corresponding theorems in *Symbolic Logic*.

4°. THEOREM. *If the system of strict implication is interpreted as a truth-value system with a finite number of truth-values n_1, n_2, \dots, n_k , then n_1, n_2, \dots, n_k must form a Boolean algebra \mathfrak{B} with respect to the operations of addition, multiplication and negation derived from the matrices for $p + q$, pq and p' .*

For suppose that the matrices for p' and $p + q$ are

p	p'	p	q	n_1	n_2	\dots	n_k
n_1	β_1	n_1	α_{11}	α_{12}	\dots	\dots	α_{1k}
n_2	β_2	n_2	α_{21}	α_{22}	\dots	\dots	α_{2k}
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot	\dots	\cdot
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot	\dots	\cdot
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot	\dots	\cdot
n_k	β_k	n_k	α_{k1}	α_{k2}	\dots	\dots	α_{kk}

where each α and β stands for a definite truth-value n . We then define the operations of negation and addition over n_1, n_2, \dots, n_k by

$$n'_i = \beta_i, \quad n_i + n_j = \alpha_{ij} \quad (i, j = 1, \dots, k)$$

and it is immediately obvious that the conditions $H_0 - H_6$ of section 3° are all satisfied.

† For a detailed analysis of the correspondence between Σ and a Boolean algebra, see E. V. Huntington, *Bulletin of the American Mathematical Society*, vol. 40 (October, 1934), pp. 729-735.

COROLLARY. *The number of truth-values in any representation of Σ as a truth-value system is either infinite or a power of 2.*

Let us use the letters θ and ϵ to stand for designated values † and undesignated values in \mathfrak{B} respectively. Then θ and ϵ combine in \mathfrak{B} as follows:

TABLE II.
Combination of Truth-Values.

$+$	$\theta \quad \epsilon$	\times	$\theta \quad \epsilon$	$'$	$\theta \quad \epsilon$
ϵ	$\theta \quad \theta$	θ	$\theta \quad \epsilon$	θ	ϵ
θ	$\theta \quad \epsilon$	ϵ	$\epsilon \quad \epsilon$	ϵ	θ

For example, the second table tells us that the product of two designated values is a designated value, the product of a designated value and an undesignated value is an undesignated value, and so on.

These facts result from the obvious propositions of Σ

$$p \cdot q : \Leftarrow : p + q \cdot pq; \quad pq' : \Leftarrow : p + q' \cdot (p'q)'; \quad p \cdot \Leftarrow \cdot (p')'.$$

5°. We consider now the possible representations of Σ as a four-valued truth-value system. In accordance with the results of section 4°, we may take for the set of truth-values \mathfrak{B} the four numbers 1, 2, 3 and 6, which form a Boolean algebra if addition and multiplication are taken as the operations of finding the greatest common divisor and least common multiple, while negation is defined by $1' = 6$, $2' = 3$.

TABLE III.
Truth-Values of p' , p^* and so on.

p	p'	p^*	$p + p'$	pp'	pp'^*	$\triangleleft p$
1	6	a	1	6	d	a'
2	3	b	1	6	d	b'
3	2	c	1	6	d	c'
6	1	d	1	6	d	d'

There are in all $4^4 = 256$ such interpretations of Σ conceivable obtained by giving each of a , b , c , d , its four possible values 1, 2, 3, or 6. We shall use the definitions and postulates of Σ in Table I to reduce this number to eight.

From Table III, we see that ‡

$$(i) \quad d = \theta, \quad (ii) \quad 6 \neq \theta, \quad (iii) \quad 1 = \theta.$$

† *Symbolic Logic*, pp. 231-233.

‡ We use the letter “ θ ” to stand for some designated value. Thus $6 \neq \theta$ means that 6 is not a designated value, and ab , ac , $ad = \theta$ would mean that ab , ac , and ad are all designated values.

From the last theorem of 4° and (ii) we see that

$$(iv) \quad \text{if } 2 = \theta, 3 \neq \theta; \quad \text{if } 3 = \theta, 2 \neq \theta.$$

TABLE IV.
Matrices for pq , pq' and so on.

pq	pq'	$p \prec q$	$q \prec p$	$p = q$
1 2 3 6	6 3 2 1	$d c b a$	$d d d d$	d
2 2 6 6	6 6 2 2	$d d b b$	$c d c d$	$d c$
3 6 3 6	6 3 6 3	$d c d c$	$b b d d$	$a b$
6 6 6 6	6 6 6 6	$d d d d$	$a b c d$	$d a$

Now since equality over Σ is defined as logical equivalence,[†] $p = q$ when and only when p and q have the same truth-values. Therefore, we infer from the matrix for $p = q$ that $ad, bc, bd, cd \neq \theta$. Hence by (i) and Table II,

$$(v) \quad a, b, c \neq \theta.$$

From (v), (i) and (iii), we see that

$$(vi) \quad a, b, c \neq d$$

$$(vii) \quad a, b, c \neq 1.$$

TABLE V.
The Principle of the syllogism.

p	q	q'	$p \prec q$	$p \cdot p \prec q$	$p \cdot p \prec q : q' : 11.7 \cdot = \cdot (p \cdot p \prec q : q')^*$
1	1	6	d	d	6
1	2	3	c	c	$3c$
1	3	2	b	b	$2b$
1	6	1	a	a	a
2	1	6	d	$2d$	6
2	2	3	d	$2d$	6
2	3	2	b	$2b$	$2b$
2	6	1	b	$2b$	$2b$
3	1	6	d	$3d$	6
3	2	3	c	$3c$	$3c$
3	3	2	d	$3d$	6
3	6	1	c	$3c$	$3c$
6	1	6	d	6	6
6	2	3	d	6	6
6	3	2	d	6	6
6	6	1	d	6	6

[†] Lewis and Langford, pp. 123-124.

From the last column of Table V, we see that

$$(viii) \quad a^*, (2b)^*, (3c)^* = \theta.$$

I say that $a = 6$. For by (vii), $a \neq 1$. And if $a = 2$ or 3 , by (viii), $a^* = 2^*$ or $a^* = 3^*$. Hence $a^* = b$ or $c = \theta$ contradicting (v).

I say that $b = 3$ or $b = 6$. For by (vii), $b \neq 1$. And if $b = 2$, then by (viii), $(2b)^* = 2^* = b = 2 = \theta$ contradicting (v).

Finally, $c = 2$ or $c = 6$. For by (vii), $c \neq 1$. And if $c = 3$, then by (viii) $(3c)^* = 3^* = c = 3 = \theta$ contradicting (v).

We cannot have $b = 3$ and $c = 2$. For then $d = 1$ by (ii) and (v). Hence $\Diamond p \cdot = \cdot p'$ and Σ will degenerate into a system of material implication, contradicting 20.01.

We summarize our results in the following

THEOREM. *There are at most eight possible four-valued systems of strict implication, distinguished by the truth-values of $\Diamond p$; namely*

TABLE VI.
Possible Systems Σ .

p	$\Diamond p$	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1		1	1	1	1	1	1	1	1
2		1	1	2	2	1	1	1	1
3		3	3	1	1	1	1	1	1
6		6	2	6	3	6	6	3	2
Designated									
Values †		1, 3	1, 3	1, 2	1, 2	1, 2	1, 2	1, 2	1, 3

These systems may be grouped into four pairs, (7) and (8); (1) and (3); (5) and (6); (2) and (4); which are permuted into one another by the interchange of the truth-values 2 and 3, and are hence not essentially distinct. Finally, the four pairs are immediately seen to agree with the systems called Group I, Group II, Group III and Group V, in Appendix II of *Symbolic Logic*.

I have verified that the first three pairs satisfy all the postulates of Σ , while the last pair satisfy all the postulates save 19.01, as was first proved by W. T. Parry, M. Wajsberg and P. Henle.‡ I shall denote these three systems of strict implication by Σ_1 , Σ_2 , Σ_3 .

† Obtained by (i), (ii) and (iv).

‡ *Symbolic Logic*, footnote, page 492.

6° . It remains to show that there is no representation of Σ as a truth-value system of finite order \dagger essentially distinct from Σ_1 , Σ_2 and Σ_3 .

Suppose that a representation of Σ as a truth-value system maps Σ upon a Boolean algebra \mathfrak{B}_N of order 2^N , $N \geq 3$ such that all the postulates of Σ are satisfied in accordance with the matrix method.

Let N generating elements of the algebra \mathfrak{B}_N be $\alpha_1, \alpha_2, \dots, \alpha_N$. Since $N \geq 3$, we see from Table II that there are at least two generators which are both designated values, or at least two generators which are undesignated values. With a proper choice of notation, we may assume that α_1, α_2 are such a pair.

Now every element v of the algebra \mathfrak{B}_N may be uniquely represented in the form

$$(1) \quad v = \alpha_1^{e_1} \alpha_2^{e_2} \cdots \alpha_N^{e_N}$$

where the exponents e are either zero or one, and by convention, the universal element of \mathfrak{B}_N is denoted by 1, $\alpha^0 = 1$.

Consider now the effect of equating α_1 and α_2 . An inspection of Table II and (1) shows us that this operation does not convert any designated value into an undesignated value, or vice versa. Hence the truth-value table establishing the validity of any one of our postulates for Σ in \mathfrak{B}_N , is unaffected by the operation. \ddagger

This operation, however, throws \mathfrak{B}_N into a Boolean algebra \mathfrak{B}_{N-1} of order 2^{N-1} on which Σ is, therefore, mapped. On repeating this process $N - 2$ times, we obtain a mapping upon the Boolean algebra \mathfrak{B}_2 . On retracing our steps from \mathfrak{B}_2 to \mathfrak{B}_3 to \mathfrak{B}_4 and so on to \mathfrak{B}_N , we see that we have a multiple isomorphism between \mathfrak{B}_N and \mathfrak{B}_2 which preserves the assertion values of all the postulates for Σ . Hence, the mapping on \mathfrak{B}_N is not essentially distinct from one of the three possible mappings on \mathfrak{B}_2 .

INSTITUTE FOR ADVANCED STUDY.

\dagger The question of whether representations of Σ as a truth-value system of infinite order exist is left open.

\ddagger The reader may find it helpful to glance back at Table V. In the mapping over \mathfrak{B}_N , 1, 2, 3, 6, will be replaced by the 2^N elements of \mathfrak{B}_N . However, the elements on the extreme right of Table V which are all designated values of \mathfrak{B}_N , will remain designated values after equating α_1 and α_2 .

CONDITIONS FOR FACTORIZATION IN A SET CLOSED UNDER A SINGLE OPERATION

BY MORGAN WARD

(Received October 20, 1934)

1°. Consider a system S consisting of a set of elements a, b, c, \dots over which an equality relation and a binary operation multiplication have been defined satisfying the following four conditions.

P 1 *To every pair of elements a, b of S there corresponds an element c of S unique to within equal elements.* We write $c = ab$.

P 2 *If $a = a'$ and $b = b'$ then $ab = ab' = a'b = a'b'$.*

P 3 $a(bc) = (ab)c$ for all a, b, c in S .

P 4 $ab = ba$ for all a, b in S .

Recently A. H. Clifford¹ and others have considered the following problem: to determine what additional conditions it is necessary to impose on S in order that each integral element in it may be uniquely resolved into a product of powers of irreducible elements (up to unit factors) as in the case when S is the set of positive integers and the operation ordinary multiplication.²

I propose to show here that we can discard the requirement of *unicity* in the resolution into prime factors and still retain many of the essential features of common arithmetic. The set of conditions which I shall develop will assign to each integral element a certain canonical decomposition into prime factors to which it is equivalent. If we know this canonical decomposition, we know all divisors of the element and the canonical decomposition of each divisor. Any two elements of the system will have a least common multiple, and if they have any common divisors, a greatest common divisor. On the other hand, we cannot obtain the canonical decomposition of a product from a knowledge of the canonical decompositions of its factors, nor need irreducible elements be primes.³

We shall show that our system includes as special instances the arithmetics previously discussed by J. Koenig,⁴ Clifford,¹ Fritz Klein⁵ and others.

2°. We must first lay down a few definitions. a is said to divide b either if

¹ Bulletin Am. Math. Soc. 40 (1934), pp. 326-330. We shall refer to this paper as Clifford.

² We refer to this case hereafter as common arithmetic.

³ An element of S is called a prime if it cannot divide the product of two elements of S without dividing at least one factor.

⁴ *Algebraischen Größen*, Leipzig (1903), Chapters 1, 4.

⁵ Math. Annalen 106 (1932), pp. 114-130; Math. Zeitschr. 37 (1933), pp. 39-60.

$a = b$ or if there exists an element c such that $ac = b$. We write then $a | b$. We observe that

- (1) If $a_i | b_i$, ($i = 1, \dots, k$), then $a_1 \dots a_k | b_1 \dots b_k$.
- (1) is untrue if multiplication is not commutative.

If $a | b$ and $b | a$, a and b are said to be associate, written $a \sim b$. Non-associate elements are said to be distinct. If $a | x$ for every x in S , a is called a unit. Non-units are called integral elements. A divisor of an element is called proper if it is neither a unit nor an associate. Units have no proper divisors. An integral element with no proper divisors is called an irreducible. An element with only one distinct irreducible divisor is called a power of that divisor. The number of distinct proper divisors of a power increased by unity is called its multiplicity. We write $p^{(n)}$ for a power of the irreducible p of finite multiplicity n . Thus $p^{(1)} \sim p$.

An element a of S is called indecomposable if in every decomposition of a into a product of two or more factors, one of the factors is associate to a . An irreducible is necessarily indecomposable. To avoid trivialities, we shall assume

P 5 *S contains at least one integral element.*

We shall call a system which satisfies the five postulates P 1 – P 5 a band.⁶

3°. The next four postulates complete our definition of S .

P 6 *Every element of S has only a finite number of distinct divisors.*

P 7 *Two powers of the same irreducible are either equivalent or else one divides the other.*

P 8 *If an element of S is divisible by two distinct irreducibles, it is decomposable.*

P 9 *If an element of S is divisible by a number of other elements each of which is a power of a different distinct irreducible, then it is divisible by their product.*

We shall call any system satisfying all nine of our postulates an abstract arithmetic. The simplest such systems are common arithmetic with our operation interpreted either as addition, multiplication or the operation of finding a least common multiple of two or more integers.

All of our postulates save P 5 and P 9 are used by Fritz Klein in defining his “B-Menge.”⁷ But P 9 is also true in a B-Menge since multiplication there is idempotent. *Therefore every B-Menge containing integral elements is an abstract arithmetic.*

J. Koenig⁸ and A. H. Clifford define a power of p of multiplicity n as $p \cdot p \dots p$ to n factors. But since factorization is unique in both systems, a power of p in their sense will be a power of p in our sense, and P 7 and P 9 will be both satisfied in each system. P 6 is a postulate in Koenig's system, and P 8 is satisfied because Koenig's system is a semi-group. In Clifford's system P 6 is replaced by the weaker “Teilerketten” condition, but it is true by virtue

⁶ This convenient term was suggested by Dr. A. H. Clifford.

⁷ Math. Zeitschr., place cited, especially pp. 47–54.

⁸ J. Koenig's system is identical with F. Klein's “A-Menge.” (Math. Zeitschr., volume cited, pp. 42–47.)

of the unique factorization. P 8 obviously holds since no indecomposables save units appear in Clifford's system. Hence: *A band satisfying the Clifford conditions for unique decomposition⁹ is an abstract arithmetic. A commutative semigroup¹⁰ in which P 6 holds and in which all irreducibles are primes is an abstract arithmetic.*

4°. It follows from P 5 and P 6 that S contains at least one irreducible, and that every integral element has at least one irreducible divisor. Furthermore, every power is of finite multiplicity, and from P 7 it readily follows that the m distinct divisors of $p^{(m)}$ are equivalent to $p^{(1)}, p^{(2)}, \dots, p^{(m)}$. Furthermore, $p^{(n)} | p^{(m)}$ when and only when $n \leq m$.

Consider now any integral element a of S . If a is a power, it is uniquely representable in the form $a \sim p^{(n)}$. In the contrary case, we deduce from P 8, P 6 and P 7 that a decomposition of a exists of the form

$$(2) \quad a \sim p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)}$$

where p_1, p_2, \dots, p_k are distinct irreducibles.

In discussing such decompositions, it is convenient to allow powers to have the superscript zero, with the understanding that such a power is to be omitted from the decomposition.¹¹ Thus, for example, $a \sim p_1^{(2)} p_2^{(4)} p_3^{(0)} p_4^{(0)} \sim p_1^{(0)} p_2^{(0)} p_3^{(1)} p_4^{(1)}$ is to be taken merely as another way of writing $a \sim p_1^{(2)} p_2^{(4)} \sim p_3^{(1)} p_4^{(1)}$.

With this understanding, let p_1, p_2, \dots, p_k now stand for all the distinct irreducibles of S which divide a . These are finite in number by P 6. Suppose that a has in all s distinct decompositions of the form (2),

$$(3) \quad a \sim p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)} \sim p_1^{(\beta_1)} p_2^{(\beta_2)} \cdots p_k^{(\beta_k)} \sim \cdots \sim p_1^{(\lambda_1)} p_2^{(\lambda_2)} \cdots p_k^{(\lambda_k)}$$

when the superscripts $\alpha, \beta, \dots, \lambda$ are now positive integers or zero. The number s of such sets is finite by P 6, since $p^{(n)}$ and $p^{(m)}$ are distinct if $n \neq m$.

Let $\mu_i = \max (\alpha_i, \beta_i, \dots, \lambda_i)$, $(i = 1, \dots, k)$.

Then $p_i^{(\mu_i)} | a$. Hence by P 9, $p_1^{(\mu_1)} \cdots p_k^{(\mu_k)} | a$. But $p_i^{(\alpha_i)} | p_i^{(\mu_i)}$, $(i = 1, \dots, k)$. Therefore, by (1),

$$p_1^{(\alpha_1)} p_2^{(\alpha_2)} \cdots p_k^{(\alpha_k)} | p_1^{(\mu_1)} p_2^{(\mu_2)} \cdots p_k^{(\mu_k)}.$$

Hence

$$(4) \quad a \sim p_1^{(\mu_1)} p_2^{(\mu_2)} \cdots p_k^{(\mu_k)}.$$

⁹ Clifford, p. 328, Theorem 1.

¹⁰ This system is merely a band with the additional condition that $ab = ac$ when and only when $b = c$.

¹¹ If S contains units, we would define $p^{(0)}$ as an associate to a unit. The simplification resulting from adjoining a unit or an identity element to the abstract system is lost in the applications to ring theory where the ring need contain no units, and the additive properties of the adjoined elements must be considered.

Thus the decomposition (4) appears among the set (3). We shall call it the canonical decomposition of a .

5°. If $b \sim q_1^{(\nu_1)} q_2^{(\nu_2)} \cdots q_s^{(\nu_s)}$, it is clear that necessary and sufficient conditions that $b | a$ are that every q be a p and that the multiplicity of each $q^{(\nu)}$ be less than or equal to the multiplicity of the corresponding $p^{(\mu)}$. Hence the divisors of a are given by the set of elements $p_1^{(n_1)} p_2^{(n_2)} \cdots p_k^{(n_k)}$, ($n_i = 0, 1, \dots, \mu_i; i = 1, \dots, k$).

Given two integral elements c and d , let s_1, s_2, \dots, s_m be the distinct irreducible elements dividing either or both of them. With the convention adopted in section 4°, we may write their canonical decompositions in the form

$$c \sim s_1^{(\gamma_1)} \cdots s_m^{(\gamma_m)}, \quad d \sim s_1^{(\delta_1)} \cdots s_m^{(\delta_m)}.$$

Then if $\theta_i = \max(\gamma_i, \delta_i)$, $\xi_i = \min(\gamma_i, \delta_i)$, ($i = 1, \dots, k$) it is clear that

$$[c, d] \sim s_1^{(\theta_1)} \cdots s_m^{(\theta_m)}, \quad (c, d) \sim s_1^{(\xi_1)} \cdots s_m^{(\xi_m)}$$

are the least common multiple and greatest common divisor of c and d in the sense of common arithmetic. Moreover $c \sim [s_1^{(\gamma_1)}, s_2^{(\gamma_2)}, \dots, s_m^{(\gamma_m)}]$.

If we assume that S contains a unit, so that c and d will always have a common divisor, it is easily verified that the operations $[x, y]$ and (x, y) just defined satisfy Klein's postulates for a "Sternverband."¹² Hence even if we do not have unique decomposition with respect to multiplication, we always have unique decomposition with respect to the least common multiple operation.

THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

¹² Annalen paper already cited.

ON THE FACTORIZATION OF POLYNOMIALS TO A PRIME MODULUS

BY MORGAN WARD

(Received December 4, 1934)

1. Let

$$A(x) = x^N - a_1x^{N-1} - a_2x^{N-2} - \cdots - a_N$$

be a polynomial in x with rational integral coefficients¹ and N distinct roots, $\alpha_1, \alpha_2, \dots, \alpha_N$ and let p be a prime which does not divide its discriminant. Then we have a unique factorization modulo p :

$$(1.1) \quad A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod{p}$$

where the polynomials $A_i(x)$ are all distinct, and all irreducible modulo p . I give here two formulas connecting the degrees of the polynomials $A_i(x)$ with the powers of p dividing certain of the numbers

$$(1.2) \quad \Delta_{(n)}(A) = \prod_{v=1}^N (\alpha_v^{p^n} - \alpha_v) = \text{Res}\{x^{p^n} - x, A(x)\}, n \text{ a positive integer.}$$

These numbers have been studied recently by D. H. Lehmer in another connection.²

2. Let \mathfrak{A} denote the residue class of all polynomials of degree N which are congruent to $A(x)$ modulo p , and consider for each polynomial $A'(x)$ of \mathfrak{A} the highest power of p which divides $\Delta_{(n)}(A') = \text{Res}\{x^{p^n} - x, A'(x)\}$. For a given value of n , this power is either zero for every such polynomial, or else a positive integer, which may be thought of as arbitrarily large if the resultant happens to vanish. If the power is not zero there clearly exist polynomials of \mathfrak{A} for which it assumes a minimum value. We denote this minimum by p^{q_M} , so that we shall have for some polynomial $A'(x)$ of degree N ,

$$\Delta_{(n)}(A') = p^{q_M}w, \quad (p, w) = 1, \quad A'(x) \equiv A(x) \pmod{p},$$

while if $A''(x)$ is any other polynomial of degree N and congruent to $A(x)$ modulo p ,

$$(2.1) \quad \Delta_{(n)}(A'') \equiv 0 \pmod{p^{q_M}}.$$

¹ This restriction will be understood in all that follows.

² These Annals, vol. 34, July 1933, pp. 461-479. The notation $\Delta_{(n)}(A)$ in place of the more natural $\Delta_{p^n}(A)$ is used for typographical reasons. With Lehmer's notation our $\Delta_{(n)}(A)$ would be written $(-1)^{N+1}a^N\Delta_{p^n-1}(A)$.

THEOREM 1. *The number T_M of irreducible factors $A_i(x)$ of $A(x)$ modulo p of degree M is given by the formula*

$$(2.2) \quad T_M = \frac{1}{M} \sum_{d|M} \mu(d) q_{M/d}.$$

THEOREM 2. *If p^{u_n} is the highest power of p dividing $\Delta_{(n)}(A)$, then $A(x)$ has an irreducible factor of degree M modulo p when and only when the integer*

$$(2.3) \quad s_M = \sum_{d|M} \mu(d) u_{M/d}$$

is positive.

In both theorems, $\mu(d)$ is Möbius' function, and the summation extends over all the divisors d of M .

3. As an illustration, consider the algebraically irreducible polynomial $A(x) = x^5 - 2x^3 + x^2 + 2x + 2$ for the case $p = 5$. We find by direct computation that the discriminant of $A(x)$ is congruent to 2 modulo 5, while $\Delta_{(1)}(A) \equiv 4$ modulo 5, $\Delta_{(2)}(A) \equiv 75$ modulo 125. Hence $r_1 = q_1 = 0$, $r_2 = q_2 = 2$, $T_1 = 0$, $T_2 = 1$, so that $A(x)$ has an irreducible quadratic factor (modulo 5), and no linear factors. Hence $A(x)$ must be the product of an irreducible cubic and an irreducible quadratic, (modulo 5). As a matter of fact

$$A(x) \equiv (x^2 + 2)(x^3 + x + 1) \pmod{5}.$$

4. In order to prove theorems 1 and 2, we need a chain of lemmas some of which are familiar (for example lemmas 4 and 5), while others contain results of a certain arithmetical interest in themselves. In any event, none of the proofs offer any difficulties, and they are accordingly omitted here.

Let $F(x)$ be any polynomial, and p any prime such that $F(x) \not\equiv 0 \pmod{p}$. Denote by τ , if it exists, the least positive value of n such that

$$(4.1) \quad x^{p^n} \equiv x \pmod{p, F(x)}.$$

LEMMA 1. $x^{p^n} \equiv x \pmod{p, F(x)}$ when and only when n is divisible by τ .

LEMMA 2. If $x^{p^\tau} \equiv x \pmod{p, F(x)}$ and $x^{p^\tau} - x$ is not exactly divisible by $F(x)$, so that there exists a positive integer s such that

$$x^{p^\tau} \equiv x \pmod{p^s, F(x)}, \quad x^{p^\tau} \not\equiv x \pmod{p^{s+1}, F(x)},$$

then if q is any positive integer,

$$x^{p^{q\tau}} \equiv x \pmod{p^s, F(x)}, \quad x^{p^{q\tau}} \not\equiv x \pmod{p^{s+1}, F(x)}.$$

LEMMA 3. There exists no value of n for which

$$x^{p^n} \equiv x \pmod{p, F^2(x)}.$$

COROLLARY 3.1. If the polynomial $F(x)$ has a squared factor, (4.1) is impossible for any positive n , and any prime p .

COROLLARY 3.2. If the prime p divides the discriminant of $F(x)$, (4.1) is impossible for any positive n .

LEMMA 4. If $F(x)$ is irreducible, modulo p , and if

$$\Delta_{(n)} = \Delta_{(n)}(F) = \text{Res} \{x^{pn} - x, F(x)\},$$

then $\Delta_{(n)} \equiv 0 \pmod{p}$ when and only when $x^{pn} - x \equiv 0 \pmod{p, F(x)}$.

LEMMA 5. If $F(x)$ is an irreducible polynomial modulo p of degree M , then the least positive value of n for which (4.1) is satisfied is M .

LEMMA 6. If $F(x)$ is an irreducible polynomial modulo p of degree M , and if k is such that

$$x^{pk} \equiv x \pmod{p^2, F(x)},$$

then one can find an indefinite number of polynomials $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{pk} \equiv x \pmod{p, F'(x)}, \quad x^{pk} \not\equiv x \pmod{p^2, F'(x)}.$$

LEMMA 7. If $F(x)$ is an irreducible polynomial modulo p of degree M , so that by lemma 5,

$$x^{pM} \equiv x \pmod{p, F(x)},$$

and if R is any assigned positive integer, it is possible to find a polynomial $F'(x)$ of degree M and congruent to $F(x)$ modulo p such that

$$x^{pM} \equiv x \pmod{p^R, F'(x)}, \quad x^{pM} \not\equiv x \pmod{p^{R+1}, F'(x)}.$$

LEMMA 8. If $F(x)$ is an irreducible polynomial modulo p of degree M and if

$$x^{pk} \equiv x \pmod{p^R, F(x)}, \quad x^{pk} \not\equiv x \pmod{p^{R+1}, F(x)},$$

then

$$\Delta_{(k)}(F) \equiv 0 \pmod{p^{RM}}, \quad \Delta_{(k)}(F) \not\equiv 0 \pmod{p^{RM+1}}.$$

LEMMA 9. If $F(x)$ is a polynomial with no repeated roots, and if p is a prime which does not divide its discriminant, there exist positive values of n for which the congruence (4.1) holds.

5. Let us return now to the congruence (1.1):

$$A(x) \equiv A_1(x)A_2(x) \cdots A_r(x) \pmod{p}.$$

By lemmas 6, 2 and 8, we can choose each $A_i(x)$ so that if $\Delta_{(M)}(A_i) = \text{Res} \{x^{pM} - x, A_i(x)\}$ is divisible by p , it is divisible by p^{d_i} and no higher power of p , where d_i is the degree of $A_i(x)$, and by lemmas 2, 5, and 8, $\Delta_{(M)}(A_i)$ is divisible by p when and only when d_i divides M . We may write therefore

$$\Delta_{(M)}(A_i) = p^{q_{Mi}} w_i, \quad (p, w_i) = 1, \quad (i = 1, 2, \dots, r)$$

where

$$(5.1) \quad q_{Mi} = d_i \quad \text{if } d_i \text{ divides } M; \quad q_{Mi} = 0 \quad \text{otherwise.}$$

Let the $A_i(x)$ be chosen in this manner, and let

$$A_1(x)A_2(x) \cdots A_r(x) = \bar{A}(x).$$

Then $A(x) \equiv \bar{A}(x) \pmod{p}$, and the highest power of p dividing $\Delta_{(M)}(\bar{A})$ is

$$(5.2) \quad q_M = q_{M_1} + q_{M_2} + \cdots + q_{M_r}.$$

For

$$\begin{aligned} \Delta_{(M)}(\bar{A}) &= \text{Res } \{x^{p^M} - x, \bar{A}(x)\} = \prod_{i=1}^r \text{Res}_{i=1}^r \{x^{p^M} - x, A_i(x)\} = \\ &\qquad\qquad\qquad \Delta_{(M)}(A_1) \cdots \Delta_{(M)}(A_r). \end{aligned}$$

I say that p^{q_M} is the minimal power of p dividing $\Delta_{(M)}(A')$ for all polynomials $A'(x)$ of degree N which are congruent to $A(x)$ modulo p .

For given any such polynomial, and any positive integer L , by Schönemann's second theorem,³ there exists a decomposition of $A'(x)$ modulo p^L of the form

$$A'(x) \equiv A'_1(x)A'_2(x) \cdots A'_r(x) \pmod{p^L}$$

where $A'_i(x)$ is congruent to $A_i(x)$ modulo p , and of the same degree in x . Therefore,

$$\Delta_{(M)}(A') \equiv \Delta_{(M)}(A'_1) \cdots \Delta_{(M)}(A'_r) \pmod{p^L}.$$

If u_{M_i} is the highest power of p dividing $\Delta_{(M)}(A'_i)$, we infer that the highest power of p dividing $\Delta_{(M)}(A')$ is

$$u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r},$$

for the integer L may be chosen arbitrarily large. Since $A'_i(x)$ is congruent to $A_i(x)$ and of the same degree, $u_{M_i} \geq q_{M_i}$ so that $u_M \geq q_M$.

Let T_d denote the total number of irreducible factors of $A(x)$ of degree d . Then by (5.1), (5.2) may be written

$$(5.3) \quad q_M = \sum_{d|M} dT_d.$$

Our first theorem now follows immediately by applying Dedekind's inversion formula to (5.3).⁴

6. To prove our second theorem, we construct a Schönemann decomposition of $A(x)$ itself modulo p^L similar to that of $A'(x)$ in section 5, obtaining successively

$$A(x) \equiv A''_1(x)A''_2(x) \cdots A''_r(x) \pmod{p^L},$$

$$\Delta_{(M)}(A) \equiv \Delta_M(A''_1)\Delta_M(A''_2) \cdots \Delta_M(A''_r) \pmod{p^L},$$

$$(6.1) \quad u_M = u_{M_1} + u_{M_2} + \cdots + u_{M_r},$$

³ Fricke, *Algebra*, vol. III, Braunschweig (1928), p. 67.

⁴ Landau, *Vorlesungen über Zahlentheorie*, vol. I, Leipzig (1927), p. 22.

where $A''_i(x)$ is congruent to $A_i(x)$ modulo p , and of the same degree, and u_M is now the highest power of p dividing $\Delta_M(A'')$.

By lemma 2, u_M is zero unless the degree of $A''_i(x)$ —that is, the degree of $A_i(x)$ —divides M . We may write then

$$u_M = S_M + S'_M$$

where S_M is the contribution to the right side of (6.1) of all those irreducible factors $A''_i(x)$ of $A(x)$ modulo p^L of degree M , and S'_M the contribution of all the factors whose degrees are proper divisors of M . Thus S_M is different from zero when and only when $A(x)$ has at least one irreducible factor of degree M . From lemma 2, it is clear that

$$(6.2) \quad u_M = \sum_{d|M} s_d.$$

On applying Dedekind's inversion formula to (6.2), we obtain our second theorem.

7. If the factorization of $A(x)$ modulo p is known, q_M may be calculated by (5.3), and the minimal property of q_M gives us the congruence

$$\Delta_{(M)}(A) \equiv 0 \pmod{p^{q_M}}$$

In particular, if q_M is zero, $\Delta_{(M)}(A)$ is not divisible by p . We give in conclusion a formula for $\Delta_n(A) = \text{Res}\{x^n - x, A(x)\}$ which is useful in numerical applications; namely

$$\Delta_n(A) = \begin{vmatrix} W_n - W_0, & W_{n+1} - W_1, & \cdots & W_{n+N-1} - W_{N-1}, \\ W_{n+1} - W_1, & W_{n+2} - W_2, & \cdots & W_{n+N} - W_N, \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ W_{n+N-1} - W_{N-1}, & W_{n+N} - W_N, & \cdots & W_{n+2N-2} - W_{2N-2}, \end{vmatrix}.$$

Here (W) is that solution of the difference equation

$$\Omega_{n+N} = a_1\Omega_{n+N-1} - a_2\Omega_{n+N-2} - \cdots - a_N\Omega_n$$

associated with the polynomial $A(x)$ with the initial values $W_0 = 0$,

$$W_1 = 0, \quad W_2 = 0, \dots, W_{N-2} = 0, \quad W_{N-1} = 1.$$

The essential points in the proof of this formula will be found in a paper of mine in the Transactions of the American Mathematical Society.⁵

CALIFORNIA INSTITUTE OF TECHNOLOGY.

⁵ Vol. 35, July (1933), page 608. The element in the lower right hand corner of the determinant $\Delta(U)$ given there should read u_{2k-2} instead of u_{2k-1} , and similarly for the determinant on page 604.

THE DIOPHANTINE EQUATION $X^2 - DY^2 = Z^M$ *

BY
MORGAN WARD

I. INTRODUCTION

It has been known since the time of Euler and Lagrange† that solutions of the diophantine equation

$$(1.1) \quad X^2 - DY^2 = Z^M$$

may be obtained by setting

$$X + D^{1/2}Y = (a + D^{1/2}b)^M, \quad Z = a^2 - Db^2,$$

where a and b are any rational integers. In 1891, Pepin‡ claimed to prove that if M is odd, and prime to the class-number of the quadratic field $\mathfrak{K}(D^{1/2})$ while a and b are co-prime, *all* solutions of (1.1) in which X , Y and Z have no common factor—for short, “primitive” solutions of (1.1)—are given by the formulas above. Later, Pepin§ recognized that Z must be restricted to be odd, while Landau|| has pointed out (for a special case of (1.1)) that if D is positive, the units of the quadratic field $\mathfrak{K}(D^{1/2})$ must be taken into account.

Consider for example the equation $X^2 - 5Y^2 = Z^3$ to which Pepin’s procedure should apply, since M is odd and the class-number of $\mathfrak{K}(5^{1/2})$ is unity. This equation has the primitive solution $X = 2$, $Y = 1$, $Z = -1$. It should therefore be possible to choose rational integers a and b such that

$$2 + 5^{1/2} = (a + 5^{1/2}b)^3, \quad -1 = a^2 - 5b^2.$$

From the second equation, $a + 5^{1/2}b$ is a unit of $\mathfrak{K}(5^{1/2})$ and hence some power of the fundamental unit η multiplied by plus or minus one. But since the fundamental unit is $2 + 5^{1/2}$, the first equation would imply that $2 + 5^{1/2}$ is a root of unity. To obtain this particular solution, it would suffice to multiply $(a + 5^{1/2}b)^3$ by η^{-2} . But it is not at all obvious that such a device will always prove successful.

In the second part of the paper I utilize the theory of ideals to obtain explicit formulas for all the primitive solutions of (1.1) under the restrictions given below.

* Presented to the Society, December 2, 1933; received by the editors December 26, 1933.

† Dickson’s *History*, vol. II, chapter XX.

‡ Memorie della Pontificia Accademia dei Nuovi Lincei, vol. 8 (1891), pp. 41–42.

§ Annales de la Société Scientifique de Bruxelles, vol. 27 (1909), pp. 121–170.

|| L’*Intermédiaire des Mathématiciens*, vol. 8 (1901), pp. 145–147.

FUNDAMENTAL THEOREM. Let D be square-free, not equal to -3 or -1 ,* and incongruent to 1 modulo 8 , and let M be any positive integer greater than one, and prime to the class-number h of the quadratic field $\mathfrak{K}(D^{1/2})$, but not necessarily odd.

Let a and b be rational integers such that $(a, Db) = 1$, and of opposite parity unless the contrary is expressly stated. Define A_M and B_M by

$$(1.2) \quad (a + bD^{1/2})^M = A_M + D^{1/2}B_M.$$

Let $1, \omega$ be the canonical basis of the field $\mathfrak{K}(D^{1/2})$, and if D is positive, let

$$(1.3) \quad \eta = r + \omega s$$

be the fundamental unit of the field. Define U_T and V_T ($T = 0, 1, \dots, M$) by

$$U_T + D^{1/2}V_T = \eta^T, \quad D \equiv 2, 3 \pmod{4} \text{ or } D \equiv 5 \pmod{8}, \quad h \equiv 0 \pmod{3};$$

$$U_T + D^{1/2}V_T = 2\eta^T, \quad D \equiv 5 \pmod{8}, \quad h \not\equiv 0 \pmod{3}.$$

Then all primitive solutions, and only primitive solutions, of the diophantine equation

$$(1.1) \quad X^2 - DY^2 = Z^M$$

are given by the following formulas.

(I) D negative.

$$X = \pm A_M, \quad Y = \pm B_M, \quad Z = \pm (a^2 - Db^2).$$

(II) D positive and either congruent to $2, 3 \pmod{4}$ or congruent to $5 \pmod{8}$ with $h \equiv 0 \pmod{3}$.

$$X = \pm (A_M U_T + DB_M V_T), \quad Y = \pm (A_M V_T + B_M U_T), \quad Z = \pm (a^2 - Db^2) \\ (T = 0, 1, \dots, M-1).$$

(III) D positive, congruent to $5 \pmod{8}$, $h \not\equiv 0 \pmod{3}$.

$$2X = \pm (A_M U_{3T} + DB_M V_{3T}), \quad 2Y = \pm (A_M V_{3T} + B_M U_{3T}), \quad Z = \pm (a^2 - Db^2) \\ (T = 0, 1, \dots, [(M-1)/3]).$$

$$2^{M+1}X = \pm (A_M U_T + DB_M V_T), \quad 2^{M+1}Y = \pm (A_M V_T + B_M U_T), \quad 4Z = a^2 - DB^2,$$

$$a, b \text{ both odd. } M + T \equiv 0 \pmod{3} \text{ if } \frac{a+b}{2} + r \equiv 0 \pmod{2}, \text{ and}$$

$$M - T \equiv 0 \pmod{3} \text{ if } \frac{a+b}{2} + r \equiv 1 \pmod{2}$$

$$(T = 0, 1, \dots, M-1).$$

* The solutions in the cases $D = -1$ or $D = -3$ are well known.

If $M = 2$, we have in addition

$$2^M X = \pm (A_M U_T + DB_M V_T), \quad 2^M Y = \pm (A_M V_T + B_M U_T), \quad 2Z = a^2 - Db^2,$$

a, b both odd, $T = 0$ or 1 .

In the final part of the paper, these formulas are applied to discuss several allied diophantine equations; notably $X^2 + D = Z^M$, $1 + DY^2 = Z^M$, $X^{2N} - DY^{2N} = Z^N$.

II. THE PRIMITIVE SOLUTIONS OF $X^2 - DY^2 = Z^M$

1. Let D be a square-free integer not equal to -1 or -3 and incongruent to 1 modulo 8 , and let M be an integer ≥ 2 and prime to the class-number of the quadratic field $\mathfrak{K} = \mathfrak{K}(D^{1/2})$. A solution $X = A$, $Y = B$, $Z = C$ of the diophantine equation

$$(1.1) \quad X^2 - DY^2 = Z^M$$

will be said to be primitive if A, B, C are rational integers with no common factor save unity. For brevity, we shall speak of “the solution A, B, C .”

We shall adhere to the notations of Landau's *Vorlesungen*; italic letters are reserved for rational integers, small Greek letters for integers of the field \mathfrak{K} , and small German letters for ideals of \mathfrak{K} . A square bracket enclosing a Greek letter denotes the corresponding principal ideal; thus $[\alpha], [\beta], \dots$. Round parentheses enclosing two or more letters denote greatest common divisors, (a, b) , (α, β) , \dots ; enclosing a single letter, they denote that it is to be used as a modulus. The conjugate of a number α of \mathfrak{K} is denoted by $\bar{\alpha}$.

The following three lemmas are easily proved.

LEMMA 1.1. *If A, B, C is a primitive solution of the diophantine equation (1.1), then both A, B, C and A, D, C are relatively prime in pairs.*

LEMMA 1.2. *If A, B, C is a primitive solution of the diophantine equation (1.1), then (i) if $M \geq 3$, C must be odd unless $D \equiv 1 \pmod{8}$; (ii) if $M = 2$, C must be odd unless $D \equiv 1$ or $5 \pmod{8}$. In the latter case, if C is even, $C/2$ must be odd.*

LEMMA 1.3. *If M is prime to the class-number of the algebraic field \mathfrak{K} , and if α is any ideal of \mathfrak{K} , then if α^M is a principal ideal, α is a principal ideal.*

LEMMA 1.4. *If A, B, C is a primitive solution of the diophantine equation (1.1) and if C is odd, then the principal ideals $[A + D^{1/2}B]$ and $[A - D^{1/2}B]$ of the quadratic field \mathfrak{K} are co-prime.*

For otherwise, there exists a prime ideal \mathfrak{p} of \mathfrak{K} such that

$$[A + D^{1/2}B] \equiv 0 \pmod{\mathfrak{p}}, \quad [A - D^{1/2}B] \equiv 0 \pmod{\mathfrak{p}}.$$

Then $[C^M] = [A + D^{1/2}B][A - D^{1/2}B] \equiv 0 \pmod{\mathfrak{p}}$, so that

$C \equiv 0 \pmod{p}$, and $([2], p) = 1$ since C is odd.

Since p contains both $A + D^{1/2}B$ and $A - D^{1/2}B$, it contains their sum $2A$ and hence A itself. Therefore the rational prime which p divides divides both A and C contrary to Lemma 1.1.

LEMMA 1.5. *If D is congruent to 5 modulo 8, and if $1, \omega$ is the canonical basis for the integers of the field \mathfrak{R} , and if $(c+\omega d)^M = c' + \omega d'$, where c and d are rational integers, then if M is prime to three, d' is even when and only when d is even. If M is divisible by three, d' is always even.*

For $5 \equiv D = (2\omega + 1)^2 \equiv 4\omega^2 + 4\omega + 1 \pmod{8}$, so that

$$\omega^2 \equiv \omega + 1 \pmod{2}.$$

If d is even, d' is obviously even for any value of M . If d is odd, we have either $c + \omega d \equiv 1 + \omega \pmod{2}$ or $c + \omega d \equiv \omega \pmod{2}$. In the first case, $(c + \omega d)^2 \equiv \omega^2 + 1 \equiv \omega \pmod{2}$, $(c + \omega d)^3 \equiv \omega^2 + \omega \equiv 1 \pmod{2}$, $(c + \omega d)^4 \equiv c + \omega d \pmod{2}$. In the second case, $(c + \omega d)^2 \equiv \omega^2 \equiv 1 + \omega \pmod{2}$, $(c + \omega d)^3 \equiv \omega^2 + \omega \equiv 1 \pmod{2}$, $(c + \omega d)^4 \equiv c + \omega d \pmod{2}$. Hence in either case, if $M \equiv N \pmod{3}$, $N = 0, 1$ or 2 , $(c + \omega d)^M \equiv (c + \omega d)^N \pmod{2}$, from which the rest of the lemma easily follows.

LEMMA 1.6. *If D is congruent to 5 modulo 8, not equal to -3 , and negative, the class-number of the quadratic field \mathfrak{R} is always divisible by three.**

LEMMA 1.7. *If D is congruent to 5 modulo 8 and positive, and if*

$$(1.3) \quad \eta = r + \omega s$$

is the fundamental unit of the quadratic field \mathfrak{R} , then the class-number of \mathfrak{R} is divisible by three when and only when the rational integer s is even.†

2. Let A, B, C be a primitive solution of (1.1). During the next three sections of the paper, we assume that $M \geq 3$, so that C is necessarily odd.

If $1, \omega$ is the canonical basis of the field \mathfrak{R} , we have

$$(2.1) \quad \begin{aligned} \omega^2 &= D^{1/2}, & \bar{\omega} &= -\omega \text{ if } D \equiv 2, 3 \pmod{4}, & 2\omega + 1 &= D^{1/2}, \\ && \bar{\omega} &= -1 - \omega \text{ if } D \equiv 5 \pmod{8}. \end{aligned}$$

Let

$$(2.2) \quad \begin{aligned} \kappa &= A + \omega B, & \lambda &= \bar{\kappa} = A - \omega B \text{ if } D \equiv 2, 3 \pmod{4}, \\ \kappa &= A + B + 2\omega B, & \lambda &= \bar{\kappa} = A - B - 2\omega B \text{ if } D \equiv 5 \pmod{8}. \end{aligned}$$

Then in either case, κ and λ are integers of \mathfrak{R} , and $\kappa\lambda = A^2 - DB^2 = C^M$ or

$$(2.3) \quad [\kappa][\lambda] = [C]^M.$$

* Dirichlet-Dedekind, *Zahlentheorie*, 4th edition, 1894, p. 244.

† Dirichlet-Dedekind, work cited, p. 250.

Since C is odd, the principal ideals $[\kappa]$ and $[\lambda]$ in (2.3) are co-prime by Lemma 1.4. Hence there exist two ideals \mathfrak{a} and \mathfrak{b} of \mathfrak{K} such that

$$[\kappa] = \mathfrak{a}^M, \quad [\lambda] = \mathfrak{b}^M, \quad [C] = \mathfrak{ab}, \quad (\mathfrak{a}, \mathfrak{b}) = 1.$$

Since M is prime to the class-number of the field \mathfrak{K} , \mathfrak{a} and \mathfrak{b} are principal ideals of \mathfrak{K} by Lemma 1.3. Denote them by $[\alpha]$ and $[\beta]$ respectively. Then

$$[\kappa] = [\alpha^M], \quad [\lambda] = [\beta^M], \quad [C] = [\alpha][\beta], \quad ([\alpha], [\beta]) = 1.$$

Moreover, since λ is conjugate to κ , β is conjugate to α . Therefore there exist two units ϵ_1 and ϵ_2 of \mathfrak{K} such that

$$\kappa = \epsilon_1 \alpha^M, \quad \lambda = \bar{\epsilon}_1 \bar{\alpha}^M, \quad C = \epsilon_2 \alpha \bar{\alpha}, \quad ([\alpha], [\bar{\alpha}]) = 1.$$

Since $\alpha \bar{\alpha} = N\alpha$ is a rational integer, $\epsilon_2 = \pm 1$. Let η be the fundamental unit of the field \mathfrak{K} . Then there exists an integer R such that $\epsilon_1 = \pm n^R$.

Divide R by M , and let the quotient and remainder be Q , $T: R = QM + T$, $0 \leq T \leq M - 1$. Then if we write α' for $\eta^Q \alpha$, we have

$$(2.4) \quad \kappa = \pm \eta^T \alpha'^M, \quad \lambda = \pm \eta^{-T} \bar{\alpha}'^M, \quad C = \pm \alpha' \bar{\alpha}', \quad 0 \leq T \leq M - 1,$$

$$(2.5) \quad ([\alpha'], [\bar{\alpha}']) = 1.$$

If D is negative, the only units in \mathfrak{K} are ± 1 , since $D \neq -1, -3$, and (2.4) holds with $T=0$. Henceforth we retain only the positive signs in (2.4).

3. If $D \equiv 2, 3 \pmod{4}$, α' and $\bar{\alpha}'$ in (2.4) are of the form

$$\alpha' = a + \omega b, \quad \bar{\alpha}' = a - \omega b, \quad \omega^2 = D,$$

where a and b are rational integers. Then

$$(3.1) \quad (a, Db) = 1.$$

For otherwise, there exists a prime ideal \mathfrak{p} of \mathfrak{K} such that $\alpha' \equiv 0 \pmod{\mathfrak{p}}$, $Db \equiv \omega^2 b \equiv 0 \pmod{\mathfrak{p}}$, so that $a \equiv \omega b \equiv 0 \pmod{\mathfrak{p}}$, $\alpha' \equiv \bar{\alpha}' \equiv 0 \pmod{\mathfrak{p}}$ contradicting (2.5).

Since $C = a^2 - Db^2$ is odd, we must have

$$(3.2) \quad a, b \text{ of opposite parity if } D \text{ is odd, } a \text{ odd if } D \text{ is even.}$$

Now $\alpha'^M = A_M + D^{1/2}B_M$, where

$$(3.3) \quad \begin{aligned} A_M &= a^M + \binom{M}{2} Da^{M-2}b^2 + \binom{M}{4} D^2 a^{M-4}b^4 + \dots; \\ B_M &= \binom{M}{1} a^{M-1}b + \binom{M}{3} Da^{M-3}b^3 + \dots. \end{aligned}$$

If the fundamental unit η is $r + \omega s$ in the case when D is positive, we write $r = u_1$, $s = v_1$, $\omega = D^{1/2}$,

$$\eta^T = (r + \omega s)^T = U_T + D^{1/2}V_T \quad (T = 0, 1, \dots, M-1).$$

(2.4) then gives us our final formulas:

$$(3.4) \quad A = U_T A_M + D V_T B_M, \quad B = U_T B_M + V_T A_M, \quad C = a^2 - D b^2,$$

where if D is positive, T may have any integral value from 0 to $M-1$, but if D is negative, T is zero.

We have thus shown that in the case $D \equiv 2, 3 \pmod{4}$, every primitive solution A, B, C of (1.1) is of the form (3.4). We shall now show that if a and b are rational integers subject to the conditions (3.1), (3.2), the formulas (3.4) always give a primitive solution of (1.1).

It is obvious the formulas always give a solution of (1.1), and that for such a solution, C is odd. To show that the solution is primitive, it suffices to prove that $(A, B) = 1$.

If $(A, B) \neq 1$, there exists a prime ideal \mathfrak{p} of \mathfrak{K} such that $A \equiv B \equiv 0 \pmod{\mathfrak{p}}$ so that $A \pm D^{1/2}B \equiv 0 \pmod{\mathfrak{p}}$. Since $U_T \pm D^{1/2}V_T$ is a unit of \mathfrak{K} and $A \pm D^{1/2}B = (U_T \pm D^{1/2}V_T)(A_M \pm D^{1/2}B_M)$, $A_M \pm D^{1/2}B_M = (a \pm D^{1/2}b)^M \equiv 0 \pmod{\mathfrak{p}}$ or $a \pm D^{1/2}b \equiv 0 \pmod{\mathfrak{p}}$. Therefore $2a \equiv 2D^{1/2}b \equiv 0 \pmod{\mathfrak{p}}$; or since $(a, Db) = 1$, $2 \equiv 0 \pmod{\mathfrak{p}}$, and $A \equiv B \equiv 0 \pmod{2}$. But then $C^M = A^2 - DB^2 \equiv 0 \pmod{2}$, so that C would be even.

4. If $D \equiv 5 \pmod{8}$, α' and $\bar{\alpha}'$ in (2.4) are of the form

$$(4.1) \quad \alpha' = c + \omega d, \quad \bar{\alpha}' = c - d - \omega d, \quad (2\omega + 1)^2 = D,$$

where c and d are rational integers which are co-prime by (2.5). There are two cases according as D is negative or positive.

If D is negative, the class-number of \mathfrak{K} is divisible by three by Lemma 1.6. Hence $(M, 3) = 1$. Since 1 is the fundamental unit, we obtain from (2.4) $\alpha'^M = (c + \omega d)^M = \kappa = A + B + 2B\omega$. Therefore, by Lemma 1.5, d is even. If we write $d = 2b$, $c = a - b$, we have $\alpha' = a + D^{1/2}b$. Hence

$$\kappa = A + BD^{1/2} = (a + D^{1/2}b)^M = A_M + D^{1/2}B_M.$$

Thus we obtain as in the previous case D negative and congruent to 2 or 3 (4),

$$(4.2) \quad A = A_M, \quad B = B_M, \quad C = a^2 - D b^2 \alpha, \quad (a, Db) = 1.$$

Since $M \geq 3$, C is odd by Lemma (1.2). Therefore a and b must be of opposite parity. A_M and B_M are as in (3.3).

Conversely, it may be shown as in §3 that if a and b are rational integers of opposite parity, the formulas (4.2) always give a primitive solution of (1.1).

Next, assume that D is positive, and denote the fundamental unit of the field \mathfrak{K} by

$$(1.3) \quad \eta = r + \omega s,$$

as in Lemma 1.7. Then if the class-number of \mathfrak{R} is divisible by three, s is even. Writing $s = 2v$, $r = u - v$,

$$\eta = u + vD^{1/2}, \quad \eta^T = U_T + V_T D^{1/2} \quad (T = 0, 1, \dots, M-1).$$

Then by (2.4), (4.1)

$$\alpha'^M = (c + \omega d)^M = \bar{\eta}^T \kappa = c' + \omega d'$$

where d' is even. Since $(M, 3) = 1$, d is therefore even by Lemma 1.5. On writing $d = 2b$, $c = a - b$, we obtain therefore

$$(4.3) \quad A = U_T A_M + D V_T B_M, \quad B = U_T B_M + V_T A_M, \quad C = a^2 - Db^2.$$

a and b here are of opposite parity, and $(a, Db) = 1$. Conversely, we may show as in §3 that (4.3) always gives a primitive solution of (1.1).

If the class-number of \mathfrak{R} is not divisible by three, the integer s in (1.3) is odd. We obtain therefore from (2.4) and (4.1)

$$(r + \omega s)^T(c + \omega d)^M = \kappa = c' + \omega d', \quad d' \text{ even.}$$

Therefore if d is even, T must be divisible by three by Lemma 1.5. On the other hand, if d is odd, we have the following restrictions on T and M according to the parity of r in order that d' may be even.

- If $r + \omega s \equiv 1 + \omega \pmod{2}$ and $c + \omega d \equiv 1 + \omega \pmod{2}$, then $T + M \equiv 0 \pmod{3}$;
- if $r + \omega s \equiv 1 + \omega \pmod{2}$ and $c + \omega d \equiv \omega \pmod{2}$, then $T - M \equiv 0 \pmod{3}$;
- if $r + \omega s \equiv \omega \pmod{2}$ and $c + \omega d \equiv \omega \pmod{2}$, then $T + M \equiv 0 \pmod{3}$;
- if $r + \omega s \equiv \omega \pmod{2}$ and $c + \omega d \equiv 1 + \omega \pmod{2}$, then $T - M \equiv 0 \pmod{3}$.

Let us write

$$2\eta^T = U_T + V_T D^{1/2} \quad (T = 0, 1, \dots, M-1).$$

$\alpha' = a + D^{1/2}b$ if d is even; $2\alpha' = a + D^{1/2}b$ if d is odd, where, in the first case, $d = 2b$, $c = a - b$, and in the second case, $d = b$, $a = 2c - b$, so that a and b are both odd. The four cases above when s is odd may then be stated as follows:

$$(4.4) \quad \begin{aligned} T + M &\equiv 0 \pmod{3} \text{ if } r - (a + b)/2 \equiv 0 \pmod{2}, \\ T - M &\equiv 0 \pmod{3} \text{ if } r - (a + b)/2 \equiv 1 \pmod{2}. \end{aligned}$$

The solutions of (1.1) are given by the following formulas:

$$(4.5) \quad \begin{aligned} 2A &= U_{3T} A_M + D V_{3T} B_M, \quad 2B = U_{3T} B_M + V_{3T} A_M, \quad C = a^2 - Db^2, \\ a, b \text{ of opposite parity, } (a, Db) &= 1, \quad 0 \leq T \leq [(M-1)/3], \end{aligned}$$

or

$$(4.6) \quad 2^{M+1}A = U_T A_M + D V_T B_M, \quad 2^{M+1}B = U_T B_M + V_T A_M, \quad 4C = a^2 - Db^2,$$

a, b both odd, $(a, Db) = 1$, and T restricted by (4.4).

It is easily shown as before that both (4.5) and (4.6) give us primitive solutions of (1.1) with the specified restrictions on a, b and T .

The possibility of primitive solutions of (1.1) of the form (4.6) seems to have been overlooked heretofore. On taking $D=5$, $M=3$, $T=0$, $a=b=1$ in (4.6), we obtain the solution $2, 1, -1$ of $X^2 - 5Y^2 = Z^3$ discussed in the introduction.

5. The case when $M=2$, $D=5$ (8) requires separate discussion, as we see from Lemma 1.2 that primitive solutions of

$$(5.1) \quad X^2 - DY^2 = Z^2$$

will exist of the form $X=A$, $Y=B$, $Z=C=2E$, where A, B, E are odd and co-prime. The other solutions with C odd may be obtained from our general formulas in §4. In the present case, we write

$$(5.2) \quad 2\kappa = A + B + 2\omega B, \quad 2\lambda = A - B - 2\omega B \text{ where as usual } 2\omega + 1 = D^{1/2},$$

or letting $A+B=2G$,

$$\kappa = G + \omega B, \quad \lambda = \bar{\kappa}, \quad \kappa\lambda = E^2, \quad [\kappa][\lambda] = [E]^2.$$

If we now apply the reasoning used in §2 to this ideal equation, we deduce that either

$$(5.3) \quad \begin{aligned} \kappa &= (c + \omega d)^2, & E &= (c + \omega d)(c + \bar{\omega}d), & \text{or} \\ \kappa &= (r + \omega s)(c + \omega d)^2, & E &= (c + \omega d)(c + \bar{\omega}d), \end{aligned}$$

where $r+\omega s$ is the fundamental unit of the field \mathfrak{R} . To agree with our former notation, let $U_0=2$, $V_0=0$, $U_1=2r-s$, $V_1=s$, $2c-d=a$, $d=b$. Then

$$8\kappa = (U_T + D^{1/2}V_T)(a + D^{1/2}b)^2, \quad 4E = a^2 - Db^2, \quad T = 0, 1,$$

so that

$$(5.4) \quad \begin{aligned} 4A &= U_T(a^2 + Db^2) + 2abDV_T, & 4B &= V_T(a^2 + Db^2) + 2abU_T, \\ 2C &= a^2 - Db^2, & T &= 0, 1, \end{aligned}$$

where a and b are both odd, and $(a, Db)=1$. As before, (5.4) always gives a primitive solution of (5.1) with Z even.

For the case $M=2$, it may be noted, a knowledge of all of the primitive solutions of (1.1) gives us immediately the most general solution of (1.1). On collecting all of our results, we obtain the fundamental theorem stated in the introduction.

III. APPLICATIONS OF THE FORMULAS

6. Consider the diophantine equation

$$(6.1) \quad X^2 - D = Z^M,$$

where D is square-free, negative, $\neq -1$ or -3 , incongruent to 1 (8), while M is prime to the class-number of the quadratic field $\mathfrak{K}(D^{1/2})$. Then if $X=A$, $Z=C$ is a solution of (6.1), $A, \pm 1, C$ is a primitive solution of (1.1). Conversely, any primitive solution of (1.1) with $B=\pm 1$ gives a solution of (6.1). Accordingly, all solutions of (6.1) are obtainable by setting $Y=\pm 1$ in the formulas of case I of the fundamental theorem; thus

$$(6.2) \quad \pm 1 = \binom{M}{1} a^{M-1} b + \binom{M}{3} D a^{M-3} b^3 + \dots.$$

If M is even, the last term on the right of (6.2) is $\binom{M}{M-1} D^{(M-2)/2} a b^{M-1}$. Since the numbers $\binom{M}{1}, \binom{M}{3}, \dots, \binom{M}{M-1}$ are all even when M is even, (6.2) is impossible, so that (6.1) *has no solutions if M is even*.

If M is odd, the last term on the right of (6.2) is $D^{(M-1)/2} b^M$. Hence every term is divisible by b , so that $b=\pm 1$, and a must be a root of the equation

$$(6.21) \quad \binom{M}{1} x^{M-1} + \binom{M}{3} D x^{M-3} + \dots + D^{(M-1)/2} \mp 1 = 0.$$

For fixed D and M meeting our restrictions, the solution of (6.1) reduces then to finding all the integral roots of (6.2).

Under the same restrictions on D and M , we can obtain information about the diophantine equation

$$(6.3) \quad 1 - DY^2 = Z^M.$$

We have in place of (6.2) the condition

$$(6.4) \quad \pm 1 = a^M + \binom{M}{2} a^{M-2} b^2 + \dots.$$

If M is even, we obtain no direct information. But if M is odd, the right side of (6.4) is divisible by a , so that $a=\pm 1$, and b must be an integral root of the equation*

$$(6.41) \quad \begin{aligned} & \binom{M}{M-1} D^{(M-3)/2} x^{M-3} + \binom{M}{M-3} D^{(M-5)/2} x^{M-5} + \dots \\ & + \binom{M}{4} D x^2 + \binom{M}{2} = 0. \end{aligned}$$

* The conceivable case when $a=\mp 1$ and the left side of (6.4) is ± 1 is easily shown to be impossible.

To give a numerical example, consider the equation $X^2 + 42 = Z^5$ to which the method is applicable since the class-number of $\mathfrak{K}(42^{1/2}i)$ is 4. If M is a prime,

$$D^{(M-1)/2} \equiv \binom{D}{M} (M),$$

while $(\frac{M}{1}), (\frac{M}{3}), \dots, (\frac{M}{M-2})$ are all divisible by M . We must therefore choose the ambiguous sign in (6.21) equal to $-(\frac{D}{M})$, or $+1$ in this case. On dividing out $M=5$, (6.21) becomes

$$x^4 - 84x^2 + 353 = 0.$$

Since $84^2 - 4 \cdot 353 = 5644$ is not a square, the initial diophantine equation has no solutions.

7. Consider now the diophantine equation

$$(7.1) \quad X^2 - 16DY^{2N} = Z^4.$$

We assume as before that D is square-free, negative, incongruent to 1 (8), and in addition, that the class-number of the quadratic field $\mathfrak{K}(D^{1/2})$ is odd.*

Let A, B, C be a primitive solution of (7.1). Then $A, 4B^N, C$ is a primitive solution of

$$(7.2) \quad X^2 - DY^2 = Z^4.$$

Hence by case I of our fundamental theorem, there exist rational integers a and b such that $(a, Db)=1$, $a+b$ odd, and

$$A = a^4 + 6a^2b^2D + D^2b^4, \quad 4B^N = 4ab(a^2 + Db^2), \quad C = a^2 - Db^2.$$

From the expression for $4B^N$, we deduce that $a, b, a^2 + Db^2$ are perfect N th powers: $a = E^N, b = F^N, a^2 + Db^2 = G^N$ so that $X = E, Y = F, Z = G$ is a primitive solution of

$$(7.3) \quad X^{2N} + DY^{2N} = Z^N.$$

Conversely, a primitive solution of (7.3) gives us a primitive solution of (7.1). But it is easy to see that if (7.3) has any solutions whatever, it has primitive solutions. Therefore: *A necessary and sufficient condition that the diophantine equation (7.3) be solvable is that the diophantine equation (7.1) have a primitive solution.*

Assume next that D is negative, and congruent to 2 or 3 (4), and that the class-number of $\mathfrak{K}(D^{1/2})$ is prime to 3, while D is divisible by three. Consider

* This always occurs for example if D is a prime, $\equiv 5$ (8). See Dirichlet's Works, vol. I, 1889, pp. 357-370, or Crelle's Journal, vol. 18 (1838), pp. 259-274.

$$(7.4) \quad X^2 - 9DY^{2N} = Z^3.$$

A similar procedure to that given for (7.1) connects (7.4) with the diophantine equation

$$(7.5) \quad X^N + \frac{DY^N}{3} = Z^N,$$

and we have the theorem that *a necessary and sufficient condition that the diophantine equation (7.5) be solvable is that the diophantine equation (7.4) have a primitive solution.*

For example take $D = -21$. The class number of $\mathfrak{K}(21^{1/2}i)$ is four, and for $N = 7$,

$$X^7 - 7Y^7 = Z^7$$

is known to have no solutions.* Hence

$$X^2 + 189Y^{14} = Z^3$$

has no primitive solutions.

This result generalizes an interesting correspondence recently obtained by Kapferer† between the solutions of Fermat's equation and the primitive solutions of an equation of the form (7.4).

* Maillet, Comptes Rendus, vol. 129 (1899), pp. 189–199.

† Sitzungsberichte, Heidelberg Akademie, 1933, part 2, pp. 32–37.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

Chapter 10

1936

A CALCULUS OF SEQUENCES.

By MORGAN WARD.

I. *Introduction.*

1. I propose in this paper to give a generalization of a large portion of the formal parts of algebraic analysis and the calculus of finite differences. The generalization consists in systematically replacing the ordinary binomial coefficient $n(n-1)\cdots(n-r+1)/1\cdot2\cdots r$ by a "binomial coefficient to the base (u) ," $[n, r] = u_n \cdot u_{n-1} \cdots u_{n-r+1}/u_1 \cdot u_2 \cdots u_r$ where $(u) : u_0, u_1, u_2, \dots$ is a fixed sequence of complex numbers subject to the restrictions $u_0 = 0$; $u_1 = 1$; $u_n \neq 0$, $n > 1$. The exponential function for example is replaced by the formal series $1 + \sum_{n=1}^{\infty} x^n/u_1 \cdot u_2 \cdots u_n$, differentiation by an operation which throws x^n into $[n, 1]x^{n-1}$, and differencing by an operation which throws x^n into $\sum_{r=1}^n [n, r]x^{n-r}$.

The formula $n^r = (1 + 1 + \cdots + 1)^r = \sum_{(s)} r!/s_1!s_2!\cdots s_n!$ guides us in replacing the powers of rational integers where necessary by sums of multinomial coefficients to the base (u) ; for example, $\sum_{s=0}^r [n, r]$ may replace 2^r . We are thus enabled to generalize successfully a great variety of formulas involving the exponential functions, the Bernoulli numbers and polynomials.

2. In a series of papers which have appeared during the past thirty years [1],¹ F. H. Jackson has developed a somewhat similar extension of elementary analysis for the particular sequence (u) in which $u_n = (q^n - 1)/(q - 1)$ q a fixed complex number, $|q| \neq 1$. His results are based essentially on an identity of Euler's [2]:

$$(2.1) \quad (x + y)(x + qy) \cdots (x + q^{n-1}y) = \sum_{r=0}^n [n, r]q^{r(r-1)/2}x^{n-r}y^r.$$

In effect he replaces the ordinary binomial coefficient by $[n, r]q^{r(r-1)/2}$. But the presence of this power of q introduces a lack of symmetry in his formulas,

¹ The numbers in square brackets refer to references at the end of the paper. Jackson wrote in all over thirty papers on this subject. We have listed only those directly connected with the present paper.

and leads to certain complications in defining the exponential functions.² He was not led furthermore to consider the developments of the calculus of finite differences which we give here. These appear to be among the most striking results of the entire theory.

The present work originated in an (unsuccessful) attempt to frame a definition of the Bernoulli numbers in Jackson's calculus to which the Staudt-von Klausen theorem might apply.

II. Formal theory.

3. Let

$$(u) : u_0 = 0, \quad u_1 = 1, \quad u_2, \dots, u_n, \dots$$

be a fixed sequence of complex numbers subject for the present to the single restriction $u_n \neq 0$, $n > 1$. For convenience, we shall write $[n]$ for u_n . We define:

$$\begin{aligned} [n]! &\text{ to be } 1 \text{ if } n = 0, \text{ and } [n][n-1]\cdots[1] \text{ if } n > 0; \\ [n, r] &\text{ to be } [n]!/[r]![n-r]! \end{aligned}$$

where n, r are positive integers,³ and $n \geq r$. Then

$$[n, 0] = 1, \quad [n, 1] = [n], \quad [n, n-r] = [n, r].$$

We shall call $[n, r]$ a binomial coefficient to the base (u) , or simply a *basic*⁴ binomial coefficient.

We write $(x+y)^n$ for the polynomial $\sum_{r=0}^n [n, r]x^{n-r}y^r$. It is evident that

$$\begin{aligned} (x+y)^0 &= 1, \quad (x+y)^1 = x+y, \quad (x+0)^n = x^n \\ (cx+cy)^n &= c^n(x+y)^n, \quad (x+y)^n = (y+x)^n. \end{aligned}$$

From the identities⁵

$$\begin{aligned} (x-y)^{2n+1} &= \sum_{r=0}^n (-1)^r [2n+1, r] x^r y^r (x^{2n+1-2r} - y^{2n+1-r}) \\ (x-y)^{2n} &= \sum_{r=0}^{n-1} (-1)^r [2n, r] x^r y^r (x^{2n-2r} + y^{2n-2r}) + (-1)^n [2n, n] x^n y^n \end{aligned}$$

² It is necessary to consider not only the series $1 + \sum_{r=1}^{\infty} xn/u_1 u_2 \cdots u_n$ as an analogue of the exponential, but also the series $1 + \sum_{r=1}^{\infty} q^{n(n-1)/2} xn/u_1 u_2 \cdots u_n$ with a corresponding complexity in the theory of the trigonometric functions.

³ We count zero as a positive integer.

⁴ This convenient terminology is due to F. H. Jackson.

⁵ We write $(x-y)^n$ for $(x+(-y))^n = \sum_{r=0}^n [n, r] x^{n-r} (-y)^r$.

we see that

$$(x - x)^{2n+1} = 0; \quad (n = 0, 1, 2, \dots).$$

On the other hand,

$$(x - x)^{2n} = x^{2n}(1 - 1)^{2n} = x^{2n}\left\{2 \sum_{r=0}^{n-1} (-1)^r [2n, r] + (-1)^n [2n, n]\right\}$$

generally does *not* vanish. A sequence (u) such that

$$(1 - 1)^{2n} = 0, \quad (n = 1, 2, 3, \dots)$$

will be said to be *normal*.

4. More generally, we define

$$(x_1 + x_2 + \dots + x_k)^n \text{ to be } \sum_{(s)} \frac{[n]!}{[s_1]! \dots [s_k]!} x_1^{s_1} \dots x_k^{s_k}$$

where the summation is over all integers s satisfying the conditions

$$s_1 + s_2 + \dots + s_k = n, \quad 0 \leq s_i \leq n.$$

If we denote this polynomial by $P_{kn}(x) = P_{kn}(x_1, x_2, \dots, x_k)$ then it is a symmetric function of its k arguments, and if c is any constant, then

$$P_{kn}(cx_1, cx_2, \dots, cx_k) = c^n P_{kn}(x_1, x_2, \dots, x_k).$$

Furthermore,

$$(4.1) \quad P_{k+1n}(x) = P_{kn}(x_1, x_2, \dots, x_{k-1}, x_k + x_{k+1}).$$

For consider $P_{2n}(x) = (x_1 + x_2)^n$. We have

$$\begin{aligned} (x_1 + x_2)^n &= \sum_{t=0}^n \frac{[n]!}{[n-t]! [t]!} x_1^{n-t} x_2^t \\ (x_1 + (x_2 + x_3))^n &= \sum_{t=0}^n \frac{[n]!}{[n-t]! [t]!} x_1^{n-t} (x_2 + x_3)^t \\ &= \sum_{t=0}^n \sum_{r=0}^t \frac{[n]! [t]!}{[n-t]! [t]! [t-r]! [r]!} x_1^{n-t} x_2^{t-r} x_3^r \\ &= \sum_{(s)} \frac{[n]!}{[s_1]! [s_2]! [s_3]!} x_1^{s_1} x_2^{s_2} x_3^{s_3}, \\ &\quad s_1 + s_2 + s_3 = n, \quad 0 \leq s_i \leq n \\ &= (x_1 + x_2 + x_3)^n = P_{3n}(x). \end{aligned}$$

Hence (4.1) is true for $k = 2$. Its validity for any value of k follows by an easy induction.

It is evident that formula (4.1) can be extended so as to express $P_{k+l n}(x)$ in terms of $P_{kn}(x)$ in various ways. For example,

$$P_{4n}(x_1, x_2, x_3, x_4) = P_{2n}(x_1 + x_2, x_3 + x_4).$$

5. The numerical values of the polynomials $P_{kn}(x)$ when all of the arguments x_i are equal to plus one play an important rôle in the developments which are to follow. We shall write \bar{k}^n for the number

$$P_{kn}(1, 1, \dots, 1) = (1 + 1 + \dots + 1)^n = \sum_{(s)} \frac{[n]!}{[s_1]! \dots [s_k]!}.$$

We see from the formulas of section 4 that

$$\bar{3}^n = (\bar{2} + \bar{1})^n, \quad \bar{4}^n = (\bar{2} + \bar{2})^n = (\bar{3} + \bar{1})^n.$$

It is easily shown by induction that we have quite generally

$$(5.1) \quad \overline{r+s}^n = (\bar{r} + \bar{s})^n$$

where r and s are any positive integers.

If furthermore the sequence (u) is normal (section 3) then we can show by induction that (5.1) holds for any integral values of r and s . A somewhat longer induction establishes the formula

$$(5.2) \quad \overline{m_1 + m_2 + \dots + m_t}^n = (\bar{m}_1 + \bar{m}_2 + \dots + \bar{m}_t)^n$$

where if (u) is normal, m_1, \dots, m_t are any integers, but if (u) is not normal, the integers are to be positive.

In case (u) is normal, there is no gain in generality in replacing some of the plus signs in formula (5.2) by minus signs because we can show that

$$(5.3) \quad (\bar{r} - \bar{s})^n = (\bar{r} + \overline{-s})^n.$$

6. If $F(x)$ denotes the formal power series

$$(6.1) \quad F(x) = \sum_{n=0}^{\infty} c_n x^n,$$

we define $F(x+y)$ to mean the series

$$\sum_{n=0}^{\infty} c_n (x+y)^n = \sum_{n=0}^{\infty} \sum_{r=0}^n c_n [n, r] x^{n-r} y^r.$$

In like manner

$$(6.2) \quad \begin{aligned} F(x_1 + x_2 + \dots + x_k) &= \sum_{n=0}^{\infty} c_n (x_1 + x_2 + \dots + x_k)^n \\ &= \sum_{n=0}^{\infty} c_n P_{kn}(x). \end{aligned}$$

We have furthermore formal identities of the type

$$\begin{aligned} F(x_1 + x_2) &= F(x_2 + x_1), \\ F(x_1 + x_2 + x_3) &= F(x_1 + (x_2 + x_3)) \\ F(x_1 + x_2 + x_3 + x_4) &= F((x_1 + x_2) + (x_3 + x_4)) \end{aligned}$$

since the like identities hold for the polynomials $P_{kn}(x)$.

If in the series (6.2) we make all the arguments x_i equal to x , the right side becomes $\sum_{n=0}^{\infty} c_n(x + x + \cdots + x)^n = \sum_{n=0}^{\infty} c_n \bar{k}^n x^n$. We shall accordingly denote the resulting series by $F(\bar{k}x)$. It is obvious then from the formula (5.2) that

$$(6.3) \quad F(\overline{m_1 + m_2 + \cdots + m_t} x) = F(\overline{m}_1 x + \overline{m}_2 x + \cdots + \overline{m}_t x)$$

for suitably restricted integers m_i .

Let $F(x)$, $G(x)$, $H(x)$ be three formal power series in x . Then the following theorem is easily seen to be true.

THEOREM 6.1. *If $F(x) = G(x) \pm H(x)$ and m, n are any positive integers, then $F(\bar{m}x) = G(\bar{m}x) \pm H(\bar{m}x)$ and*

$$F(\bar{m}x + \bar{n}y) = G(\bar{m}x + \bar{n}y) \pm H(\bar{m}x + \bar{n}y).$$

7. We next define an operator $D = D_x$ which transforms the formal power series (6.1) into

$$(7.1) \quad F'(x) = DF(x) = \sum_{n=0}^{\infty} [n] c_n x^{n-1}.$$

In particular then, $Dx^n = [n]x^{n-1}$. The operator D is easily shown to be linear and distributive, and it converts a polynomial of degree n in x into one of degree $n - 1$.

If we define $F^{(r)}(x) = D^r F(x)$ recursively by $F^{(r+1)}(x) = DF^{(r)}(x)$; $F^{(0)}(x) = F(x)$, it easily follows that

$$\frac{F^{(r)}(x)}{[r]!} = \sum_{n=r}^{\infty} [n, r] c_n x^{n-r}.$$

The expansion $F(x + y) = \sum_{n=0}^{\infty} c_n(x + y)^n$ is formally replaceable by

$$(7.2) \quad F(x + y) = \sum_{n=0}^{\infty} \frac{F^{(n)}(x)}{[n]!} y^n.$$

We shall refer to (7.2) as *Taylor's formula* for the base (u) .

Finally, we note that

$$D_x^r F(x + y) = F^{(r)}(x + y).$$

8. As a simple concrete example of such an operator D , let us assume that the sequence (u) is a linear recurring series of order k whose associated polynomial $x^k - a_1x^{k-1} - \dots - a_k$ has k distinct roots $\alpha_1, \alpha_2, \dots, \alpha_k$. Then u_n is of the form

$$u_n = \beta_1\alpha_1^n + \beta_2\alpha_2^n + \dots + \beta_k\alpha_k^n$$

where the constants α and β are subject to the conditions

$$\beta_1 + \beta_2 + \dots + \beta_k = 0, \quad \beta_1\alpha_1 + \beta_2\alpha_2 + \dots + \beta_k\alpha_k = 1, \quad u_n \neq 0, n > 1.$$

It is obvious then that

$$DF(x) = (\beta_1F(\alpha_1x) + \dots + \beta_kF(\alpha_kx)) / (\beta_1\alpha_1x + \dots + \beta_k\alpha_kx).$$

This operator can therefore be applied to any function of x regular at $x = 0$, and transforms it into another function regular at $x = 0$.

In particular, if $k = 2$, $\alpha_1 = q$, $\alpha_2 = 1$, $\beta_1 = (q - 1)^{-1}$, $\beta_2 = -\beta_1$, where q is not a root of unity,

$$DF(x) = \frac{F(qx) - F(x)}{qx - x}$$

is the operation of q -differencing.

In case some of the roots α of the polynomial associated with the recurrence relation are repeated, a similar but more complicated formula for $DF(x)$ may be given which involves both $F(x)$ and its ordinary derivatives. For example, if $k = 2$ and $\alpha_1 = \alpha_2 \neq 0$, $u_n = n\alpha_1^{n-1}$ and $DF(x) = \frac{1}{\alpha_1} \frac{dF(\alpha_1x)}{dx}$.

III. The exponential and trigonometric functions.

9. We shall now assume that the sequence (u) is chosen in such a manner that the series

$$(9.1) \quad \mathcal{E}(x) = \sum_{n=0}^{\infty} \frac{x^n}{[n]!}$$

is convergent in the neighborhood of $x = 0$. It accordingly is an element of an analytic function of x which we shall call the *basic exponential*. There exists then a positive number ρ such that the series (9.1) converges absolutely within the circle $|x| = \rho$.

The basic exponential has the following properties for sufficiently small absolute values of its arguments x, y, x_i :

$$(9.2) \quad D\mathcal{E}(x) = \mathcal{E}(x), \quad \mathcal{E}^{(n)}(cx) = c^n\mathcal{E}(cx), \quad c \text{ a constant},$$

$$(9.21) \quad \mathcal{E}(x+y) = \mathcal{E}(x)\mathcal{E}(y),$$

$$(9.22) \quad \mathcal{E}(x_1 + x_2 + \dots + x_k) = \mathcal{E}(x_1)\mathcal{E}(x_2)\dots\mathcal{E}(x_k).$$

Consider for example the formula (9.21). That it is formally true is immediately obvious from the basic Taylor's formula (7.2). For

$$\mathcal{E}(x+y) = \sum_{n=0}^{\infty} \frac{\mathcal{E}^{(n)}(x)y^n}{[n]!} = \mathcal{E}(x)\mathcal{E}(y)$$

since by (9.2), $\mathcal{E}^{(n)}(x) = \mathcal{E}(x)$.

But the series

$$\sum_{n=0}^{\infty} \frac{(x+y)^n}{[n]!} = \sum_{n=0}^{\infty} \sum_{r=0}^n \frac{x^{n-r}y^r}{[n-r]![r]!}$$

is in fact the Cauchy product of the series $\sum \frac{x^n}{[n]!}, \sum \frac{y^n}{[n]!}$ so that the formula is actually true provided the latter two series are both absolutely convergent. And by our initial hypothesis, both series converge absolutely if $|x| < \rho, |y| < \rho$.

10. The trigonometric and hyperbolic functions are defined by Euler's formulas:

$$(10.1) \quad \begin{aligned} \sin(x) &= \frac{\mathcal{E}(ix) - \mathcal{E}(-ix)}{2i}, & \cos(x) &= \frac{\mathcal{E}(ix) + \mathcal{E}(-ix)}{2}, \\ \sinh(x) &= -i\sin(ix), & \cosh(x) &= \cos(ix). \end{aligned}$$

Among the many formal analogies with the ordinary trigonometric functions, we shall merely note here:

$$\begin{aligned} \sin(x+y) &= \sin(x)\cos(y) + \cos(x)\sin(y), \\ \cos(x+y) &= \cos(x)\cos(y) - \sin(x)\sin(y), \\ D\sin(x) &= \cos(x), & D\cos(x) &= -\sin(x). \end{aligned}$$

As a consequence of the last two formulas, we see that both $\sin(x)$ and $\cos(x)$ satisfy the basic differential equation $y^{(2)}(x) + y(x) = 0$.

On the other hand

$$(10.2) \quad \sin^2(x) + \cos^2(x) = \mathcal{E}(ix)\mathcal{E}(-ix)$$

and in general, $\mathcal{E}(ix)\mathcal{E}(-ix) \neq 1$.

The remaining trigonometric and hyperbolic functions are defined in terms of the basic sine and cosine as in the ordinary case.

11. It is possible to give analogues of De Moivre's and Simpson's formulas. For in formula (9.22), take $k = n$ and let $x_1 = x_2 = \dots = x_n = i\theta$. Then with the notation explained in section 6,

$$(11.1) \quad \mathcal{E}(ni\theta) = (\mathcal{E}(i\theta))^n.$$

Hence we obtain from the formulas (10.1) and theorem 6.1 the basic form of De Moivre's formula,⁶ $\cos(\bar{n}\theta) + i\sin(\bar{n}\theta) = (\cos(\theta) + i\sin(\theta))^n$.

THEOREM 11.1. *The sequence (u) is normal when and only when $\mathcal{E}(x)\mathcal{E}(-x) = 1$ or when and only when $\sin^2(x) + \cos^2(x) = 1$.*

For by formula (9.21), and the previous definitions, if $|x| < \rho$,

$$\mathcal{E}(x)\mathcal{E}(-x) = \mathcal{E}(x-x) = \sum_{n=0}^{\infty} \frac{(x-x)^n}{[n]!} = \sum_{n=0}^{\infty} \frac{(1-1)^n}{[n]!} x^n.$$

Now we have seen in section 3 that $(1-1)^{2n+1} = 0$, ($n = 0, 1, 2, \dots$). Therefore

$$\mathcal{E}(x)\mathcal{E}(-x) = 1 + \sum_{n=0}^{\infty} \frac{(1-1)^{2n}}{[2n]!} x^{2n}.$$

Hence the first part of the theorem follows. The second part of the theorem is an immediate consequence of formula (10.2).

Let us assume now that (u) is normal. We see from formula (11.1) that

$$(11.3) \quad \begin{aligned} \mathcal{E}(\overline{n+2}i\theta) &= \mathcal{E}(i\theta)\mathcal{E}(\overline{n+1}i\theta), \\ \mathcal{E}(i\theta)\mathcal{E}(\overline{ni}\theta) &= \mathcal{E}(\overline{n+1}i\theta). \end{aligned}$$

But by theorem 11.1, $\mathcal{E}(-i\theta)\mathcal{E}(i\theta) = 1$. Therefore this last equation may be written

$$(11.31) \quad \mathcal{E}(\overline{ni}\theta) = \mathcal{E}(-i\theta)\mathcal{E}(\overline{n+1}i\theta).$$

On adding and subtracting the two formulas (11.3), (11.31) and applying (10.1) and theorem (6.1), we obtain the basic Simpson's formulas:

$$\begin{aligned} \cos(\overline{n+2}\theta) &= 2\cos(\theta)\cos(\overline{n+1}\theta) - \cos(\overline{n}\theta), \\ \sin(\overline{n+2}\theta) &= 2\cos(\theta)\sin(\overline{n+1}\theta) - \sin(\overline{n}\theta). \end{aligned}$$

12. In order that the results of the previous section may have more than a purely formal significance, it is necessary to show that we can choose the sequence (u) so that (u) is normal and so that $E(\overline{nx})$ is an entire function of x for any integer n . Since $E(\overline{-nx}) = E(-\overline{nx})$, $E(\overline{nx}) = (E(\overline{1}x))^n$, $E(\overline{1}x) = E(x)$, we need only consider the case when $n = +1$.

Now it is easy to show that the most general solution of the functional equation

$$(12.1) \quad \Phi(x)\Phi(-x) = 1$$

⁶ It should be noted here that $(\cos(\theta) + i\sin(\theta))^n$ stands for the product $(\cos(\theta) + i\sin(\theta))(\cos(\theta) + i\sin(\theta))\dots$ taken to n factors, and not for the result of substituting $\cos(\theta)$ for x_1 , and $i\sin(\theta)$ for x_2 in the polynomial $P_{2n}(x) = (x_1 + x_2)^n$.

which is regular at the origin is of the form

$$(12.2) \quad \Phi(x) = \pm \exp(x\Psi(x^2))$$

where $\Psi(x)$ is regular at the origin. But by theorem 11.1, (u) is normal when and only when $\mathcal{E}(x)$ is a solution of (12.1). Since $\mathcal{E}(x)$ was assumed to be regular at the origin, $\mathcal{E}(x)$ must be of the form (12.2) where $\Psi(x)$ is an entire function of x . We must also satisfy the conditions⁷

$$\mathcal{E}(0) = 1, \quad \mathcal{E}'(0) = 1, \quad \frac{\mathcal{E}^{(n)}(0)}{n!} = \frac{1}{u_1 u_2 \cdots u_n} \neq 0,$$

as then $u_n = n\mathcal{E}^{(n-1)}(0)/\mathcal{E}^{(n)}(0) \neq 0$ ($n = 1, 2, \dots$) and $u_1 = 1$.

It will therefore suffice to choose for $\Psi(x)$ an entire function $G(x)$ with a series expansion of the form $G(x) = 1 + \sum_{n=1}^{\infty} g_n x^n$ where the quantities g_n are all real and non-negative. The ordinary case ensues on taking all the quantities g_n equal to zero.

13. If we assume that $\mathcal{E}(x)$ is an entire function satisfying the condition $\mathcal{E}(x)\mathcal{E}(-x) = 1$, we can generalize the periodic properties of the exponential function. For since $\mathcal{E}(x)$ never vanishes, by Picard's theorem there exists a complex number $\lambda \neq 0$ such that $\mathcal{E}(\lambda) = 1$. But then if n is a positive integer,

$$\begin{aligned} \mathcal{E}(x + \bar{n}\lambda) &= \mathcal{E}(x)\mathcal{E}(\bar{n}\lambda) = \mathcal{E}(x)(\mathcal{E}(\lambda))^n = \mathcal{E}(x), \\ \mathcal{E}(x) &= \mathcal{E}(x - \bar{n}\lambda + \bar{n}\lambda) = \mathcal{E}(x - \bar{n}\lambda)\mathcal{E}(\bar{n}\lambda) = \mathcal{E}(x - \bar{n}\lambda). \end{aligned}$$

We have therefore proved the following theorem.

THEOREM 13.1. *If (u) is a normal sequence so chosen that the basic exponential function $\mathcal{E}(x)$ is an entire function of x , and if $\lambda \neq 0$ is any zero of the function $\mathcal{E}(x) - 1$, and m any integer, then*

$$\mathcal{E}(x + \bar{m}\lambda) = \mathcal{E}(x).$$

Furthermore one such zero λ always exists.

On utilizing the formulas of section 10, we can easily show that under the hypotheses of theorem 13.1, we also have

$$\sin(x + \bar{m}i\lambda) = \sin(x), \quad \cos(x + \bar{m}i\lambda) = \cos(x).$$

⁷ The superscripts here denote ordinary differentiation.

IV. *The calculus of finite differences.*

14. Let (u) now be subject only to the conditions $u_0 = 0$, $u_1 = 1$, $u_n \neq 0$, $n \neq 0$. We shall denote by \mathfrak{N} the ring of all polynomials in x with coefficients in the field of all complex numbers.

If

$$(14.1) \quad \phi = \phi(x) = \sum_{r=0}^n a_{n-r}x^r, \quad a_0 \neq 0$$

is any element of \mathfrak{N} of degree n , we define the basic displacement symbol E by

$$(14.2) \quad \begin{aligned} E\phi(x) &= \phi(x+1) = \sum_{r=0}^n \sum_{s=0}^r a_{n-r}[r,s]x^{r-s} \\ E^{t+1}\phi(x) &= E(E^t\phi(x)), \quad E^0\phi(x) = \phi(x) \end{aligned}$$

where t is any positive integer.

It is obvious that E is a linear and distributive operator over \mathfrak{N} , and it may readily be shown that

$$(14.3) \quad E^t\phi(x) = \phi(x+\bar{t}).$$

If (u) is normal, formula (14.3) holds for all integral values of t .

15. The *basic difference operator* Δ is defined to be $E - 1$, where 1 stands for the identity operator over \mathfrak{N} . The following properties of Δ may be mentioned.

(i) Δ is linear and distributive over \mathfrak{N} , and converts an element of \mathfrak{N} of degree n into one of degree $n - 1$. Moreover E , Δ and D are commutative over \mathfrak{N} .

(ii) The only solutions of $\Delta\phi = 0$ lying in \mathfrak{N} are $\phi =$ a constant.

(iii) $\Delta^t\phi(x) = \sum_{s=0}^t (-1)^s \binom{t}{s} \phi(x+\bar{s})$.

(iv) We have the operational identity over \mathfrak{N}

$$(15.1) \quad \Delta = \mathcal{E}(D) - 1$$

where formally $\mathcal{E}(D) = \sum_{n=0}^{\infty} \frac{D^n}{[n]!}$.

The last one of these properties is the only one requiring comment. If ϕ of formula (14.1) is operated on by D of section 7, then

$$\frac{D^s\phi(x)}{[s]!} = 0, \quad s > n; \quad = \sum_{r=s}^n [r,s] a_{n-r} x^{r-s}, \quad s \leq n.$$

Hence

$$\mathcal{E}(D)\phi(x) = \sum_{s=0}^n \sum_{r=s}^n [r,s] a_{n-r} x^{r-s} = \sum_{r=0}^n \sum_{s=0}^r [r,s] a_{n-r} x^{r-s} = E\phi(x)$$

by formula (14.2), so that (15.1) follows.

16. The *basic Bernouilli numbers* $B_0, B_1, \dots, B_n, \dots$ are defined by the recurrences

$$B_0 = 1; \quad (B + 1)^n - B^n = 0, \quad n > 1; \quad (B + 1)^1 - B^1 = 1.$$

Here after expansion the exponents of B are to be degraded into suffices as in the usual theory [3].

The *basic Bernouilli polynomials* $B_n(z)$ may then be defined by

$$B_n(z) = (z + B)^n, \quad (n = 0, 1, \dots)$$

or non-symbolically,

$$B_n(z) = \sum_{r=0}^n [n, r] B_r z^{n-r}.$$

The following results [4] may be established precisely as in the ordinary theory.

$$(16.1) \quad B_n(0) = B_n, \quad B_n(1) = B_n, \quad n \neq 1; \quad B_1(1) = B_1 + 1.$$

$$(16.2) \quad B_n(x + y) = \sum_{r=0}^n [n, r] x^r B_{n-r}(y).$$

THEOREM 16.1. If $\phi'(x) = D\phi(x)$ denotes the basic derivative of the polynomial $\phi(x)$, then a polynomial solution of the difference equation

$$\Delta\Psi(x) = \phi'(x)$$

is given by

$$(16.3) \quad \Psi(x) = \phi(x + B).$$

$$(16.31) \quad \phi(x + B) = \sum_{r=0}^n \frac{\phi^{(r)}(x)}{[r]!} B_r = \sum_{r=0}^n \frac{\phi^{(r)}(0)}{[r]!} B_r(x).$$

$$(16.32) \quad \Delta B_n(x) = [n] x^{n-1}.$$

THEOREM 16.2. If the sequence (u) be chosen so that the series (9.1) for $\mathcal{E}(x)$ is convergent near $x = 0$ then for sufficiently small values of $|t|$ and $|x|$

$$(16.4) \quad \sum_{n=0}^{\infty} \frac{B_n t^n}{[n]!} = \frac{t}{\mathcal{E}(t) - 1}, \quad \sum_{n=0}^{\infty} \frac{B_n(x) t^n}{[n]!} = \frac{t \mathcal{E}(xt)}{\mathcal{E}(t) - 1}.$$

$$(16.5) \quad \bar{1}^r + \bar{2}^r + \dots + \bar{n}^r = \frac{B_{r+1}(\bar{n}) - B_{r+1}}{[r+1]},$$

if r is a positive integer ≥ 1 .

To prove the last written formula for example, we observe by theorem 6.1 that (16.32) implies that $B_{r+1}(\overline{s+1}) - B_{r+1}(\overline{s}) = [r+1]\overline{s^r}$, s a positive integer. On summing this equation with respect to s from 0 to $n-1$, we obtain (16.5).

THEOREM 16.3. $B_{2n} = 0$ ($n = 1, 2, 3, \dots$) when and only when

$$B_n(1-z) = (-1)^n B_n(z), \quad (n = 2, 3, \dots).$$

If moreover the series (9.1) for $\mathcal{E}(x)$ converges for some $x \neq 0$, then

$$B_{2n} = 0, \quad n \leq 1$$

when and only when (u) is normal.

The equivalences stated follow immediately from formulas (16.1), (16.2) and (16.4).

We plan to give elsewhere a detailed treatment of the basic analogues for the numbers of Euler, Genocchi, Lucas and Stirling and their associated polynomials and difference operators.

REFERENCES.

1. F. H. Jackson, *American Journal of Mathematics*, vol. 32 (1910), pp. 305-314; *Messenger of Mathematics*, vol. 39 (1910), pp. 26-28, vol. 38 (1909), pp. 57-61, 62-64; *Proceedings of the Edinburgh Mathematical Society*, vol. 22 (1904), pp. 28-39.
2. L. Euler, *Introductio in Analysis Infinitorum* (1748), chapter VII; Netto, *Combinatorik*, 2d. ed. (1927), p. 143.
3. D. H. Lehmer, *Annals of Mathematics* (2), vol. 36, no. 3, July (1935), p. 639 and references on p. 637.
4. Nörlund, *Differenzenrechnung*, Berlin (1924), chapter II.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA.

THE CONTINUOUS ITERATION OF REAL FUNCTIONS*

BY MORGAN WARD AND F. B. FULLER

1. *Continuous Iterations.* Let $E(x)$ be a real, continuous, steadily increasing function of x in the range $-\infty < a \leq x < \infty$ such that

$$(1) \quad E(x) > x, \quad (x \geq a),$$

and let $E_1(x) = E(x)$, $E_2(x) = E(E_1(x))$, . . . denote its successive iterates. In a previous note in this Bulletin, referred to hereafter as Note, one of us† has developed a simple formula for continuously iterating the function $E(x)$. We propose here to determine all continuous iterations of $E(x)$ subject to a restriction to be explained presently.

By a continuous iteration of $E(x)$ we shall understand a real function $\Theta_y(x)$ of the two real variables x and y with the following two properties

$$\begin{aligned} (i) \quad \Theta_0(x) &= x, \quad \Theta_1(x) = E(x), \quad (x \geq a). \\ (ii) \quad \Theta_{y+z}(x) &= \Theta_y(\Theta_z(x)), \quad (x \geq a, y, z \geq 0). \end{aligned}$$

The restriction which we shall impose upon the functions $\Theta_y(x)$ is the following:

(iii) $\Theta_y(a)$ is a steadily increasing continuous function of y in the range $0 \leq y \leq 1$.

2. *Prior Investigations.* The continuous iteration of real functions was discussed in detail by A. A. Bennett.‡ So far as the authors are aware, other investigators have confined their attention to the continuous iteration of analytic functions.§ The functional equation (ii) was first considered by A. Korkine,|| who

* Presented to the Society, February 29, 1936.

† Ward, *Note on the iteration of functions of one variable*, this Bulletin, vol. 40 (1934), pp. 688–690.

‡ Annals of Mathematics, (2), vol. 17 (1916), pp. 23–69.

§ See the references in the Note.

|| Bulletin des Sciences Mathématiques, (2), vol. 6 (1882), part 1, pp. 228–242.

proved formally a result equivalent to the first theorem of this paper, assuming that $\Theta_y(x)$ was differentiable with respect to y .

A complete discussion of the functional equation $E_n(x) = x$ with $x, E(x)$ real, n a positive integer, has been given by J. F. Ritt,* and W. Chayoth† has recently proved certain very general existence theorems on functional equations in the real domain.

3. THEOREM 1. *Any function Θ satisfying the conditions (i), (ii), and (iii) is continuous and steadily increasing in both x and y . Moreover for each such function $\Theta = E_y(x)$ there exists a unique, continuous, steadily increasing solution $\psi = f(x)$ of the functional equation*

$$(2) \quad \psi(x + 1) = E(\psi(x)), \quad \psi(0) = 0$$

such that‡

$$(3) \quad E_y(x) = f(f^{-1}(x) + y), \quad (x \geq 0, y \geq 0).$$

We have taken here and throughout the remainder of the paper, $a = 0$ and $E(a) = 1$ as was shown to be possible without loss of generality in the Note.

To prove this theorem, let $\Theta = E_y(x)$ be a particular function satisfying the conditions (i), (ii), and (iii). Since $E_{x+1}(0) = E(E_x(0))$, we see from (iii) that $E_x(0)$ is continuous and steadily increasing in the range $0 \leq x < \infty$.

Write $f(x)$ for $E_x(0)$. Then $f(x)$ has a unique, continuous, steadily increasing inverse $f^{-1}(x)$ in the range $0 \leq x < \infty$ such that

$$f(f^{-1}(x)) = f^{-1}(f(x)) = x, \quad f(0) = f^{-1}(0) = 0.$$

Also $f(x+y) = E_{x+y}(0) = E_y(E_x(0)) = E_y(f(x))$. Hence $f(x+1) = E(f(x))$, and $\psi = f(x)$ is a solution of (2). Then

$$E_y(x) = E_y(f\{f^{-1}(x)\}) = f(f^{-1}(x) + y),$$

* Annals of Mathematics, (2), vol. 17 (1916), pp. 113–122. See also the note by A. A. Bennett, loc. cit., p. 123.

† Monatshefte für Mathematik und Physik, vol. 39 (1932), pp. 279–288.

‡ The converse of this theorem is well known. See, for example, A. A. Bennett, Annals of Mathematics, volume cited, pp. 74–75; pp. 23–30.

which is (3). It is now evident that $E_y(x)$ is a continuous and steadily increasing function both of x and of y .

Finally, the function $f(x)$ in formula (3) is uniquely determined by $E_y(x)$. For letting $x=y=0$, and using (1), we see that $f(0)=0$. Hence $f^{-1}(0)=0$. Therefore on letting $x=0$ and $y=x$, $f(x)=E_x(0)$. The problem of determining all continuous iterations of $E(x)$ is thus reduced to the solution of the functional equation (2).

4. THEOREM 2. *Let $\theta(x)$ be a continuous function of x in the interval $0 \leq x < 1$, which increases steadily from $\theta(0)=0$ to $\theta(1-0)=1$. Then every continuous steadily increasing solution ψ of the functional equation (2) is of the form*

$$(4) \quad \psi(x) = E_{[x]}(\theta(x - [x])),$$

where $[x]$ denotes the greatest integer in x .

Conversely, for every such choice of $\theta(x)$, (4) gives a continuous steadily increasing solution of the functional equation (2).

First of all, every such increasing solution ψ of (2) tends to infinity with x . For assume that $\psi(x)$ tends to a finite limit L as $x \rightarrow \infty$. Then $\psi(x) < L$ for all finite values of x . Now by (1), $E(L) > L$. Hence, since $E(x)$ is continuous, there exists a positive number δ such that $E(L-\delta) > L$. Choose x_0 so that $\psi(x) > L-\delta$, $x \geq x_0$. Then $\psi(x+1) = E(\psi(x)) > E(L-\delta) > L$, giving a contradiction.

It follows that in the interval $0 \leq x < \alpha$, $\psi(x)$ has a unique, continuous, steadily increasing inverse $\phi = \phi(x) = \psi^{-1}(x)$ such that $\phi \rightarrow \infty$ as $x \rightarrow \infty$. This inverse is readily seen to satisfy the famous functional equation of Abel,*

$$(5) \quad \phi(E(x)) = \phi(x) + 1, \quad \phi(0) = 0.$$

For convenience, write e_n for $E_n(0)$, ($n = 0, 1, 2, \dots$). Then $e_0 = 0$, $e_1 = 1$, and since by (1), $E(x) > x$, it follows that $e_n < e_{n+1}$.

We shall now show that $e_n \rightarrow \infty$. For otherwise, e_n tends to a finite limit k , and $e_n < k$, ($n = 0, 1, 2, \dots$). Since $k > 1$, if $E_{-1}(x)$ denotes the inverse of $E(x)$, then $E_{-1}(k) = M$, where $0 < M < k$. For $k = E(E_{-1}(k)) = E(M) > M$. Hence for all sufficiently large n , $e_n > M$. But then $e_{n+1} = E(e_n) > E(M) = k$, giving a contradiction.

* Works, vol. 2, Posthumous Papers, 1881, pp. 36–39.

It follows that, given any positive value of x , we can determine an integer k such that

$$(6) \quad e_k \leq x < e_{k+1}.$$

Let x lie in the interval (6). Then from the properties of $E(x)$ and its ordinary iterates, we can write

$$x = E_k(y), \quad y = E_{-k}(x), \quad (0 \leq y < 1),$$

where $E_{-k}(x)$ denotes the inverse of $E_k(x)$ in the interval $e_k \leq x < \infty$.

Now in the interval $0 \leq x < 1$, let us write $\theta^{-1}(x)$ for $\phi(x)$. Then $\theta^{-1}(0) = 0$, and $\theta^{-1}(x)$ increases steadily and continuously as x increases, and $\theta^{-1}(1 - 0) = \lim_{x \rightarrow 1} \theta^{-1}(x) = 1$ by (5). Furthermore, the inverse of $\theta^{-1}(x)$, which we denote by $\theta(x)$, exists and has the properties stated in Theorem 2. From (5), we see that

$$\phi(x) = \phi(E_k(y)) = \phi(y) + k = \theta^{-1}(y) + k$$

or

$$(7) \quad \phi(x) = \theta^{-1}(E_{-k}(x)) + k.$$

Since $0 \leq E_{-k}(x) < 1$, we observe also that $k = [\phi]$, the greatest integer in $\phi(x)$.

To determine ψ , we need only solve (7) for x in terms of ϕ . We have

$$\begin{aligned} \phi - [\phi] &= \theta^{-1}(E_{-[\phi]}(x)), \\ \theta(\phi - [\phi]) &= E_{-[\phi]}(x), \\ x &= E_{[\phi]}(\theta(\phi - [\phi])). \end{aligned}$$

Hence*

$$(4) \quad \psi(x) = E_{[x]}(\theta(x - [x])).$$

The proof of the converse for a function θ satisfying the conditions of the theorem is almost word for word the same as in the special case $\theta(x) = x$, which has been given in full in the Note.

The function $\theta(x)$ is arbitrary save for the restrictions stated in the theorem. Once chosen, it fixes the iteration completely; it is in fact $E_x(0)$.

CALIFORNIA INSTITUTE OF TECHNOLOGY AND WHITTIER, CALIF.

* It is obvious that if $\pi(x)$ denotes a periodic function of x with period one, such that $\pi(x) = \theta(x)$, ($0 \leq x < 1$), then we can write $\psi(x) = E_{[x]}(\pi(x))$, or more concisely still, $\psi(x) = E_{[x]}(\psi(x - [x]))$, since $\psi(x - [x]) = \theta(x - [x])$.

NOTE ON DIVISIBILITY SEQUENCES

BY MORGAN WARD

1. *Introduction.* We call a sequence of rational integers

$$(u) : \quad u_1, u_2, u_3, \dots, u_n, \dots$$

a *divisibility sequence* if u_r divides u_s whenever r divides s . The divisibility sequences most frequently studied are the *linear* sequences which satisfy linear difference equations with constant, integral coefficients.* In particular, the divisibility sequence associated with a difference equation of order two is essentially one of the important functions of Lucas.† I propose here to deduce two striking properties of divisibility sequences which do not depend on the fact that the sequence is linear.

2. *Preliminary Definitions.* An integer m will be said to be a *divisor* of (u) if it divides some term of (u) , and a *prime divisor* if it is a prime. The suffix of the first term of (u) divisible by m is called the *rank of apparition* of m . If p is a prime divisor of (u) , the rank of apparition of p^a , if it exists, will be denoted by ρ_a .

If we assume that no term of (u) is zero, we can build up from (u) a set of numbers $[n, r]$, the *binomial coefficients belonging to* (u) ,‡ defined by

$$\begin{aligned} [n, r] &= 1, & (r = 0; n = 0, 1, 2, \dots), \\ [n, r] &= u_n \cdot u_{n-1} \cdots u_{n-r+1} / u_1 \cdot u_2 \cdots u_r, \\ && (r = 1, \dots, n; n = 1, 2, \dots). \end{aligned}$$

They will not in general be rational integers.

If a and b are any rational integers, we shall write as usual $a | b$ for a divides b and (a, b) for the greatest common divisor of a

* See Marshall Hall, *Divisibility sequences of the third order*, American Journal of Mathematics, vol. 58 (1936), pp. 577–584, for an account of these sequences and references to the work of Pierce, Poulet, and Lehmer.

† u_n equals the function $(\alpha^n - \beta^n)/(\alpha - \beta)$ up to a constant factor.

‡ For a systematic account of the remarkable properties of these numbers formed from any sequence (u) with no non-vanishing terms see Morgan Ward, *A calculus of sequences*, American Journal of Mathematics, vol. 58 (1936), pp. 255–266.

and b . If a^r is the highest power of a which divides b , we shall write $a^r \parallel b$.

Finally, since u_1 must divide every term of (u) , we may assume that $u_1 = 1$.

3. *Statement of Results.* A divisibility sequence will be said to have property A provided that

A. If $c = (a, b)$, then $u_c = (u_a, u_b)$, for every pair of terms u_a, u_b of (u) .

It will be said to have property B provided that

B. For every prime divisor p and every positive integer a , $u_r \equiv 0 \pmod{p^a}$ when and only when $r \equiv 0 \pmod{\rho_a}$, where ρ_a is the rank of apparition of p^a in (u) .

The results of this note may now be stated as follows.

THEOREM 1. *Property A and property B are equivalent to one another.*

THEOREM 2. *The binomial coefficients belonging to every divisibility sequence having property A or property B are all rational integers.*

Theorem 2 was proved for the Lucas function by Lucas himself,* and for a more general type of linear divisibility sequence by T. A. Pierce.†

4. *Proof of First Theorem.* Assume that the divisibility sequence (u) has property A, and let ρ_a be the rank of apparition of p^a , where p is any prime divisor of (u) . Suppose that $u_r \equiv 0 \pmod{p^a}$. Then if $c = (r, \rho_a)$, $(u_r, u_{\rho_a}) = u_c$ by property A. Therefore since $u_r \equiv u_{\rho_a} \equiv 0 \pmod{p^a}$, $u_c \equiv 0 \pmod{p^a}$. Therefore $c \geq \rho_a$. But c divides ρ_a . Therefore $c = \rho_a$ so that ρ_a divides r . Since (u) is a divisibility sequence, if ρ_a divides r , $u_r \equiv 0 \pmod{p^a}$. Therefore the sequence has property B.

Conversely, assume that (u) has property B. Let u_a and u_b be any two terms of (u) , and let p be any common prime divisor of u_a and u_b . Suppose that $p^m \parallel u_a$ and $p^n \parallel u_b$. Then if l is the smallest of the integers m and n , it suffices to show that $p^l \mid u_c$, where $c = (a, b)$. For since $c \mid a$ and $c \mid b$, $u_c \mid u_a$ and $u_c \mid u_b$, so that

* Lucas, Nouvelle Correspondance Mathématique, vol. 4 (1878), pp. 1–8.
Dickson's *History*, vol. 1, p. 349.

† Annals of Mathematics, (2), vol. 18 (1916–17), p. 56.

$u_c \mid (u_a, u_b)$. But $p^l \parallel (u_a, u_b)$. Therefore if $p^l \mid u_c$ for every common prime divisor p of u_a and u_b , we have $(u_a, u_b) \mid u_c$, so that $(u_a, u_b) = u_c$, and property A follows.

Now let ρ_m, ρ_n be the ranks of apparition of p^m and p^n , respectively. Without loss of generality we may assume that $m \geq n$, so that $l = n$. Since property B holds, $\rho_m \mid a, \rho_n \mid b$ and $\rho_n \mid \rho_m$. Hence $\rho_n \mid a$ and $\rho_n \mid b$, so that $\rho_n \mid c = (a, b)$. But then $u_{\rho_n} \mid u_c$, so that $p^l = p^n \mid u_c$.

5. *Proof of Second Theorem.* It suffices to show that $[n, r]$ is an integer modulo p for every prime divisor p of (u) when (u) has property B. If we let $[0]! = 1$, then $[s]! = u_1 u_2 \cdots u_s$, ($s \geq 1$), $[n, r] = [n]/[n-r][r]!$.

Now the highest power of p dividing $[n]!$ is clearly $\sum_{s=1}^{\infty} [n/\rho_s]$, where as usual $[a/b]$ denotes the greatest integer in a/b . (If p^s does not divide (u) , then neither does p^t , ($t \geq s$), and we break off the sum after $s-1$ terms. Since $\rho_s \rightarrow \infty$ with s if every power of p divides the sequence, the sum is finite in every case.)

It therefore suffices to show that

$$\sum_{s=1}^{\infty} \left[\frac{n}{\rho_s} \right] \geq \sum_{s=1}^{\infty} \left[\frac{n-r}{\rho_s} \right] + \sum_{s=1}^{\infty} \left[\frac{r}{\rho_s} \right],$$

and this follows as in the ordinary case when $u_n = n$ from the elementary inequality

$$\left[\frac{n+m}{\rho} \right] \geq \left[\frac{n}{\rho} \right] + \left[\frac{m}{\rho} \right].$$

Chapter 11

1937

LINEAR DIVISIBILITY SEQUENCES*

BY
MORGAN WARD

I. INTRODUCTION

1. A sequence of rational integers

(u): $u_0, u_1, \dots, u_n, \dots$

is called a *divisibility sequence* if u_n divides u_m whenever n divides m . (u) is *linear*† if it satisfies a linear difference equation with integral coefficients and *normal* if $u_0=0$, $u_1=1$. Marshall Hall has shown that a linear divisibility sequence is usually normal [2]. If

$$(1.1) \quad f(x) = x^k - c_1 x^{k-1} - \dots - c_k, \quad c_1, \dots, c_k \text{ integers,}$$

is the polynomial associated with the difference equation of lowest order which (u) satisfies, (u) is said to be of *order* k and to *belong to its characteristic polynomial* $f(x)$.

An integer dividing every term of (u) beyond a certain point is called a *null divisor* of (u) [3]. If (u) has no null divisors save ± 1 , it is said to be *primary*.

If u_s is any fixed non-vanishing term of (u), the sequence

$$u_0/u_s, u_s/u_s, u_{2s}/u_s, \dots, u_{ns}/u_s, \dots$$

is called a *subsequence* of (u). The various subsequences of (u) are themselves normal linear divisibility sequences of order $\leq k$.

2. The object of this paper is to prove the following results:

Let the characteristic polynomial of the linear divisibility sequence (u) have no repeated roots, and let its coefficients be relatively prime. Then:

I. *If (u) is primary and if q is any large prime number,*

$$(2.1) \quad u_q^\sigma \equiv 1 \pmod{q},$$

where σ is the least common multiple of 1, 2, 3, \dots , k .

II. *If (u) is not primary it always contains an infinity of subsequences which are primary. Furthermore the characteristic polynomials of such subsequences satisfy the hypotheses imposed above upon the polynomial (1.1).*

* Presented to the Society, June 18, 1936; received by the editors May 5, 1936.

† T. A. Pierce appears to have been the first to discuss sequences of order greater than two [1]. (Numbers in square brackets refer to the bibliography at the end of the paper.)

III. There exists a rational number

$$B = B(u) = B(u_0, u_1, \dots, u_{k-1}; c_1, \dots, c_k) = \frac{p}{q}, \quad (p, q) = 1$$

such that

- (i) if p is a prime number dividing neither the numerator p nor the denominator q of B , then the rank of apparition* of p in the sequence (u) is the restricted period* of (u) modulo p ;
- (ii) the prime factors of the denominator of B all divide the discriminant of the polynomial to which (u) belongs;
- (iii) the numerator of B can never vanish if the Galois group of $f(x)$ is alternating or symmetric.†

II. PROOF OF FIRST RESULT

3. Given any modulus m , the least period of (u) modulo m is called its characteristic number and the number of non-periodic terms in (u) modulo m its numeric. The reader will be assumed to be familiar with my previous paper in these Transactions [4] (referred to hereafter as T) devoted to the determination of these numbers.

Henceforth let (u) be a normal linear divisibility sequence of order k , and let D denote the discriminant of its characteristic polynomial. We assume:

$$(3.1) \quad D \neq 0.$$

LEMMA 3.1 [4]. *If $\nmid (q, D) = 1$, q a prime, and if σ is the least common multiple of $2, 3, \dots, k$, then (u) admits the period $q^\sigma - 1$ modulo q .*

THEOREM 3.1. *If (u) is a linear divisibility sequence of order k and q a prime such that $u_q \equiv 0 \pmod{q}$, then either q divides D or q divides c_k .*

Assume that $\nmid q | u_q$, q a prime. The assumption $(q, c_k) = (q, D) = 1$ then yields a contradiction. For if $(q, c_k) = 1$, (u) is purely periodic modulo q [5]. And if $(q, D) = 1$, (u) admits the period $q^\sigma - 1$ modulo q . Determine positive integers x and y such that $xq = y(q^\sigma - 1) + 1$. Then $u_{xq} \equiv u_1 \equiv 1 \pmod{q}$. But $q | u_q$ and $u_q | u_{xq}$.

The following lemma is a direct consequence of Theorem 3.1.

* The rank of apparition of p is the index ρ of the first term of (u) excluding u_0 which divides $u_\tau \equiv 0 \pmod{p}$; $u_n \not\equiv 0 \pmod{p}$, $0 < n < \rho$. The restricted period [5] of (u) modulo p is the least positive integer τ such that $u_{n+\tau} \equiv cu_n \pmod{p}$, $n = 0, 1, 2, \dots, c$ an integer. ρ always divides τ [2].

† It is unknown whether divisibility sequences exist whose characteristic polynomial is restricted as in (iii). No such sequences exist when $k = 3$ [2].

‡ If a, b, c, \dots are rational integers, we write as usual (a, b, c, \dots) for the greatest common divisor of a, b, c, \dots , and $a | b$ for a divides b .

LEMMA 3.2. *There exists a rational integer q_0 such that*

$$(3.2) \quad u_q \not\equiv 0 \pmod{q}, \quad q \text{ a prime} \geq q_0.$$

LEMMA 3.3 [4]. *For any prime p , $p^k(p^\sigma - 1)$ is a period of (u) modulo p .*

LEMMA 3.4 [4]. *For any prime p , the numeric of (u) modulo p is less than or equal to k .*

THEOREM 3.2. *If p is a prime dividing a term u_q of the divisibility sequence (u) with a sufficiently large prime index q , then either*

$$(3.3) \quad p^\sigma \equiv 1 \pmod{q}$$

or else (u) is a null sequence modulo p .

Choose a prime $q > k$ and q_0 of (3.2), and assume that $u_q \equiv 0 \pmod{p}$, p a prime. By (3.2), $p \neq q$. Hence if $(p^\sigma - 1, q) = 1$, for each positive integer r there exist positive integers x, y, z such that

$$(3.4) \quad xq + yp^k(p^\sigma - 1) = r + zp^k(p^\sigma - 1).$$

By Lemma 3.3, $p^k(p^\sigma - 1)$ is a period of (u) modulo p . Therefore if $r > k$, (3.4) and Lemma 3.4 give $u_{xq} \equiv u_r \pmod{p}$. Since $p | u_q$ and $u_q | u_{xq}$, $u_r \equiv 0 \pmod{p}$ so that (u) is a null sequence modulo p .

THEOREM 3.3. *If the linear divisibility sequence (u) is primary, and if k is its order and σ the least common multiple of the numbers $2, 3, \dots, k$, then for all sufficiently large prime indices q we have*

$$(2.1) \quad u_q^\sigma \equiv 1 \pmod{q}.$$

Choose the prime $q > k$ and q_0 of (3.2), and let the factorization of u_q be $u_q = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$. Since (u) is assumed primary none of the primes p_i are null divisors. Therefore Theorem 3.2, $p_i^\sigma \equiv 1 \pmod{q}$, so that

$$p_i^{\sigma e_i} \equiv 1 \pmod{q}, \quad (i = 1, 2, \dots, t).$$

On multiplying these t congruences together, we obtain (2.1), and our first result is proved.

III. PROOF OF SECOND RESULT

4. We assume that (u) is a normal linear divisibility sequence for which

$$(4.1) \quad (c_1, c_2, \dots, c_k) = 1.$$

A *proper* null divisor of a linear sequence is one which divides neither its initial terms nor the coefficients of its recursion. Any other null divisor is called *trivial*. (u) obviously has no trivial null divisors.

THEOREM 4.1. *No subsequence of (u) has trivial null divisors.*

LEMMA 4.1 (Schatanovskis Principle) [6, 7, 8]. *If $\Phi(x_1, x_2, \dots, x_k)$ is an integral symmetric function of the arguments x_1, \dots, x_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

$$\Phi(\alpha_1, \alpha_2, \dots, \alpha_k) \equiv \Phi(\gamma_1, \gamma_2, \dots, \gamma_k) \pmod{m}.$$

LEMMA 4.2. *Let*

$$f^{(s)}(x) = x^k - d_1 x^{k-1} - \cdots - d_k$$

be the polynomial whose roots are the s th powers of the roots of $f(x)$, and p a prime number. Then if t is any positive integer $\leq k$, (A) $p \mid (c_k, c_{k-1}, \dots, c_{k-t+1})$ when and only when (B) $p \mid (d_k, d_{k-1}, \dots, d_{k-t+1})$.

Assume that (A) holds. Then

$$f(x) \equiv g(x) = x^{k-t}(x^t - c_1 x^{t-1} - \cdots - c_{k-t}) \pmod{p}.$$

Let the k roots of $g(x) = 0$ be $\gamma_1, \gamma_2, \dots, \gamma_t; \gamma_{t+1} = \gamma_{t+2} = \cdots = \gamma_k = 0$. If the roots of $f(x) = 0$ are $\alpha_1, \alpha_2, \dots, \alpha_k$, then $d_i = \Phi(\alpha_1, \alpha_2, \dots, \alpha_k)$, where Φ is a symmetric polynomial in its arguments with rational integral coefficients. Hence by the preceding lemma

$$d_i \equiv \Phi(\gamma_1, \gamma_2, \dots, \gamma_k) \pmod{p}.$$

But if $g^{(s)}(x) = x^k - e_1 x^{k-1} - \cdots - e_k$ is the equation whose roots are the s th powers of the roots of $g(x) = 0$, then

$$e_i = \Phi(\gamma_1, \gamma_2, \dots, \gamma_k) = \sum \gamma_1^s \gamma_2^s \cdots \gamma_i^s = 0 \text{ if } i > k - t.$$

Hence $d_i \equiv 0 \pmod{p}$ if $i > k - t$, so that (B) follows.

To prove the converse, it suffices to show that (A) and $c_{k-t} \not\equiv 0 \pmod{p}$ imply that $d_{k-t} \not\equiv 0 \pmod{p}$. But by what precedes,

$$d_{k-t} \equiv \sum (\gamma_1 \gamma_2 \cdots \gamma_t)^s \equiv (\gamma_1 \gamma_2 \cdots \gamma_t)^s \equiv c_{k-t}^s \pmod{p}.$$

Proof of Theorem 4.1. With the notation of Lemma 4.2, any subsequence $(v) : v_n = u_{ns}/u_s$ of (u) is normal, so that the only possible trivial null divisors of (v) are common divisors of d_1, d_2, \dots, d_k . On taking $t = k$ in Lemma 4.2, we see that if $(c_1, c_2, \dots, c_k) = 1$ then $(d_1, d_2, \dots, d_k) = 1$.

5. We begin our discussion of the proper null divisors of (u) by restating some properties of linear sequences used in T. Let

$$f_0(x) = 0, \quad f_r(x) = x^r - c_1 x^{r-1} - \cdots - c_r, \quad (r = 1, 2, \dots, k).$$

The polynomial

$$(5.1) \quad u(x) = u_0 f_{k-1}(x) + u_1 f_{k-2}(x) + \cdots + u_{k-1} f_0(x)$$

is called the *generator* of the sequence (u) .* If furthermore

$$(5.2) \quad \Delta(u) = \begin{vmatrix} u_0, & u_1, & \cdots, & u_{k-1} \\ u_1, & u_2, & \cdots, & u_k \\ \vdots & \vdots & & \vdots \\ u_{k-1}, & u_k, & \cdots, & u_{2k-2} \end{vmatrix},$$

then

$$(5.3) \quad \Delta(u) = (-1)^{k(k-1)/2} \operatorname{Res} \{u(x), f(x)\} = \beta_1 \beta_2 \cdots \beta_k D,$$

where $u_n = \beta_1 \alpha_1^n + \cdots + \beta_k \alpha_k^n$ and $\alpha_1, \dots, \alpha_k$ are the roots of $f(x)$. Since (u) is of order k and $D \neq 0$, $\Delta(u) \neq 0$.

Consider next the $k+1$ greatest common divisors

$$\begin{aligned} e_0 &= (u_0, u_1, u_2, \cdots, u_{k-1}) \\ e_1 &= (c_k, u_1, u_2, \cdots, u_{k-1}) \\ e_2 &= (c_k, c_{k-1}, u_2, \cdots, u_{k-1}) \\ &\cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ e_{k-1} &= (c_k, c_{k-1}, c_{k-2}, \cdots, u_{k-1}) \\ e_k &= (c_k, c_{k-1}, c_{k-2}, \cdots, c_1). \end{aligned}$$

Then

$$e_0 = e_1 = e_k = 1.$$

The following lemma easily follows from formula (5.1) and the results of part IV of T.

LEMMA 5.1. *Necessary and sufficient conditions that a linear sequence of order k be primary are that the $k+1$ greatest common divisors e_i be all equal to unity.*

THEOREM 5.1. *If the prime p is a null divisor of the normal linear divisibility sequence (u) , then p divides both $\Delta(u)$ and the discriminant D of the characteristic polynomial $f(x)$ of (u) .*

It is easily shown that every such p must divide one or the other of the numbers e_i . Since $e_k = 1$, $p | u_{k-1}$. Hence $p | u_k, p | u_{k+1}, \dots$ by Lemma 3.4.

* We have the identity $u(x)/f(x) = \sum_0^\infty u_n/x^{n+1}$ for $|x|$ large. See T, p. 606, and [3].

Hence $p|\Delta(u)$ by formula (5.2). Since $e_0 = e_1 = 1$, $p|c_k$ and $p|c_{k-1}$. Hence $x=0$ is a multiple root of the congruence $f(x) \equiv 0 \pmod{p}$ and $p|D$.

As a corollary, we have

LEMMA 5.2. *A sufficient condition that the divisibility sequence (u) be primary is that D and $\Delta(u)$ be co-prime.*

If p is a prime proper null divisor of (u) , the exponent of the highest power of p which is a null divisor of (u) is called the *index* of p in (u) [3].

LEMMA 5.3 [3]. *Let (u) be a linear sequence for which (4.1) holds. Then the index of any prime null divisor p is $\leq r$, where p^r is the highest power of p dividing $\Delta(u)$.*

THEOREM 5.2. *A subsequence of a normal linear divisibility sequence can have no prime null divisor which is not a possible null divisor of (u) itself.*

Every prime null divisor of (u) must divide c_k in (1.1) [5]. Let (v) be any subsequence of (u) . By Theorem 4.1, (v) can have only proper null divisors. Hence any prime null divisor of (v) must divide the constant term d_k of the polynomial to which (v) belongs. But obviously d_k divides some power of c_k .

6. Let $f^{(s)}(x) = (x - \alpha_1^s) \cdots (x - \alpha_k^s)$ be the polynomial whose roots are the s th powers of the roots of $f(x)$, and let $D^{(s)}$ be its discriminant. $D^{(s)}/D$ is clearly an integer.

THEOREM 6.1. *The integer s may be chosen in an infinite number of ways so that $D^{(s)}/D$ is prime to D .*

Let p be any prime factor of D , \mathfrak{F} the Galois field of $f(x)$, and \mathfrak{p} a prime ideal factor of p in \mathfrak{F} . Then since $D^{1/2} = \prod_{i < j} (\alpha_i - \alpha_j)$, $p|D$ only when $\alpha_i - \alpha_j \equiv 0 \pmod{\mathfrak{p}}$ for some values of the subscripts i and j .

Now

$$\left(\frac{D^{(s)}}{D}\right)^{1/2} = \prod_{i < j} \frac{\alpha_i^s - \alpha_j^s}{\alpha_i - \alpha_j} \quad \text{and} \quad \frac{\alpha_i^s - \alpha_j^s}{\alpha_i - \alpha_j} \equiv s \pmod{[\alpha_i - \alpha_j]}. *$$

Hence if $\alpha_i - \alpha_j \equiv 0 \pmod{\mathfrak{p}}$, then $\alpha_i^s - \alpha_j^s / (\alpha_i - \alpha_j) \equiv 0 \pmod{\mathfrak{p}}$ if and only if $s \equiv 0 \pmod{\mathfrak{p}}$; that is, if and only if $s \equiv 0 \pmod{p}$. Choose s prime to D . Then if $D^{(s)}/D$ and D have a common factor, and hence a common prime factor p , we must have for some k and l

$$(6.1) \quad \alpha_k^s \equiv \alpha_l^s \pmod{\mathfrak{p}},$$

$$(6.11) \quad \alpha_k \not\equiv \alpha_l \pmod{\mathfrak{p}},$$

where $\mathfrak{p}|p$. If both (6.1) and (6.11) hold, then

* The square bracket denotes a principal ideal.

$$(6.2) \quad (\alpha_k, \mathfrak{p}) = (\alpha_l, \mathfrak{p}) = (\alpha_k - \alpha_l, \mathfrak{p}) = \mathfrak{o},$$

where \mathfrak{o} as usual is the unit ideal of \mathfrak{F} .

Now for each pair of distinct roots α_i, α_j of $f(x)$ for which $(\alpha_i, \mathfrak{p}) = (\alpha_j, \mathfrak{p}) = (\alpha_i - \alpha_j, \mathfrak{p}) = \mathfrak{o}$, let s_{ij} be the least positive integer y such that

$$(6.3) \quad \alpha_i^y \equiv \alpha_j^y \pmod{\mathfrak{p}}.$$

Then s_{ij} divides every other such y , and in particular the number $N(\mathfrak{p}) - 1 = p^t - 1$. Here $t \leq k!$, the maximum possible degree of \mathfrak{F} .

Let m_p be the least common multiple of the numbers $p-1, p^2-1, \dots, p^{k!}-1$ and if D has in all k distinct prime factors p_1, p_2, \dots, p_k let M be the least common multiple of $m_{p_1}, m_{p_2}, \dots, m_{p_k}$. Then if s is chosen prime to both M and D (and this choice can be made in an infinity of ways), $D^{(s)}/D$ is prime to D .

For if $(s, D) = 1$ and $(D^{(s)}/D, D) \neq 1$, (6.1) holds. Then $s_{kl} | s$. Since $(s, M) = 1$ and $s_{kl} | M$, $s_{kl} = 1$ contradicting (6.11).

7. As in §6, let p_1, \dots, p_k be the distinct prime factors of D . By Theorems 4.5, 5.1 and Lemma 5.4, these primes are the only possible prime null divisors of (u) and its subsequences. Write

$$\Delta(u) = p_1^{r_1} \cdots p_k^{r_k} q, \quad (q, D) = 1, \quad r_i \geq 0,$$

and let θ_i be the index of p_i in (u) , where if p_i is not a null divisor, $\theta_i = 0$. By Lemma 5.3, $0 \leq \theta_i \leq r_i$, ($i = 1, 2, \dots, k$).

Now if r is the largest of r_1, r_2, \dots, r_k , the numeric of p^{θ_i} is always less than kR^r . Choose $s > kR^r$ as in Theorem 6.1, and let (v) be the subsequence of (u) with general term $v_n = u_{ns}/u_s$ belonging to the polynomial $f^{(s)}(x)$. As in Theorem 6.1, let the discriminant of $f^{(s)}(x)$ be $D^{(s)}$. Then since $u_{ns} = \beta_1 \alpha_1^{n_s} + \cdots + \beta_k \alpha_k^{n_s}$, we have by formula (5.3),

$$(7.1) \quad \Delta(v) = \frac{\Delta(u)}{u_s^k} \frac{D^{(s)}}{D}.$$

Now $u_s \equiv 0 \pmod{p_i^{\theta_i}}$ and $(p_i, D^{(s)}/D) = 1$. Hence since $\Delta(v)$ is an integer, $\Delta(u) \equiv 0 \pmod{p_i^{k\theta_i}}$. Therefore $r_i \geq k\theta_i$. If $\Delta(v) = p_1^{r'_1} \cdots p_k^{r'_k} q'$, $(q', D) = 1$, then $r'_i = r_i - k\theta_i$. Therefore

$$(7.2) \quad r'_i < r_i \text{ if } \theta_i > 0; \quad r'_i = r_i \text{ if } \theta_i = 0.$$

8. We now prove our second result indirectly. Suppose that the result is false. Then in any infinite set of normal divisibility sequences

$$\mathfrak{S}: \quad (u^{(1)}) = (u), (u^{(2)}), (u^{(3)}), \dots, (u^{(m)}), (u^{(m+1)}), \dots,$$

such that each sequence is a subsequence of its immediate predecessor, there must occur an infinity of non-primary sequences. Therefore there must exist a prime p dividing D which is a null divisor of an infinite number of the sequences $(u^{(m)})$. The general term of $(u^{(m+1)})$ is of the form $u_n^{(m+1)} = u_{ns_m}^{(m)} / u_{s_m}^{(m)}$, where the integer s_m specifies the particular subsequence of $(u^{(m)})$ selected. Consider now a set \mathfrak{S} in which each $u^{(m)}$ satisfies the conditions imposed upon s in §6.

The considerations of the preceding section carry over to the relationship between $(u^{(m)})$ and $(u^{(m+1)})$. With an obvious extension of notation, let $\theta^{(m)}$ denote the index of p in $(u^{(m)})$ and p^{r_m} and $p^{r_{m+1}}$ the highest powers of p dividing $\Delta(u^{(m)})$ and $\Delta(u^{(m+1)})$. Then as in (7.2)

$$(8.1) \quad r_{m+1} < r_m \text{ if } \theta^{(m)} > 0; \quad r_{m+1} = r_m \text{ if } \theta^{(m)} = 0.$$

By our hypothesis, an infinite number of the $\theta^{(m)}$ are positive. But then (8.1) leads to an absurdity; for obviously $r = r_1 \geq r_2 \geq r_3 \geq \dots \geq 0$.

IV. PROOF OF THIRD RESULT

9. We assume as in the previous proofs that $D \neq 0$. In the Galois field \mathfrak{F} of $f(x)$, a rational prime p which does not divide D remains unramified [9]. Accordingly the decomposition of p into prime ideal factors in \mathfrak{F} is of the form

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_l,$$

where the \mathfrak{p} are all distinct.

Let σ_i be the least positive integer n such that

$$(9.1) \quad \alpha_1^n \equiv \alpha_2^n \equiv \cdots \equiv \alpha_k^n \pmod{\mathfrak{p}_i} \quad (i = 1, \dots, l).$$

The restricted period τ of (u) modulo p is defined as the least value of n such that

$$u_{n+m} \equiv au_n \pmod{p} \quad (m = 0, 1, 2, \dots),$$

where a is some rational integer [5]. If p is prime to $\Delta(u)$, τ may be equally defined as the least positive integer n such that we have in \mathfrak{F}

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

The following lemma therefore follows.

LEMMA 9.1. *If p is a prime dividing neither $\Delta(u)$ nor D , then the restricted period τ of (u) modulo p is the least common multiple of the numbers $\sigma_1, \sigma_2, \dots, \sigma_l$ associated with the congruence (9.1) above.*

10. Since $u_n = \beta_1 \alpha_1 + \cdots + \beta_k \alpha_k^n$ and the α_i are distinct,

$$(10.1) \quad \beta_i = u(\alpha_i) / f'(\alpha_i) \neq 0, \quad (i = 1, \dots, k).$$

Here $u(x)$ is the generator of the sequence (u) and $f'(x)$ the derivative of $f(x)$. Since $D = f'(\alpha_1)f'(\alpha_2) \cdots f'(\alpha_k)$, every prime ideal factor of the denominators of the β_i divides D . Let p be a rational prime. Since $\Delta(u) = \beta_1\beta_2 \cdots \beta_k D = u(\alpha_1)u(\alpha_2) \cdots u(\alpha_k)$ we can state

LEMMA 10.1. *If $(p, D) = (p, \beta_1\beta_2 \cdots \beta_k) = 1$, then $(p, \Delta(u)) = 1$. Conversely if $(p, \Delta(u)) = (p, D) = 1$, then $(p, \beta_1\beta_2 \cdots \beta_k) = 1$, p a rational prime.*

Form the k sets of sums of the β taken $1, 2, \dots, k$ at a time:

$$(10.2) \quad \beta_1 + \beta_2 + \cdots + \beta_i, \dots, \beta_{k-i+1} + \beta_{k-i+2} + \cdots + \beta_k,$$

where ($i = 1, 2, \dots, k$), and each set contains ζC_i summands, not necessarily all distinct. Then take the symmetric products over each set

$$B_i = \prod (\beta_1 + \beta_2 + \cdots + \beta_i) \quad (i = 1, 2, \dots, k; B_k = 0).$$

Finally let $B = B(u) = B_1B_2 \cdots B_{k-1}$. Then B is a rational number of the form p/q , where p and q are integers, co-prime if $B \neq 0$ and the only primes dividing q are divisors of D .

THEOREM 10.1. *If a prime p divides neither numerator nor denominator of B , its rank of apparition is the restricted period of (u) modulo p .*

By Lemma 10.1 any such prime p satisfies the hypothesis of Lemma 9.1. Let \mathfrak{p} be any prime ideal factor of p , and ρ the rank of apparition of p . Since $p|u_\rho$ implies that $p|u_{n\rho}$,

$$(10.3) \quad \beta_1\alpha_1^{n\rho} + \beta_2\alpha_2^{n\rho} + \cdots + \beta_k\alpha_k^{n\rho} \equiv 0 \pmod{\mathfrak{p}} \quad (n = 0, 1, \dots, k-1).$$

Since the β_i are integers modulo \mathfrak{p} and prime to \mathfrak{p} , the determinant of this set of congruences is divisible by \mathfrak{p} . But this determinant is the difference product of the numbers $\alpha_1^\rho, \alpha_2^\rho, \dots, \alpha_k^\rho$. Hence these numbers are not all distinct modulo p . I say that

$$(10.4) \quad \alpha_1^\rho \equiv \alpha_2^\rho \equiv \cdots \equiv \alpha_k^\rho \pmod{\mathfrak{p}}.$$

Otherwise the numbers can be grouped into two or more sets:

$$\begin{aligned} \alpha_{i_1}^\rho &\equiv \alpha_{i_2}^\rho \equiv \cdots \equiv \alpha_{i_s}^\rho \equiv \zeta_1 \pmod{\mathfrak{p}} \\ &\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\ \alpha_{j_1}^\rho &\equiv \alpha_{j_2}^\rho \equiv \cdots \equiv \alpha_{j_t}^\rho \equiv \zeta_m \pmod{\mathfrak{p}} \end{aligned}$$

such that the ζ are all distinct modulo p . The congruences (10.3) can then be replaced by

$$\beta_1'\zeta_1^n + \beta_2'\zeta_2^n + \cdots + \beta_m'\zeta_m^n \equiv 0 \pmod{\mathfrak{p}},$$

where the β' occur in the sets (10.2) of sums of β 's. The determinant of the first m of these congruences as the difference product of the ζ is prime to p . Thus $\beta'_1 \equiv \beta'_2 \equiv \cdots \equiv \beta'_m \equiv 0 \pmod{p}$, so that $p \mid B$, contrary to hypothesis.

From (10.4) and the definition of the numbers σ in §9, we see that $\sigma \mid \rho$. Since this argument applies to all of the prime ideal factors of p , the least common multiple of $\sigma_1, \dots, \sigma_l$ divides ρ . That is, by Lemma 9.1, $\tau \mid \rho$. But ρ always divides $\tau[2]$. Hence $\rho = \tau$.

LEMMA 10.1. *If the number $B = B(u)$ is not zero, the rank of apparition of all save a finite number of primes in (u) is their restricted period.*

11. We now prove

THEOREM 11.1. *A sufficient condition that the number B be not zero is that the group of the characteristic polynomial of (u) be either alternating or symmetric.*

If B vanishes, one of the numbers of the set (10.2) vanishes. With a proper choice of notation we may assume that*

$$(11.1) \quad \beta_1 + \beta_2 + \cdots + \beta_i = 0, \quad (k/2 \leq i \leq k).$$

We may also assume that $k > 4$, as the cases $k = 2, 3, 4$ may be easily discussed directly (see next theorem). Hence $i \geq 3$.

If we represent the Galois group \mathfrak{G} of $f(x)$ as a permutation group upon the k roots $\alpha_1, \dots, \alpha_k$, then formula (10.1) shows that any permutation of the α induces the corresponding permutation upon the β . If \mathfrak{G} is alternating or symmetric, it contains the permutation $S = (\alpha_1 \alpha_{i+1})(\alpha_2 \alpha_3)$. On applying S to (11.1), we obtain $\beta_{i+1} + \beta_2 + \beta_3 + \cdots + \beta_i = 0$. Hence $\beta_1 = \beta_{i+1}$. Similarly, $\beta_2 = \beta_{i+1}, \dots, \beta_i = \beta_{i+1}$. Hence $\beta_{i+1} = 0$ contrary to (10.1).

The following result is proved by similar reasoning.

THEOREM 11.2. *For low orders of (u) , sufficient conditions that $B(u) \neq 0$ are as follows:*

<i>Order of (u)</i>	<i>Condition of Galois group or characteristic polynomial</i>
2, 3	<i>none</i>
4	<i>order of group divisible by 3</i>
5	<i>$f(x)$ irreducible, or product of an irreducible quartic and linear factor</i>
6, 7	<i>group transitive and primitive.</i>

* It will be recalled that $\beta_1 + \beta_2 + \cdots + \beta_k = u_0 = 0$.

REFERENCES

1. Annals of Mathematics, (2), vol. 18 (1916–17), pp. 51–64.
2. American Journal of Mathematics, vol. 58 (1936), pp. 577–584.
3. Duke Mathematical Journal, vol. 2 (1936), pp. 472–476.
4. These Transactions, vol. 35 (1933), pp. 600–628.
5. R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372.
6. Bulletin de la Sciences Physiques Mathématiques de Kazan, (2), vol. 12 (1902), pp. 33–49.

(In Russian.)

7. S. Lubelski, Crelle's Journal, vol. 102 (1930), pp. 66–67.
8. S. Lubelski, Prace Matematyczno-Fizyczne, vol. 43 (1936), p. 214.
9. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Works, vol. 1, p. 85, Theorem 31; p. 144, Theorem 85.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

ARITHMETIC FUNCTIONS ON RINGS

BY MORGAN WARD

(Received September 1, 1936)

I. INTRODUCTION

1. The classic arithmetic properties of the Lucas^[1]¹ function

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad \alpha + \beta \quad \alpha\beta \quad \text{rational integers,}$$

can be shown to depend ultimately upon its periodicity to any integral modulus and its divisibility property: u_n divides u_m if n divides m . While the first property extends to any recurring series of integers^{[2], [3], [4]} and the second may be similarly generalized,^{[5], [6], [7]} the divisibility property is shared by numerous functions bearing no evident relation to recurring series, such as the totient function and its generalizations^[8] and the polynomials γ_n of Halphen^[9] associated with the rational multiplication of the Weierstrass \wp and σ functions.

I show here that a much more extensive generalization is possible which not only reveals inner connections between the arithmetical properties of the Lucas function, but also appears to be of some independent interest.

The generalization consists in systematically developing the divisibility properties and modular periodicity of a function $y = \phi_x$ where x lies in an abstract commutative ring² while y lies in a structure³ (usually another ring).

2. Let \mathfrak{o} be a commutative ring, Σ a structure. We assume that to each element x of \mathfrak{o} there corresponds a unique element

$$X = \phi(x) = \phi_x$$

of Σ . In the phraseology of general analysis, we call ϕ a *function on \mathfrak{o} to Σ* . ϕ_a, ϕ_b are *values* of ϕ , a, b specific elements of \mathfrak{o} . We call ϕ *arithmetic* if ϕ_a divides ϕ_b in Σ whenever a divides b in \mathfrak{o} .

If \mathfrak{o} and Σ are both the ring of rational integers, and $\phi_{-n} = -\phi_n$, an arithmetic function is equivalent to M. Hall's^[6] divisibility sequence.⁴ If \mathfrak{o} itself is a structure, say a principal ideal ring, any homomorphism between \mathfrak{o} and

¹ The [1] refers to the list of references concluding this paper.

² The Lucas function is brought within the scope of this generalization by letting $u_n = -u_n$.

³ We use the term recently introduced by O. Ore^[10] in these Annals. Equivalent terms are dual group, lattice.

⁴ See the references in Hall^[6] for earlier work on these sequences.

the values of ϕ in Σ with respect to cross-cut or union (O. Ore^[10] pp. 416–419) defines an arithmetic function.⁵

3. We use the following notation: $\tilde{\sigma}$ denotes the structure of all ideals of $\mathfrak{o}, a, \dots, z$ elements of $\mathfrak{o}, \mathfrak{a}, \dots, \mathfrak{z}$ ideals of $\mathfrak{o}, (a), \dots, (z)$ principal ideals. We use $x | y, \mathfrak{x} \supseteq \mathfrak{y}, \mathfrak{y} \subseteq \mathfrak{x}$ for division in \mathfrak{o} and $\tilde{\sigma}, xy, \mathfrak{xy}$ for product, and $(\mathfrak{x}, \mathfrak{y}), [\mathfrak{x}, \mathfrak{y}]$ for union and cross-cut respectively.⁶

Corresponding entities in Σ are denoted by capital letters. We use A, \dots, Z for values of ϕ in Σ . These are on occasion imbedded in a ring \mathfrak{Q} . Σ then denotes the structure of all ideals of \mathfrak{Q} . We use $\mathfrak{A}, \dots, \mathfrak{Z}$ for elements of Σ and write $\mathfrak{X} \supseteq \mathfrak{Y}, \mathfrak{Y} \subseteq \mathfrak{X}$ for \mathfrak{X} divides $\mathfrak{Y}, (\mathfrak{X}, \mathfrak{Y}), [\mathfrak{X}, \mathfrak{Y}]$ for union and cross-cut. If \mathfrak{X} divides $X = \phi_x$, we write $X \equiv 0 \pmod{\mathfrak{X}}$ even when the X are not imbedded in a ring.

Ordinary Greek letters ϕ, ρ, μ, τ stand for functions.

4. Following Ore,^[10] we define the structure Σ by means of its division relation \supset and not by postulates on the cross-cut and union.

(4.1) $\mathfrak{X} \supset \mathfrak{Y}$; if $\mathfrak{X} \supset \mathfrak{Y} \supset \mathfrak{Z}$ then $\mathfrak{X} \supset \mathfrak{Z}$. $\mathfrak{X} = \mathfrak{Y}$ if and only if $\mathfrak{X} \supset \mathfrak{Y}$ and $\mathfrak{Y} \supset \mathfrak{X}$. We write $\mathfrak{X} \supset \mathfrak{Y}$ or $\mathfrak{Y} \subseteq \mathfrak{X}$ if $\mathfrak{X} \supset \mathfrak{Y}$ or $\mathfrak{X} = \mathfrak{Y}$.

The cross-cut $[\mathfrak{X}, \mathfrak{Y}]$ is defined by

(4.2) $\mathfrak{X} \supseteq [\mathfrak{X}, \mathfrak{Y}], \mathfrak{Y} \supseteq [\mathfrak{X}, \mathfrak{Y}]$; if $\mathfrak{X} \supseteq \mathfrak{Z}$ and $\mathfrak{Y} \supseteq \mathfrak{Z}$, then $[\mathfrak{X}, \mathfrak{Y}] \supseteq \mathfrak{Z}$.

The union is defined by

(4.3) $(\mathfrak{X}, \mathfrak{Y}) \supseteq \mathfrak{X}, (\mathfrak{X}, \mathfrak{Y}) \supseteq \mathfrak{Y}$; if $\mathfrak{Z} \supseteq \mathfrak{X}$ and $\mathfrak{Z} \supseteq \mathfrak{Y}$ then $\mathfrak{Z} \supseteq (\mathfrak{X}, \mathfrak{Y})$.

Let Ω be any sub-set of Σ . Since the division relation in Σ determines that in Ω , a pair of elements $\mathfrak{A}, \mathfrak{B}$ of Ω may have a cross-cut and union satisfying definitions (4.2), (4.3) for all elements of Ω . We write then $[\mathfrak{A}, \mathfrak{B}]_\Omega, (\mathfrak{A}, \mathfrak{B})_\Omega$ denoting the set relative to which we consider the cross-cut or union by a sub-script. Obviously

$$(4.4) \quad (\mathfrak{A}, \mathfrak{B}) \supseteq (\mathfrak{A}, \mathfrak{B})_\Omega \supseteq [\mathfrak{A}, \mathfrak{B}]_\Omega \supseteq [\mathfrak{A}, \mathfrak{B}]_\Omega.$$

We call a set closed in this sense with respect to cross-cut and union a *structure within Σ* . If $(\mathfrak{A}, \mathfrak{B})_\Omega = (\mathfrak{A}, \mathfrak{B}), [\mathfrak{A}, \mathfrak{B}]_\Omega = [\mathfrak{A}, \mathfrak{B}]$ for every pair of elements of Ω , we call Ω a *sub-structure of Σ* . (Ore^[10] p. 409.)

If any set of elements of Σ , finite or infinite have a unique cross-cut and union, we shall say that Σ is a *completely closed structure*.

II. DIVISORS OF ARITHMETICAL FUNCTIONS AND THEIR RANKS OF APPARITION

5. Let ϕ be an arithmetical function on \mathfrak{o} to Σ . An element of Σ dividing one or more values of ϕ is said to divide ϕ or to be a *divisor of ϕ* . Obviously any factor of a divisor of ϕ divides ϕ . Hence:

⁵ An arithmetic function need not however determine any structure homomorphism.

⁶ The meaning of the symbols (...) and [...] is reversed in Ore's paper^[10]. See section 4.

THEOREM 5.1. *The set of all divisors of an arithmetical function is closed under union.*

We denote this set by Δ .

Let \mathfrak{A} be any divisor of ϕ . If $\mathfrak{A} \supseteq \phi_a$, we call a a place of apparition of \mathfrak{A} in ϕ . We now assume

AXIOM 1. *The places of apparition of every divisor of ϕ form an ideal of \mathfrak{o} .*

The ideal \mathfrak{r} corresponding to a divisor \mathfrak{Y} is called the rank of apparition of \mathfrak{Y} in ϕ . We write $\mathfrak{r} = \rho(\mathfrak{Y})$. The set of all ranks of apparition is denoted by δ . The following theorem is now obvious.

THEOREM 5.2. *The correspondence between divisors and ranks of apparition defines an arithmetical function ρ on Δ to δ .*

We cannot prove that the set Δ is closed under cross-cut as well as union. We assume:

AXIOM 2. *The set Δ of all divisors of ϕ is a completely closed sub-structure of Σ .*

THEOREM 5.3. *If $\mathfrak{A}, \mathfrak{B}$ are divisors of ϕ and $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, then $[\rho(\mathfrak{A}), \rho(\mathfrak{B})] = \rho(\mathfrak{M})$.*

PROOF. By axiom 2, \mathfrak{M} is a divisor of ϕ and by (4.2) $\mathfrak{A} \supseteq \mathfrak{M}$. Hence $\rho(\mathfrak{A}) \supseteq \rho(\mathfrak{M})$ by theorem 5.2. Similarly $\rho(\mathfrak{B}) \supseteq \rho(\mathfrak{M})$ so that $[\rho(\mathfrak{A}), \rho(\mathfrak{B})] \supseteq \rho(\mathfrak{M})$ by (4.2).

Assume that m lies in $[\rho(\mathfrak{A}), \rho(\mathfrak{B})]$. Then $m \equiv 0 \pmod{\rho(\mathfrak{A})}$, $m \equiv 0 \pmod{\rho(\mathfrak{B})}$ by (4.2). Hence $\phi_m \equiv 0 \pmod{\mathfrak{A}}$, $\phi_m \equiv 0 \pmod{\mathfrak{B}}$ or by (4.2) again, $\phi_m \equiv 0 \pmod{\mathfrak{M}}$. Hence $m \equiv 0 \pmod{\rho(\mathfrak{M})}$ so that $\rho(\mathfrak{M}) \supseteq [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.

THEOREM 5.31. "DECOMPOSITION THEOREM." *If the values of ϕ lie in a commutative ring \mathfrak{D} with a unit element and if $\mathfrak{A}, \mathfrak{B}$ are any two divisors of ϕ such that $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $\rho(\mathfrak{AB}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.*

PROOF. If $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $[\mathfrak{A}, \mathfrak{B}] = \mathfrak{AB}$ (van der Waerden,^[11] p. 45).

If \mathfrak{o} is a principal ideal ring, the following theorem allows us to replace axiom 1 by a simple structure condition. The result is independent of axiom 2.

THEOREM 5.4.⁸ *If \mathfrak{o} is a principal ideal ring, the places of apparition of every divisor of ϕ form an ideal if and only if ϕ defines a homomorphism with respect to union between \mathfrak{o} and the values of ϕ in Σ .*

PROOF. If \mathfrak{o} is a principal ideal ring, the union (m, n) of (m) and (n) is a principal ideal (d) : we write $d = (m, n)$. Let \mathfrak{A} be a divisor of ϕ , and assume that $\phi_m \equiv 0 \pmod{\mathfrak{A}}$, $\phi_n \equiv 0 \pmod{\mathfrak{A}}$. Also assume that $(m, n) = d$ in \mathfrak{o} implies that $(\phi_m, \phi_n) = \phi_d$ in Σ . Then by (4.3) $\phi_d \equiv 0 \pmod{\mathfrak{A}}$. Now $d \mid m$, $d \mid n$. Hence $d \mid m - n$ so that $\phi_d \supseteq \phi_{m-n}$. Hence by (4.1) $\phi_{m-n} \equiv 0 \pmod{\mathfrak{A}}$. Thus if m and n are places of apparition of \mathfrak{A} , so is $m - n$. But since ϕ is arithmetical, if a is a place of apparition so is xa , x any element of \mathfrak{o} . Hence the places of apparition of \mathfrak{A} form an ideal.

Assume conversely that \mathfrak{o} is a principal ideal ring and that the places of

⁷ It suffices to assume the places of apparition form a module, since ϕ is arithmetical.

⁸ Given by Ward^[12] for the case \mathfrak{o} and Σ the ring of rational integers.

apparition of any divisor \mathfrak{A} of ϕ form an ideal $a = (a)$. Let $(\phi_m, \phi_n) = D$, and let (d') be the rank of apparition of D in ϕ (Theorem 5.1). Since m, n lie in (d') , $d' | m, d' | n$. Hence if $(m, n) = d$, $d' | d$ by (4.3). Hence $\phi_d \equiv 0 \pmod{D}$. But since $d | m, d | n, \phi_d \supseteq \phi_m, \phi_d \supseteq \phi_n$ so that $\phi_d \supseteq D$ by (4.3). Thus $\phi_d = D$.

6. It is possible to have divisors $\mathfrak{A}, \mathfrak{B}$ of ϕ for which $\rho(\mathfrak{A}) = \rho(\mathfrak{B})$ $\mathfrak{A} \neq \mathfrak{B}$. Let $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$. Then by Theorem 5.3, $\rho(\mathfrak{M}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})] = \rho(\mathfrak{A})$. Thus the set of all elements \mathfrak{Z} of Δ such that $\rho(\mathfrak{Z}) = n$ is closed under cross-cut. Hence by axiom 2, for every rank of apparition n there exists a divisor \mathfrak{N} of ϕ such that

$$(6.1) \quad \rho(\mathfrak{N}) = n; \text{ if } \mathfrak{C} \text{ divides } \phi \text{ and } \rho(\mathfrak{C}) = n \text{ then } \mathfrak{C} \supseteq \mathfrak{N}.$$

We call such a divisor a *maximal* divisor of ϕ .⁹ We denote the set of all maximal divisors of ϕ by $\hat{\mu}$.

THEOREM 6.1. *Let \mathfrak{A} be any divisor of ϕ and a its rank of apparition. If \mathfrak{N} is a maximal divisor of ϕ such that $a \supseteq \rho(\mathfrak{N})$, then $\mathfrak{A} \supseteq \mathfrak{N}$.*

PROOF. Let $[\mathfrak{A}, \mathfrak{N}] = \mathfrak{B}$. \mathfrak{B} is a divisor of ϕ by axiom 2. Hence $\rho(\mathfrak{B})$ exists, and by theorem 5.3, $\rho(\mathfrak{B}) = [\rho(\mathfrak{A}), \rho(\mathfrak{N})] = \rho(\mathfrak{N})$ since $\rho(\mathfrak{A}) \supseteq \rho(\mathfrak{N})$. Since \mathfrak{N} is maximal, $\mathfrak{B} \supseteq \mathfrak{N}$. But $\mathfrak{A} \supseteq \mathfrak{B}$.

As a corollary, we have

THEOREM 6.11. *If \mathfrak{A} and \mathfrak{B} are maximal divisors of ϕ with ranks of apparition a and b respectively, then $\mathfrak{A} \supseteq \mathfrak{B}$ when and only when $a \supseteq b$.*

THEOREM 6.2. *The set $\hat{\mu}$ of all maximal divisors of ϕ is closed under union.*

PROOF. Let $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$. By (4.3),

$$(i) \quad \mathfrak{D} \supseteq \mathfrak{A}, \mathfrak{D} \supseteq \mathfrak{B};$$

$$(ii) \quad \text{If } \mathfrak{C} \supseteq \mathfrak{A}, \mathfrak{C} \supseteq \mathfrak{B} \text{ then } \mathfrak{C} \supseteq \mathfrak{D}.$$

By theorem 5.1, \mathfrak{D} divides ϕ . Let b be its rank of apparition and \mathfrak{C} any divisor of ϕ such that $\rho(\mathfrak{C}) = b$. By (i) and theorem 5.2, $\rho(\mathfrak{C}) \supseteq \rho(\mathfrak{A})$. Hence since \mathfrak{A} is maximal, $\mathfrak{C} \supseteq \mathfrak{A}$. Similarly $\mathfrak{C} \supseteq \mathfrak{B}$. Hence $\mathfrak{C} \supseteq \mathfrak{D}$ by (ii) so that \mathfrak{D} is maximal.

THEOREM 6.21. *If \mathfrak{A} and \mathfrak{B} are maximal divisors of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$ then $(\rho(\mathfrak{A}), \rho(\mathfrak{B}))$ exists and equals $\rho(\mathfrak{D})$.*

PROOF. By theorem 6.2, \mathfrak{D} is maximal. Hence by theorem 6.11, if $a = \rho(\mathfrak{A}), b = \rho(\mathfrak{B}), c = \rho(\mathfrak{C})$ and $d = \rho(\mathfrak{D})$, (i) $d \supseteq a, d \supseteq b$; (ii) if $c \supseteq a, c \supseteq b$ then $c \supseteq d$. (i) and (ii) are the definition of union.

Since to every rank of apparition corresponds a maximal divisor, in view of theorem 6.21 and 5.3, we can state

THEOREM 6.211. *The ranks of apparition of the divisors of ϕ form a structure within $\hat{\sigma}$.*

⁹ For example let ϕ_n denote the n^{th} of the Fibonacci numbers 1, 1, 2, 3, 5, 8, \dots . Then $\phi_{19} = 4181 = 37 \times 113$. Hence for $\mathfrak{A} = (37), \mathfrak{B} = (113), n = \rho(\mathfrak{A}) = \rho(\mathfrak{B}) = (19)$ while $\mathfrak{N} = (4181)$.

THEOREM 6.3. *If \mathfrak{A} and \mathfrak{B} are maximal divisors of ϕ , then the cross-cut $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$ within $\bar{\mu}$ exists, and $\rho(\mathfrak{M}) = [\rho(\mathfrak{A}), \rho(\mathfrak{B})]$.*

PROOF. Let $[\mathfrak{A}, \mathfrak{B}] = \mathfrak{N}$. By axiom 2, \mathfrak{N} divides ϕ . Let $m = \rho(\mathfrak{N})$ and let \mathfrak{M} be the corresponding maximal divisor such that $m = \rho(\mathfrak{M})$. Then $\mathfrak{N} \supseteq \mathfrak{M}$. I say that $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$. For $\mathfrak{A} \supseteq \mathfrak{M}$, $\mathfrak{B} \supseteq \mathfrak{M}$ by (4.4), (4.2). Let \mathfrak{C} be any other maximal divisor such that $\mathfrak{A} \supseteq \mathfrak{C}$, $\mathfrak{B} \supseteq \mathfrak{C}$. Then $\mathfrak{N} \supseteq \mathfrak{C}$ by (4.2). Hence $\rho(\mathfrak{N}) \supseteq \rho(\mathfrak{C})$ by theorem 6.2, so that $\rho(\mathfrak{M}) \supseteq \rho(\mathfrak{C})$. Since \mathfrak{M} and \mathfrak{C} are maximal, $\mathfrak{M} \supseteq \mathfrak{C}$ by theorem 6.1, so that $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_\mu$ by (4.2).

THEOREM 6.31. *The maximal divisors of ϕ form a structure within Σ isomorphic (Ore,^[10] pp. 416–418) to the structure of ranks of apparition within $\bar{\sigma}$.*

PROOF. Theorems 6.3, 6.2, 6.11.

III. MODULAR PERIODICITY

7. We assume henceforth that the values of ϕ lie in a commutative ring \mathfrak{D} . Σ now denotes the structure of all ideals of \mathfrak{D} , so that the values of ϕ *qua* elements of Σ are principal ideals of \mathfrak{D} .

For the present ϕ is any function on \mathfrak{o} to \mathfrak{D} , not necessarily arithmetical, and $\bar{\sigma}$ denotes the structure of all *modules* of \mathfrak{o} . We use small German letters now for modules instead of ideals. If m is a module, $m \equiv 0 \pmod{m}$ means m contains m .

Let \mathfrak{S} be any element of Σ . If there exists an element $m \neq 0$ of \mathfrak{o} such that

$$(7.1) \quad \phi_{x+m} \equiv \phi_x \pmod{\mathfrak{S}}, \quad \text{every } x \text{ of } \mathfrak{o},^{10}$$

\mathfrak{S} is called a *modulus* of ϕ , and m a *period* of ϕ modulo \mathfrak{S} . The periods (0 included) obviously form a module, \mathfrak{s} the *characteristic module of ϕ modulo \mathfrak{S}* . We shall also call \mathfrak{s} the module of \mathfrak{S} , writing

$$(7.2) \quad \mathfrak{s} = \mu(\mathfrak{S}).$$

Let Π denote the set of all moduli of ϕ in Σ , and $\bar{\pi}$ the set of all characteristic modules in $\bar{\sigma}$. Clearly as in section 5, we have

THEOREM 7.1. *Π is closed under union.*

THEOREM 7.2. *μ is an arithmetic function on Π to $\bar{\sigma}$.*

We cannot prove in general that Π is closed under cross-cut. We assume:

AXIOM 3. *The set of all moduli of ϕ is a completely closed sub-structure of Σ .*

Then the following theorems follow precisely as in section 5.

THEOREM 7.3. *If $\mathfrak{A}, \mathfrak{B}$ are moduli of ϕ and if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, then $\mu(\mathfrak{M}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

THEOREM 7.31. "DECOMPOSITION THEOREM."¹¹ *If $\mathfrak{A}, \mathfrak{B}$ are moduli of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $\mu(\mathfrak{AB}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

¹⁰ We shall omit this phrase henceforth, reserving the letter x exclusively to denote every element of \mathfrak{o} .

¹¹ Stated in Ward^[13] for linear recurring series. The analogous theorems 5.31 and 10.31 appear to be new.

8. The theory of maximal moduli exactly parallels the theory of maximal divisors.

For every possible module of periods n there exists a maximal modulus \mathfrak{N} such that

$$(8.1) \quad \mu(\mathfrak{N}) = n; \quad \text{if} \quad \mu(\mathfrak{S}) = n, \mathfrak{S} \text{ a module, } \mathfrak{S} \supseteq \mathfrak{N}.$$

THEOREM 8.1. *Let \mathfrak{A} be any modulus of ϕ , a its characteristic module. Then if \mathfrak{N} is a maximal modulus such that $\phi \supseteq a(\mathfrak{N})$, $\mathfrak{A} \supseteq \mathfrak{N}$.*

THEOREM 8.11. *If \mathfrak{A} and \mathfrak{B} are maximal moduli of ϕ with characteristic modules a and b respectively, then $\mathfrak{A} \supseteq \mathfrak{B}$ when and only when $a \supseteq b$.*

THEOREM 8.2. *The set of all maximal moduli of ϕ is closed under union.*

THEOREM 8.21. *If \mathfrak{A} and \mathfrak{B} are maximal moduli of ϕ and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $(\mu(\mathfrak{A}), \mu(\mathfrak{B}))_*$ exists and equals $\mu(\mathfrak{D})$.*

THEOREM 8.211. *The characteristic modules of the moduli of ϕ form a structure within $\tilde{\sigma}$.*

THEOREM 8.3. *If \mathfrak{A} and \mathfrak{B} are maximal moduli of ϕ then $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]_*$ exists, and $\mu(\mathfrak{M}) = [\mu(\mathfrak{A}), \mu(\mathfrak{B})]$.*

THEOREM 8.31. *The maximal moduli of ϕ form a structure within Σ isomorphic to the structure of characteristic modules within $\tilde{\sigma}$.*

It is easily seen that if we assume in analogy with axiom 1,

AXIOM 4. *The periods of any modulus of ϕ form an ideal.*

Then all the theorems of this section and the preceding one hold if the word module is everywhere replaced by ideal, and the notation a, \dots, \mathfrak{z} is understood to mean ideals instead of modules.

IV. RESTRICTED PERIODS. RELATIONSHIPS BETWEEN DIVISORS AND MODULI OF AN ARITHMETIC FUNCTION

9. The concept of "restricted period" which we formulate abstractly here is very important in the theory of the Lucas function and linear recurring series in general. (Carmichael,^[2] Ward^[4].) As in sections 7, 8 we assume that the values of ϕ lie in a commutative ring \mathfrak{D} containing a unit element. Let \mathfrak{S} be an ideal of \mathfrak{D} . If there exist elements M and m of \mathfrak{D} and \mathfrak{o} such that

$$(9.1) \quad \phi_{x+m} \equiv M\phi_x \pmod{\mathfrak{S}} \text{ all } x \text{ in } \mathfrak{o}$$

$$(9.11) \quad ((M), \mathfrak{S}) = \mathfrak{D}$$

then m is called a *restricted period* of ϕ modulo \mathfrak{S} , and M a *multiplier* of ϕ modulo \mathfrak{S} .

THEOREM 9.1. *The multipliers of ϕ modulo \mathfrak{S} are closed under multiplication. The restricted periods of ϕ modulo \mathfrak{S} form an additive semi-group.*

PROOF. Assume that $\phi_{x+m_i} \equiv M_i\phi_x \pmod{\mathfrak{S}}$, $((M_i), \mathfrak{S}) = \mathfrak{D}$, $i = 1, 2$. Then $\phi_{x+m_1+m_2} \equiv M_1\phi_{x+m_2} \equiv M_1M_2\phi_x \pmod{\mathfrak{S}}$. Also (Van der Waerden,^[1] p. 45) $((M_1M_2), \mathfrak{S}) = \mathfrak{D}$.

We shall now assume

AXIOM 5.¹² *For any modulus \mathfrak{S} the multipliers of ϕ modulo \mathfrak{S} form a multiplicative group in \mathfrak{D} (Ward,^[13] p. 162).*

We denote this group by \mathfrak{G} .

THEOREM 9.11. *The restricted periods of ϕ modulo \mathfrak{S} form a module.*

PROOF. With the notation of theorem 9.1, let N_1 be the inverse of M_1 in \mathfrak{G} , so that $N_1 M_1 \equiv 1 \pmod{\mathfrak{S}}$. Then by (7.2)

$$\phi_{x+m_2-m_1} \equiv N_1 M_1 \phi_{x-m_1+m_2} \equiv N_1 M_1 M_2 \phi_{x-m_1} \equiv N_1 M_2 \phi_x \pmod{\mathfrak{S}}.$$

By axiom 5, theorem 7.1 $N_1 M_2$ is a multiplier so that $m_2 - m_1$ is a period.

THEOREM 9.2. *Let \mathfrak{S} be a modulus, \mathfrak{G} its group, \mathfrak{s} its restricted period. Let \mathfrak{T} be any divisor of \mathfrak{S} . Then \mathfrak{T} also is a modulus. If \mathfrak{K} is its group and \mathfrak{t} its restricted period, $\mathfrak{G} \subseteq \mathfrak{K}$, $\mathfrak{t} \supseteq \mathfrak{s}$.*

PROOF. Clear.

THEOREM 9.3. *The set of all moduli of ϕ and the set of all moduli of restricted periods are identical.*

PROOF. If \mathfrak{S} is an ordinary modulus, its group of multipliers consists of the single element 1 of \mathfrak{D} . On the other hand, if \mathfrak{S} is a modulus of restricted periods, \mathfrak{S} has the multiplier 1 by axiom 5 and hence is an ordinary modulus.

THEOREM 9.31.¹³ *If $\tau(\mathfrak{S})$ and $\mu(\mathfrak{S})$ are respectively the module of restricted periods and the module of periods of the modulus \mathfrak{S} of ϕ , then $\tau(\mathfrak{S}) \supseteq \mu(\mathfrak{S})$.*

PROOF. Clear from Theorem 9.3 and axiom 5.

10. In view of theorem 9.3, it is unnecessary to show that the moduli of the restricted periods of ϕ are closed under union, and theorem 9.2 makes it evident that τ is an arithmetical function on $\tilde{\mathfrak{A}}$ to $\tilde{\mathfrak{S}}$. Even if we retain axiom 3 of section 7, we cannot prove the analogue of theorems 5.3 and 7.3 viz.:—"If $\mathfrak{A}, \mathfrak{B}$ are moduli of ϕ and if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, then $\tau(\mathfrak{M}) = [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$." We must content ourselves with $\tau(\mathfrak{M}) \subseteq [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$.

To see why this lack occurs, let us try to show that $[\tau(\mathfrak{A}), \tau(\mathfrak{B})] \subseteq \tau(\mathfrak{M})$. If m is any element of $[\tau(\mathfrak{A}), \tau(\mathfrak{B})]$, we infer from (4.2) that

$$\begin{aligned} \phi_{x+m} &\equiv M\phi_x \pmod{\mathfrak{A}}, & \phi_{x+m} &\equiv N\phi_x \pmod{\mathfrak{B}} \\ ((M), \mathfrak{A}) &= \mathfrak{D}, & ((N), \mathfrak{B}) &= \mathfrak{D}. \end{aligned}$$

To show that m lies in $\tau(\mathfrak{M})$, it is necessary and sufficient to show that there exists an element S of \mathfrak{D} such that

$$\phi_{x+m} \equiv S\phi_x \pmod{\mathfrak{M}}, \quad ((S), \mathfrak{M}) = \mathfrak{D}.$$

Since $\mathfrak{A} \supseteq \mathfrak{M}$, $\mathfrak{B} \supseteq \mathfrak{M}$, we must also have

$$S \equiv M \pmod{\mathfrak{A}}, \quad S \equiv N \pmod{\mathfrak{B}}.$$

¹² This axiom always holds if \mathfrak{D} is a ring of algebraic integers or more generally whenever the ring $\mathfrak{D}/\mathfrak{S}$ is finite.

¹³ Generalizes Carmichael^[2], p. 355.

Now such an element S need not exist. For example, take for \mathfrak{D} the ring of rational integers, and let $\mathfrak{A} = (6)$, $\mathfrak{B} = (9)$, $M = 5$, $N = 4$. Then $\mathfrak{M} = (18)$, and no S exists.

On the other hand if $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, such an S does exist since the Chinese remainder theorem holds in a commutative ring with unit element (van der Waerden,^[11] p. 85). Thus a "decomposition theorem" holds for the restricted period analogous to theorems 5.31 and 7.31.

DECOMPOSITION THEOREM 10.31. *If $\mathfrak{A}, \mathfrak{B}$ are moduli and $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{D}$, then $\tau(\mathfrak{AB}) = [\tau(\mathfrak{A}), \tau(\mathfrak{B})]$.*

Since theorem 7.3 fails, we cannot introduce maximal restricted period moduli, and the theorems of sections 6 and 8 have no analogues.

11. It remains to discuss the relationship between the rank of apparition and restricted period of any element of Σ . Let us suppose that ϕ is an arithmetic function on \mathfrak{o} to \mathfrak{D} , and that axioms 1, 2, 3 and 5 hold.

Consider the elements ϕ_0 and ϕ_1 . Since $x | 0, 1 | x$ for every x of \mathfrak{o} , $\phi_x \supseteq \phi_0$ and $\phi_1 \supseteq \phi_x$ for every value of ϕ in \mathfrak{D} . The simplest way to satisfy these two conditions is for ϕ_0 to equal the zero element and ϕ_1 the unit element of the ring \mathfrak{D} . An arithmetic function with this property will be called *normal*. We assume

AXIOM 6. *ϕ is a normal arithmetic function on \mathfrak{o} to \mathfrak{D} .*

THEOREM 11.1.^[14] *Every modulus of ϕ is a divisor of ϕ , and the rank of apparition of any modulus divides its restricted period.*

PROOF. Let \mathfrak{S} be any modulus, m a restricted period of \mathfrak{S} . Then since

$$\phi_{m+x} \equiv M\phi_x \pmod{\mathfrak{S}}, \quad \phi_m \equiv M\phi_0 \equiv 0 \pmod{\mathfrak{S}}.$$

Hence $m \equiv 0 \pmod{\rho(\mathfrak{S})}$.

CALIFORNIA INSTITUTE OF TECHNOLOGY.

REFERENCES

- [1] E. Lucas, *Amer. Jour. of Math.* vol. 1 (1878) pp. 184–239, 289–321.
- [2] R. D. Carmichael, *Quarterly Journal* vol. 48 (1920) pp. 343–372.
- [3] H. T. Engstrom, *Trans. Amer. Math. Soc.* vol. 33 (1931) pp. 210–218.
- [4] M. Ward, *Trans. Amer. Math. Soc.* vol. 35 (1933) pp. 600–628.
- [5] D. H. Lehmer, *Annals of Math.* (2), vol. 31 (1930) pp. 419–448.
- [6] M. Hall, *Amer. Jour. of Math.* vol. 58 (1936) pp. 577–584.
- [7] M. Ward, *Trans. Amer. Math. Soc.* (reference later).
- [8] L. E. Dickson, *History*, vol. 1, chapter V.
- [9] G. H. Halphen, *Traite des Fonctions Elliptiques*, Part I, chap. IV.
- [10] O. Ore, *Annals of Math.* (2) vol. 36 (1935), pp. 406–437.
- [11] Van der Waerden, *Modern Algebra Part 2*, Berlin (1931).
- [12] M. Ward, *Bulletin Amer. Math. Soc.* (reference later).
- [13] M. Ward, *Trans. Amer. Math. Soc.* vol. 33 (1931) pp. 153–165.

^[14] This result generalizes a theorem of Hall^[6] on linear divisibility sequences. For the Lucas function, the rank of apparition and restricted period are equal.

SOME ARITHMETICAL APPLICATIONS OF RESIDUATION.

By MORGAN WARD.

1°. The operation of residuation was apparently first considered by Dedekind in his theory of the modules in a ring of algebraic integers [1].¹ It was introduced into polynomial ideal theory by Emanuel Lasker [2], and has since been used systematically by F. S. Macaulay [3] and others. I propose to show here how the operation may be applied to various arithmetical problems,² in particular to developing a systematic calculus for the periods of elements in any finite Abelian group.

2°. Consider first for simplicity a cyclic group \mathbf{G} of order n written additively. Every element α of \mathbf{G} may be uniquely represented as

$$(2.1) \quad \alpha = a\gamma, \quad 0 < a \leq n$$

where γ is a fixed primitive element of \mathbf{G} and $a\gamma$ means $\gamma + \gamma + \cdots + \gamma$ taken a times. We write L_a for a in (2.1); for example $L_0 = n$. Let P_a denote the period of α ; that is the least positive integer p such that $p\alpha = 0$. The starting point of our investigation is the observation that P_a is the residual of L_a with respect to n .

L_ξ considered as an operation on \mathbf{G} to the finite ring K_n of the integers modulo n is linear and distributive:

$$L_{m\alpha+n\beta} \equiv mL_\alpha + nL_\beta \pmod{n}, \quad m, n \text{ integers.}$$

On the other hand, P_ξ is neither a linear nor a distributive operation; given P_α and P_β , all we can assert about $P_{\alpha+\beta}$ is that it divides $[P_\alpha, P_\beta]$, the least

¹ The numbers [1], [2], . . . in square brackets refer to the bibliography at the close of the paper.

² For example, consider the problem of solving

$$(1) \quad AX \equiv 0 \pmod{\mathfrak{m}, F}.$$

Here A and F are given polynomials in indeterminates x_1, \dots, x_s with coefficients in a commutative ring \mathfrak{R} while \mathfrak{m} is an ideal of \mathfrak{R} . We seek all solutions X in the quotient ring $\mathfrak{R}[x_1, \dots, x_s]/\mathfrak{m}$. If \mathfrak{A} and \mathfrak{F} denote the ideals (\mathfrak{m}, A) , (\mathfrak{m}, F) then the totality of such solutions of (1) constitute the residual ideal of \mathfrak{A} with respect to \mathfrak{F} (Van der Waerden [4] Chapter XIII). Thus the solution of (1) is equivalent to specifying this residual, say by determining a basis for it. I have given a complete solution for the case when $s = 1$ and \mathfrak{R} is the ring of rational integers. Ward [5].

common multiple of P_α and P_β .³ Simple numerical examples show that $P_{\alpha+\beta}$ may be any divisor whatever of $[P_\alpha, P_\beta]$.

These facts suggest that we introduce in \mathfrak{G} one or more new operations $\xi \circ \eta$, $\xi \times \eta$ such that $P_{\alpha \circ \beta}$, $P_{\alpha \times \beta}$ may be calculated knowing only the values of P_α , P_β ; the definition of P_α as a residual immediately suggests how these operations should be defined. But before introducing these operations, we shall briefly summarize the properties of residuation of which we make use.

3. Let \mathfrak{D} be the set of ideals⁴ A, B, C, \dots of a fixed commutative ring containing a unit element. If A and B are any two elements of \mathfrak{D} , the residual of B with respect to A is by definition an ideal C such that

$$A \supset BC; \text{ if } A \supset BX \text{ then } C \supset X.$$

We write as usual $C = A : B$. The residual always exists and has the following properties:

$$(3.1) \quad \begin{aligned} A : B - A : (A, B) &= [A, B] : B, \\ (A : B) : C &= (A : C) : B = A : BC, \\ A = M : N \text{ and } B = M : (M : N) &\text{ imply } B = M : A, A = M : B, \\ M : (A_1, A_2, \dots, A_k) &= [M : A_1, M : A_2, \dots, M : A_k], \\ [A_1, A_2, \dots, A_k] : M &= [A_1 : M, A_2 : M, \dots, A_k : M]. \end{aligned}$$

If we restrict \mathfrak{D} to be a principal ideal ring, then $A \supset B$ if and only if there exists a quotient $Q = A/B$ such that $A = QB$. Furthermore this quotient is unique. It is easily shown that $A : B = A/B$ whenever the quotient A/B exists, so that formula (3.1) becomes

$$(3.11) \quad A : B = \frac{A}{(A, B)} = \frac{B}{[A, B]}.$$

On using this result and the unicity of the quotient, we easily find that the following additional rules for residuation hold in any principal ideal ring.⁵

$$\begin{aligned} (M, N) &= M : (M : N), \quad M : AB = \{(M : A)(M : B)\} : M, \\ (A_1, A_2, \dots, A_k) : M &= (A_1 : M, \dots, A_k : M), \\ M : [A_1, A_2, \dots, A_k] &= (M : A_1, \dots, M : A_k). \end{aligned}$$

³ We use (A, B, \dots) , $[A, B, \dots]$ both for the union and join of ideals A, B, \dots or the greatest common divisor and least common multiple of integers A, B, \dots

⁴ We use the notation of van der Waerden [4], chapter XII save that roman capitals are used for ideals instead of gothic capitals.

⁵ A detailed analysis of the properties of residuation, is given in Ward [6], Dilworth [7].

4°. The formulas of section 3° give the fundamental relations

$$(4.1) \quad P_a = n : L_a = \frac{n}{(n, L_a)} = \frac{[n, L_a]}{L_a},$$

$$P_a = n : (n : P_a), \quad L_a = n : P_a \text{ if and only if } L_a \text{ divides } n.$$

We define our new operations over the group \mathfrak{G} as follows. We write

$$\begin{aligned} \delta &= (\xi, \eta) \text{ if } L_\delta = (L_\xi, L_\eta), \\ \mu &= [\xi, \eta] \text{ if } L_\mu \equiv [L_\xi, L_\eta] \pmod{n}. \end{aligned}$$

It is clear that the group \mathfrak{G} forms an arithmetic structure⁶ with respect to the operations of union and cross-cut thus defined which is simply isomorphic with the structure of the ring K_N .

The third operation over \mathfrak{G} which we shall consider is a multiplication simply isomorphic with multiplication in K_N : we write

$$\pi = \xi \cdot \eta \text{ if } L_\pi \equiv L_\xi L_\eta \pmod{n}.$$

If we call two elements of \mathfrak{G} equivalent if and only if each divides the other, then equivalent elements have the same period and conversely.

The periods of δ , μ and π obey the following simple rules which are easy consequences of (4.1) and the formulas of section 3°:

$$\begin{aligned} P_{(\xi, \eta)} &= [P_\xi, P_\eta], \quad P_{\xi_1, \xi_2, \dots, \xi_k} = [P_{\xi_1}, P_{\xi_2}, \dots, P_{\xi_k}], \\ P_{[\xi, \eta]} &= (P_\xi, P_\eta), \quad P_{[\xi_1, \xi_2, \dots, \xi_k]} = (P_{\xi_1}, P_{\xi_2}, \dots, P_{\xi_k}), \\ P_{\xi \cdot \eta} &= \{P_\xi P_\eta\} : n, \quad P_{\xi_1 \cdot \xi_2 \dots \cdot \xi_k} = \{P_{\xi_1} P_{\xi_2} \dots P_{\xi_k}\} : n^{k-1}. \end{aligned}$$

Thus for each operation the period is readily calculated from the period of its constituents. It is possible to define a residual $\xi : \eta$ in \mathfrak{G} by $L_{\xi : \eta} = L_\xi : L_\eta$, but its period is not calculable in terms of the periods of ξ and η alone.

5°. If we choose a different primitive element γ' in place of γ defining a new operator L'_ξ over \mathfrak{G} we have

$$L'_a \equiv L'_\gamma L_a \pmod{n}, \quad L_a \equiv L_\gamma L'_a \pmod{n}$$

where $L'_\gamma L_\gamma \equiv 1 \pmod{n}$, so that both L'_γ and L_γ are prime to n . It readily follows that the operations (ξ, η) , $[\xi, \eta]$ are independent of the particular base γ chosen to define them. The situation for the product is different. We

⁶Or distributive lattice. See Ore [8] or Ward [6] for detailed definition

find that $(\alpha \cdot \beta)' = \gamma' \cdot (\alpha \cdot \beta)$. On the other hand $P'_a = P_a$. The formulas (4.1) are thus unchanged. For example:

$$P'_{(\xi, \eta)} = P_{\gamma' \cdot (\xi, \eta)} = \{P_{\gamma'} P_{\xi, \eta}\}_{:N} = \{N, P_{\xi, \eta}\}_{:N} = P_{\xi, \eta}.$$

6°. Suppose now that the group \mathbf{G} is the direct sum of κ cyclic groups $\mathbf{G}^{(1)}, \dots, \mathbf{G}^{(k)}$ of orders $N^{(1)}, \dots, N^{(k)}$:

$$(6.1) \quad \mathbf{G} = \mathbf{G}^{(1)} + \mathbf{G}^{(2)} + \dots + \mathbf{G}^{(i)} + \dots + \mathbf{G}^{(k)},$$

so that the typical element α of \mathbf{G} is of the form

$$\alpha = \alpha^{(1)} + \alpha^{(2)} + \dots + \alpha^{(i)} + \dots + \alpha^{(k)}.$$

We select in each group $\mathbf{G}^{(i)}$ a primitive element $\gamma^{(i)}$ and define operators $L_{\alpha^{(i)}}$ as in section 2° by

$$L_{\alpha^{(i)}} = a^{(i)}, \quad \alpha^{(i)} = a^{(i)}\gamma^{(i)}, \quad (i = 1, 2, \dots, k).$$

We then associate with the element α the vector \mathfrak{L}_α whose i -th component is $L_{\alpha^{(i)}}$. The operations (α, β) , $[\alpha, \beta]$, $\alpha \cdot \beta$ over \mathbf{G} of union, cross-cut and product are defined by the vectors $\mathfrak{L}_{(\alpha, \beta)}$, $\mathfrak{L}_{[\alpha, \beta]}$, $\mathfrak{L}_{\alpha \cdot \beta}$ with components $(L_{\alpha^{(i)}}, L_{\beta^{(i)}})$, $[L_{\alpha^{(i)}}, L_{\beta^{(i)}}]$, $L_{\alpha^{(i)}} L_{\beta^{(i)}}$ respectively where the components are taken modulo $N^{(i)}$ in the associated rings $K_{N^{(i)}}$.

With an obvious extension of notation, we write

$$\begin{aligned} \mathfrak{L}_{(\alpha, \beta)} &= (\mathfrak{L}_\alpha, \mathfrak{L}_\beta), & \mathfrak{L}_{[\alpha, \beta]} &= [\mathfrak{L}_\alpha, \mathfrak{L}_\beta] \\ \mathfrak{L}_{\alpha \cdot \beta} &= \mathfrak{L}_\alpha \cdot \mathfrak{L}_\beta. \end{aligned}$$

The *vectorial period* of α is defined as the vector \mathfrak{P}_α with components $P_{\alpha^{(i)}} = N^{(i)}; L^{(i)}$. If \mathfrak{N} denotes the vector with components $N^{(1)}, N^{(2)}, \dots, N^{(k)}$ (\mathfrak{N} is simply \mathfrak{L}_0 , where 0 is the identity element of \mathbf{G}) then we write

$$\mathfrak{P}_\alpha = \mathfrak{N} : \mathfrak{L}_\alpha.$$

These definitions allow us to extend immediately the formulas of section 4°; thus

$$\mathfrak{P}_{[\alpha, \beta]} = (\mathfrak{P}_\alpha, \mathfrak{P}_\beta), \quad \mathfrak{P}_{(\alpha, \beta)} = [\mathfrak{P}_\alpha, \mathfrak{P}_\beta], \quad \mathfrak{P}_{\alpha \cdot \beta} = \mathfrak{P}_\alpha \cdot \mathfrak{P}_\beta : \mathfrak{N}.$$

The actual period of α (that is, the least positive integer p such that $p\alpha = 0$) is simply the least common multiple of the components of the vectorial period. Denoting it as before by P_α , we have

$$P_\alpha = [P_{\alpha^{(1)}}, P_{\alpha^{(2)}}, \dots, P_{\alpha^{(k)}}].$$

We cannot calculate the scalar period of $\alpha \cdot \beta$ or $[\alpha, \beta]$ directly in terms of the scalar periods of α and β . But for the union (α, β) we have the elegant formula

$$P_{(\alpha, \beta)} = [P_\alpha, P_\beta].$$

These considerations apply to any finite Abelian group since every such group may be represented as a direct sum of cyclic groups. If we assume as is always possible that the order of each summand is a power of a prime, then the number of summands $G^{(i)}$ is uniquely specified and also the orders $N^{(i)}$.

To remove in part the ambiguity in the definition of the components of \mathfrak{L}_ξ and \mathfrak{P}_ξ due to the fact that the order of the groups $G^{(i)}$ in (6.1) is unspecified, we agree to arrange the prime power orders $N^{(i)}$ first in the natural order of the primes, and then arrange the powers of each prime in order of magnitude. The remaining ambiguity in the order of the components due to adjoining isomorphic groups in the decomposition (6.1) appears to be inherent, as the set of all vector functions \mathfrak{P}_ξ over G can be regarded as a basis for a representation of the group of automorphisms of G , each function being corollated with the sub-group of automorphisms leaving its components unchanged in order, but changing possibly the basis elements $\gamma^{(i)}$ in terms of which the components $L_\xi^{(i)}$ are specified. We have already seen in section 5° that the components of \mathfrak{P}_ξ are unaffected by such changes of base. The remaining automorphisms of G will permute isomorphic groups in (6.1) thus inducing a permutation of the vector functions \mathfrak{P}_ξ . In any event the scalar period function P_ξ remains unaffected.

Since any finite field excluding its zero element is a cyclic group with respect to multiplication, the calculus we have developed in section 4° carries over entire to the periods of elements in any such field. The vectorial calculus of the present section similarly applies to the periods of the units in any finite commutative ring.

7°. The operations which we have defined over the finite group have analogues in common arithmetic. For if

$$A = \prod_1^\infty P_n^{a_n}, \quad B = \prod_1^\infty P_n^{b_n}$$

are the decompositions of the positive integers A and B into their prime factors, where P_1, P_2, P_3, \dots denote the primes $2, 3, 5, \dots$ in their natural order and only a finite number of the exponents a_n, b_n are not zero, we may define a "union," "cross-cut" and "product" of A and B "of the second kind" by

$$(A, B) = \prod_1^{\infty} P_n^{(a_n, b_n)} \quad [A, B] = \prod_1^{\infty} P_n^{[a_n, b_n]} \\ A \cdot B = \prod_1^{\infty} P_n^{a_n, b_n}.$$

The product of the second kind is distributive with respect to the ordinary product $A \times B$ or "product of the first kind":

$$A \cdot (B \times C) = (A \cdot B) \times (A \cdot C).$$

The analogy with our treatment of groups becomes evident if we think of A as specified by the vector with components a_1, a_2, \dots .

Indeed our product is the arithmetical analogue of the "multiplication of the second order" considered by De Morgan [9] and others [10] in the hierarchy of operations

$$A + B, A \times B = \exp(\log A + \log B), A \cdot B = \exp(e^{\log \log A + \log \log B}) = A^{\log B}, \dots$$

PASADENA, CALIFORNIA.

REFERENCES.

1. R. Dedekind, Supplement XI of Dirichlet's *Vorlesungen*, 4th edition (1894), § 170; *Collected Works*, vol. III, p. 71.
2. E. Lasker, *Mathematische Annalen*, vol. 60 (1905), pp. 20-116.
3. F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge (1916).
4. B. L. van der Waerden, *Moderne Algebra*, vol. 2 (Berlin, 1931).
5. M. Ward, *Transactions of the American Mathematical Society*, vol. 35 (1933), pp. 254-260.
6. M. Ward, Paper submitted to the *Duke Journal*.
7. R. P. Dilworth, Paper submitted to the *Transactions of the American Mathematical Society*.
8. O. Ore, *Annals of Mathematics*, vol. 36 (1935), pp. 406-437.
9. A. De Morgan, *Trigonometry and Double Algebra*, p. 166.
10. R. E. Moritz, *Tohoku Journal*, vol. 21 (1921), pp. 51-64.

Chapter 12

1938

ARITHMETICAL PROPERTIES OF SEQUENCES IN RINGS

BY MORGAN WARD

(Received February 1, 1937; Revised June 21, 1937)

INTRODUCTION

1. Let S be the set of numbers $0, 1, 2, \dots, \mathfrak{O}$, a commutative ring of elements A, B, \dots, Z, \dots containing a unit element, and let U_n be a one-valued function on S to \mathfrak{O} ; that is, a sequence

$$(U): \quad U_0, U_1, \dots, U_n, \dots$$

of elements of \mathfrak{O} . The object of this paper is to study the periodicity and divisibility of such sequences relative to ideals of \mathfrak{O} . If we extend¹ U_n over the ring of rational integers by letting $U_{-n} = U_n$, we have a special instance of a correspondence between a commutative ring and a structure (lattice) studied in a previous paper in these Annals (Ward [1]²).

The less general hypotheses of the present paper allow us to prove as theorems many of the axioms assumed in W. A. The results of the paper are however of a quite different character from those in W. A., and the paper may be read independently.

In conjunction with W. A. this paper gives a general theory of the arithmetic properties of sequences which renders any half-hearted generalizations of the ordinary theory of linear sequences of rational integers³ such as to linear sequences of algebraic integers, to a large extent superfluous. In addition, we obtain many results for the special case of linear sequences of rational integers under much less restrictive hypotheses than heretofore.⁴

The existence of a smaller period for the places of apparition of a divisor of a linear divisibility sequence than the restricted period of the sequence which we prove here abstractly⁵ is a fact of some arithmetical interest which does not seem to have been observed previously.

¹ We include the case when U_n is defined over a sub-set T of S by letting U_n be the zero of \mathfrak{O} over the complementary set $S - T$. For example a function defined merely for $n = 0, 1$ and 2 is regarded as a sequence in which all terms vanish after the third.

² The bracketed numerals refer to the reference listed at the close of the paper. I shall refer to this particular paper as W. A.

³ See W. A. for references to recent papers.

⁴ See for example theorems 3.2, 4.1, 4.2 and 4.3. Theorem 3.2 is given in Ward [2] for a very special case. See also Carmichael [1]. Theorems 4.1-4.3 are closely connected with Marshall Hall's Theorem III (Hall [1], p. 579).

⁵ Numerical examples over the ring of rational integers can be constructed without much difficulty, but unfortunately satisfy difference equations of quite high order.

2. We shall adhere to the following scheme of notation based on van der Waerden [1] and used in W. A. Elements of \mathfrak{O} are denoted by roman capitals; small italic and Greek letters denote ordinary integers. The ideals of \mathfrak{O} are denoted by German letters $\mathfrak{A}, \mathfrak{B}, \dots$ ($\mathfrak{A}, \mathfrak{B}$) and $[\mathfrak{A}, \mathfrak{B}]$ denote the union and cross-cut of the ideals \mathfrak{A} and \mathfrak{B} ; (a, b) and $[a, b]$ the greatest common divisor and least common multiple of the numbers a and b ; (A, B) the union of the principal ideals $[A]$ and $[B]$. The letters U and V are reserved to denote sequences. Thus (U) stands for a function. If the ideals \mathfrak{A} and $[A]$ are co-prime ("teilerfremd," van der Waerden [1], §85), we write $(\mathfrak{A}, A) = \mathfrak{O}$. a divides b is written as usual $a | b$.

II. MODULAR PERIODICITY AND DIVISIBILITY SEQUENCES

3. We begin with some definitions. The sequence (U) is said to be *finite* if it contains only a finite number of non-vanishing terms. It is said to be *linear over \mathfrak{O}* if its terms satisfy a recursion relation

$$(3.1) \quad U_{n+k} = C_1 U_{n+k-1} + \dots + C_k U_n, \quad (n = 0, 1, 2, \dots)$$

with coefficients C_i in \mathfrak{O} .

(U) is said to be a *divisibility sequence* (M. Hall [1], Ward [1], [4]) if U_n divides U_m in \mathfrak{O} whenever n divides m . If (U) is both a linear sequence and a divisibility sequence we shall call (U) "Lucasian"⁶ in honor of the French mathematician E. Lucas who first systematically studied a special class of such sequences. (Lucas [1], [2], Dickson [1].)

It may happen that the terms of (U) become periodic when taken to a fixed ideal modulus \mathfrak{A} of \mathfrak{O} ; that is, there exist numbers λ and ν such that

$$(3.2) \quad U_{n+\lambda} \equiv U_n \pmod{\mathfrak{A}}, \quad n \geq \nu.$$

The least such λ and ν are called the *period* and *numeric* of (U) for the modulus \mathfrak{A} . This minimal period is easily seen to divide every other period. If $\nu = 0$, (U) is said to be *purely periodic* modulo \mathfrak{A} .

If there exists at least one term U_k of (U) such that $U_k \equiv 0 \pmod{\mathfrak{A}}$ then \mathfrak{A} is called a divisor of (U) . If all terms of (U) are divisible by $\mathfrak{A} \neq \mathfrak{O}$ from a certain point on, then \mathfrak{A} is called a *null divisor* of (U) , and (U) a null sequence modulo \mathfrak{A} . Every finite sequence is thus a null sequence for any modulus.

A positive integer μ is said to be a *restricted period* of (U) modulo \mathfrak{A} if there exists an element A of \mathfrak{O} such that

$$(3.3) \quad U_{n+\mu} \equiv AU_n \pmod{\mathfrak{A}}, \quad \text{all large } n.⁷$$

Here A depends on μ . We call A a multiplier of (U) modulo \mathfrak{A} . The least μ for which (3.3) holds is called the restricted period of (U) .

⁶ The more euphonious term "Lucas sequence" already has a precise meaning in the literature.

⁷ It usually suffices to consider (3.3) for n greater than the numeric of (U) modulo \mathfrak{A} .

THEOREM 3.1. *Let (U) be a sequence of \mathfrak{D} , and \mathfrak{A} any ideal of \mathfrak{D} such that no divisor of \mathfrak{A} is a null divisor of (U) . Then if (U) is periodic modulo \mathfrak{A} , the minimal restricted period μ of (U) modulo \mathfrak{A} exists, and divides every other restricted period, and in particular the actual period λ . Furthermore the multipliers of (U) modulo \mathfrak{A} are all prime to \mathfrak{A} ,⁸ and form a group with respect to multiplication modulo \mathfrak{A} .*

PROOF. If \mathfrak{A} is a null divisor of (U) , (3.3) becomes a triviality. In any event, if (U) is periodic modulo \mathfrak{A} , the actual period λ is a restricted period with $A = I$. Hence a minimal μ exists $\leq \lambda$, and we may write $\lambda = s\mu - t$ where $s \geq 1$, $0 \leq t < \mu$. Then for all large n ,

$$U_{n+t} \equiv U_{n+t+\lambda} \equiv U_{n+s\mu} \equiv A^s U_n \pmod{\mathfrak{A}}$$

Hence $t = 0$ by the minimal property of μ , and

$$(3.4) \quad (A^s - 1)U_n \equiv 0 \pmod{\mathfrak{A}}, \text{ all large } n.$$

I say that

$$(3.41) \quad (A, \mathfrak{A}) = \mathfrak{D}.$$

For if $(A, \mathfrak{A}) = \mathfrak{B} \neq \mathfrak{D}$, then $(A^s - 1, \mathfrak{B}) = \mathfrak{D}$ so that by (3.4), $U_n \equiv 0 \pmod{\mathfrak{B}}$, all large n , contradicting the hypothesis that no divisor of \mathfrak{A} is a null divisor of (U) .

Let ϕ be any other restricted period with multiplier B , and write $\phi = u\mu + \theta$, $u \geq 1$, $0 \leq \theta < \mu$. Then by (3.3)

$$(3.5) \quad A^u U_{n+\theta} \equiv U_{n+\theta+u\mu} \equiv U_{n+\phi} \equiv BU_n \pmod{\mathfrak{A}}.$$

Therefore

$$(3.51) \quad (B, \mathfrak{A}) = \mathfrak{D}.$$

For if $(B, \mathfrak{A}) = \mathfrak{B} \neq \mathfrak{D}$, then by (3.5) and (3.41) $U_{n+\theta} \equiv 0 \pmod{\mathfrak{B}}$ for all large n , contradicting the hypothesis that no divisor of \mathfrak{A} is a null divisor of (U) .

Now the set of all elements of \mathfrak{D} which are prime to \mathfrak{A} form a group with respect to multiplication modulo \mathfrak{A} . (van der Waerden [1], Chapter XII.) Hence by (3.41) there exists an element A' of \mathfrak{D} such that $A'A \equiv I \pmod{\mathfrak{A}}$. Thus by (3.5)

$$U_{n+\theta} \equiv (A'A)^u U_{n+\theta} \equiv A'^u BU_n \pmod{\mathfrak{A}}.$$

Therefore $\theta = 0$ by the minimal property of μ , and μ divides ϕ .

It remains to prove the group property of the multipliers. It follows from (3.51) that the multipliers of (U) form a semi-group. All that remains is to show the existence of an inverse for each multiplier B .

⁸This statement is taken as an axiom in the discussion of the restricted period in part IV of W. A.

Since $(B, \mathfrak{A}) = \mathfrak{D}$, there exists an element B' of \mathfrak{D} such that $BB' \equiv 1 \pmod{\mathfrak{A}}$ while $U_{n+\phi} \equiv BU_n \pmod{\mathfrak{A}}$, $n \geq \nu$. On replacing n by $n - \phi$, we obtain for $n \geq \nu + \phi$

$$U_{n-\phi} \equiv (B'B)U_{n-\phi} \equiv B'U_n \pmod{\mathfrak{A}}.$$

Determine positive integers x, y such that $x\phi = y\lambda$ where λ as usual is the period of (U) . Then

$$U_{n+(x-1)\phi} \equiv U_{n-\phi+y\lambda} \equiv U_{n-\phi} \equiv B'U_n \pmod{\mathfrak{A}}.$$

Hence B' is a multiplier. This proof fails if $x = 1$. But then $\phi = \lambda$, $B \equiv I \pmod{\mathfrak{A}}$ so that $B' \equiv I \pmod{\mathfrak{A}}$ directly.

THEOREM 3.2. *Let \mathfrak{D} be a ring in which the chain condition ("Teilerkettenforderung") holds for ideals. Let (U) be a sequence of \mathfrak{D} and \mathfrak{A} an ideal such that (U) is periodic modulo \mathfrak{A} , but such that no divisor of \mathfrak{A} is a null divisor of (U) . Then if λ is the period and μ the restricted period of (U) modulo \mathfrak{A} , the multipliers of (U) form a cyclic group of order λ/μ . Furthermore the multiplier A of (3.3) associated with the restricted period is a generator of this group. (Ward [2].)*

PROOF. Consider the sequence of ideals

$$\mathfrak{A}_0 = (\mathfrak{A}, U_r), \quad \mathfrak{A}_1 = (\mathfrak{A}, U_r, U_{r+1}), \quad \mathfrak{A}_2 = (\mathfrak{A}, U_r, U_{r+1}, U_{r+2}), \dots$$

where r is a fixed number greater than the numeric of (U) . Then $\mathfrak{A}_{i+1} \supset \mathfrak{A}_i$, ($i = 0, 1, 2, \dots$). Therefore by the chain condition, all the \mathfrak{A}_i are equal from a certain point on. This resulting ideal \mathfrak{T} divides both \mathfrak{A} and every term of (U) beyond a certain point. Since (U) has no null divisors dividing \mathfrak{A} , $\mathfrak{T} = \mathfrak{D}$. Thus for some number l ,

$$(\mathfrak{A}, U_r, U_{r+1}, \dots, U_{r+l-1}) = \mathfrak{D}.$$

It follows that the ideal $(U_{r+1}, U_{r+2}, \dots, U_{r+l-1})$ contains a number

$$(3.6) \quad W = X_1 U_r + \dots + X_l U_{r+l-1}, \quad X \text{ in } \mathfrak{D}$$

such that $(W, \mathfrak{A}) = \mathfrak{D}$.

With the notation of the previous theorem, choose r so that the congruences (3.4) and (3.5) hold for $n \geq r$. Then by (3.6) $(A^* - 1)W \equiv (B - A^*)W \equiv 0 \pmod{\mathfrak{A}}$, or $A^* \equiv 1$, $B \equiv A^* \pmod{\mathfrak{A}}$. Now if we define s as the least integer such that $A^s \equiv 1 \pmod{\mathfrak{A}}$ the multipliers are seen to form a cyclic group of order s with A as a generator. From the minimal property of λ , $\lambda = \mu s$ and $s = \lambda/\mu$.

4. The following easily proved theorem on the divisors of any sequence extends a previous theorem of mine (Ward [1] theorem 5.3) and is the basis for the study of divisors of divisibility sequences.

THEOREM 4.0. *Let (U) be a sequence over \mathfrak{D} , and \mathfrak{M} any divisor of (U) . Then if $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, the set of places of apparition of \mathfrak{M} in (U) is the cross-cut of the sets of places of apparition of \mathfrak{A} and \mathfrak{B} in (U) .*

If in particular (U) is a divisibility sequence, the places of apparition of any divisor of (U) have the property of being closed under multiplication by positive integers. Furthermore, for any place of apparition s of a divisor \mathfrak{A} of (U) there will exist a number r dividing s and such that

$$(4.1) \quad U_r \equiv 0 \pmod{\mathfrak{A}}, \quad U_x \not\equiv 0 \pmod{\mathfrak{A}} \text{ if } x \mid r.$$

Following M. Hall [1], we call such a number r a *rank of apparition*⁹ of \mathfrak{A} in (U) . Of paramount interest and simplicity are the cases when a divisor of (U) has only a *finite* number of ranks of apparition. We then say the ranks of apparition constitute a *multiplicative set*. The theory of such sets is developed in part III of this paper. In the present section, we give a series of theorems on the finiteness of the ranks of apparition.

THEOREM 4.1. *If \mathfrak{A} is a divisor of the divisibility sequence (U) and if (U) is also periodic modulo \mathfrak{A} , then a necessary and sufficient condition that \mathfrak{A} shall have only a finite number of ranks of apparition are that all its ranks of apparition divide the restricted period of (U) modulo \mathfrak{A} .*

PROOF. The sufficiency of this condition is obvious. To establish its necessity, let r be a rank of apparition of \mathfrak{A} which does not divide the restricted period μ , and let $(r, \mu) = d \neq r$. For any positive integer t , we can choose positive integers x_t, y_t such that $td = y_t r - x_t \mu$. Then if $t \geq v/d$ (where v is the numeric of (U)),

$$U_{x_t \mu + t d} \equiv A^{x_t} Y_{td} \equiv U_{v_t r} \equiv 0 \pmod{\mathfrak{A}},$$

for (U) is a divisibility sequence and $U_r \equiv 0 \pmod{\mathfrak{A}}$. By theorem 3.2, $(A, \mathfrak{A}) = \mathfrak{D}$, so that $U_{td} \equiv 0 \pmod{\mathfrak{A}}$. Hence td is a place of apparition of \mathfrak{A} in (U) and is hence divisible by one or more ranks of apparition r' of \mathfrak{A} . If t is a prime number, r' must be divisible by t . For otherwise $r' \mid td$ implies $r' \mid d$, so that $r' \mid r$, $r' = r$, $d = r$. Hence

$$(4.2) \quad td \geq r' \geq t \quad t \text{ a prime.}$$

Since the number of primes is infinite, we may choose an infinite sequence of primes t_0, t_1, t_2, \dots such that $t_{n+1} > t_n d$, $t_0 d \geq v$. Then the inequality (4.2) implies the existence of an infinity of ranks of apparition.

THEOREM 4.2. *Let (U) be a divisibility sequence, and \mathfrak{A} a divisor of (U) such that (U) is purely periodic modulo \mathfrak{A} . Then \mathfrak{A} has only a finite number of ranks of apparition and each such rank divides the restricted period of (U) modulo \mathfrak{A} .*

PROOF. Let r be a rank of apparition of \mathfrak{A} in (U) . In view of the previous theorems we need only show that r divides μ . Let $(r, \mu) = d$. Then it suffices to show that d is a place of apparition of \mathfrak{A} , for then since $d \mid r$, $r = d$ and $r \mid \mu$.

⁹ In Ward [1], [3], [4], a rank of apparition was defined by the stricter requirement $U_r \equiv 0 \pmod{\mathfrak{A}}$, $U_x \not\equiv 0 \pmod{\mathfrak{A}}$ if $0 < x < r$, or in the case considered in Ward [1], the places of apparition were required to form an ideal. Although such a definition leads to many interesting results and is apparently met with frequently in the numerical cases of the Lucasian sequences from which the theory springs, (4.1) appears preferable.

Now there exist positive integers x, y such that $d = rx - \mu y$. Then by (3.3) and our hypotheses on r and (U) ,

$$A^y U_d \equiv U_{d+\mu y} \equiv U_{rx} \equiv 0 \pmod{\mathfrak{A}}.$$

But $(A, \mathfrak{A}) = \mathfrak{D}$. Hence $U_d \equiv 0 \pmod{\mathfrak{A}}$.

III. MULTIPLICATIVE SETS

5. Let r_1, r_2, \dots, r_n be n fixed numbers. The set M consisting of all their integral multiples will be called the *multiplicative set based on r_1, r_2, \dots, r_n* . If r_i divides r_j only for $i = j$, ($i, j = 1, \dots, n$), the r_i will be called the *generators* of the set. A generator is thus any element of the set which is irreducible in the set. Henceforth we assume that r_1, \dots, r_n are a set of generators of M .

The multiplicative set based on r_1, \dots, r_n is thus the maximal multiplicative semi-group containing r_1, \dots, r_n as its only irreducible elements.

The number $r = [r_1, r_2, \dots, r_n]$ (where here and later $[x, \dots, z]$ denotes the least common multiple or L.C.M. of the numbers x, \dots, z) is called the *rank* of the set M .

THEOREM 5.1. *If r is the rank of the multiplicative set M , every element of M is congruent modulo r to an element of the set greater than or equal to zero and less than r .*

PROOF. If x lies in M , there exists a generator r_i dividing x : $x = yr_i$. Also $r = zr_i$ by the definition of L.C.M. Hence if $x = qr + t$ where $0 \leq t < r$, then $t \equiv 0 \pmod{r_i}$ so that t lies in M and $x \equiv t \pmod{r}$.

We call a set of distinct elements of M which lie in a complete residue system modulo r a *representative set* of M .

THEOREM 5.2. *The number of elements in a representative set of M is given by the formula*

$$r \sum_{s=1}^n (-1)^{s-1} \sum_{(i)} \frac{1}{[r_{i_1}, r_{i_2}, \dots, r_{i_s}]}.$$

Here the inner summation is taken over all the $\binom{n}{s}$ distinct combinations i_1, \dots, i_s of the subscripts 1 to n of the generators r_i taken s at a time. We omit the (simple) proof of this theorem here.¹⁰

THEOREM 5.3. *The cross-cut of any two multiplicative sets is a multiplicative set, and each generator of the cross-cut is the L.C.M. of generators of the component sets.*

PROOF. Let the sets be M_1 and M_2 and let $M_3 = [M_1, M_2]$ be their cross-cut. M_3 is obviously a multiplicative set. Every element of M_3 lies both in M_1

¹⁰ For example take $r_1 = 6, r_2 = 10, r_3 = 15$. Then $r = 30$. A representative set consists of the eight numbers 0, 6, 10, 12, 15, 18, 20 and 24. The formula gives

$$30 \left\{ \left(\frac{1}{6} + \frac{1}{10} + \frac{1}{15} \right) - \left(\frac{1}{30} + \frac{1}{30} + \frac{1}{30} \right) + \left(\frac{1}{30} \right) \right\} = 5 + 3 + 2 - 3 + 1 = 8.$$

and M_2 and is hence divisible by a generator r_i of M_1 and a generator r'_j of M_2 and hence by their L.C.M. $[r_i, r'_j]$. Therefore M_3 is based on the set of nm elements $[r_1, r'_1], \dots, [r_n, r'_m]$ where the r_i and r'_j are respectively the generators of M_1 and M_2 . Hence the generators of M_3 consist of the irreducible elements in the set $[r_i, r'_j]$.

In like manner it is easy to prove

THEOREM 5.4. *The union of two multiplicative sets is a multiplicative set. If $r_1, \dots, r_n; r'_1, \dots, r'_m$ are the generators of the two sets, the generators of their union consist of the irreducible elements in the set of $n + m$ elements r_1, \dots, r'_m .*

THEOREM 5.5. *The aggregate of all multiplicative sets forms an arithmetic structure (O. Ore [1])—or (distributive) C-lattice—(G. Birkoff [1]) with respect to the operations of forming the union and cross-cut.¹¹*

PROOF. Let M_1, M_2, M_3 be any three multiplicative sets with generators $r_1, \dots, r_n; r'_1, \dots, r'_m; r''_1, \dots, r''_p$. Let $[M_i, M_j], (M_i, M_j)$ stand for cross-cut and union respectively. Then it suffices to show that

$$[M_1, (M_2, M_3)] = ((M_1, M_2), [M_1, M_3]).$$

But this equality is obvious, since by the preceding two theorems, both sets are based upon the numbers $[r_1, r'_1], \dots, [r_n, r'_m], [r_1, r''_1], \dots, [r_n, r''_p]$.

It is evident that the theorems of this section will also be true with slight changes of wording for multiplicative sets defined over a principal ideal ring \mathfrak{D} all of whose quotient rings $\mathfrak{D}/\mathfrak{A}$ are finite.

IV. LINEAR SEQUENCES

6. THEOREM 6.1. *Let (U) be a linear sequence, and let \mathfrak{A} be an ideal of \mathfrak{D} whose quotient ring $\mathfrak{D}/\mathfrak{A}$ is of finite order. Then (U) is periodic modulo \mathfrak{A} . Furthermore, if \mathfrak{A} is relatively prime to the last term C_k in the recursion (3.1) defining (U) , then (U) is purely periodic modulo \mathfrak{A} .*

PROOF. (Ward [2].) The sequence (U) will become periodic modulo \mathfrak{A} if any set of k residues of k consecutive terms of (U) modulo \mathfrak{A} occurs more than once. Now the first $n + k - 1$ terms of (U) contain the $n + 1$ sets of k consecutive terms $U_0, \dots, U_{k-1}; \dots; U_n, \dots, U_{n+k-1}$. Let T be the order of the finite ring $\mathfrak{D}/\mathfrak{A}$, so that a complete residue system modulo \mathfrak{A} contains T distinct elements. Then the period λ of (U) modulo \mathfrak{A} is at most $T^k - 1$. Thus (3.2) holds with $\lambda \leq T^k - 1, \nu \leq T^k - 1$.

¹¹ No simple relation appears to exist between the rank of two sets and the ranks of their cross-cut and union. For example, let $M_1 = \{36, 54\}, M_2 = \{18, 24\}$. Then $[M_1, M_2] = M_1, (M_1, M_2) = M_2$ so that M_2 contains M_1 . The rank of M_1 is 108, while the rank of M_2 is 72. Thus, the L. C. M. of the ranks of M_1 and M_2 is not the rank of their cross-cut, the G. C. D. of their ranks is not the G. C. D. of their union, nor does one rank divide the other.

Now assume that $(\mathfrak{A}, C_k) = \mathfrak{D}$. If (3.2) holds for $n \geq n_0 > 0$ we have from the recursion relation

$$\begin{aligned} U_{n_0+k-1+\lambda} &= C_1 U_{n_0+k-2+\lambda} + \cdots + C_k U_{n_0-1+\lambda} \\ U_{n_0+k-1} &= C_1 U_{n_0+k-2} + \cdots + C_k U_{n_0-1}. \end{aligned}$$

But by (3.2), $U_{n_0+k-r+\lambda} \equiv U_{n_0+k-r} \pmod{\mathfrak{A}}$, ($r = 1, 2, \dots, k$). Hence by subtraction

$$C_k(U_{n_0-1+\lambda} - U_{n_0-1}) \equiv 0 \pmod{\mathfrak{A}}.$$

Since $(C_k, \mathfrak{A}) = \mathfrak{D}$, (3.2) holds for $n \geq n_0 - 1$. Therefore (3.2) holds for $n \geq 0$ and (U) is purely periodic.

THEOREM 6.2.¹² *Let \mathfrak{D} be a domain of integrity, K a finite extension of its quotient field. Let $\Phi = \Phi(x_1, \dots, x_r; y)$ be a polynomial in the $r+1$ indeterminates x_1, \dots, x_r, y with coefficients in K and let $\omega_1, \omega_2, \dots, \omega_r$ be r fixed integers of K . Define a sequence (V) over K by*

$$V_n = \Phi(\omega_1^n, \omega_2^n, \dots, \omega_r^n; n), \quad (n = 0, 1, 2, \dots).$$

Then (V) is linear, and satisfies a recursion of the form (3.2) with coefficients in \mathfrak{D} . Every sequence which is linear over \mathfrak{D} may be thus obtained by a suitable choice of the extension field K and polynomial Φ .

PROOF. Let N be the maximum degree of Φ in the x , and M the maximum degree of Φ in y . Suppose that the polynomial Φ when written in the form

$$\Phi = \sum_{(k)} \Gamma_{(k)}(p) x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r} \quad 0 \leq k_1 + k_2 + \cdots + k_r \leq N$$

has precisely s terms $X_{(k)} = x_1^{k_1} \cdots x_r^{k_r}$. Here the $\Gamma_{(k)}(y)$ are polynomials in y of degree $\leq M$ with coefficients in K . Let $\Omega_k = \omega_1^{k_1} \cdots \omega_r^{k_r}$. Then there exists a polynomial $f(x) = x^t - c_1 x^{t-1} - \cdots - c_t$ with coefficients in \mathfrak{D} such that $f_{t-1}(\Omega_{(k)}) = 0$, ($k = 1, \dots, s$). Let

$$F(x) = f(x)^M = x^T - D_1 x - \cdots - D_T.$$

Then each $\Omega_{(k)}$ is a root of $F(x) = 0$ of multiplicity at least M , and D_1, \dots, D_T lie in \mathfrak{D} . But

$$(6.1) \quad V_n = \sum_{k=1}^s \Gamma_{(k)}(n) \Omega_{(k)}^n.$$

Hence (V) satisfies the recurrence

$$(6.2) \quad Y_{n+T} = D_1 Y_{n+T-1} + \cdots + D_T Y_n$$

associated with $F(x)$.

Now let (V) be a linear sequence of \mathfrak{D} defined by (6.2) and assume that the

¹² We discard the scheme of notation explained in section 2 for the statement and proof of this theorem.

distinct roots of the associated polynomial $F(x)$ are $\Omega_{(1)}, \dots, \Omega_{(s)}$. The Ω then lie in a finite extension K of the quotient field of \mathfrak{D} . Furthermore let each Ω be of multiplicity $\leq M$. Then every solution of (6.2) in \mathfrak{D} is of the form (6.1) if the coefficients of the polynomials $\Gamma_{(k)}(n)$ are suitably chosen in K .

It suffices then to take $\Phi = \sum_{k=1}^s \Gamma_{(k)}(y)X_{(k)}$ where $X_{(1)}, \dots, X_{(s)}$ and y are now our indeterminates.

THEOREM 6.21. *If \mathfrak{D} is a domain of integrity and $(U), (V)$ are linear over \mathfrak{D} , then the sequence (UV) whose general term is $U_n V_n$ is also linear over \mathfrak{D} .*

PROOF. It suffices to observe that the product of two polynomials Φ_1 and Φ_2 with different indeterminates x but the same y with coefficients in the finite extension fields K_1 and K_2 is again a polynomial of the same form whose coefficients lie in the union of K_1 and K_2 .

We shall call (UV) the *product* of the sequences (U) and (V) writing $(U) \cdot (V) = (UV)$. The operation of obtaining (UV) from (U) and (V) will be called *multiplication* of sequences. If we define the sum of two sequences as in Ward [5] by $(U) + (V) = (U + V)$, the following theorem is evident.

THEOREM 6.3. *The set of all sequences linear over a domain of integrity forms a commutative ring with respect to the operations of addition and multiplication defined above.*

This ring contains as its unit element the sequence $1, 1, 1, \dots$ satisfying the recursion $Y_{n+1} = Y_n$. It in general has no finite basis and is not a domain of integrity.

We may apply the operation of multiplication to divisibility sequences. The following theorem has important applications (Ward [6]).

THEOREM 6.4. *The product $(U) \cdot (V)$ of two divisibility sequences (U) and (V) is again a divisibility sequence. The set of places of apparition of any prime divisor \mathfrak{P} of $(U) \cdot (V)$ is the union of the sets of places of apparition of \mathfrak{P} in (U) and (V) . The ranks of apparition of \mathfrak{P} in $(U) \cdot (V)$ are contained among the ranks of apparition of \mathfrak{P} in (U) and (V) .*

The proof is simple, and will be omitted here. It is essential that the ideal divisor be a prime.

V. LUCASIAN SEQUENCES

7. We lose little generality¹³ by assuming that a given divisibility sequence is *normal*; that is, $U_0 = 0, U_1 = 1$. (Ward [1], section 11.) If in addition (U) is Lucasian, the results of part III and IV of the paper yield at once a great deal of information about the divisors of (U) and their places of apparition. For any ideal \mathfrak{A} prime to C_k and such that the quotient ring $\mathfrak{D}/\mathfrak{A}$ is finite is at

¹³ Since any number divides zero, every divisor of a divisibility sequence divides U_0 . This fact restricts the divisors at the outset unless $U_0 = 0$. Since 1 divides every number, U_1 divides every term of (U) . If U_1 is not zero, we can divide it out of the sequence obtaining a new divisibility sequence in which $U_1 = 1$.

once a divisor of (U) , and all its ranks of apparition divide the restricted period of (U) . The least common multiple r of these ranks of apparition gives us the period of the places of apparition of \mathfrak{A} in the sequence. In contrast to the behavior of the period and restricted period of (U) modulo \mathfrak{A} , the rank r modulo \mathfrak{A} does not appear to be effectively calculable merely from a knowledge of the ranks of constituent factors of \mathfrak{A} . However if $\mathfrak{A} = [\mathfrak{B}, \mathfrak{C}]$, the set of places of apparition of \mathfrak{A} are effectively calculable from the places of apparition of \mathfrak{B} and \mathfrak{C} by virtue of theorems 4.0 and 5.3.

I hope to discuss the theory of Lucasian sequences in relation to the operation of multiplication of sequences defined in part IV in some detail elsewhere.

CALIFORNIA INSTITUTE OF TECHNOLOGY

REFERENCES

- G. BIRKHOFF, 1 Bulletin American Math. Soc. vol. 45 (1934) pp. 613-619.
R. D. CARMICHAEL, 1. Quarterly Journal of Mathematics, vol. 48 (1920) pp. 343-372.
L. E. DICKSON, 1. *History*, volume 1, chapter XVII.
MARSHALL HALL, 1. American Journal of Mathematics, vol. 47 (1936) pp. 577-584.
E. LUCAS, 1. American Journal of Mathematics, vol. 1 (1878) pp. 184-240, pp. 289-321.
2. *Theorie des Nombres*, Paris 1891.
O. ORE, 1. These Annals, (2) vol. 36 (1935) pp. 406-437.
B. L. VAN DER WAERDEN, *Modern Algebra*, vol. 2, Berlin 1931.
M. WARD, 1. These Annals, vol. 38 (1937) pp. 725-732.
2. Transactions of the American Math. Soc., vol. 33 (1931) pp. 162-164.
3. Bulletin of the American Math. Soc., vol. 42 (1936) pp. 843-845.
4. Transactions of the American Math. Soc., vol. 41 (1937), pp. 276-286.
5. Transactions of the American Math. Soc., vol. 35 (1933) pp. 600-628.
6. To appear in the Transactions of the American Math. Soc.

RESIDUATED LATTICES*

BY

MORGAN WARD AND R. P. DILWORTH

I. INTRODUCTION

1. We propose to develop here a systematic theory of lattices† over which an auxiliary operation of multiplication or residuation is defined. We begin by showing that the two operations correspond to one another; under quite general conditions in every lattice over which a multiplication is defined a residuation may be defined and conversely. The residuation and multiplication we introduce have the properties of the like-named operations in the particular instance of polynomial ideal theory.

We next give various necessary conditions and sufficient conditions that such operations may exist in an arbitrary lattice, and apply our results to projective geometries and Boolean algebras.

In the third division of the paper we extend E. Noether's decomposition theorems of the ideal theory of commutative rings to general lattice theory. The introduction of a multiplication is obviously necessary for such a generalization. The surprising result emerges that the decomposition theorems are largely independent of the modular axiom, as we show by specific examples. We take this occasion to correct an error made in the preliminary account of our researches (Ward and Dilworth [1]). Since we wrote this, we have obtained many new results which we give here for the first time.

We plan to describe the main part of our investigations of distributive residuated lattices elsewhere (Ward and Dilworth [1], §§5, 6). Here we settle some questions raised by one of us (Ward [1]) as to the significance of certain auxiliary conditions which a residuation may satisfy by showing in all cases that they imply that the lattice is distributive.

2. It was not until this paper was virtually completed that we learned of the investigation of Krull upon this subject (Krull [1]). There is, however, very little duplication between our results and Krull's. Krull was chiefly concerned with the problem of finding out in what manner the Noether decomposition theorems could be extended to a residuated lattice in which the chain condition was weakened and no connection was assumed between irreducibles and primary elements.

* Presented to the Society, March 27, 1937, and April 9, 1938; received by the editors April 21, 1938.

† For a connected account of lattice theory and the literature up to 1937, see Köthe [1].

3. We shall use the following terminology and notation. \mathfrak{S} is a fixed lattice with elements a, \dots, y with or without subscripts. Sublattices of \mathfrak{S} are denoted by German capitals $\mathfrak{A}, \mathfrak{B}$. The letters $\mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}$ are reserved to denote subsets of \mathfrak{S} which are not necessarily sublattices. We write $x \in \mathfrak{X}$ for "the set \mathfrak{X} contains the element x ." The expressions $x \triangleright y$ or $y \triangleleft x$, $x \ntriangleright y$ denote, as usual, x divides y , x does not divide y . We write $x = y$ if $x \triangleright y$ and $y \triangleright x$ (Ore [1], p. 42) and $x > y$ or $y < x$ for x covers y (Birkhoff [1]). We use (x, y) and $[x, y]$ for union and cross-cut. If the unit and null elements exist, we denote them by i and z , respectively. Elements covered by i are called divisor-free. If $(a, b) = i$, a and b are said to be co-prime. If every pair of distinct elements of a set \mathfrak{X} are co-prime, the set is said to be co-prime. An element n of \mathfrak{S} is called a node if either $x \triangleright n$ or $n \triangleright x$ for every x of \mathfrak{S} . A sublattice \mathfrak{A} is said to be dense over \mathfrak{S} if $a_1, a_2 \in \mathfrak{A}$ and $a_1 \triangleright x \triangleright a_2$ imply \mathfrak{A} contains x . If every set of elements finite or infinite of \mathfrak{S} has a cross-cut (union), \mathfrak{S} is said to be completely closed relative to cross-cut (union). Two properties P and Q which \mathfrak{S} may possess are said to be completely independent if there exist instances of lattices in which both P and Q hold, neither holds, P holds but not Q , Q holds but not P .

We shall find it convenient to use the following conditions for a distributive lattice either of which is equivalent to the usual formulation:

- (i) $b \triangleright [a, c]$ implies $b = [(b, a), (b, c)]$.
- (ii) $(a, c) \triangleright b$ implies $b = ([b, a], [b, c])$.

II. RESIDUATIONS AND MULTIPLICATIONS

4. Assume that \mathfrak{S} contains i . A well-defined one-valued binary operation $x:y$ is called a residuation over \mathfrak{S} if the following conditions are satisfied:

- R 1. If \mathfrak{S} contains a, b , then \mathfrak{S} contains $a:b$.
- R 2. $a:b = i$ if and only if $a \triangleright b$.
- R 3. $a \triangleright b$ implies that $a:c \triangleright b:c$ and $c:b \triangleright c:a$.
- R 4. $(a:b):c = (a:c):b$.
- R 5. $[a, b]:c = [a:c, b:c]$.
- R 6. $c:(a, b) = [c:a, c:b]$.

We postpone the consideration of the dual residuation for our second paper.

A well defined binary operation $x \cdot y$ (or xy) is called a multiplication over \mathfrak{S} if the following conditions are satisfied:

- M 1. If \mathfrak{S} contains a, b , then \mathfrak{S} contains $a \cdot b$.
- M 2. If $a = b$, then $a \cdot c = b \cdot c$.
- M 3. $a \cdot b = b \cdot a$.

M 4. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

M 5. If \mathfrak{S} contains i , then $a \cdot i = a$.

M 6. $a \cdot (b, c) = (a \cdot b, a \cdot c)$.

It may be shown (Ward [1]) that a residuation exists satisfying R 1–R 6 if a multiplication over \mathfrak{S} exists satisfying M 1–M 6 and the following condition:

M 7. \mathfrak{S} is completely closed with respect to union, and the product of the unions of any two sets of elements of \mathfrak{S} is the union of the products of all pairs of elements in the sets.

This residual $a:b$, satisfying R 1–R 6, is defined as follows:

DEFINITION 4.1. (i) $a \triangleright (a:b)b$; (ii) if $a \triangleright xb$, then $a:b \triangleright x$.

If we take for $x \cdot y$ the cross-cut $[x, y]$, then conditions M 1–M 6 are all satisfied provided that \mathfrak{S} is distributive. If M 7 holds, the lattice is said to be completely distributive with respect to union. Hence (Ward [2]) every completely distributive lattice may be residuated in at least one way.

Another condition* insuring the existence of a residual is the following:

M 8. For any two elements a, b of \mathfrak{S} , the ascending chain condition holds in the set \mathfrak{X} of all x such that $a \triangleright xb$.

M 8 insures the existence of a union of the set \mathfrak{X} expressible as the union of a finite number of elements of \mathfrak{X} (Ore [1], §2). This union is the required residual.

We list for reference the more important properties of residuation and multiplication (Ward [1], Dilworth [1]):

$$(4.1) \quad a:b \triangleright a.$$

$$(4.7) \quad \text{If } r=a:b \text{ and } s=a:r, \text{ then}$$

$$(4.2) \quad a:(a:b) \triangleright (a, b).$$

$$r=a:s.$$

$$(4.3) \quad (a:b):c = a:(bc).$$

$$(4.71) \quad a \triangleright b \text{ implies } ac \triangleright bc.$$

$$(4.4) \quad [a, b]:b = a:b.$$

$$(4.8) \quad [a, b] \triangleright ab \triangleright a, b.$$

$$(4.5) \quad a:(a, b) = a:b.$$

$$(4.81) \quad ab:a \triangleright b.$$

$$(4.51) \quad c:[a, b] \triangleright (c:a, c:b).$$

$$(4.9) \quad a=bc \text{ implies } b \triangleright a.$$

$$(4.6) \quad \text{If } a:b = a, \text{ then } a \triangleright bx \\ \text{implies } a \triangleright x.$$

$$(4.10) \quad (a, b) = i \text{ implies } ab = [a, b] \\ \text{and } (a, bc) = (a, c).$$

$$(4.11) \quad (a, b):c \triangleright (a:c, b:c).$$

$$(4.12) \quad \text{In any chain of powers } a, a^2, a^3, \dots \text{ either all elements are distinct or} \\ \text{all are equal from a certain point on.}$$

* This axiom is equivalent to the ascending chain condition, as may be seen on taking $a=b=i$. We state it in this manner to emphasize the analogy with R 8 which is not equivalent to the descending chain condition.

5. We shall now exhibit a remarkable reciprocity between the operations of residuation and multiplication.

THEOREM 5.1. *If a residuation $x:y$ exists in \mathfrak{S} satisfying conditions R 1–R 6, and if either of the conditions R 7 or R 8 below holds, then a multiplication $x \cdot y$ exists in \mathfrak{S} satisfying M 1–M 6.*

R 7. *\mathfrak{S} is completely closed with respect to cross-cut, and if c is the cross-cut of a set \mathfrak{X} , then the cross-cut of the set of all $a:x$, where $a \in \mathfrak{S}$, $x \in \mathfrak{X}$, equals $a:c$.*

R 8. *For any two elements a, b of \mathfrak{S} the descending chain condition holds in the set \mathfrak{Y} of all elements y such that $y:a \triangleright b$.*

R 8 is satisfied in many important instances where R 7 does not hold and where the descending chain condition does not hold; for example, in polynomial ideal theory and the classical ideal theory of algebraic rings.

The proof is as follows. Define the “product” $a \cdot b$ of any two elements a and b of \mathfrak{S} :

DEFINITION 5.1. (i) $a \cdot b : a \triangleright b$; (ii) if $y:a \triangleright b$, then $y \triangleright a \cdot b$.

Postulate M 1 is satisfied. For the set \mathfrak{Y} of all y such that $y:a \triangleright b$ is non-empty, since it includes b by (4.1). If R 7 holds, \mathfrak{Y} has a cross-cut $p = a \cdot b$ satisfying Definition 5.1, (ii), and the cross-cut $[\mathfrak{Y}:a]$ equals $p:a$. Definition 5.1, (i) is therefore satisfied with $p = a \cdot b$ by the definition of cross-cut.

If R 8 holds, then \mathfrak{Y} again has a cross-cut p representable as the cross-cut of a finite number of y , $p = [y_1, \dots, y_k]$. Thus Definition 5.1, (ii) is satisfied, and Definition 5.1, (i) is satisfied by R 5.

Postulate M 2 is satisfied. For by R 3, $a=b$ implies $a \triangleright b$ implies $a \cdot c:b \triangleright a \cdot c:a$. Hence by Definition 5.1, (i), $a \cdot c:b \triangleright c$ so that by Definition 5.1, (ii), $a \cdot c \triangleright b \cdot c$. Similarly $a=b$ implies $b \cdot c \triangleright a \cdot c$, so that M 2 follows.

Postulate M 3 is satisfied. For $b \cdot a$ exists, and by Definition 5.1, if $y:b \triangleright a$, then $y \triangleright b \cdot a$. Now by R 4, Definition 5.1, (i) and R 2, $(a \cdot b:b):a = (a \cdot b:a):b = i$. Hence by R 2, $a \cdot b:b \triangleright a$. Hence $a \cdot b \triangleright b \cdot a$. Similarly, $b \cdot a \triangleright a \cdot b$, $a \cdot b = b \cdot a$. Condition R 4 is thus seen to insure that multiplication is commutative.

Postulate M 4 is satisfied. For by Definition 5.1, (i), $\{a \cdot (c \cdot b)\}:a \triangleright c \cdot b$. Hence $\{\{a \cdot (c \cdot b)\}:a\}:c \triangleright c \cdot b:c$ by R 3. But $c \cdot b:c \triangleright b$ by Definition 5.1, (i). Therefore $\{\{a \cdot (c \cdot b)\}:a\}:c \triangleright b$ or by R 4, $\{\{a \cdot (c \cdot b)\}:c\}:a \triangleright b$. Hence $\{a(cb):c\} \triangleright ab$ and $a(cb) \triangleright c(ab)$ by Definition 5.1, (ii). Interchanging a and c , $c(ab) \triangleright a(cb)$. Hence $a(cb) = c(ab)$, or by M 3 and M 2, $(ab)c = a(bc)$.

Postulate M 5 is satisfied. For by R 2, $a:a \triangleright i$. Hence $a \triangleright ai$ by Definition 5.1, (ii). Now $ia:i \triangleright a$ by Definition 5.1, (i). But by (4.10) and M 3, $ia:i = ia = ai$. Hence $ai \triangleright a$, $a = ai$.

Postulate M 6 is satisfied. For since $(b, c) \triangleright b$, $a(b, c) \triangleright ab$ by (4.71). Similarly $a(b, c) \triangleright ac$. Hence $a(b, c) \triangleright (ab, ac)$. Next $(ab, ac):a \triangleright ab:a \triangleright b$ by R 3

and (4.81). Similarly $(ab, ac):a \triangleright c$. Hence $(ab, ac):a \triangleright (b, c)$. Therefore by Definition 5.1, (ii), $(ab, ac) \triangleright a(b, c)$ giving M 6. This completes the proof.

DEFINITION 5.2. (i) $a \triangleright (a \circ b)b$; (ii) if $a \triangleright xb$, then $a \circ b \triangleright x$.

The following theorem further illustrates the reciprocity between multiplication and residuation:

THEOREM 5.2. If $a \circ b$ is defined as above, where the multiplication xy is defined by Definition 5.1, then $a \circ b = a:b$.

For since $a:b \triangleright a:b$, we have $a \triangleright (a:b)b$ by Definition 5.1, (ii). Therefore by Definition 5.2, (ii), $a \circ b \triangleright a:b$. Now $a \triangleright (a \circ b)b$ by Definition 5.2, (i). Therefore by R 3, $a:b \triangleright \{(a \circ b)b:b\}$. But by M 3 and Definition 5.1, (ii), $(a \circ b)b:b \triangleright a \circ b$. Hence $a:b \triangleright a \circ b$, $a:b = a \circ b$.

Hereafter when we speak of a "residuated lattice," we shall mean a lattice in which both a residuation and its associated multiplication are defined satisfying M 1–M 6, R 1–R 6 and the conditions of Definitions 5.1 and 5.2.

6. We may prove by simple examples the following theorem:

THEOREM 6.1. The Dedekind modular condition and the existence of a residual or a multiplication are completely independent properties of a lattice.

It is important to observe that a given lattice may usually be residuated in several different ways. To give a simple example, consider the lattice of four elements $i > a > b > z$. The tables for $x:y$ and $x \cdot y$ are as follows:

$x:y$	i	a	b	z	$x \cdot y$	i	a	b	z
i	i	i	i	i	i	i	a	b	z
a	a	i	i	i	a	a	*	*	z
b	b	*	i	i	b	b	*	*	z
z	z	*	*	i	z	z	z	z	z

A brief analysis discloses that the combinations denoted by stars may be determined in six ways so as to satisfy R 1–R 8, M 1–M 8:

	I	II	III	IV	V	VI
$b:a$	a	a	b	a	b	b
$z:a$	a	b	b	z	z	z
$z:b$	a	a	a	z	b	z
$a \cdot a$	z	b	a	b	a	a
$a \cdot b$	z	z	z	b	b	b
$b \cdot b$	z	z	z	b	z	b

Cases II and VI are illustrated in the lattice of the ring of integers modulo 8. Here i is the set of residue classes $\{1, 3, 5, 7\}$, a is $\{2, 6\}$, b is $\{4\}$, and z is $\{8\}$. Case. II ensues on taking for $x \cdot y$ multiplication modulo 8, and case VI on taking for $x \cdot y$ the L.C.M. operation.

The only other lattice of order four is i, a, b, z with $(a, b) = i$, $[a, b] = z$. This lattice may be residuated in only one way, an illustration of a general theorem on the residuation of Boolean algebras which we prove later.

III. CONDITIONS FOR RESIDUATION

7. In this division of the paper we shall give various sufficient conditions and necessary conditions for the existence of a residuation in a given lattice.

THEOREM 7.1. *A necessary condition that a lattice \mathfrak{S} can be residuated is that any co-prime set of elements of \mathfrak{S} , a_1, a_2, \dots, a_r , generates a Boolean algebra \mathfrak{B} of order 2^r .*

This condition is not sufficient for a residuation to exist. It is satisfied, for example, in Dedekind's free modular lattice on three elements of order twenty-eight (Dedekind [1], Birkhoff [1], Ore [1]) which we shall prove later cannot be residuated.

Let a_1, a_2, \dots, a_r be a co-prime set so that

$$(7.1) \quad (a_u, a_v) = i, \quad u, v = 1, \dots, r; u \neq v.$$

The set will remain co-prime if we adjoin i to it. We shall suppose that this has been done, and for definiteness choose our notation so that $a_1 = i$.

Form from the set of a 's the "ray" Π of 2^r formally distinct cross-cuts:

$$u = [a_{u_1}, a_{u_2}, \dots, a_{u_L}], \quad 1 \leq u_1 < u_2 < \dots < u_L \leq r; 1 \leq L \leq r.$$

We call the a_u the *constituents* of u . The ray Π is obviously closed under cross-cut. We shall show that Π is the Boolean algebra required.

LEMMA 7.1. *If x is any element of \mathfrak{S} , then*

$$(x, [a_u, a_v]) = [(x, a_u), (x, a_v)].$$

This result is trivial if $u = v$. But if $u \neq v$, $(a_u, a_v) = i$. Hence $((x, a_u), (x, a_v)) = i$. Therefore by (4.10) and M 6,

$$\begin{aligned} [(x, a_u), (x, a_v)] &= (x, a_u)(x, a_v) = (x^2, xa_v, a_u x, a_u a_v) \\ &= (x^2, x(a_u, a_v), a_u a_v) = (x, a_u a_v) = (x, [a_u, a_v]) \end{aligned}$$

by M 3 and M 6.

The following two corollaries of this lemma may be proved by induction:

LEMMA 7.2. *If $u = [a_{u_1}, \dots, a_{u_L}]$, then $(x, u) = [(x, a_{u_1}), \dots, (x, a_{u_L})]$.*

LEMMA 7.3. *If $u = [a_{u_1}, \dots, a_{u_L}]$ and $v = [a_{v_1}, \dots, a_{v_M}]$, then*

$$(u, v) = [(a_{u_1}, a_{v_1}), \dots, (a_u, a_v), \dots, (a_{u_L}, a_{v_M})].$$

LEMMA 7.4. *If x is any element of \mathfrak{S} and if $(x, b) = (x, c) = i$, then*

$$(x, [b, c]) = [(x, b), (x, c)].$$

It suffices to show that $(x, [b, c]) = i$. But $(x, [b, c]) = \sup(x bc) = (x, bx, bc)$ (by (4.10)) $= (x, b(x, c)) = (x, b) = i$.

We return to the proof of our theorem. *The ray Π is a lattice.* For by Lemma 7.3 and (7.1) it is closed under union. *The lattice is of order 2^r .* It suffices to show that if $u = v$, the constituents of u and v are identical. But if $u = v$, $a_u \supseteq v$. Hence by Lemma 7.2,

$$a_u = (a_u, v) = [(a_u, a_{v_1}), \dots, (a_u, a_{v_M})].$$

Since $(a_u, a_v) = a_u$ or i , a_u must be a constituent of v . Thus every constituent of u is a constituent of v . Similarly every constituent of v is a constituent of u , so that u and v are not formally distinct.

The lattice is distributive. For by Lemma 7.3, if $w = [a_{w_1}, \dots, a_{w_N}]$, then

$$\begin{aligned} (w, [u, v]) &= [\dots, (a_w, [u, v]), \dots] \\ &= [\dots, [(a_w, u), (a_w, v)], \dots] \\ &= [[\dots, (a_w, u), \dots], [\dots, (a_w, v), \dots]] \\ &= [(w, u), (w, v)], \end{aligned}$$

by Lemma 7.2.

The lattice is complemented. For we assign to the element u the complement

$$u' = [a_{u'_{L+1}}, \dots, a_{u'_r}]$$

where u'_{L+1}, \dots, u'_r is the selection complementary to u_1, \dots, u_L from $1, 2, \dots, r$. Then $[u, u'] = [a_1, a_2, \dots, a_r]$, the null element of the lattice \mathfrak{B} , and $(u, u') = i$ by Lemma 7.3. Hence \mathfrak{B} is a complemented distributive lattice and thus a Boolean algebra.

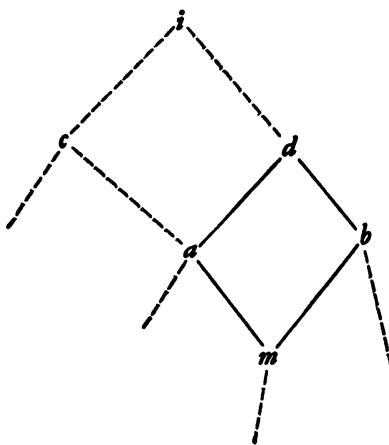
THEOREM 7.2. *If a_1, \dots, a_r is a co-prime set of divisor-free elements of a residuated lattice \mathfrak{S} , then the Boolean algebra \mathfrak{B} which they generate is dense over \mathfrak{S} .*

For if u lies in \mathfrak{B} and $x \supseteq u$, then $x = [(x, a_{u_1}), \dots, (x, a_{u_L})]$ by Lemma 7.2. Since $(x, a_u) = i$ or a_u , the result follows.

This theorem is quite useful in examining finite lattices to see whether or not they can be residuated. We have also found the following exclusion principle useful in this connection. The proof (which we omit) follows from Lemma 7.4.

THEOREM 7.3. EXCLUSION PRINCIPLE. Let a, b, c , and d be any four elements of a residuated lattice \mathfrak{S} with an ascending chain condition such that $c \triangleright a, c \neq i; (b, c) = i, d > a, d > b$. Then if $m = [b, c]$ we must have $[a, b] = m$ and $a > m, b > m$. Furthermore a and b are the only elements covered by d and covering m in the lattice.

In schematic form (Klein [1], Birkhoff [2]) the lattice must have the following structure, where the dotted lines indicate that the configuration of the remaining lattice parts is irrelevant.



As a simple application, if the reader will diagram the lattice of order nine on three elements b, c , and f where $c \triangleright f$ (Dedekind [1]) and take $a = [c, (f, b)], d = (f, b)$, he will see that this lattice cannot be residuated.

THEOREM 7.31. The only complemented lattices which can be residuated are Boolean algebras.

Since by hypothesis the lattice is complemented, it is sufficient to show that it is distributive. We need the following lemma:

LEMMA 7.5. If $(b, c) = i$ and $a \triangleright [b, c]$, then $(a:b, a:c) = i$.

For we have

$$\begin{aligned} (a:b, a:c) &= (a:b, a:c):(b, c) = [(a:b, a:c):b, (a:b, a:c):c] \\ &\triangleright [(a:c):b, (a:b):c] = a:cb = a:[c, b] = i. \end{aligned}$$

A complement a' of a is defined by the following conditions:

DEFINITION 7.1. $(a, a') = i, [a, a'] = z$, where z is the null element of \mathfrak{S} .

Let a, b, c be any three elements of \mathfrak{S} and assume that

$$(i) \quad a \triangleright [b, c].$$

Let $u = [(a, b), (a, c)]$ and $v = ([b, c], a')$. It suffices to show that (i) im-

plies $u=a$. We have trivially $u \triangleright a$ and $v \triangleright a'$. Hence $(u, v) = i$ by Definition 7.1 so that $uv = [u, v]$. Hence $b:uv = b:[u, v] \triangleright (b:u, b:v)$ by (4.51). Now $b:u \triangleright b:a$ by R 3 and $b:v = [b:[b, c], b:a'] = b:a'$. Hence $b:uv \triangleright (b:a, b:a')$. But by Definition 7.1, $(a, a') = i$ and $b \triangleright [a, a']$. Hence by Lemma 7.5, $(b:a, b:a') = i$ so that $b \triangleright uv$. Similarly $c \triangleright uv$ so that $[b, c] \triangleright uv$, or by (i), $a \triangleright uv$, $a:v \triangleright u$. But $a:v = [a:[b, c], a:a'] = a:a' = a$ by (i) and Definition 7.1. Hence $a \triangleright u$ so that $a=u$.

COROLLARY. *The only projective geometries (Birkhoff [3]) which can be residuated are Boolean algebras.*

In case the ascending chain condition holds in \mathfrak{S} , one can give a much shorter proof by showing that each element may be represented as a cross-cut of a finite number of divisor-free elements and appealing to Theorem 7.1.

THEOREM 7.4. *The only multiplication which can be defined over a Boolean algebra is the cross-cut operation.*

In view of our reciprocity theorems it suffices to show that only one residual is definable. One of us has shown elsewhere (Dilworth [1]) that $a \vee b'$ is a residuation in a Boolean algebra. Suppose that $a:b$ were another. Then

$$(a:b):(a \vee b') = (a:b):b' = a:bb' = i;$$

$$(a \vee b'):(a:b) \triangleright \{a:(a:b)\} \vee \{b':(a:b)\} \triangleright b \vee b' = i.$$

Hence $a:b = a \vee b'$.

An interesting consequence of Theorem 7.4 is the following corollary:

COROLLARY. *In the ring of integers modulo a square-free integer, the operations of multiplication and L.C.M. are identical.*

8. We consider in this section some sufficient conditions for residuation. We have the following theorem:

THEOREM 8.1. *Every lattice in which only one divisor-free element exists can be residuated in at least one way.*

Let d be the single divisor-free element. We define the residual $a:b$ by the conditions:

$$(i) \quad a:i = a; \quad (ii) \quad a:b = i \text{ if } a \triangleright b; \quad (iii) \quad a:b = d \text{ if } a \ntriangleright b, b \neq i.$$

Then postulates R 1 and R 2 are obviously satisfied.

R 3 is satisfied. For assume $a \triangleright b$. Then $a:c$ always divides $b:c$ except possibly when $b:c = i$. But then $b \triangleright c$; so $a \triangleright c$, $a:c = i$. Similarly $c:b \triangleright c:a$.

R 4 is satisfied. For R 4 obviously holds if a , b , or c equals i . If $a \triangleright b$, $a \neq i$,

then $a:c \triangleright a \triangleright b$; so $(a:c):b = (a:b):c = i$. If $a:b \triangleright c$ but $a \not\triangleright b$, $b \neq i$, $a \not\triangleright c$, $c \neq i$, then $a:b = a:c = d$, whence $(a:b):c = d:c = i = d:b = (a:c):b$. If $a \not\triangleright b$, $a \not\triangleright c$, $a:b \not\triangleright c$, $a:c \not\triangleright b$, then b or $c = i$.

R 5 is satisfied. For if $c = i$, R 5 is trivial. If $a \triangleright c$, $b \triangleright c$, then $[a, b] \triangleright c$ and R 5 obviously holds. If $a \not\triangleright c$, $c \neq i$, then $[a, b] \not\triangleright c$ and $[a, b]:c = d = [a:c, b:c]$. Hence R 5 holds in general.

In exactly the same way we show that R 6 is satisfied.

F. Klein has shown (Klein [1]) that the modular or distributive properties of a lattice built up of sublattices connected by nodes ("Schnurstellen") depend upon the modular or distributive properties of the sublattices. We prove a similar result for residuation.

THEOREM 8.2. *A lattice built up out of a set of residuated lattices connected into a chain by nodes can be residuated.*

It will suffice to prove the theorem for the case of two lattices connected by a node.

Let \mathfrak{S} be composed of two lattices \mathfrak{S}_1 and \mathfrak{S}_2 connected by a node, so that $x_1 \in \mathfrak{S}_1$ and $x_2 \in \mathfrak{S}_2$ imply $x_1 \triangleright x_2$. Let i be the unit element of \mathfrak{S}_1 . We shall consider the nodal element as belonging to \mathfrak{S}_1 , and let $x:y$ denote the residuation in \mathfrak{S}_1 , $x \circ y$, the residuation in \mathfrak{S}_2 when the nodal element is replaced by i .

We now define a residual in \mathfrak{S} by the conditions:

$$\begin{aligned} a:b &= a : b \text{ if } a, b \in \mathfrak{S}_1, \quad a:b = a \circ b \text{ if } a, b \in \mathfrak{S}_2, \\ a:b &= i \text{ if } a \in \mathfrak{S}_1, b \in \mathfrak{S}_2, \quad a:b = a \text{ if } a \in \mathfrak{S}_2, b \in \mathfrak{S}_1. \end{aligned}$$

Then postulates R 1, R 2, and R 3 are obviously satisfied.

Postulate R 4 is satisfied. For clearly $a:c \triangleright a$. Hence if $a \triangleright b$, then $(a:b):c = (a:c):b$ by R 3. Also if $a \in \mathfrak{S}_1$, then $(a:b):c = (a:c):b$. Suppose that $a \in \mathfrak{S}_2$. Then if $b \in \mathfrak{S}_2$, $c \in \mathfrak{S}_2$, we have $(a:b):c = (a:c):b$. Similarly if $b \in \mathfrak{S}_1$, $c \in \mathfrak{S}_1$, then $(a:b):c = (a:c):b$. Finally if $b \in \mathfrak{S}_1$, $c \in \mathfrak{S}_2$, then $(a:b):c = a \circ c = (a:c):b$.

Postulate R 5 is satisfied. For R 5 is trivial if a , b , or $c = i$. If $a \triangleright b$, R 5 follows from R 3. If $a, b \in \mathfrak{S}_1$ or $a, b \in \mathfrak{S}_2$, R 5 holds since it holds in \mathfrak{S}_1 and \mathfrak{S}_2 .

In a similar manner one can show that R 6 is satisfied, and the proof is complete.

By the *direct product* (Birkhoff [4]) \mathfrak{S} of the lattices $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ we mean the set of vectors $a = \{a_1, \dots, a_n\}$, $(a_i \in \mathfrak{S}_i)$, where the operations are defined by

$$\begin{aligned} [a, b] &= \{[a_1, b_1], \dots, [a_n, b_n]\}, \\ (a, b) &= \{(a_1, b_1), \dots, (a_n, b_n)\}, \end{aligned}$$

and $a \triangleright b$ if and only if $a_i \triangleright b_i$, ($i = 1, \dots, n$).

If the \mathfrak{S}_i are residuated lattices, then \mathfrak{S} can be residuated, since we may define $a:b$ to be $\{a_1:b_1, \dots, a_n:b_n\}$.

We shall call two sublattices $\mathfrak{S}_1, \mathfrak{S}_2$ of \mathfrak{S} co-prime if $a_1 \in \mathfrak{S}_1, a_2 \in \mathfrak{S}_2$ implies that $(a_1, a_2) = i$. The sublattices $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ will be called a co-prime set if they are co-prime in pairs.

We note that if \mathfrak{S} is the direct product of the sublattices $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ with unit elements, then \mathfrak{S} contains sublattices $\mathfrak{S}'_1, \dots, \mathfrak{S}'_n$ simply isomorphic to $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ and such that $\mathfrak{S}'_1, \dots, \mathfrak{S}'_n$ is a co-prime set. Birkhoff (Birkhoff [4]) has defined sublattices $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ to be "strongly" co-prime if each \mathfrak{S}_i is co-prime to the lattice generated by the remaining lattices. Clearly strong co-primeness implies co-primeness in the ordinary sense. Moreover if \mathfrak{S} is residuated, Lemma 7.4 shows that co-primeness implies strong co-primeness, so that for residuated lattices the notions are identical. We now prove a converse result.

THEOREM 8.3. *Let $\mathfrak{S}_1, \mathfrak{S}_2, \dots, \mathfrak{S}_n$ be a set of co-prime sublattices of a residuated lattice \mathfrak{S} such that each element of \mathfrak{S} can be expressed as a cross-cut of elements of $\mathfrak{S}_1, \dots, \mathfrak{S}_n$. Then \mathfrak{S} is the direct product of $\mathfrak{S}_1, \dots, \mathfrak{S}_n$, and each \mathfrak{S}_i can be residuated.*

Let $a = [a_1, a_2, \dots, a_n], (a_i \in \mathfrak{S}_i), b = [b_1, b_2, \dots, b_n], (b_i \in \mathfrak{S}_i)$. Then $[a, b] = [[a_1, b_1], \dots, [a_n, b_n]]$. Furthermore

$$(a, b) = [(a_1, b_1), \dots, (a_n, b_n)].$$

For by Lemma 7.2,

$$\begin{aligned} (a, b) &= (a, [b_1, \dots, b_n]) = [(a, b_1), \dots, (a, b_n)] \\ &= [\dots, (a_j, b_k), \dots] = [(a_1, b_1), \dots, (a_n, b_n)], \end{aligned}$$

since $(a_j, b_k) = i$ if $j \neq k$.

LEMMA 8.1. *If b_1, b_2, \dots, b_n are a co-prime set, then*

$$a:[b_1, \dots, b_n] = (\dots (((a:b_1):b_2):b_3) \dots):b_n.$$

This result follows by repeated applications of Lemma 7.4, (4.3), and (4.10).

We have now $a:b = a:[b_1, \dots, b_n] = (\dots (((a:b_1):b_2) \dots):b_n$ by Lemma 8.1. But

$$\begin{aligned} a:b_i &= [a_1, \dots, a_n]:b_i = [a_1:b_i, \dots, a_n:b_i] \\ &= [a_1, \dots, a_{i-1}, a_i:b_i, a_{i+1}, \dots, a_n]. \end{aligned}$$

Hence $a:b = [a_1:b_1, a_2:b_2, \dots, a_n:b_n]$.

If $a = b$, then $(a_i, [a_1, \dots, a_n]) = (a_i, [b_1, \dots, b_n])$ or $a_i = (a_i, b_i), a_i \supseteq b_i$.

Similarly $b_i \triangleright a_i$. Hence \mathfrak{S} is simply isomorphic with the direct product of the \mathfrak{S}_i . We note that if $x = [x_1, \dots, x_n], (x \triangleright a_i, a_i \in \mathfrak{S}_i)$, then

$$x = (x, a_i) = ([x_1, \dots, x_n], a_i) = (x_i, a_i) \in \mathfrak{S}_i.$$

Since $a_i : b_i \triangleright a_i$, we see that \mathfrak{S}_i is closed under residuation, which completes the proof.

We conclude with a theorem of a more special character.

THEOREM 8.4. *The free modular lattice of order twenty-eight on three elements cannot be residuated.*

We shall use Dedekind's original notation for the elements of this lattice in the proof of the theorem (Dedekind [1]). Assume that a residuation $x:y$ exists. Then \mathfrak{d}''' is the unit element. Hence $a_0:\mathfrak{d}' = b_0:\mathfrak{d}' = c_0:\mathfrak{d}' = \mathfrak{h} \neq \mathfrak{d}'''$. Now $a_0 = [a', a''']$. Hence $a_0:a''' = a':a''' \triangleright a'$. But $a''' \triangleright \mathfrak{d}'$. Therefore $a_0:\mathfrak{d}' \triangleright a_0:a'''$ or $\mathfrak{h} \triangleright a'$. Similarly, $\mathfrak{h} \triangleright b'$, $\mathfrak{h} \triangleright c'$. Hence $\mathfrak{h} \triangleright (a', b', c')$ or $\mathfrak{h} \triangleright \mathfrak{d}''''$, $\mathfrak{h} = \mathfrak{d}''''$ giving a contradiction.

It may be observed that the "exclusion principle" of Theorem 7.3 cannot be applied to prove this theorem.

IV. NOETHER LATTICES*

9. Consider any residuated lattice \mathfrak{S} . An element c of \mathfrak{S} is *irreducible* if in every decomposition $c = [g, f]$ into a cross-cut of two elements of \mathfrak{S} , either $g = c$ or $f = c$. An element p is a *prime* if $p \triangleright ab$ implies $p \triangleright a$ or $p \triangleright b$, and *primary* if $p \triangleright ab$, $p \nmid a$ implies $p \triangleright b^s$ for some integer s . The irreducible elements are thus determined by an intrinsic lattice property, while the primes and primary elements depend upon the particular multiplication introduced into the lattice.

We propose here the name "Noether lattice" for any lattice \mathfrak{S} satisfying the following three conditions:

- N 1. *The lattice \mathfrak{S} may be residuated.*
- N 2. *The ascending chain condition holds in \mathfrak{S} .*
- N 3. *Every irreducible element of \mathfrak{S} is primary.*

By N 1 we mean that \mathfrak{S} is closed under operations $x:y, xy$ having the properties R 1-R 6, M 1-M 6 and connected by the relationships expressed

* Our definition differs from that in Ward and Dilworth [1]. We have found that some of the results stated in §4 of this paper are in error. In postulate D 1, the exponent r must be replaced by 1. The condition $ab = [a, b]$ on the idempotent elements of a finite modular lattice is consequently *necessary* for the truth of D 1 but not sufficient. The postulate M 7 is *not* a sufficient condition for a Noether lattice as stated in the theorem preceding M 7.

in Definitions 4.1, 5.1. By N 2 we mean (Ore [1]) that every chain of lattice elements $a_1 < a_2 < a_3 < \dots < i$ terminates.

We choose the name in honor of Emmy Noether because the decomposition theorems first proved by her for the ideals of a commutative ring with chain condition all hold. It is to be observed that we do not assume a modular condition.

The proof that the usual decomposition theorems hold may be made by a mere transcription of the proofs given in van der Waerden [1] into lattice language. With each primary q is associated a prime p with the properties $p \triangleright q$ and $p \triangleright b$ implies $q \triangleright b^r$. A cross-cut of primaries is said to be "simple" if no primary in it divides the cross-cut of any of the remaining primaries. *Every element not equal to i of a Noether lattice may be represented as a simple cross-cut of a finite number of primaries each of which is associated with a different prime. The primes themselves and the total number of primaries are uniquely determined by the element.* We obtain from each such representation a representation as the cross-cut of "isolated components" by grouping together the cross-cuts of primaries whose associated primes divide one another. *The isolated components of an element and the corresponding representation as their cross-cut are unique.*

As was pointed out by Krull (Krull [1]), the decompositions into relatively prime ("teilerfremd") elements depend merely upon N 1 and N 2. From our standpoint, they are simple consequences of Theorem 7.1 and the chain condition.

We may specialize our lattice still more by the following assumption:

N 4. *Every prime of \mathfrak{S} is divisor-free.*

Then, since we have trivially from N 1 that every divisor-free element is a prime, we easily see that all primaries associated with a given prime form a lattice which we may say "belongs" to this prime.

The lattices belonging to distinct primes have no elements save i in common. Hence the decomposition theorems in this case are merely an instance of Birkhoff's decomposition of a lattice into direct products relative to cross-cut (Birkhoff [4]).

10. We shall now give some general properties of any Noether lattice.

THEOREM 10.1. *If a and b are any two elements of a Noether lattice, there exists an exponent s such that the following condition holds:*

D 1. $ab \triangleright [a, b^s]$.

Let $ab = [q_1, \dots, q_k]$ be a decomposition of ab into a cross-cut of primaries. Then for each q_i , $q_i \triangleright ab$; hence either $q_i \triangleright a$ or $q_i \ntriangleright a$, $q_i \triangleright b^{s_i}$. With

a proper choice of notation, we may assume that $q_i \triangleright a$, ($i=1, \dots, l$), $q_i \triangleright b^{s_i}$, ($i=l+1, \dots, k$). Hence if s is the largest of the s_i , $[q_1, \dots, q_l] \triangleright a$, $[q_{l+1}, \dots, q_k] \triangleright b^s$ giving D 1.

The following three theorems are immediate corollaries:

THEOREM 10.2. *If b is an idempotent element in a Noether lattice, then $[a, b] = ab$ for any other element a of the lattice, and $b[a, c] = [ba, bc]$ for any elements a and c .*

THEOREM 10.3. *In a Noether lattice, every idempotent element is neutral.**

THEOREM 10.4. *In a Noether lattice, the idempotent elements form a distributive lattice. The product of any two idempotent elements is their cross-cut.*

It is easy to show that this last mentioned property of idempotent elements holds in any lattice in which multiplication is distributive with respect to cross-cut; for if a, b are idempotent,

$$\begin{aligned} ab \triangleright a, b &= [a(a, b), b(a, b)] \\ &= [(a^2, ab), (ba, b^2)] = [(a, ab), (b, ab)] = [a, b]. \end{aligned}$$

The following lattice of order six illustrates how the definition of a Noether lattice depends upon the type of multiplication introduced. The elements are i, j, a, b, k , and z with the coverings $i > j, j > a, j > b; a > k, b > k; k > z$. The lattice is distributive and hence a Noether lattice if multiplication is identified with cross-cut (see §11). Define an operation xy by $ix = xi = x; zx = xz = z; j^2 = j, a^2 = a, b^2 = b, k^2 = z; ja = aj = a; jb = bj = b; jk = kj = z; ab = ba = ak = ka = bk = kb = z$. It may be shown that xy is a multiplication satisfying M 1–M 8. But D 1 does not hold; for $ab = z$ and $[a, b] = k$, while a and b are idempotent. Hence N 3 is false by Theorem 10.1.

11. We shall next give some sufficient conditions that a lattice be a Noether lattice.

THEOREM 11.1. *Let \mathfrak{S} be a residuated lattice with ascending chain condition. Then sufficient conditions that \mathfrak{S} be a Noether lattice are as follows:*

D 1. $ab \triangleright [a, b^s]$.

D 2. \mathfrak{S} is modular.

It suffices to show that N 3 holds. Let m be irreducible, $m \triangleright ab$, $m \ntriangleright a$. Then if $d = (a, m)$, $d \triangleright m \triangleright db$. Now by D 1, $db \triangleright [d, b^s]$ for some s . Hence $d \triangleright m \triangleright [d, b^s]$. Therefore by D 2, $m = [(m, d), (m, b^s)]$. Since m is irreducible and $(m, d) = (m, a) \neq m$, $(m, b^s) = m$. Hence $m \triangleright b^s$ and m is primary.

* Following Ore [1], we call an element n of a lattice “neutral” if $[n, (b, c)] = ([n, b], [n, c])$ for every pair of elements b, c of the lattice.

COROLLARY. *Every distributive lattice in which the ascending chain condition holds is a Noether lattice for a suitably defined multiplication.*

We take for the multiplication the cross-cut operation. Then M 1–M 6 and M 8 all hold; so \mathfrak{S} may be residuated. Since \mathfrak{S} is distributive, it is modular. Thus N 1, N 2, and D 2 hold. But D 1 is trivially true. The result now follows from the previous theorem.

We shall next give some conditions enabling us to view the ideal theory of commutative rings from a lattice-theoretic standpoint. It is first necessary to introduce a new concept. Let \mathfrak{S} be a residuated lattice.

DEFINITION 11.1. *An element q of \mathfrak{S} is principal if $q \triangleright b$ implies that there exists an element c such that $qc = b$.*

Neither c nor b need be principal.

Suppose that a is principal, $a \triangleright b$. The set \mathfrak{Z} of elements z such that $az = b$ is closed with respect to union. If either postulate M 7 or M 8 holds, the union b/a of \mathfrak{Z} has the properties stated in the following definition:

DEFINITION 11.2. $a \cdot (b/a) = b$; if $ax = b$ then $b/a \triangleright x$.

We call b/a the *quotient* of b by a . It is easily shown (Ward [1]) that if a is principal and $a \triangleright b$, then the quotient b/a equals the residual $b:a$ of a with respect to b .

As a simple consequence, we have the following lemma:

LEMMA 11.1. *If a is principal and if $a \triangleright b$, then $b = (b:a)a$.*

We may observe that M 8 always holds if the ascending chain condition holds. Hence Lemma 11.1 is true for all principal elements of a residuated lattice with ascending chain condition. We shall now prove the following fundamental theorem:

THEOREM 11.2. *Let \mathfrak{S} be a lattice in which the following conditions hold:*

N 1. *The lattice \mathfrak{S} may be residuated.*

N 2. *The ascending chain condition holds in \mathfrak{S} .*

D 2. *\mathfrak{S} is modular.*

D 3. *Every element of \mathfrak{S} is the union of a finite number of principal elements.*

D 4. *The principal elements of \mathfrak{S} are closed under multiplication.*

Then \mathfrak{S} is a Noether lattice.

The instance of ideal theory is obtained by identifying the principal elements of the lattice with the principal ideals or the corresponding ring ele-

ments. D 3 is then the basis theorem, and D 4 the closure property of ring multiplication.

It suffices to show that every irreducible element is primary, or inversely that every non-primary element is reducible. Let m be non-primary. Then there exist elements a and b of the lattice such that

$$(11.1) \quad m \triangleright ab, \quad m \ntriangleright a, \quad m \ntriangleright b \text{ for any } r.$$

We shall show that m is reducible. By D 3, $b = (b_1, b_2, \dots, b_k)$ where the b_i are principal. Then $m \triangleright ab_i$. For at least one b_i , $m \ntriangleright b_i^r$ for any r . For otherwise, for each b_i there exists an exponent r_i such that $m \triangleright b_i^{r_i}$. Then if $r > r_1 + r_2 + \dots + r_k - l$, we have $m \triangleright b^r$ contrary to hypothesis. Therefore, we may assume that b in (11.1) is principal.

By N 2, the chain $m:b, m:b^2, \dots, m:b^k, \dots$ terminates so that $m:b^k = m:b^{k+1}$ for some fixed k . Consider the cross-cut $c = [(m, a), (m, b^k)]$. We have trivially $c \triangleright m$. Now $(m, b^k) \triangleright c \triangleright m$. Hence by D 2 (Ore [1]),

$$(11.2) \quad c = ([c, m], [c, b^k]).$$

Now $m \triangleright [c, m]$. We shall show next that $m \triangleright [c, b^k]$. By D 4, b^k is principal, and $b^k \triangleright [c, b^k]$. Hence by Lemma 11.1, $[c, b^k] = \{[c, b^k]:b^k\}b^k = (c:b^k)b^k$. Also since $(m, a) \triangleright c$, $b(m, a) \triangleright bc$. But $b(m, a) = (bm, ba) \subset m$ by (11.1). Hence $m \triangleright bc \triangleright b[c, b^k]$ by (11.2). That is, $m \triangleright b\{(c:b^k)b^k\}$ or $m:b^{k+1} \triangleright c:b^k$. But $m:b^{k+1} = m:b^k$. Hence $m:b^k \triangleright c:b^k$ or $m \triangleright (c:b^k)b^k$, $m \triangleright [c, b^k]$. It follows therefore that $m \triangleright c$. Hence $m = c$ or $m = [(m, a), (m, b^k)]$. But $m \ntriangleright a$, $m \ntriangleright b^k$. Hence $(m, a) \neq m$, $(m, b^k) \neq m$, and m is reducible. This completes the proof.

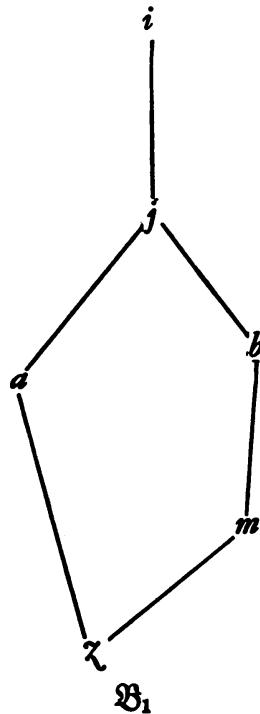
12. To show the significance of the hypotheses of Theorems 11.1 and 11.2, we shall exhibit various lattices in which not all the hypotheses are satisfied.

We first consider the following lattice \mathfrak{B}_1 ; and we define a multiplication xy over \mathfrak{B}_1 by the following table:

$x \backslash y$	i	j	a	b	m	z
i	i	j	a	b	m	z
j	j	a	a	z	z	z
a	a	a	a	z	z	z
b	b	z	z	z	z	z
m	m	z	z	z	z	z
z	z	z	z	z	z	z

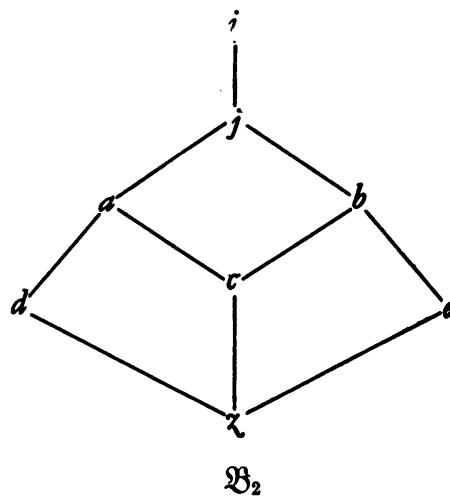
The reader may verify that M 1–M 8 are satisfied. Thus \mathfrak{B}_1 is a residuated lattice in which the ascending chain condition holds. \mathfrak{B}_1 is obviously non-modular. Now it is easily verified that D 1 holds in the lattice: $xy \triangleright [x, y^2]$,

for every x, y of the lattice. Nevertheless, *not every irreducible element is primary*. For consider the irreducible m . We have $m \triangleright ab$ and $m \ntriangleright b$. But since a is idempotent, $m \ntriangleright ar$ for any r .



Next, consider the lattice \mathfrak{B}_2 .

We assign the residuation $x:y$ to \mathfrak{B}_2 described in Theorem 8.1. The associated multiplication given by Definition 5.1 is then as follows: $xy=y$, if $x=i$; $xy=x$ if $y=i$; $xy=x$ otherwise.

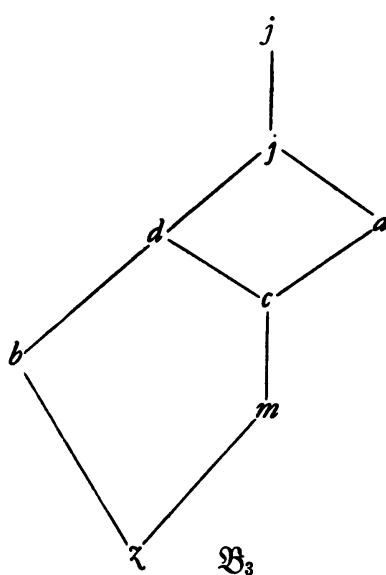


This lattice is non-modular, as it contains the non-modular sublattice j, a, d, e, z . The irreducible elements in it are j, a, b, d, e , and these are all primary since $x \triangleright y^2$ for any $y \neq i$ and any x . Furthermore, the elements i, c, d, e , and z are principal and $a = (d, c)$, $b = (c, e)$, $j = (a, b)$. Finally the principal

elements are closed with respect to multiplication. Thus in this lattice, all hypotheses of Theorem 11.2 hold save modularity; and yet the lattice is a Noether lattice.

Our last example is one in which all the hypotheses of Theorem 11.2 hold save modularity and the lattice is *not* a Noether lattice. We define a multiplication over \mathfrak{B}_3 by the following table:

Then it may be verified that the multiplication satisfies M 1–M 8, and that the elements i, a, b, c, m, z are principal and closed under multiplication.



Since $d = (b, m)$, $j = (a, d)$, every element is the union of a finite number of principal elements. The lattice is evidently non-modular. It is not a Noether lattice. For consider the irreducible element m . Then $m \triangleright ab$, $m \ntriangleright a$, and $m \ntriangleright b^s$ for any s , since b is idempotent.

V. CONDITIONS FOR DISTRIBUTIVITY

13. We shall conclude by answering some of the questions raised in Ward [4] as to the import of certain auxiliary conditions in a residuated lattice. We consider a residuated lattice in which one or more of the following conditions hold:

$$R\ 9.\ (a:b, b:a) = i. \quad R\ 10.\ a:[b, c] = (a:b, a:c). \quad R\ 11.\ (b, c):a = (b:a, c:a).$$

THEOREM 13.1. *R 9, R 10, R 11 are equivalent and imply distributivity.*

R 9 implies R 11. For

$$\begin{aligned} (b:a, c:a): \{(b, c):a\} &\supset ((b:a): \{(b, c):a\}, (c:a): \{(b, c):a\}) \\ &= ((b: \{(b, c):a\}):a, (c: \{(b, c):a\}):a). \end{aligned}$$

But $(b: \{(b, c):a\}):a \supset b:c$ since

$$\begin{aligned} \{(b: \{(b, c):a\}):a\}: (b:c) &= (\{b:(b:c)\}: \{(b, c):a\}):a \\ &\supset ((b, c): \{(b, c):a\}):a \supset a:a = i. \end{aligned}$$

Similarly $(c: \{(b, c):a\}):c \supset c:b$. Hence $(b:a, c:a): \{(b, c):a\} \supset (b:c, c:b) \supset i$ by R 9. Thus $(b:a, c:a) \supset (b, c):a$. But $(b, c):a \supset (b:a, c:a)$ trivially.

R 11 implies R 10. For by R 11,

$$\begin{aligned} (a:b, a:c): \{a:[b, c]\} &= ((a:b): \{a:[b, c]\}, (a:c): \{a:[b, c]\}) \\ &= ((a: \{a:[b, c]\}):b, (a: \{a:[b, c]\}):c) \\ &\supset ([b, c]:b, [b, c]:c) \\ &= (c:b, b:c) = (c:(b, c), b:(b, c)) = (c, b):(b, c) = i \end{aligned}$$

by R 11. Hence $(a:b, a:c) \supset a:[b, c]$. But $a:[b, c] \supset (a:b, a:c)$ trivially.

R 10 implies R 9. For $(a:b, b:a) = ([a, b]:b, [a, b]:a) = [a, b]:[a, b] = i$ by condition R 10.

R 10 implies distributivity. For let $a \supset [b, c]$. Then

$$a: [(a, b), (a, c)] = (a:(a, b), a:(a, c)) = (a:b, a:c) = a:[b, c] = i.$$

Hence $a \supset [(a, b), (a, c)]$ and $[(a, b), (a, c)] \supset a$ trivially. Therefore $a = [(a, b), (a, c)]$.

THEOREM 13.2. *If every element of a residuated lattice is principal, then the lattice is distributive.*

Let $(b, c) \supset a$. We have $a \supset ([a, b], [a, c])$. Hence

$$\begin{aligned} a:(b, c) \supset ([a, b], [a, c]):(b, c) &= ([([a, b], [a, c]):b, ([a, b], [a, c]):c] \\ &\supset [[a, b]:b, [a, c]:c] = [a:b, a:c] = a:(b, c). \end{aligned}$$

Thus $a:(b, c) = ([a, b], [a, c]):(b, c)$. But $(b, c) \triangleright a \triangleright ([a, b], [a, c])$. Hence

$$a = (a:(b, c))(b, c) = \{([a, b], [a, c]):(b, c)\}(b, c) = ([a, b], [a, c])$$

by Lemma 13.1.

THEOREM 13.3. *A sufficient condition that a residuated lattice with ascending chain condition be a Noether lattice is that every element in it be principal.*

For by Theorem 13.2, the lattice is distributive and hence modular; so all the hypotheses of Theorem 11.2 are satisfied.

REFERENCES

GARRETT BIRKHOFF

1. *On the combination of sub-algebras*, Proceedings of the Cambridge Philosophical Society, vol. 39 (1933), pp. 441–464.
2. *On the structure of abstract algebras*, ibid., vol. 41 (1935), pp. 433–454.
3. *Combinatorial relations in projective geometries*, Annals of Mathematics, (2), vol. 36 (1935), pp. 743–748.
4. *On the lattice theory of ideals*, Bulletin of the American Mathematical Society, vol. 40 (1934), pp. 613–619.

R. DEDEKIND

1. *Ueber die von drei Moduln erzeugte Dualgruppe*, Gesammelte mathematische Werke, vol. 2, 1931, paper 30, pp. 236–271.

R. P. DILWORTH

1. *Abstract residuation over lattices*, Bulletin of the American Mathematical Society, vol. 44 (1938), pp. 262–268.

FRITZ KLEIN

1. *Dedekindsche und distributive Verbände*, Mathematische Zeitschrift, vol. 41, pp. 261–280.

G. KÖTHE

1. *Die Theorie der Verbände* . . . , Jahresbericht der deutschen Mathematiker-Vereinigung, vol. 47 (1937), pp. 125–142.

W. KRULL

1. *Axiomatische Begründung der allgemeinen Idealtheorie*, Sitzungsberichte der physikalisch-medicinischen Societät zu Erlangen, vol. 56 (1924), pp. 47–63.

O. ORE

1. *On the foundation of abstract algebra*, I, Annals of Mathematics, (2), vol. 36 (1935), pp. 406–437.

B. L. VAN DER WAERDEN

1. *Moderne Algebra*, vol. 2, Berlin, 1931.

M. WARD AND R. P. DILWORTH

1. *Residuated lattices*, Proceedings of the National Academy of Sciences, vol. 24 (1938), pp. 162–164.

M. WARD

1. *Residuation in structures over which a multiplication is defined*, Duke Mathematical Journal, vol. 3 (1937), pp. 627–636.
2. *Structure residuation*, Annals of Mathematics, (2), vol. 39 (1938), pp. 558–568.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

THE LAW OF APPARITION OF PRIMES IN A LUCASIAN SEQUENCE*

BY
MORGAN WARD

I. INTRODUCTION

1. We call a sequence of rational integers

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

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 $\rho_1, \rho_2, \dots, \rho_s$ called the ranks of apparition of m in (u) with the defining properties

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

The least common multiple|| $\rho = [\rho_1, \rho_2, \dots, \rho_s]$ 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], ... 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 $[a, b, \dots]$ and (a, b, \dots) to denote the least common multiple and greatest common divisor of the integers a, b, \dots .

¶ The restricted period of (u) modulo m is the least positive integer μ such that $u_{n+\mu} \equiv au_n \pmod{m}$ 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].

partition 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

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

be two polynomials with rational integral coefficients c_1, \dots, c_k , d_1, \dots, d_l . For simplicity of exposition we assume that $f(x)$ and $g(x)$ have non-vanishing discriminants and resultant. \dagger Let $\alpha_1, \dots, \alpha_k; \beta_1, \dots, \beta_l$ 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, \dots ; (R) : R_0, R_1, \dots , where

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

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]. \ddagger

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. \S (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.

\dagger This restriction is removed in the body of the paper.

\ddagger 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 $\epsilon_1, \epsilon_2, \dots, \epsilon_{kl}$, 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.

\S 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 $\{\alpha_1\}, \{\alpha_2\}, \dots, \{\alpha_k\}$.

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

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

$$\begin{aligned} & \{\alpha_{i_1}, \alpha_{i'_1}\}, \{\alpha_{i_2}, \alpha_{i'_2}\}, \dots, \{\alpha_{i_s}, \alpha_{i'_s}\} \\ & i = 1, 2, \dots, \kappa; s_1 + s_2 + \dots + s_K = k(k-1)/2. \end{aligned}$$

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

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

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 $f(x) = x^4 - c_1x^3 - c_2x^2 - c_3x - c_4 = x^4 + (2Q-R)x^2 + Q^2$ 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

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

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

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

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 $k = q_1^{e_1} q_2^{e_2} \cdots q_K^{e_K}$ 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 K numbers $\rho(k/q_1), \dots, \rho(k/q_K)$, the rank of p in (U) divides $\rho(k/q_1 q_2 \cdots q_K)$, and p has at most K 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 $x^\lambda \equiv 1 \pmod{p, f(x)}$.

† 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 $\sigma_1, \sigma_2, \dots, \sigma_l$ modulo p of the algebraic numbers $\alpha\beta^{-1}, \alpha\beta^{-p}, \dots, \alpha\beta^{-p^{l-1}}$ 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 $x; y_1, y_2, \dots, y_k; z_1, z_2, \dots, z_l$ be $k+l+1$ indeterminates, and let $Y_1, -Y_2, \dots, (-1)^{k-1}Y_k; Z_1, -Z_2, \dots, (-1)^{l-1}Z_l$ be the $k+l$ elementary symmetric functions of the indeterminates y, z defined by*

$$(x - y_1)(x - y_2) \cdots (x - y_k) = x^{k+1} - Y_1 x^{k-1} - \cdots - Y_k,$$

$$(x - z_1)(x - z_2) \cdots (x - z_l) = x^l - Z_1 x^{l-1} - \cdots - Z_l.$$

By the fundamental theorem on symmetric functions, the polynomials

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

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

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

Suppose now that t_1, t_2, \dots, t_m are m new indeterminates where $k \geq m \geq 1$, $l \geq m \geq 1$, 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)

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

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

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

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

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

be two polynomials with fixed rational integral coefficients. Let $\alpha_1, \dots, \alpha_k$; β_1, \dots, β_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

$$(R): R_0, R_1, R_2, \dots,$$

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

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

$$(7.1) \quad f(x) = f'(x)h'(x), \quad g(x) = g'(x)h'(x),$$

where

$$(7.2) \quad \begin{aligned} f'(x) &= x^{k-m} - c'_1 x^{k-m-1} - \cdots - c'_{k-m}, \\ g'(x) &= x^{l-m} - d'_1 x^{l-m-1} - \cdots - d'_{l-m}, \\ h'(x) &= x^m - e'_1 x^{m-1} - \cdots - e'_m, \end{aligned} \quad k \geq m \geq 1; l \geq m \geq 1,$$

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 $R_{f',g'} \not\equiv 0 \pmod{p}$:

$$f(x) \equiv f'(x)h'(x) \pmod{p}, \quad g(x) \equiv g'(x)h'(x) \pmod{p}.$$

We now make use of the following principle:

SCHATANOVSKI'S PRINCIPLE.† If $\phi(y_1, y_2, \dots, y_k)$ is an integral symmetric function of the indeterminates y_1, y_2, \dots, 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

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

Let

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

and let $\gamma_1, \gamma_2, \dots, \gamma_k$ 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

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

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

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

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

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

Here the polynomials $f_1(x), \dots, g_s(x)$ 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

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

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

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

$$a_1 k_1 + a_2 k_2 + \cdots + a_r k_r = k, \quad k_1 + k_2 + \cdots + k_r = h,$$

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, \dots, 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

$$(9.2) \quad \pm n^l \prod_{u=1}^r T_{u1}^{A_u(n-1)} \prod_{u=1}^r \{Q_{ku}(T_u)\}^{a_u^2} \prod_{\substack{u, v=1 \\ u < v}}^r \{P_{ku, kv}(T_u, T_v)\}^{a_u a_v},$$

$$A_u = \frac{1}{2} a_u(a_u - 1), \quad l = k_1 A_1 + k_2 A_2 + \cdots + k_r A_r,$$

in analogy with formula (6.3).

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

$$f(x) = x^k - c_1 x^{k-1} - \cdots - c_k = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

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

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

If D_f vanishes, we have

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

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

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

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

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

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

$$\begin{aligned} f(x) &= x^k - c_1 x^{k-1} - \cdots - c_k = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k), \\ g(x) &= x^l - d_1 x^{l-1} - \cdots - d_l = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_l) \end{aligned}$$

be the generators of (R) . Both $f(x)$ and $g(x)$ are algebraically irreducible. Let \mathfrak{R} denote the Galois field of the roots of $f(x) = 0$ and $g(x) = 0$ obtained by adjoining the $k+l$ quantities α_1, \dots, β_l to the field of rationals.

LEMMA 10.1. p is a prime ideal of \mathfrak{R} .

Proof. If C is the ring of integers of \mathfrak{R} , it suffices to show that the quotient ring $\mathfrak{O}/[p]$ is a field. Let \mathfrak{o} 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

$$(10.1) \quad \mathfrak{O}/[p] = \mathfrak{o}/[p].$$

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

$$(10.2) \quad (p, \bar{D}) = 1.$$

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

We can choose rational integers $e_1, \dots, e_k; f_1, \dots, f_l$ 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{R} . But we have the congruences in \mathfrak{O}

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

where $r_1, \dots, r_k; s_1, \dots, s_l$ are the integers $1, \dots, k; 1, \dots, l$ 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{R} and \bar{D} as before its discriminant, the n elements $\bar{D}^{-1}, \theta\bar{D}^{-1}, \dots, \theta^{n-1}\bar{D}^{-1}$ are a basis of \mathfrak{Q} . 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), $\mathfrak{Q}/[p]$ 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

$$(11.1) \quad \alpha_i^n \equiv \beta_j^n \pmod{p}$$

in \mathfrak{Q} 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 †

$$(11.2) \quad \{\alpha\beta^{-ps}\}^n \equiv 1 \pmod{p}, \quad 1 \leq s \leq l.$$

Now $\alpha\beta^{-ps}$ is an element of the finite galois field $\mathfrak{R}^* = \mathfrak{R}[\alpha, \beta]/[p]$ 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

$$(11.3) \quad n \equiv 0 \pmod{\sigma_s}.$$

We thus obtain the following theorem:

THEOREM 11.1. *If σ_s is the period of $\alpha\beta^{-ps}$ modulo p in $\mathfrak{Q}/[p]$, then $\sigma_1, \sigma_2, \dots, \sigma_l$ 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 $\sigma_1, \sigma_2, \dots, \sigma_l$, 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_i , 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 $\beta^{-1} \equiv d'_l (\beta^{l-1} - d, \beta^{l-2} - \dots - d_{l-1}) \pmod{p}$.

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 $\sigma_1, \dots, \sigma_t$ 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 ≥ 1 and $\leq k$, 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,

$$(12.1) \quad \rho_s = \lambda : p^s - 1.$$

We observe in particular that

$$(12.2) \quad \rho_k = 1, \quad \rho_1 = \mu.$$

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

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

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

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

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

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

† 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 $d \mid d' \mid k$, then $\rho_{d'} \mid \rho_d$.

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 $\rho_s \mid \pi_{ks}$, ($s = 1, 2, 3, \dots, k$).

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 $p^k - 1/p^{k/q_1} - 1, p^k - 1/p^{k/q_2} - 1, \dots, p^k - 1/p^{k/q_K} - 1$. Here q_1, \dots, q_K are the K prime factors of k .*

If $Q = q_1 q_2 \cdots q_K$, 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{R}^* . Then

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

where a and b are positive integers.‡ Hence

$$(13.1) \quad \sigma_s = p^m - 1 : (a - bp^s), \quad (s = 1, 2, \dots, l).$$

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

$$(13.2) \quad \sigma_r = \sigma_s \quad \text{if} \quad r \equiv s \pmod{l}.$$

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*

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

† We use the usual notation $a \mid b$ 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

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

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

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

By (13.1) and elementary properties of residuals

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

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 $[\sigma_s, \sigma_t]$, ($s, t = 1, \dots, l; s < t$), 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 $\alpha^n \equiv \beta^{p^k n} \pmod{p}$ to the p^l th and p^k th powers successively, we obtain $\alpha^{(p^l-1)n} \equiv 1 \pmod{p}$, $\beta^{p^k(p^l-1)n} \equiv 1 \pmod{p}$. Hence if λ_1 and λ_2 denote the periods of $f(x)$ and $g(x)$,

$$n \equiv 0 \pmod{\lambda_1 : p^l - 1}, \quad n \equiv 0 \pmod{\lambda_2 : p^k - 1},$$

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 $n \equiv 0 \pmod{[\lambda_1 : p^{(k,l)} - 1, \lambda_2 : p^{(k,l)} - 1]}$ or

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

(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

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

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*

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

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

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) ,*

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

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 $\alpha_i^\sigma \equiv \beta_i^\sigma \pmod{p}$, (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, \dots be a Lucasian sequence belonging to the polynomial $f(x) = x^k - \dots - c_k = (x - \alpha_1) \dots (x - \alpha_k)$, 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

$$u_n = A_1\alpha_1^n + \dots + A_k\alpha_k^n,$$

where DA_1, \dots, DA_k are integers of \mathfrak{K} , so that A_1, \dots, A_k are integers modulo \mathfrak{p} . Since (u) is a divisibility sequence, $u_n \equiv 0 \pmod{\mathfrak{p}}$ if and only if

$$A_1\alpha_1^{mn} + A_2\alpha_2^{mn} + \dots + A_k\alpha_k^{mn} \equiv 0 \pmod{\mathfrak{p}}, \quad m = 1, 2, \dots, k.$$

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) n th powers of the roots of $f(x) = 0$ are grouped modulo \mathfrak{p} into t incongruent sets:

$$(16.1) \quad \begin{aligned} \alpha_{i_1}^n &\equiv \alpha_{i_2}^n \equiv \dots \equiv \alpha_{i_{s_i}}^n \equiv \xi_i \pmod{\mathfrak{p}}, & i &= 1, 2, \dots, t, \\ \xi_i &\not\equiv \xi_j \pmod{\mathfrak{p}} \quad \text{if} \quad i \neq j; \quad s_1 + s_2 + \dots + s_t &= k. \end{aligned}$$

Furthermore let

$$(16.2) \quad \Lambda_i = A_{i_1} + A_{i_2} + \dots + A_{i_{s_i}}, \quad i = 1, 2, \dots, t.$$

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*

$$\Lambda_i \equiv 0 \pmod{\mathfrak{p}}, \quad (i = 1, 2, \dots, t).$$

Here Λ_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 $\gamma_1^{(i)}, \gamma_2^{(i)}, \dots, \gamma_{k_i}^{(i)}$.

Then by Schatanovski's principle

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

where

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

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

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

(Ward [2], p. 283).

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

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

$$(16.3) \quad \{ \gamma^{(i)} \}^n \equiv \{ \gamma^{(j)} \}^n \pmod{p}, \quad i \neq j.$$

Then we deduce as in §14 that

$$(16.4) \quad n \equiv 0 \pmod{[\lambda^{(i)}, \lambda^{(j)}]: p^{(k_i, k_j)} - 1}.$$

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.

STRUCTURE RESIDUATION

BY MORGAN WARD

(Received Dec. 27, 1937)

I. INTRODUCTION

1. Given any two elements A and B of a structure¹ Σ , we define the residual of B with respect to A relative to cross-cut as an element $R = A : B$ of Σ with the properties

(1.1) $A \supset [A : B, B]$,

(1.2) $A \supset [X, B]$ implies that $A : B \supset X$ for any element X of Σ .

The residual $S = A - B$ of B with respect to A relative to union is defined dualistically by

$$(A - B, B) \supset A,$$

$(X, B) \supset A$ implies that $X \supset A - B$ for any element X of Σ .

The properties of these two operations may be summarized as follows: We define a structure as *residually closed* (relative to cross-cut) if any two elements in it have a residual with the properties (1.1), (1.2). *Every residually closed structure is distributive.*¹ A structure will be said to be *distributively closed*² (relative to cross-cut) if given any two sets Θ and Φ of elements of Σ , and the set Γ of all cross-cuts of elements of Θ with elements of Φ , the union of Γ is the cross-cut of the unions of Θ and Φ .

*Every distributively closed structure is residually closed.*³ Sufficient conditions that a structure Σ be distributively closed are (i) Σ contains an all element O_0 ; (ii) Σ is distributive; (iii) the ascending chain condition holds in Σ . Thus every finite distributive structure is residually closed. Similar results hold by duality for residuation with respect to union.

2. The results of a recent paper (Ward [1]) in which I have considered residuation in a structure over which a multiplication is defined which is distributive with respect to union apply to the present case on identifying multiplication with cross-cut. The assumption $(A, B) = A : (A : B)$ analyzed there is a

¹ We use the terminology of Ore's recent memoir in these Annals (Ore, [1]), save for the substitution of the term "distributive structure" for Ore's "arithmetic structure," and the interchange of the symbols (\dots) and $[\dots]$.

² MacNeille [1] uses the term "lattice with completely distributive products."

³ Compare MacNeille [1] lemma 7.6. MacNeille's "product complement" A' is our "residual of A with respect to E_0 ."

necessary and sufficient condition that a structure residually closed with respect to cross-cut and containing a unit element E_0 may be a Boolean algebra.

If Σ is a distributive structure containing an all element in which the ascending chain condition holds, then the general decomposition theorems for Dedekind structures become almost trivial (Ore [1] page 415); every element of Σ save O_0 has a unique representation as the cross-cut of a finite number of prime elements none of which divides any other. A very interesting situation arises however if the accompanying structure residuation has any one of the three equivalent properties⁴

$$A : [B, C] = (A : B, A : C), (B, C) : A = (B : A, C : A), (A : B, B : A) = O_0.$$

In this case, the primes in the canonical representation of any element as a cross-cut may be chosen relatively prime in pairs. The primes themselves are not necessarily powers of irreducible elements as in common arithmetic, but they may be associated with such powers in a relatively simple manner.

I propose here the name "semi-arithmetical structure (or lattice)" for these systems. A simple example is the set of numbers 1, 2, 3, 6 and 12 with $[\dots]$ and (\dots) the L.C.M. and G.C.D. operations. We may remark that *every finite distributive structure may be represented as a finite set of positive integers closed under L.C.M. and G.C.D.* I have constructed a proof of this fact by induction; but it is also an immediate consequence of the recent result of Mac Neille's [1] allowing us to imbed any distributive structure in a Boolean algebra. Conversely, it implies Mac Neille's theorem for the case of a finite structure.

II. PROPERTIES OF RESIDUALLY CLOSED STRUCTURES

3. We define a structure following Ore as a system Σ of elements A, B, C, \dots over which there is a well defined division relation $X \supseteq Y$ such that

POSTULATE I. $A \supseteq A; A \supseteq B$ and $B \supseteq C$ imply $A \supseteq C$.

POSTULATE II. For each pair of elements A, B of Σ there exist elements D and M such that: $D \supseteq A, D \supseteq B; S \supseteq A, S \supseteq B$ implies $S \supseteq D$. $A \supseteq M, B \supseteq M; A \supseteq T, B \supseteq T$ implies $M \supseteq T$.

If $A \supseteq B, B \supseteq A$ we write $A = B$. We write $M = [A, B]$ $D = (A, B)$ reversing Ore's usage.

We shall now examine the consequences of assuming

POSTULATE III. (a). Σ is residually closed relative to cross-cut; or (b) Σ is residually closed relative to union.

Assume IIIa. Then taking $B = A$ in (1.1), we see that Σ contains an all element $O_0 = A : A$ dividing every other element. Similarly on assuming IIb, we see that Σ contains a unit element $E_0 = A - A$ divisible by every other element. Since all properties of residuation relative to union may be obtained

⁴ The first two equalities are the third and fourth "distributive laws for residuation" analyzed at length in Ward [1].

by a similar dualizing, we shall confine ourselves to stating results only for residuation relative to cross-cut.

We list here for reference some elementary properties of residuation. We use \rightarrow for "implies that", $\dots + \dots$ for "both \dots and \dots " and \curvearrowright for "implies and is implied by."

- (i) $A : B \supset A$.
- (ii) $A \supset B \rightarrow A : C \supset B : C + C : B \supset C : A$.
- (iii) $A = B \rightarrow A : C = B : C + C : A = C : B$.
- (iv) $A \supset B \curvearrowright A : B = O_0$.
- (v) $A : A = O_0 + A : O_0 = A$.
- (vi) $A : B \supset C \curvearrowright A \supset [B, C]$.
- (vii) $A : (A : B) \supset (A, B)$.
- (viii) $A : [B, C] = (A : B) : C = (A : C) : B$.
- (ix) $A : B = (A : B) : B$.
- (x) $[A, B] : B = A : B$.
- (xi) $A : B = R \rightarrow R : B = R$.
- (xii) If $A : B = A$, then $A \supset [X, B] \curvearrowright A \supset X$.
- (xiii) $R = A : B + S = A : R \rightarrow R = A : S$.
- (xiv) If $B^{(1)} = B$, $B^{(n+1)} = A : B^{(n)}$, then
 $B^{(2n)} = B^{(2)}, B^{(2n+1)} = B^{(3)}, \dots$ ($n = 1, 2, 3, \dots$).
- (xv) $A : B = A : (A, B)$.
- (xvi) $(A, B) = O_0 \rightarrow A : B = A$.

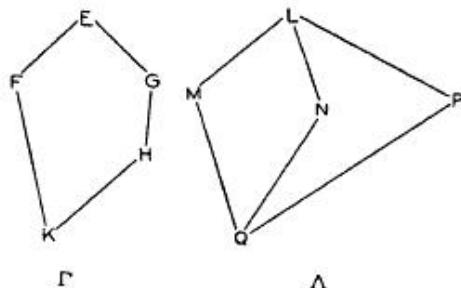
These rules all readily follow from the definition (1.1), (1.2) and postulates I, II, III a. Consider for example (xv). Since $(A, B) \supset B$, $A : B \supset A : (A, B)$ by (ii). By (vii), $A : (A : B) \supset (A, B)$. Therefore by (ii) again, $A : (A, B) \supset A : \{A : (A : B)\}$. But by (xiii), $A : \{A : (A : B)\} = A : B$. Hence $A : (A, B) \supset A : B$ by (iii), giving (xv).

THEOREM 3.1. *If Σ is residually closed relative to cross-cut, then Σ is a distributive structure.*

PROOF. All structures of order less than five are easily seen to be distributive. If Σ is not a Dedekind structure, it is known (Dedekind [1] p. 255) that Σ contains a sub-structure Γ of order five which is not a Dedekind structure. Similarly, if Σ is not distributive but is a Dedekind structure, it contains a sub-structure Λ of order five which is not distributive. (Birkhoff [1] p. 617.) The types of these sub-structures are well known; their lattice diagrams are given in the illustration (see next page). (Klein [1] pp. 222-223).

Suppose that Σ is not a Dedekind structure. Consider the residual $H : G$

of the elements G and H of the sub-structure Γ . Since $H \supset [F, G]$, $H : G \supset F$ by (1.2). Also $H : G \supset H$ by rule (i). Therefore $H : G \supset (H, F)$ or $H : G \supset E$. Then by rule (vi), $H \supset [G, E]$ or $H \supset G$ which is false.



The structure Σ must therefore be Dedekindian. If it is non-distributive, consider the residual $M : N$ of the elements M and N in the sub-structure Δ . Since $M \supset [N, P]$, $M : N \supset P$ by (1.2). Also $M : N \supset M$ by rule (i). Therefore $M : N \supset (M, P)$ or $M : N \supset L$. Then by rule (vi), $M \supset [N, L]$ or $M \supset N$ which is false.

Hence every structure of order greater than four which is residually closed must be distributive, and the proof is complete.

4. Theorem 3.1 allows us to apply all the results obtained in Ward [1] for residuation in a structure closed with respect to multiplication. For on identifying cross-cut with the multiplication defined there, the three conditions given for a multiplication $X \cdot Y$ are satisfied (Ward [1] section 3); namely

$$A \cdot B \text{ is in } \Sigma \text{ if } A, B \text{ are in } \Sigma; A \cdot (B \cdot C) = (A \cdot B) \cdot C; A \cdot B = B \cdot A.$$

$$O_0 \cdot A = A \quad \text{for every } A \text{ in } \Sigma.$$

$$A \cdot (B, C) = (A \cdot B, A \cdot C).$$

In particular, if when $B \supset A$ we define the quotient of A by B as an element A/B of Σ such that

$$(4.1) \quad A = \left[B, \frac{A}{B} \right], \quad A = [B, X] \text{ implies that } \frac{A}{B} \supset X,$$

it follows that if the quotient A/B exists it equals the residual $A : B$. But more is true; namely

THEOREM 4.1. *If $B \supset A$, the quotient A/B always exists and equals the residual $A : B$.*

PROOF. By (1.1), $A \supset [A : B, B]$. But $B \supset A$ and $A : B \supset A$ by rule (i). Hence $[A : B, B] \supset A$, $A = [A : B, B]$. Also if $A = [B, X]$, $A \supset [B, X]$ so that $A : B \supset X$ by (1.2). Therefore $A : B = A/B$ by the definition (5.1).

We obtain as a corollary the following important rule of manipulation⁵:

$$(xvii) \quad B \supset A \rightsquigarrow A = [A : B, B].$$

⁵ We may observe that (xvii) shows that postulate D of Ward [1] is always satisfied in a residually closed structure.

We also have the two "distributive laws" (Ward [1], section III)

$$\text{LI} \quad M : (A_1, A_2, \dots, A_n) = [M : A_1, \dots, M : A_n]$$

$$\text{LII} \quad [A_1, A_2, \dots, A_n] : M = [A_1 : M, \dots, A_n : M].$$

The remaining two distributive laws

$$\text{LIII} \quad (A_1, \dots, A_n) : M = (A_1 : M, \dots, A_n : M)$$

$$\text{LIV} \quad M : [A_1, \dots, A_n] = (M : A_1, \dots, M : A_n)$$

are not generally valid. We shall analyze their meaning and validity when we come to discuss the arithmetical properties of residually closed structures.

A large portion of Ward [1] was devoted to analyzing the consequences of assuming*

POSTULATE C. *If $A \supset B$, there exists an element F such that $A = B : P$.*

This assumption was shown to be equivalent to assuming the rule

$$(4.2) \quad (A, B) = A : (A : B).$$

In case Σ has a unit element E_0 , this last rule implies that Σ is a Boolean algebra. For consider $A' = E_0 : A$ for any element A of Σ . We have $(A, A') = A' : (A' : A) = E_0 : A : \{(E_0 : A) : A\} = O_0$ by rules (iii), (iv) and (v). Also since $A \supset E_0$, $[A, A'] = E_0$ by rule (xvii). Finally $(A')' = E_0 : (E_0 : A) = (E_0, A) = A$. Thus A' is the negative of A . Conversely in a Boolean algebra $A : B = (A, B')$ (Dilworth [1]), and (4.2) is easily seen to be satisfied.

III. DISTRIBUTIVELY CLOSED STRUCTURES

5. Let Σ^* denote the class of all sub-sets of elements of Σ . If Θ and Φ are any two such sub-sets, we define $[\Theta, \Phi]$ and (Θ, Φ) to be the least sub-sets containing respectively all elements $[T, F]$ and (T, F) , T in Θ , F in Φ . The operations $[\dots]$ and (\dots) thus defined over Σ^* are commutative and associative and if Σ contains an all element or a unit element so does Σ^* , but the resulting algebra is not a structure since the operations are obviously not indepotent.

If every element of Θ divides every element of Φ , we write $\Theta \supset \Phi$. If $\Phi \supset \Theta$, $[\Theta, \Phi] = \Phi$, $(\Theta, \Phi) = \Phi$ but not conversely. If Θ consists of a single element T , we write when convenient $\Phi \supset T$, $T \supset \Phi$, $[T, \Phi]$ or (T, Φ) for $\Phi \supset \Theta$, $\Theta \supset \Phi$, $[\Theta, \Phi]$ or (Θ, Φ) .

The assumption that Σ is a closed structure (Ore [1] page 409) may then be formulated by saying that we have two operators u and k defined on Σ^* to Σ such that

$$u\Theta = U; U \supset \Theta; X \supset \Theta \text{ implies } X \supset U.$$

$$k\Theta = K; \Theta \supset K; \Theta \supset Y \text{ implies } K \supset Y.$$

6. Let Σ be any closed structure. Then Σ will be said to be *distributively closed (relative to cross-cut)* if

$$u[\Theta, \Phi] = [u\Theta, u\Phi]$$

and *distributively closed relative to union* if

$$k(\Theta, \Phi) = (k\Theta, k\Phi)$$

Here Θ, Φ denote any two sub-sets of Σ .

A distributively closed structure of either type is obviously distributive ("arithmetic" is Ore's terminology) in the ordinary sense. A distributively closed structure relative to both union and cross-cut is a \bar{C} lattice in Garrett Birkhoff's terminology (Birkhoff [2]); conversely, it is easily shown that any \bar{C} lattice is a distributively closed structure relative to both union and cross-cut.⁶

The assumption that Σ is distributively closed relative to cross-cut is equivalent to postulate B of Ward [1] on identifying the multiplication $X \cdot Y$ with $[X, Y]$. We accordingly obtain by the argument given in Ward [1] section 4

THEOREM 6.1. *Every structure distributively closed relative to cross-cut is residually closed relative to cross-cut.*

THEOREM 6.2. *Let Σ be a distributive structure containing an all element O_0 in which the ascending chain condition holds. Then Σ is distributively closed relative to cross-cut.*

PROOF. The hypotheses of the theorem imply that Σ is closed relative to union in the ordinary sense. (Ore [1] §2.) Let Θ and Φ be any two sub-sets of Σ with elements $\dots T_r, \dots ; \dots F_s, \dots$ and let $\Gamma = [\Theta, \Phi]$. Then $T = u\Theta$, $F = u\Phi$ and $G = u\Gamma$ all exist. We are to prove that $G = [T, F]$. Now (Ore [1] §2) Θ contains k elements T_1, \dots, T_k such that $T = (T_1, \dots, T_k)$. Similarly $F = (F_1, \dots, F_l)$ where the F_i are in Φ . Hence since Σ is distributive, $[T, F] = ([T_1, F_1], \dots [T_k, F_l])$,

Also $G = ([T_{r_1}, F_{s_1}], \dots, [T_{r_m}, F_{s_m}])$ for Γ is made up of all distinct elements $[T_r, F_s]$. Hence since $T \supseteq \Theta$, $F \supseteq \Phi$, $[T, F] \supseteq [T_{r_1}, F_{s_1}]$ or $[T, F] \supseteq G$. Also since $G \supseteq [T_r, F_s]$, $G \supseteq ([T_1, F_1], \dots [T_k, F_l])$ or $G \supseteq [T, F]$. Thus $G = [T, F]$.

COROLLARY. *Every distributive structure of finite order is residually closed.*

IV. ARITHMETICAL PROPERTIES OF RESIDUALLY CLOSED STRUCTURE

7. Let Σ be any structure. An element $Q \neq O_0$ of Σ is said to be: (i) *irreducible* if $X \supseteq Q$ implies $X = O_0$ or $X = Q$; (ii) *prime* if $Q \supseteq [X, Y]$ implies $Q \supseteq X$ or $Q \supseteq Y$; (iii) *indecomposable* if $Q = [X, Y]$ implies $Q = X$ or $Q = Y$; (iv) a *power* if it has precisely one irreducible divisor. Every irreducible is

⁶ MacNeille [1] calls such a structure a "completely distributive lattice," and proves the independence of distributive closure with respect to union and distributive closure with respect to cross-cut.

indecomposable, and in a distributive structure every irreducible is a prime. (Köthe [1].)

For the remainder of the paper we assume postulate III a and a chain condition:

POSTULATE IV. *The ascending chain condition holds in Σ*

Then as is well known every element A of $\Sigma \neq O_0$ admits of at least one decomposition:

$$(7.1) \quad A = [Q'_1, Q'_2, \dots, Q'_l]$$

into a cross-cut of a finite number of indecomposable elements Q' of Σ .

By theorem 3.1, Σ is distributive and hence Dedekindian. Now Σ contains O_0 and hence by the ascending chain condition at least one irreducible P . If P' is any power of the irreducible P , we define the "multiplicity" of P' as the length of any principal chain (Ore [1] page 411) $P > \dots > P'$ joining P and P' increased by unity. Then every power of P has a unique finite multiplicity, and P itself is of multiplicity unity. It is convenient to consider the all element O_0 as the unique power of P of multiplicity zero. The following lemmas are obvious from this definition:

LEMMA 7.1. *If R and S are both powers of P and $R \supset S$, $R \neq S$ then the multiplicity of R is less than the multiplicity of S .*

LEMMA 7.2. *The powers of any irreducible form a dense sub-structure of Σ .*

Now let A be any element of $\Sigma \neq O_0$. Then by the chain condition, A has at most a finite number of irreducible divisors P_1, P_2, \dots, P_k and for each irreducible P_i there is a power P'_i of the highest positive multiplicity which divides A . Then the element $[P'_1, P'_2, \dots, P'_k]$ is a divisor of A which we call a *kernel* of A .

THEOREM 7.1. *Every element of Σ has exactly one kernel.*

PROOF. Assign to O_0 the kernel O_0 . If $A \neq O_0$, A has at least one kernel by the argument above. Let P' and P'' be powers of the irreducible divisor P of A of maximum multiplicity m dividing A . It suffices to show that $P' = P''$. Let $P^* = [P', P'']$. Then $P^* \supset A$ and P^* is a power of P by lemma 7.2. If $P^* \neq P'$ then since $P' \supset P^*$, the multiplicity of P^* is greater than m by lemma 8.1. Hence $P^* = P'$. Similarly, $P^* = P'', P' = P''$.

We denote the kernel of any element A of Σ by θA . If $A = \theta A$, A will be said to be *regular*. Thus all powers are regular. Operations on kernels are governed by the following simple rules:

$$(7.1) \quad A \supset B \text{ implies that } \theta A \supset \theta B.$$

$$(7.2) \quad \theta A = O_0 \text{ if and only if } A = O_0.$$

$$(7.3) \quad \theta(A, B) = (\theta A, \theta B), \theta[A, B] = [\theta A, \theta B].$$

$$(7.4) \quad \theta\theta A = \theta A.$$

The converse of rule (7.1) is generally false. It is obvious from (7.3) that we have:

THEOREM 7.2. *The set of all regular elements of Σ forms a sub-structure of Σ .*

THEOREM 7.3. *The set of all elements of Σ with the same kernel forms a sub-structure of Σ .*

THEOREM 7.4. *If A is regular and $B \supset A$, then B is regular.*

PROOF. We observe that if P' is any power of P and M any element of Σ , then it follows from lemma 7.2 that $P'' = (M, P')$ is also a power of P . Assume that $B \supset A$, A regular. Then

$$\begin{aligned} B = (B, A) &= (B, \theta A) = (B, [P'_1, \dots, P'_k]) \\ &= [(B, P'_1), \dots, (B, P'_k)] = [P''_1, \dots, P''_k]. \end{aligned}$$

Hence by rule (7.3) $\theta B = \theta[P''_1, \dots, P''_k] = [\theta P''_1, \dots, \theta P''_k] = [P''_1, \dots, P''_k] = B$.

Thus the sub-structure of all kernels of Σ is dense over Σ . (Ore [1], page 429).

8. So far no direct use has been made of postulate III a. It is obvious that the sub-structure of all regular elements and the sub-structure of all powers of any irreducible element are residually closed since the structures are dense over Σ and $A : B \supset A$ by rule (i) for residuation. Let A be any indecomposable element of Σ , B any other element of Σ . Then if $A \supset B$, $A : B = O_0$ by rule (iv) and conversely. If $A \not\supset B$, $A : B = A : D$ where $D = (A, B)$ by rule (xv). Then by rule (xvii), $A = [A : D, D]$ Hence $A : D = A$. We therefore have

THEOREM 8.1. *If A is indecomposable, then $A : X = A$ or O_0 for every element X of Σ .*

THEOREM 8.2. *An element of Σ is a prime if and only if it is indecomposable.*

PROOF. Assume that A is indecomposable, $A \supset [B, C]$, $A \not\supset B$. We are to show that $A \supset C$. Since $A \not\supset B$, $A : B = A$ by theorem 8.1. But $A \supset [B, C]$ implies $A : B \supset C$ by (1.2) Hence $A \supset C$. The converse is trivial.

The following two theorems are immediate corollaries.

THEOREM 8.3. *Let A and B be any two elements of Σ with decompositions as in (7.1) $A = [Q'_1, \dots, Q'_l]$, $B = [Q''_1, \dots, Q''_k]$ into cross-cuts of indecomposable elements. Then a necessary and sufficient condition that $B \supset A$ is that every Q'' should divide at least one Q' .*

THEOREM 8.4 "DECOMPOSITION THEOREM". *Let A be any element of $\Sigma \neq O_0$. Then A admits of a decomposition*

$$A = [Q_1, Q_2, \dots, Q_l]$$

into a cross-cut of a finite number of indecomposable elements Q such that no Q_i divides a Q_j unless $i = j$. This decomposition is unique save for the order in which the factors Q are written.

Theorem 8.1 was recently proved in a different manner by Birkhoff (Birkhoff [3], page 452).

The following theorem will be useful subsequently.

THEOREM 8.5. *If A and B are any two primes of Σ , then one and only one of the following conditions hold:*

$$(i) (A, B) = A, \quad (ii) (A, B) = B, \quad (iii) (A, B) = (A : B, B : A).$$

V. SEMI-ARITHMETICAL STRUCTURES

9. We shall now develop the consequences of assuming

POSTULATE V. *If M and N are any two elements of Σ , then*

$$(M : N, N : M) = O_0.$$

A system satisfying postulates I, II, III a, IV and V will be called a "semi-arithmetical" structure.

THEOREM 9.1. *In a residually closed structure, either the third or the fourth distributive law for residuation implies postulate V.*

PROOF. We may take the third and fourth laws in the abbreviated forms

$$\text{L III} \quad (A, B) : M = (A : M, B : M),$$

$$\text{L IV} \quad M : [A, B] = (M : A, M : B),$$

the general forms in section 4 following by an easy induction. Assume L III. Then by rules (v) and (xv), $O_0 = (M, N) : (M, N) = (M : (M, N), N : (M, N)) = (M : N, N : M)$. Assume L IV. Then by rules (v) and (x),

$$O_0 = [M, N] : [M, N] = ([M, N] : M, [M, N] : N) = (N : M, M : N).$$

THEOREM 9.2. *In a semi-arithmetical structure, the powers of any irreducible form an ordered structure.*

PROOF. If P' and P'' are powers of P , $P' : P''$ and $P'' : P'$ are both powers of P . But $(P' : P'', P'' : P') = O_0$. Hence either $P' : P'' = O_0$ or $P'' : P' = O_0$, so that by rule (iv), either $P' \supset P''$ or $P'' \supset P'$.

THEOREM 9.3. *In a semi-arithmetical structure, all primes with the same kernel form an ordered structure.*

PROOF. Let A and B be primes, $\theta A = \theta B = Q \neq O_0$. Then $Q \supset A, Q \supset B$ so that $Q \supset (A, B)$. Hence $(A, B) \neq O_0$. But by theorem 8.5 and postulate V, either $(A, B) = A$ or $(A, B) = B$ or $(A, B) = O_0$. Hence either $A \supset B$ or $B \supset A$.

THEOREM 9.4. *In a semi-arithmetical structure, if A and B are primes and $\theta A \neq \theta B$, $A \supset B$ if and only if $\theta A \supset \theta B$.*

PROOF. Assume that $\theta A \neq \theta B$ and $\theta A \supset \theta B$. Then $\theta(A, B) = (\theta A, \theta B) = \theta A \neq O_0$. But $\theta(A, B) \supset (A, B)$. Hence $(A, B) \neq O_0$. Therefore as in theorem 9.3 either $A \supset B$ or $B \supset A$. If $B \supset A$, $\theta B \supset \theta A$, $\theta B = \theta A$ contrary to hypothesis. Hence $A \supset B$. The converse is trivial.

THEOREM 9.5. *Let T be any regular element of Σ . Then the structure Θ of all primes with the kernel T is dense over Σ .*

PROOF. By theorem 9.3, Θ is ordered. Suppose that $A \supset X \supset B$, A, B in Θ , X in Σ . Then $\theta X = T$ by rule 7.1. By the decomposition theorem, $X = [C_1, C_2, \dots, C_t]$, $t \geq 1$, where each C_i is a prime and divides no other C_j , $i \neq j$. Since $A \supset X$, A divides some C_i . Assume that $A \supset C_1$. Then since $C_1 \supset X$, $\theta C_1 = T$. But since $C_i \supset X$, $\theta C_i \supset \theta X$ or $\theta C_i \supset \theta C_1$ by rule (7.1). Thus by

theorem 9.4 either $C_t \supset C_1$ or $\theta C_t = T$. In the latter case, either $C_t \supset C_1$ or $C_1 \supset C_t$ by theorem 9.3. Thus in either case, $t = 1$ and X is a prime.

It follows that any set of prime elements with the same kernel form a principal chain.

We say that two elements R and S of Σ are relatively prime if $(R, S) = O_0$. The following theorem is now obvious:

THEOREM 9.6. *Every element $A \neq O_0$ of a semi-arithmetical structure may be uniquely represented save for order as the cross-cut of a finite number of prime elements which are relatively prime in pairs.*

THEOREM 9.7. *In a semi-arithmetical structure the third distributive law for residuation always holds; that is for any three elements A, B of Σ*

$$\text{L III} \quad (A, B) : C = (A : C, B : C)$$

PROOF. The law is obviously true if either A or B is O_0 . We next show it is true if A and B are primes Q and R . For then either (i) $(Q, R) = O_0$, or (ii) $(Q, R) = Q$ or (iii) $(Q, R) = R$. (i). If $(Q, R) = O_0$, $(Q, R) : C = O_0$. But then $(Q : C, R : C) = O_0$. For either $Q : C = O_0$, or $R : C = O_0$, or $Q : C = Q$ and $R : C = R$. Hence $(Q, R) : C = (Q : C, R : C)$ in this case. (ii). If $(Q, R) = Q$, then $(Q, R) : C = Q : C$. Hence if $Q : C = O_0$, $(Q, R) : C = (Q : C, R : C)$. If $Q : C = Q$, then $R : C = R$. For if $R : C = O_0$, $R \supset C$. But since $(Q, R) = Q$, $Q \supset R$, $Q \supset C$ and $Q : C = O_0$. Thus if $Q : C = Q$, $(Q : C, R : C) = (Q, R) = Q = (Q, R) : C$. In (iii) the proof is similar.

If A and B are not primes, let their canonical decompositions be

$$A = [\dots, Q, \dots], B = [\dots, R, \dots].$$

Then by the second distributive law for residuation

$$\begin{aligned} (A : C, B : C) &= ([\dots, Q, \dots] : C, [\dots, R, \dots] : C) \\ &= ([\dots, Q : C, \dots], [\dots, R : C, \dots]) \\ &= [\dots, (Q : C, R : C), \dots] \\ &= [\dots, (Q, R) : C, \dots] \\ &= [\dots, (Q, R), \dots] : C \\ &= ([\dots, Q, \dots], [\dots, R, \dots]) : C \\ &= (A, B) : C. \end{aligned}$$

In like manner we may prove

THEOREM 9.8. *In a semi-arithmetical structure, the fourth distributive law for residuation always holds.*

On combining theorems 9.1, 9.7 and 9.8, 6.1 and 6.2 we obtain

COROLLARY. *Either the third distributive law for residuation, the fourth distributive law for residuation or postulate V is a necessary and sufficient condition*

that a distributive structure containing an all element in which the ascending chain condition holds may be a semi-arithmetical structure.

Let us call a structure "arithmetical" if the only prime elements in it are powers of irreducibles. (Arithmetical structures have been exhaustively investigated by F. Klein who calls them "Sternverbande" (Klein [2])). We see then that an arithmetical structure is simply a semi-arithmetical structure in which all elements are regular, or in which the only primes are powers of irreducible elements.

REFERENCES

G. BIRKHOFF:

1. Bulletin Am. Math. Soc. vol 40 (1934), pp. 613-619.
2. Proc. Cambr. Phil. Soc. vol. 29 (1933), pp. 441-464.
3. Duke Math. Journal, vol. 3, Sept. (1937), pp. 443-454.

R. DEDEKIND: 1. Collected Works (1931), vol. II, paper 30, pp. 236-271.

R. P. DILWORTH: 1. Bulletin Am. Math. Soc., vol. 44 (1938), pp. 262-268.

F. KLEIN:

1. Deutsche Math., vol. 2 (1937), pp. 216-241.
2. Math. Annalen., vol. 106 (1932), pp. 114-134.

G. KÖTHE: Deutsche Math. Verein, '37, pp. 125-144.

H. M. MACNEILLE: 1. Trans. Am. Math. Soc., vol. 42, November 1937, pp. 416-460.

O. ORE: 1. These Annals (2), vol. 36 (1935), pp. 406-432.

M. WARD: 1. Duke Math. Journal, vol. 3, December (1937), 627-636.

CALIFORNIA INSTITUTE OF TECHNOLOGY.

Chapter 13

1939

A NOTE ON DIVISIBILITY SEQUENCES*

MORGAN WARD

1. **Introduction.** A sequence of rational integers

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

is called a *divisibility sequence* if u_r divides u_s whenever r divides s , and any integer M dividing terms of (u) with positive suffix is called a divisor of (u) . The suffix s is called a *rank of apparition of M* if $u_s \equiv 0 \pmod{M}$, but $u_r \not\equiv 0 \pmod{M}$ if r is a proper divisor of s . It follows from a previous note of mine in this Bulletin (Ward [1]) that a necessary and sufficient condition that every divisor of (u) shall have only *one* rank of apparition is that (u) have the following property:

A. *If $c = (a, b)$, then $u_c = (u_a, u_b)$ for every pair of terms u_a, u_b of (u) .*

Assume that no $u_r = 0$, ($r > 0$). Then we may introduce numbers

$$[n, r] = u_n \cdot u_{n-1} \cdot \dots \cdot u_{n-r+1} / u_1 \cdot u_2 \cdot \dots \cdot u_r, \\ r = 1, \dots, n; n = 1, 2, \dots,$$

which we call the *binomial coefficients belonging to (u)* .†

In a previous paper (Ward [1]), I proved a result equivalent to the following theorem:

THEOREM 1. *If every divisor of (u) has only one rank of apparition, the binomial coefficients belonging to (u) are rational integers.*

I give here a simple sufficient condition for integral binomial coefficients applicable when the divisors of (u) have several ranks of apparition.

2. **Main theorem.** Let (v) be any sequence of rational integers subject to the single condition $v_r \neq 0$, ($r > 0$). The sequence (u) will be said to have the property C if

$$u_n = \prod_{d|n} v_d,$$

the product being extended over all divisors d of n .

* Presented to the Society, February 25, 1939.

† If $u_n = n$, they reduce to ordinary binomial coefficients. For their properties for general (u) , see Ward [2].

THEOREM 2. *Every sequence (u) with property C is a divisibility sequence, and all of its associated binomial coefficients are rational integers.*

The proof is immediate. The sequence (u) is obviously a divisibility sequence, and no $u_r = 0$, ($r > 0$). Any one of the binomial coefficients of (u) may be put in the form

$$u_1 \cdot u_2 \cdot \dots \cdot u_{n+m} / u_1 \cdot u_2 \cdot \dots \cdot u_n \cdot u_1 \cdot u_2 \cdot \dots \cdot u_m.$$

But if $[x/d]$ denotes as usual the greatest integer in x/d , v_d appears in the denominator of the expression above $[n/d] + [m/d]$ times, and in the numerator $[(n+m)/d]$ times. Since

$$\left[\frac{n+m}{d} \right] \geq \left[\frac{n}{d} \right] + \left[\frac{m}{d} \right],$$

the expression is an integer. In like manner, all the multinomial coefficients belonging to (u) (Ward [2]) may be shown to be integral.

3. An application. Let α, β be distinct algebraic integers, and let \mathfrak{F} be the smallest normal field containing both α and β . Define a sequence (u) by

$$u_n = \prod_S (\alpha^n - \beta^n),$$

where the product is extended over all automorphisms S of \mathfrak{F} , so that u_n is a rational integer.

If $Q_d(x, y)$ is the homogeneous cyclotomic polynomial of degree $\phi(d)$, then

$$u_n = \prod_{d|n} v_d,$$

where

$$v_d = \prod_S Q_d(\alpha, \beta).$$

Since the v_d are rational integers, it follows from Theorem 2 that all of the binomial coefficients belonging to (u) are rational integers provided that no $v_d = 0$; that is, provided that α/β is not a root of unity.

This result applies to the Lucasian sequences studied in Ward [3] which appear to include all extant instances of divisibility sequences satisfying a linear recursion relation.

4. Conclusion. Sequences with property C have another interesting property which is stated in the following theorem:

THEOREM 3. *If (u) has property C, then the prime divisors of (u) and (v) are identical. Furthermore the ranks of apparition of any prime in (u) and in (v) are the same.*

The first part of this theorem is obvious. D. H. Lehmer has proved that every rank of apparition of a prime p in (u) is a rank of apparition of p in (v) (Lehmer [1], p. 462). The converse is immediate. Since (v) is not in general a divisibility sequence, a place of apparition of p in (u) need not be a place of apparition of p in (v) .

REFERENCES

D. H. LEHMER

1. Annals of Mathematics, (2), vol. 34 (1933), pp. 461–479.

M. WARD

1. This Bulletin, vol. 42 (1936), pp. 843–845.
2. American Journal of Mathematics, vol. 58 (1936), pp. 255–266.
3. Transactions of this Society, vol. 44 (1938), pp. 68–86.

CALIFORNIA INSTITUTE OF TECHNOLOGY

EVALUATIONS OVER RESIDUATED STRUCTURES

BY MORGAN WARD AND R. P. DILWORTH

(Received June 6, 1938)

I. INTRODUCTION

1. In previous papers,¹ we have developed a theory of structures over which auxiliary operations of multiplication and residuation may be defined with properties analogous to the like-named operations in polynomial ideal theory. We have applied our results to generalize the various decomposition theorems of ideal theory (van der Waerden [1]) to extensive classes of structures.²

We give here some results on the evaluations of such structures. By an evaluation we mean a homomorphism (Ore [1], Chapter II) between the structure and a set of real numbers ordered by the relation \leq under which multiplication in the structure corresponds to addition of the reals. If we are willing to assume that the structure homomorphism preserves residuation, we can obtain results of a simplicity and finality comparable with the classic evaluation theory for domains of integrity and fields. (van der Waerden [1], Albert [1]). But this assumption unduly restricts the kinds of structures which may be evaluated and complicates the arithmetical interpretation of the "discrete evaluations" (part III of paper) which are our main concern. We shall accordingly assume it only incidentally. (Part IV of paper.)

2. Our main result is an arithmetical characterization of all discrete evaluations of a residuated structure with the ascending chain condition in terms of certain chains of primary elements belonging to the structure. No appeal is necessary to the Dedekind modular axiom or to the special decomposition theorems which ensue on assuming that every irreducible is primary (Ward-Dilworth [1], [2]).

We also discuss briefly some interesting topological questions suggested by the evaluation.

¹ See the references Ward-Dilworth [1], Dilworth [1], Ward [1], Ward [2] at the close of the paper. The idea goes back to Dedekind (Dedekind [1], but our only immediate predecessor seems to have been W. Krull (Krull [1])). We have expanded and elaborated the results summarized in Ward-Dilworth [1] in a paper "Residuated Lattices" (Ward-Dilworth [2]) which has been submitted for publication elsewhere. We take this occasion to correct some errors in Ward-Dilworth [1] section 4, page 163. In condition D 1, the exponent r should be one. In the fourth theorem, the words "and sufficient" should be struck out. The fifth theorem should be struck out in toto. We may add that we have greatly extended the results of this section in Ward-Dilworth [2] and largely freed them of their dependence on the modular axiom.

² Distributive structures are studied in detail in the paper Ward [2] in this journal.

The following examples show that evaluations are of frequent occurrence. Here πx denotes the evaluation function, and \mathfrak{S} the basic structure.

(i) \mathfrak{S} , rational integers with union and cross-cut G.C.D. and L.C.M. and multiplication ordinary multiplication. $\pi a = 0$, a odd; $\pi a = 1$, a even, defines an evaluation.

(ii) \mathfrak{S} , ideals of a principal ideal ring, multiplication ordinary multiplication. Evaluation is essentially the same as the ordinary evaluation.

(iii) \mathfrak{S} , Boolean algebra or distributive structure, multiplication identified with cross-cut (Ward [2]). \mathfrak{p} any prime ideal of the structure (Stone [1], Birkhoff [1]). $\pi a = 1$ if a is in \mathfrak{p} , $\pi a = 0$ otherwise, defines an evaluation.

(iv) \mathfrak{S} a chain structure of finite length n :

$$i = a_1 > a_2 > \dots > a_n.$$

Let $n = n_1 + n_2 + \dots + n_l$ be any fixed partition of n into positive summands. Effect a class separation of \mathfrak{S} , $\mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}_1 + \dots + \mathfrak{S}_l$ by the rule $a_i \in \mathfrak{S}_k$ if $n_1 + n_2 + \dots + n_{k-1} < i \leq n_1 + n_2 + \dots + n_k$. Define a multiplication over \mathfrak{S} as follows. Let $b_k = a_{n_1+n_2+\dots+n_k}$, ($k = 1, 2, \dots, l$). Then if $a_u \in \mathfrak{S}_i$ and $a_v \in \mathfrak{S}_j$, $a_u a_v = b_{i+j}$ if $i + j \leq l$, $a_u a_v = b_l = a_n$ if $i + j \geq l$. Then $\pi a = k$ if $a \in \mathfrak{S}_k$ is an evaluation.

(v) \mathfrak{S} , finite arithmetical lattice. Since such a lattice is a direct cross-cut of chains of finite length, the procedure of (iv) allows us to construct evaluations at will. The case when each $n_i = 1$ in (iv) gives the ordinary evaluations. One of us plans to discuss the residuation of such a lattice elsewhere.

(vi) \mathfrak{S} , an arbitrary chain structure. $a_1 \supset a_2 \supset a_3 \supset \dots$ any selection of elements of \mathfrak{S} where each a_i properly divides a_{i+1} . Define \mathfrak{S}_i as the set of all elements x of \mathfrak{S} such that $a_{i-1} \supset x \supset a_i$, $x \neq a_i$. Define a multiplication by the rule if $x \in \mathfrak{S}_i$, $y \in \mathfrak{S}_j$ then $xy = a_{i+j}$. The evaluation is defined then by $\pi x = k$ if $x \in \mathfrak{S}_k$.

(vii) \mathfrak{S} , a residuated structure with ascending chain condition. p any prime of \mathfrak{S} . $\pi a = 1$ if $p \supset a$, $\pi a = 0$ otherwise defines an evaluation. (See part III of paper.) This example applies to the ideals of any commutative ring with chain condition, but no modular condition need be assumed.

3. We summarize here the notations and definitions we shall employ. We denote our structures by German capitals $\mathfrak{S}, \mathfrak{S}_i, \mathfrak{S}', \dots$. The letters $\mathfrak{U}, \dots, \mathfrak{Y}$ are reserved to denote sub-sets of elements of our basic structure \mathfrak{S} which are not necessarily structures. We use small latin letters a, b, \dots for the elements of our structure, and write $x \in \mathfrak{X}$ ($x \in \mathfrak{S}$) for the set \mathfrak{X} (the structure \mathfrak{S}) contains the element x . $x \supset y$ or $y \subset x$, $x \not\supset y$, $x = y$ denote as usual x divides y , x does not divide y , x equals y . We use (x, y) for union and $[x, y]$ for cross-cut, reversing Ore's usage. (Ore [1], Ward [1], [2].) We assume that \mathfrak{S} has a unit element i dividing every other element. The null element z divisible by

every other element need not exist. Multiplication $x \cdot y$ or xy and residuation $x:y$ are one-valued operations on \mathfrak{S} to \mathfrak{S} defined by the following conditions:

- | | |
|---|--|
| R 1. $a, b \in \mathfrak{S}$ implies $a:b \in \mathfrak{S}$. | M 1. $a, b \in \mathfrak{S}$ implies $ab \in \mathfrak{S}$. |
| R 2. $a:b = i$ if and only if $a \supset b$. | M 2. $a = b$ implies $ac = bc$. |
| R 3. $a \supset b$ implies $a:c \supset b:c$ and
$c:b \supset c:a$. | M 3. $ab = ba$. |
| R 4. $(a:b):c = (a:c):b$. | M 4. $(ab)c = a(bc)$. |
| R 5. $[a, b]:c = [a:c, b:c]$. | M 5. $ai = a$. |
| R 6. $c:(a, b) = [c:a, c:b]$. | M 6. $a(b, c) = (ab, ac)$. |

In addition, the two operations are assumed to be interconnected by the formulas

$$(3.1) \quad a \supset (a:b)b; \text{ if } a \supset xb \text{ then } a:b \supset x.$$

$$(3.2) \quad ab:a \supset b; \text{ if } y:a \supset b \text{ then } y \supset ab.$$

A structure over which both a residuation and a multiplication may be defined satisfying R 1–M 6 and (3.1)–(3.2) will be said to be *residuated* (Ward-Dilworth [1]). We shall assume that the reader is familiar with the elementary properties of residuation and multiplication such as $a:b = a:(a, b) = [a, b]:b$; $a:bc = (a:b):c$; $a:(a:b) \supset (a, b)$ and so on. (Ward [1], [2], Dilworth [1], Ward-Dilworth [2].)

If $\mathfrak{X}, \mathfrak{Y}$ are any two subsets of \mathfrak{S} , we denote by $(\mathfrak{X}, \mathfrak{Y})$ $[\mathfrak{X}, \mathfrak{Y}]$ and $\mathfrak{X}\mathfrak{Y}$ the sets consisting respectively of all unions, cross-cuts or products of elements of \mathfrak{X} with elements of \mathfrak{Y} (Ward [2]). We write $\mathfrak{X} \supseteq \mathfrak{Y}$ if every element of \mathfrak{Y} lies in \mathfrak{X} . For example, $\mathfrak{X} \supseteq \mathfrak{X}^2$ means \mathfrak{X} is closed under multiplication. We use $\mathfrak{X} + \mathfrak{Y}$ for the set-theoretic sum of \mathfrak{X} and \mathfrak{Y} .

4. An element p of \mathfrak{S} is said to be a *prime* if $p \supset ab$ implies $p \supset a$ or $p \supset b$, and *primary* if $p \supset ab$, $p \not\supset a$ implies $p \supset b^t$ for some t . The following lemmas are true in any residuated structure in which the ascending chain condition holds. They are readily proved by transcribing their analogues for commutative ideal theory (von der Waerden [1] chapter 12) into the language of structure theory.

LEMMA 4.1. *If q is primary, there exists a prime p such that $p \supset q \supset p^t$. p will be said to correspond to q .*

LEMMA 4.2. *Let q and p be elements of \mathfrak{S} with the properties*

- (α) $q \supset ab$ and $q \not\supset a$ imply $p \supset b$.
- (β) $p \supset q$.
- (γ) $p \supset b$ implies $q \supset b^t$ for some t .

Then q is primary, and p is the prime element corresponding to q .

The union of any set \mathfrak{X} will on occasion be called the leader of \mathfrak{X} .

If $q = [a, b]$ implies $q = a$ or $q = b$, q will be said to be *irreducible*.

II. EVALUATIONS

5. Any set of real numbers closed with respect to addition forms a residuated structure with respect to the division relation "less than or equal to." The union (α, β) and cross-cut $[\alpha, \beta]$ of two real numbers α and β are respectively their minimum and maximum, while their "product" $\alpha\beta$ and "residual" $\alpha:\beta$ are respectively $\alpha + \beta$ and $\alpha - (\alpha, \beta)$. (Dilworth [1]; Ward-Dilworth [1] section 2, first theorem; Ward [3].) If the set of real numbers is bounded above, they still form a residuated structure provided that we take the product $\alpha\beta$ equal to the least upper bound of the set whenever $\alpha + \beta$ is greater than it. We shall use the letter σ to denote the least upper bound of values. If no upper bound exists, we take $\sigma = +\infty$, the ideal null element of the structure of all the reals.

A function π on \mathfrak{S} to such a set of reals is called an *evaluation* of \mathfrak{S} if the following four conditions are satisfied:

E 1. For every element a of \mathfrak{S} , πa is a uniquely determined real number.

E 2. $a = b$ implies $\pi a = \pi b$.

E 3. (i) $\pi(a, b) = (\pi a, \pi b)$ and (ii) $\pi[a, b] = [\pi a, \pi b]$.

E 4. $\pi ab = (\pi a + \pi b, \sigma)$.

We shall call the real number πa the *value* of the structure element a .

If the values of πa are bounded above, we shall say that the evaluation is bounded. Since for any a , $a = ai$, $i \supset a$ and $a \supset b$ implies $a = (a, b)$, we have

$$(5.1) \quad \pi i = 0 \quad \pi x \geq 0, x \in \mathfrak{S}.$$

$$(5.2) \quad a \supset b \text{ implies } \pi a \leq \pi b.$$

Since every evaluation is a homomorphism, we may define by means of the evaluation a congruence relation $x \equiv y \pmod{\pi}$ over \mathfrak{S} , elements being congruent if and only if they have the same values. This congruence relation has the usual properties; that is, it is an equivalence relation, and if $a \equiv b \pmod{\pi}$ then for any c ,

$$(a, c) \equiv (b, c), \quad [a, c] \equiv [b, c], \quad ac \equiv bc \pmod{\pi}.$$

We call the elements congruent to i the units of \mathfrak{S} modulo π . They form a dense residuated sub-structure of \mathfrak{S} . Moreover if u is any unit

$$au \equiv a \pmod{\pi}, \text{ every } a \text{ of } \mathfrak{S}.$$

6. Since we may think of an evaluation as a mapping of the structure onto the metric space of the real numbers, the question arises as to the connection of the evaluation with the topology of the structure. Structures have been topologized in several ways. For instance, Glivenko [1, 2] has shown the identity of normed structures with certain types of metric spaces. Stone [1] has shown that Boolean algebras are mathematically equivalent to locally

bicomplete totally disconnected topological spaces, and H. Wallman [1] has similarly treated the topology of a distributive structure. In this connection one of us has found that much of Wallman's theory for a distributive structure holds in any structure over which a multiplication is defined.

If we attempt to introduce a metric into the structure by the use of the evaluation following the method of Glivenko, the difficulty arises that we may have $a \supset b$ properly with $\pi a = \pi b$. If we attempt to connect the evaluation with the topology of the structure by the method of Stone and Wallman, it is not clear what the map of a point (that is, a structure ideal) should be in terms of the evaluation. Our results in this direction are incomplete, and belong properly to the general question of the topology of residuated structures which one of us (R. P. Dilworth) will treat elsewhere.

III. DISCRETE EVALUATIONS—CLEAVAGES

7. If α is any positive value, then the elements of \mathfrak{S} whose values are $0, \alpha, 2\alpha, 3\alpha, \dots$ obviously form a multiplicatively closed sub-structure of \mathfrak{S} . A particularly interesting and important case occurs when this sub-structure coincides with \mathfrak{S} itself. We shall call the evaluation then *discrete*. For a discrete evaluation, there is no loss in generality in taking the values to be $0, 1, 2, \dots$, the set breaking off or not accordingly as the evaluation is bounded or unbounded. Let \mathfrak{S}_k denote the set of elements of \mathfrak{S} with values k . Then we have a set-theoretic separation of \mathfrak{S}

$$(7.1) \quad \mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}_1 + \mathfrak{S}_2 + \dots + \mathfrak{S}_k + \mathfrak{S}_{k+1} + \dots,$$

where each \mathfrak{S}_i is a structure, and \mathfrak{S}_0 is multiplicatively closed. We denote the set $\mathfrak{S}_1 + \mathfrak{S}_2 + \dots$ by \mathfrak{S}' , so that

$$(7.2) \quad \mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}'.$$

We shall now introduce the important notion of a *cleavage*³ of a residuated structure. Let \mathfrak{S} be a structure. From now on we assume explicitly

N 1. \mathfrak{S} is residuated.

N 2. The ascending chain condition holds in \mathfrak{S} .

DEFINITION OF A PRIME CLEAVAGE. A separation of \mathfrak{S}

(7.3) $\mathfrak{S} = \mathfrak{U} + \mathfrak{V}$, $\mathfrak{U}, \mathfrak{V}$ no elements in common, \mathfrak{U} non-empty, is called a prime cleavage of \mathfrak{S} provided that

$$(7.31) \quad \mathfrak{U} \supset \mathfrak{U}^2, \quad \mathfrak{U} \supset (\mathfrak{U}, \mathfrak{S}), \quad \mathfrak{V} \supset (\mathfrak{V}, \mathfrak{V}).$$

THEOREM 7.1. Every cleavage of \mathfrak{S} determines a prime, and with every prime is associated a cleavage.

* The idea goes back to Krull [1]. For the special case when the multiplication of the structure is the cross-cut operation (but no chain condition is assumed, so that the cleavage does not necessarily define a structure element), the notion was applied to Boolean algebras by M. H. Stone [1], and extended by G. Birkhoff [2] to any distributive structure. The "primary cleavages" we introduce here seem to be new.

PROOF. By N 2 and (7.31)(iii), the union of \mathfrak{B} exists, and lies in \mathfrak{B} (Ore [1] §2). Denote it by p . p cannot divide an element of \mathfrak{U} . For then by (7.31) (ii) $p = (p, u) \in \mathfrak{U}$ contrary to (7.3). Assume that

$$p \supset ab, \quad p \not\supset a, \quad a, b \text{ in } \mathfrak{S}.$$

Then $ab \in \mathfrak{B}$, $a \in \mathfrak{U}$. If $b \in \mathfrak{U}$, $ab \in \mathfrak{U}$ by (7.31) (i), and $p \not\supset ab$. Hence $b \notin \mathfrak{B}$ and $p \supset b$. Hence p is a prime by definition. The conceivable case $p = i$ is excluded because then since $i \supset x$, every x , \mathfrak{B} would contain \mathfrak{S} and \mathfrak{U} be empty.

We observe that the separation (7.2) induced by the evaluation of \mathfrak{S} is a cleavage. Since both \mathfrak{U} and \mathfrak{B} in (7.3) are easily shown to be structures, we shall use (7.2) henceforth to denote any prime cleavage. Conversely, given (7.2) with associated prime p , we may define a bounded evaluation over \mathfrak{S} by $\pi x = 0$ if $p \not\supset x$; $\pi x = 1$ if $p \supset x$, $x \in \mathfrak{S}$. We have thus proved

THEOREM 7.2. *Every discrete evaluation of \mathfrak{S} determines a prime, and every prime determines at least one evaluation.*

8. We shall next extend the notion of a cleavage so as to characterize the primary elements of \mathfrak{S} .

With the notation of the previous section, let

$$(7.2) \quad \mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}'$$

be a cleavage with associated prime p , so that

$$(8.1) \quad \mathfrak{S}_0 \supset \mathfrak{S}_0^2, \quad \mathfrak{S}_0 \supset (\mathfrak{S}_0, \mathfrak{S}), \quad \mathfrak{S}' \supset (\mathfrak{S}', \mathfrak{S}'),$$

while

$$(8.11) \quad p \in \mathfrak{S}'; x \in \mathfrak{S}' \text{ implies } p \supset x.$$

DEFINITION OF A PRIMARY CLEAVAGE. *A separation of \mathfrak{S}'*

(8.2) $\mathfrak{S}' = \mathfrak{U}^* + \mathfrak{B}$, \mathfrak{U}^* , \mathfrak{B} no elements in common, is called a primary cleavage of \mathfrak{S} provided that

$$(8.21) \quad \mathfrak{U}^* \supset \mathfrak{S}_0 \mathfrak{U}^*; \mathfrak{B} \supset \mathfrak{S}'^k \text{ for some positive integer } k; \mathfrak{B} \supset (\mathfrak{B}, \mathfrak{B}).$$

THEOREM 8.1. *The leader of \mathfrak{B} is a primary element q of \mathfrak{S} whose corresponding prime is p .*

PROOF. The result is trivial if \mathfrak{U}^* is empty, as then $\mathfrak{B} = \mathfrak{S}'$. Assume henceforth that \mathfrak{U}^* is non-empty. N 2 and (8.21) (iii) guarantee that the leader q exists and lies in \mathfrak{B} . Assume that $q \supset ab$, $q \not\supset a$; a, b in \mathfrak{S} . Then either $a \in \mathfrak{S}_0$ or $a \in \mathfrak{U}^*$. In either case $b \in \mathfrak{S}'$. For if $b \in \mathfrak{S}_0$, $ab \in \mathfrak{S}_0$ or $ab \in \mathfrak{U}^*$ by (8.1) (i) and (8.21) (i). But if $b \in \mathfrak{S}'$, then $p \supset b$ by (8.11). We have thus shown that

(α) $q \supset ab$ and $q \not\supset a$ imply $p \supset b$.

By (8.11) and (8.21) (ii), we have

(β) $p \supset b$. (γ) If $p \supset b$, then $q \supset b^k$.

Hence by lemma 4.2, q is primary, and p is the prime corresponding to q .

THEOREM 8.2. *Every primary element of \mathfrak{S} determines a primary cleavage.*

PROOF. Let q be any primary, and let p be its corresponding prime. Then by lemma 4.1

$$(8.3) \quad p \supset q \supset p^k$$

where we may assume that $k > 1$. Let (7.2) as before be the cleavage associated with p . We now separate \mathfrak{S}' into two disjoint classes \mathfrak{U}^* and \mathfrak{B} as in (8.2) by the rule $x \in \mathfrak{U}^*$ if $q \nmid x$; $x \in \mathfrak{B}$ if $q \supset x$, x any element of \mathfrak{S}' . We shall show that (8.21) holds.

First if $b \in \mathfrak{S}'$, then $p \supset b$. Hence $p^k \supset b^k$, so that by (8.3), $q \supset b^k$ or $b^k \in \mathfrak{B}$. Hence (8.21) (ii) holds. Also, if $q \supset b$, $q \supset c$ then $q \supset (b, c)$ so that (8.21) (iii) holds. Finally, assume that $a \in \mathfrak{S}_0$ and $b \in \mathfrak{U}^*$. Then since $p \supset ab$, either $ab \in \mathfrak{U}^*$ or $ab \in \mathfrak{B}$. If $ab \in \mathfrak{B}$, then $q \supset ab$. Since $b \in \mathfrak{U}^*$, $q \nmid b$. Hence since q is primary, $q \supset a^t$ for some t . Then by (8.3), $p \supset a^t$ or $p \supset a$, contradicting $a \in \mathfrak{S}_0$. Hence if $a \in \mathfrak{S}_0$ and $b \in \mathfrak{U}^*$, then $ab \in \mathfrak{U}^*$ giving (8.21) (i).

It is important to observe that the set \mathfrak{U}^* is in general not a sub-structure of \mathfrak{S} .

9. We return now to the evaluation π and the associated separation of \mathfrak{S} into residue classes:

$$(7.1) \quad \mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}_1 + \mathfrak{S}_2 + \cdots + \mathfrak{S}_k + \mathfrak{S}_{k+1} + \cdots$$

Let us define

$$\mathfrak{S}^* = \mathfrak{S}_1 + \mathfrak{S}_2 + \cdots + \mathfrak{S}_{k-1}, \quad \mathfrak{S}'' = \mathfrak{S}_k + \mathfrak{S}_{k+1} + \cdots$$

so that

$$\mathfrak{S}' = \mathfrak{S}^* + \mathfrak{S}''.$$

Then it is easy to see that a primary cleavage is defined, for the conditions (8.2), (8.21) are all satisfied. Hence we may state

THEOREM 9.1. *Let π be a discrete evaluation of a residuated structure in which the ascending chain condition holds, and let (7.1) be the corresponding separation into residue classes modulo π . Then the leader of the substructure \mathfrak{S}_k of all elements of \mathfrak{S} with the value $k \geq 1$ is a primary element $q^{(k)}$ of \mathfrak{S} which divides all elements of \mathfrak{S} with values $\geq k$ and belongs to the prime element $p = q^{(1)}$ leading \mathfrak{S}_1 .*

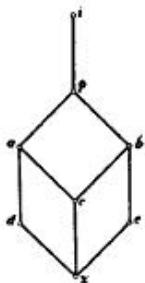
THEOREM 9.2. *The primaries $q^{(1)}, q^{(2)}, \dots$ are all irreducible.*

PROOF. If q leads \mathfrak{S}_k and $q = [a, b]$, then by E 3, either $\pi q = \pi a$ or $\pi q = \pi b$. Hence by Theorem 9.1, either $q \supset a$ or $q \supset b$. Hence $q = [a, b]$ implies $q = a$ or $q = b$ so that q is irreducible.

Although a primary cleavage can be associated with an arbitrary primary q , an evaluation cannot in general be determined having q as one of its leaders. For \mathfrak{S}^* and \mathfrak{S}'' must both be structures and admit of special multiplication rules not required in our general definition.

To give a simple illustration, consider the non-modular structure \mathfrak{L} pictured.

A residuation and multiplication may be defined over \mathfrak{L} by the rule given in theorem 8.1 of Ward-Dilworth [2]; viz. $xy = y$ if $x = i$; $xy = x$ if $y = i$; $xy = z$,



otherwise. i is the unit and p is a prime while all other elements are primary. We may define three distinct evaluations over \mathfrak{L} by the separations

- (1) $\mathfrak{L}_0 = \{i\}; \mathfrak{L}_1 = \{p, a, b, c, d, e, z\}.$
- (2) $\mathfrak{L}_0 = \{i\}; \mathfrak{L}_1 = \{p, a, d\}; \mathfrak{L}_2 = \{b, c, e, z\}.$
- (3) $\mathfrak{L}_0 = \{i\}; \mathfrak{L}_1 = \{p, b, e\}; \mathfrak{L}_2 = \{a, c, d, z\}.$

Thus the primaries a and b both have evaluations associated with them. But no other primary determines an evaluation.

Consider c for example. Its primary cleavage is $\mathfrak{L}_0 = \{i\}$, $\mathfrak{L}^* = \{p, a, b, e, d\}$, $\mathfrak{L}'' = \{c, z\}$. But \mathfrak{L}^* is not a structure, so that no evaluation is defined. Similar results hold for d, e and z .

Thus while any discrete evaluation of a structure satisfying N 1 and N 2 determines a chain of primaries all associated with the same prime, not every such chain determines an evaluation. On the other hand, every prime determines at least one evaluation; namely that determined by $\pi a = 1$ if $p \supset a$; $\pi a = 0$ if $p \not\supset a$.

If the evaluation π is bounded, so that \mathfrak{S} separates into a finite number of residue classes modulo π ,

$$\mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}_1 + \cdots + \mathfrak{S}_n,$$

then the evaluation may be defined in a manner strictly analogous to the evaluations of a finite principal ideal ring. Namely, let the leader of \mathfrak{S}_n be q , and let p be its associated prime. For any other element a of \mathfrak{S} , there is then a least power of p such that $q \supset ap^n$. We then may define

$$\pi a = n - s \text{ if } q \supset ap^n, q \not\supset ap^{n-1}.$$

In particular, this definition applies to any discrete evaluation of a residuated lattice of finite order.

IV. EVALUATIONS PRESERVING RESIDUATION

10. We shall conclude by giving a few properties of bounded evaluations under which residuation is preserved. Consider an evaluation satisfying E 1, E 2 and

E 3 (i) $\pi(a, b) = (\pi a, \pi b)$.

E 5 $\pi a:b = \pi a:\pi b = \pi a - (\pi a, \pi b)$.

E 6 *The evaluation is bounded.*

Let σ as before denote the least upper bound of the values of π . If \mathfrak{S} does not contain a null element z , we may adjoin z to \mathfrak{S} without destroying the residuation by defining $z:z = i$, $zi = z$, $z:x = zx = z$, $x \neq i$, $x \in \mathfrak{S}$. (This fact is a special instance of theorem 8.2 of Ward-Dilworth [2].) Clearly $\pi z = \sigma$.

THEOREM 10.1. *If a, b are any two elements of \mathfrak{S} , then*

E 4. $\pi ab = (\pi a + \pi b, \sigma)$.

PROOF. Adjoin z to \mathfrak{S} . Then by E 5, $\pi z:\pi ab = \pi(z:ab) = \pi((z:a):b) = (\pi z:\pi a):\pi b$ or $\sigma - \pi ab = \sigma - \pi a - (\sigma - \pi a, \pi b)$. Hence since σ is finite, $\pi ab = \pi a + (\sigma - \pi a, \pi b)$, giving E 4.

Let λ denote the greatest lower bound of all positive values of π .

THEOREM 10.2. *If $\lambda = 0$, every real number in the interval $(0, \sigma)$ is a limit point of values. If $\lambda > 0$, then the evaluation is discrete.*

This theorem does not require the evaluation to be bounded. The first part of the theorem uses only E 4, and is true for any evaluation. But the second part of the theorem depends essentially on E 5, as may be shown by simple examples.

PROOF. If $\lambda = 0$, we may select a sequence of elements $a_1, a_2, \dots, a_n, \dots$ of \mathfrak{S} such that $\alpha_n = \pi a_n > 0$, $\alpha_{n+1} \leq \alpha_n$, $\lim \alpha_n = 0$. Since α_n is positive, for any positive β there exists an integer r_n such that $r_n \alpha_n < \beta \leq (r_n + 1) \alpha_n$ for all sufficiently large n . Then if $b_n = a_n^{r_n}$, by E 4, $\pi b_n = r_n \alpha_n$ and $\lim \pi b_n = \beta$.

Suppose that $\lambda > 0$. Then there exists an element l of \mathfrak{S} such that $\pi l = \lambda$. For otherwise, we may pick a sequence of elements x_n of \mathfrak{S} such that $\pi x_n > \pi x_{n+1} > \lambda$; $\lim \pi x_n = \lambda$. Choose m so that $\pi x_m < 2\lambda$. Then by E 5, $\pi x_m:x_{m+1} = \pi x_m - \pi x_{m+1} < 2\lambda - \lambda < \lambda$. Hence $\pi x_m = \pi x_{m+1}$, giving a contradiction.

Let b be any other element of \mathfrak{S} with a positive value πb . Then we can choose a positive integer r such that $r\lambda \leq \pi b < (r + 1)\lambda$. Then by E 5 and E 4 $\pi b:l^r = \pi b - \pi(b, l^r) = \pi b - r\lambda < \lambda$. Hence $\pi b = r\lambda$, and the evaluation is discrete.

THEOREM 10.3. *If a discrete evaluation satisfies the conditions E 1, E 2, E 3 (i) and E 5, then it satisfies E 3 (ii); that is*

$$\pi[a, b] = [\pi a, \pi b] \quad \text{for any elements } a, b \text{ of } \mathfrak{S}.$$

PROOF. We may assume that $\pi b \geq \pi a \geq 0$, so that we need only prove that $\pi[a, b] = \pi b$ if $\pi a \leq \pi b$.

Since the evaluation is discrete, we may assume that $\pi a = r$, $\pi b = s$ where r and s are positive integers. Furthermore, there exists an element l of \mathfrak{S} such that $\pi l = 1$.

LEMMA 1. $\pi[l^r, l^s] = \pi l^s$.

For since $r \leq s$, $l^r \supseteq l^s$ so that $[l^r, l^s] = l^s$. The result now follows from E 2.

LEMMA 2. If $\pi a = \pi c$ then $\pi[a, b] = \pi[c, b]$.

For $\pi[a, b]:[c, b] = \pi[a:[c, b], b:[c, b]] = \pi a:[c, b]$ by E 2. Since $c \supset [c, b]$, $\pi c \leq \pi[c, b]$. Hence $\pi a \leq \pi[c, b]$, so that $\pi a:[c, b] = 0$ by E 5. Thus $\pi[a, b]:[c, b] = 0$. Hence by E 5, $\pi[a, b] \leq \pi[c, b]$. Similarly, $\pi[c, b] \leq \pi[a, b]$, giving the lemma.

The theorem now follows easily. For since $\pi a = \pi l^r$ and $\pi b = \pi l^s$ by E 4, the lemmas give

$$\pi[a, b] = \pi[l^r, b] = \pi[l^r, l^s] = \pi l^s = \pi b.$$

If the evaluation preserves residuation, the class separation

$$(7.1) \quad \mathfrak{S} = \mathfrak{S}_0 + \mathfrak{S}_1 + \mathfrak{S}_2 + \dots$$

is subject to very stringent conditions; for if $a \in \mathfrak{S}_i$ and $b \in \mathfrak{S}_j$, then we must have $a:b \in \mathfrak{S}_0$ or $a:b \in \mathfrak{S}_{i-j}$ according as $i - j \leq 0$.

The reader can easily show thereby that the structure discussed in section 9 admits of no such residuation. The interesting correspondence we have developed between primes and evaluations is thus destroyed.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA

REFERENCES

A. A. ALBERT

1. *Modern Higher Algebra*, Chicago, 1937.

GARETT BIRKHOFF

1. *Rings of sets*. Duke Math. Jour., vol. 3 (1937), pp. 443-454.

R. DEDEKIND

1. *Gesammelte Werke*, vol. 2, Braunschweig (1931), paper XXI.

R. P. DILWORTH

1. *Abstract residuation over lattices*. Bulletin Am. Math. Soc., vol. 44 (1938) pp. 262-268.

V. GLIVENKO

1. *Géométrie des systèmes de choses normées*. Am. Jour. of Math., vol. 58 (1936), pp. 799-828.

2. *Contribution à l'étude des systèmes de choses normées*. Am. Jour. of Math., vol. 59 (1937), pp. 941-956.

W. KRULL

1. *Axiomatische Begründung der allgemeinen Idealtheorie*. Erlanger Sitzungsberichte, vol. 36 (1924), pp. 47-63.

O. ORE

1. *On the foundations of abstract algebra*. These Annals, vol. 36 (1935), pp. 406-437.

M. H. STONE

1. *The theory of representations of Boolean algebras*. Trans. Am. Math. Soc., vol. 40 (1936), pp. 37-111.

B. L. VAN DER WAERDEN

1. *Moderne Algebra*, vol. 2. Berlin (1931).

H. WALLMAN

1. *Lattices and topological spaces*. These Annals, vol. 39, January 1938, pp. 112-126.

RESIDUATED LATTICES

BY MORGAN WARD AND R. P. DILWORTH

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY

Communicated February 14, 1938

1. *Introduction.*—We summarize here our investigations of a lattice $\Sigma : a, b, \dots, z$ over which a multiplication or a residuation is defined. (Ward 1, Dilworth 1.) We denote division, union and cross-cut by $x \triangleright y$, (x, y) , $[x, y]$. Σ is closed with respect to union (cross-cut) if any set of elements have a union (cross-cut). The unit and null elements i and n are defined by $i \triangleright x$, $x \triangleright n$, every $x \cdot a$ covers b (Birkhoff 1) if $a \triangleright b$, $a \neq b$ and $a \triangleright x \triangleright b$ implies $x = a$ or $x = b$. Elements covered by i are called divisor-free. A sub-lattice Λ is dense over Σ if Λ contains l, m and $l \triangleright x \triangleright m$ imply Λ contains x . An element a is a node if either $x \triangleright a$ or $a \triangleright x$, every x . Any involution of Σ interchanging union and cross-cut is called a negation. An element a is idempotent relative to a binary operation $x \circ y$ if $a \circ a = a$. Two properties P and Q which Σ may possess are completely independent if there exist instances of lattices in which both P and Q hold, neither holds, P holds but not Q , Q holds but not P .

2. *Residuations and Multiplications.*—Assume Σ contains i . A well defined binary operation $x:y$ is called a residuation over Σ provided that

- R 1. $a:b$ lies in Σ whenever a, b lie in Σ .
- R 2. $a:b = i$ if and only if $a \triangleright b$.
- R 3. $a \triangleright b$ implies $a:c \triangleright b:c$ and $c:b \triangleright c:a$.
- R 4. $(a:b):c = (a:c):b$.
- R 5. $[a, b]:c = [a:c, b:c]$ and $c:(a, b) = [c:a, c:b]$.

This residual has the formal properties of the residual in polynomial ideal theory. (Ward 1, Dilworth 1.)

THEOREM. *A residuated lattice closed with respect to cross-cut is also closed with respect to a well-defined multiplication $x \cdot y$ satisfying the following conditions:*

- M 1. $a \cdot b$ lies in Σ whenever a, b lie in Σ .
- M 2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- M 3. $a \cdot b = b \cdot a$.
- M 4. $a \cdot i = a$.
- M 5. $a \cdot (b, c) = (a \cdot b, a \cdot c)$.

If a multiplication over Σ satisfies M 1–M 5 and M 6: *The product of the unions of any two sets of elements of Σ is the union of the products of all pairs of elements of the sets*, then a residuation exists satisfying R 1–R 5. (Ward 1.) The relationship between the two operations is as follows.

$$\begin{aligned} a \triangleright (a:b) \cdot b; & \text{ if } a \triangleright x \cdot b \text{ then } a:b \triangleright x. \\ (a \cdot b):a \triangleright b; & \text{ if } x:a \triangleright b \text{ then } x \triangleright a \cdot b. \end{aligned}$$

Both operations may be dualized.

THEOREM. *The Dedekind modular condition and the existence of a residual are completely independent properties of a lattice. The existence of a residual and the existence of a negation are completely independent.*

3. Conditions for Residuation.

THEOREM. *Every distributive lattice which is closed with respect to union can be residuated in at least one way.* (Ward 2.)

THEOREM. *Every Boolean algebra can be residuated in only one way.*

The residual in this case is $a:b = a \vee b'$. (Dilworth 1.) A lattice is said to be complemented (Birkhoff 2) if it contains i and n and for every element a an element a' such that $(a, a') = i$, $[a, a'] = n$.

THEOREM. *The only complemented lattices which can be residuated are Boolean algebras.*

COROLLARY. *No non-trivial projective geometry (Birkhoff 2) can be residuated.*

THEOREM. *The free modular lattice of order twenty-eight cannot be residuated.*

THEOREM. *Every lattice in which only one divisor free element exists can be residuated in at least one way.*

THEOREM. *A lattice built up out of a set of residuated lattices connected into a chain by nodes can be residuated.*

THEOREM. *A direct product of residuated lattices can be residuated; conversely if a residuated lattice can be expressed as a direct product, each of its factors can be residuated.*

THEOREM. *A necessary condition that a residuated lattice in which an ascending chain condition holds (Ore 1) can be residuated is that every Boolean algebra generated by a finite number of divisor free elements be dense over the lattice.*

4. Noether Lattices.—We propose here the name “Noether lattice” for any residuated modular lattice in which both the (ascending) chain condition holds and

D 1. *For any two elements a, b of Σ , there exist exponents r and s such that $a \cdot b \triangleright [a^r, b^s]$.*

For the ideal theory terminology used here see van der Waerden 1.

THEOREM. *In a Noether lattice, every irreducible is primary. Conversely, if in a residuated modular lattice with chain condition every irreducible is primary, then condition D 1 holds.*

THEOREM. *The three decomposition theorems and the uniqueness theorems of E. Noether for the ideals of a commutative ring in which the chain condition holds are all valid in an abstract Noether lattice.*

THEOREM. Condition D 1 is completely independent both of the modular condition, the distributive condition and the chain condition.

THEOREM. A necessary and sufficient condition that a finite residuated modular lattice be a Noether lattice is that $a \cdot b = [a, b]$ for all idempotent elements a, b of the lattice.

THEOREM. A sufficient condition that a residuated modular lattice in which the ascending chain condition holds be a Noether lattice is

$$M\ 7. \quad a \cdot [b, c] = [a \cdot b, a \cdot c].$$

The resulting lattice need not be distributive.

5. *Distributive Residuated Lattices*.—Consider a lattice in which one or more of the following conditions hold:

- D 2. If $a \supseteq b$, there exists at least one element q such that $a \cdot q = b$.
- R 6. $(a:b, b:a) = i$.
- R 7. $a:[b, c] = (a:b, a:c)$.
- R 8. $(b, c):a = (b:a, c:a)$.

THEOREM. Every lattice closed with respect to union in which D 2 holds can be residuated, and is distributive.

THEOREM. If Σ is a residuated lattice, any one of R 6, R 7, R 8 implies Σ is distributive. R 6 and D 2 implies R 7 and R 8. R 8 implies R 7.

We call a residuated lattice satisfying D 2 and R 6 semi-arithmetical. The properties of such lattices are similar to the instance in Ward 2 where multiplication is cross-cut.

6. *Residuated Group Lattices—Dual Operations*.—On assuming Σ is a semi-group and D_2 , we may pass to the group Γ of quotients a/b . We have made Γ into a residuated lattice having properties R 1–R 8. However the lattice has no unit element.

The existence of a dual residuation and multiplication is completely independent of the existence of the initial residuation and multiplication. An interesting case arises in a residuated lattice containing n if the correspondence $a \rightarrow n:a$ is a negation. The lattice is then distributive, and multiplication and its dual are also distributive with respect to one another.

Proofs of these results will be published elsewhere.

G. Birkhoff: 1. *Proc. Cambridge Phil. Soc.*, 29, 441–464 (1933).
2. *Ann. Math.* (2), 36, 743–748 (1935).

R. P. Dilworth: 1. *Bull. Am. Math. Soc.*, 44, April (1938).

O. Ore: 1. *Ann. Math.*, (2), 36, 406–437 (1935).

B. L. van der Waerden: 1. *Moderne Algebra*, 2, Berlin (1931).

Morgan Ward: 1. *Duke Jour.*, 3, 627–636 December (1937).

2. "Structure Residuation." Submitted to the *Ann. Math.*

RING HOMOMORPHISMS WHICH ARE ALSO LATTICE HOMOMORPHISMS.*

By MORGAN WARD.

1. Given two homomorphic rings \mathfrak{Q} and \mathfrak{Q}' : what lattice properties of the rings are preserved under the homomorphism; more specifically, if \mathfrak{Q} is a lattice, will \mathfrak{Q}' be a homomorphic lattice?¹ It is easily seen that if \mathfrak{S} and \mathfrak{S}' are the lattices of ideals of \mathfrak{Q} and \mathfrak{Q}' , any ring homomorphism of \mathfrak{Q} to \mathfrak{Q}' induces a lattice homomorphism of \mathfrak{S} to \mathfrak{S}' . Unfortunately, when \mathfrak{Q} is a lattice with respect to the usual division relation, it need not be a sublattice of \mathfrak{S} . The homomorphism \mathfrak{S} to \mathfrak{S}' consequently gives little information about the lattice properties of \mathfrak{Q}' .

If we assume however that the ascending chain condition holds in the lattice \mathfrak{Q} , it is not difficult to show that \mathfrak{Q} is a sublattice of \mathfrak{S} if and only if every ideal of \mathfrak{Q} is principal and \mathfrak{Q} and \mathfrak{S} are lattice isomorphic. The object of this paper is to show in this case that all homomorphic rings \mathfrak{Q}' are also lattices of a very simple structure.

For the case when \mathfrak{Q} is a domain of integrity, my results may be more easily obtained from the fact that the fundamental theorem of arithmetic holds in every "principal ideal ring." (van der Waerden 1). The interest of the present investigation is that \mathfrak{Q} is merely required to be a commutative ring with a unit element. The methods used are based upon a theory of residuated lattices which have been developed by Mr. R. P. Dilworth and myself in a series of recent papers.²

2. Let \mathfrak{Q} be a commutative ring with a unit element, all of whose ideals are principal.

DEFINITION 2.1. DIVISION IN \mathfrak{Q} . *If a and b are any two elements of \mathfrak{Q} , a is said to divide b if and only if the principal ideal (a) contains the principal ideal (b) . If (a) equals (b) , a and b are said to be equivalent.*

We write $a \supset b$, $a \sim b$. \mathfrak{Q} evidently forms a semi-ordered set with respect

* Received December 16, 1938.

¹ This problem was propounded to me by Professor E. T. Bell for the special case when \mathfrak{Q} is the ring of rational integers.

² Ward, 1, 2; Ward-Dilworth, 1, 2.

to the relation $x \supseteq y$, and $x \sim y$ is an equivalence relation. Furthermore $a \supset b$ if and only if there exists an element c such that $ac = b$.

THEOREM 2.1. *The ascending chain condition holds for the elements of \mathfrak{D} .*

That is, if we have a chain of elements a_1, a_2, a_3, \dots such that $a_1 \subset a_2 \subset a_3 \subset \dots$, then from a certain point on, all elements are equivalent to one another. It obviously suffices to show that in the ascending chain of ideals $(a_1) \subset (a_2) \subset (a_3) \subset \dots$ all ideals are equal from a certain point on. The proof may be carried out exactly as in van der Waerden 1, § 17.

THEOREM 2.2. *The ideals of \mathfrak{D} form a distributive residuated lattice.*

Proof. The ideals of any ring form a modular lattice \mathfrak{S} over which a multiplication may be defined with the properties given in Ward 1. Since the ascending chain condition holds for ideals by the previous theorem, a residual may also be introduced, so that the lattice is residuated by definition. (Ward-Dilworth 1.) Since all ideals a, b of \mathfrak{D} are principal, a contains b if and only if there exists an ideal i such that $ai = b$. Hence the lattice is distributive. (Ward-Dilworth 2, theorem 16.2).

3. We next consider the lattice formed by the elements of \mathfrak{D} .

THEOREM 3.1. *If a and b are any two elements of \mathfrak{D} , there exists an element d with the properties*

- (i) $d \supset a, d \supset b$.
- (ii) $x \supset a, x \supset b$ imply $x \supset d$.
- (iii) $d = ua + vb$ for some u, v of \mathfrak{D} ,
- (iv) d is determined up to equivalence.

Proof. Consider the ideal $((a), (b)) = (a, b)$. Since all ideals are principal, $(a, b) = (d)$. Hence (i) follows and (iii) follows. Then (ii) follows from (iii), and (iv) from (ii).

We write $a \sim (a, b)$, and call d a union of a and b .

THEOREM 3.2. *If a and b are any two elements of \mathfrak{D} , there exists an element m such that*

- (i) $a \supset m, b \supset m$.
- (ii) $a \supset y, b \supset y$ imply $m \supset y$.
- (iii) m is determined up to equivalence.

Proof. Consider the ideal $[(a), (b)]$. Since it is principal, $[(a), (b)] =$

(m). The element m is easily seen to have the required properties. We write $m \sim [a, b]$, and call m a cross-cut of a and b .

It follows from theorem 3.1 and 3.2 that \mathfrak{D} forms a lattice with respect to the division relation $x \supset y$.

THEOREM 3.3. \mathfrak{D} forms a residuated lattice with respect to division relation $x \supset y$ and the multiplication operation xy of \mathfrak{D} .

Proof. We need only show that the multiplication has the properties given in Ward 1, p. 629, for then by theorem 3.2, a residual may be introduced (Ward 1) so that \mathfrak{D} will be residuated by definition. All of these properties are evident save the rule $a(b, c) \sim (ab, ac)$. Now $(b, c) = bu + cw$ by theorem 3.1 (iii) for some u, w of \mathfrak{D} . Hence $a(b, c) = abu + acw$. Therefore $(ab, ac) \supset a(b, c)$. But since $(b, c) \supset b$ and c , $a(b, c) \supset ab, ac$. Hence by theorem 3.1 (ii), $a(b, c) \supset (ab, ac)$. Therefore $(ab, ac) \sim a(b, c)$.

THEOREM 3.4. \mathfrak{D} is a distributive lattice.

Proof. The correspondence $a \rightarrow (a)$ is a lattice isomorphism, since "equal elements" (that is equivalent elements in \mathfrak{D}) correspond to equal elements in \mathfrak{S} and vice versa. Since \mathfrak{S} is distributive by theorem 2.3, \mathfrak{D} is distributive.

THEOREM 3.5. Every element of \mathfrak{D} may be uniquely represented up to equivalence as a cross-cut of primary elements none of which divides any other.

Proof. With the terminology of Ward-Dilworth 2, \mathfrak{D} is a distributive residuated lattice in which every element is principal. The result thus follows from theorem 14.2 of Ward-Dilworth 2, theorem 8.4 of Ward 2 and the remarks in section 12 of Ward-Dilworth 2.

4. Consider any homomorphism of the ring \mathfrak{D} . The homomorphism is completely specified by an ideal \mathfrak{m} , and its residue classes. Since \mathfrak{m} is a principal ideal (m) , $a \equiv b \pmod{\mathfrak{m}}$ if and only if $a = b + qm$ for some element q of \mathfrak{D} . Denote the residue classes of congruent elements modulo \mathfrak{m} by A, B, \dots . We wish to make these classes into a lattice. We begin by extending definition 2.1.

DEFINITION 4.1. DIVISION MODULO \mathfrak{m} . An element a of \mathfrak{D} is said to divide another element b of \mathfrak{D} modulo \mathfrak{m} if and only if there exists an element c such that $ac \equiv b \pmod{\mathfrak{m}}$.

We write $a \supset b \pmod{\mathfrak{m}}$.

DEFINITION 4.2. EQUIVALENCE MODULO m . Two elements a and b of \mathfrak{Q} are said to be equivalent modulo m if and only if each divides the other modulo m .

We write $a \sim b \pmod{m}$.

\mathfrak{Q} forms a semi-ordered set with respect to the relation of division modulo m , and equivalence modulo m is an equivalence relation in the technical sense. It is evident furthermore that we have

THEOREM 4.1. $a \supseteq b$ modulo m if and only if there exist elements r and s such that $b = ar + ms$.

We may note also that $a \sim b$ or $a \equiv b \pmod{m}$ imply $a \sim b \pmod{m}$, and $a \supseteq b$ implies $a \supseteq b \pmod{m}$. Hence the relations of division and equivalence modulo m may be immediately extended to the residue classes A, B, \dots of \mathfrak{Q} modulo m .

THEOREM 4.2. If $m = (m)$, then (i) $a \supseteq b \pmod{m}$ if and only if $(a, m) \supseteq b$ in \mathfrak{Q} , and (ii) $a \sim b \pmod{m}$ if and only if $(a, m) \sim (b, m)$.

Proof. (i) By theorem 3.1 (iii), $(a, m) \sim al + km$, l, m elements of \mathfrak{Q} . Hence $(a, m) \supseteq b$ implies that $b = (al + km)q = aql + mqk$. Therefore by theorem 4.1, $(a, m) \supseteq b$ implies that $a \supseteq b \pmod{m}$. Next, if $a \supseteq b \pmod{m}$, then by theorem 4.1, $b = ar + ms$. Hence by theorem 3.1 (i), $(a, m) \supseteq b$.

(ii) If both $a \supseteq b \pmod{m}$ and $b \supseteq a \pmod{m}$, then $(a, m) \supseteq b$ and $(b, m) \supseteq a$. Hence $(a, m) \supseteq (b, m)$ and $(b, m) \supseteq (a, m)$ or $(a, m) \sim (b, m)$. The converse is evident.

THEOREM 4.3. $a \sim (a, m) \pmod{m}$.

Proof. $(a, m) \sim ((a, m), m)$.

THEOREM 4.4. The correspondence $x \rightarrow x^* \sim (x, m)$ is a lattice homomorphism of \mathfrak{Q} .

Proof. Assume that $a \rightarrow a^*$ and $b \rightarrow b^*$. Then

$$(a, b)^* \sim (a, b), m \sim ((a, m), (b, m)) \sim (a^*, b^*).$$

Since \mathfrak{Q} is a distributive lattice we also have

$$[a, b]^* \sim ([a, b], m) \sim [(a, m), (b, m)] \sim [a^*, b^*],$$

We observe that the correspondence of theorem 4.4 maps the lattice \mathfrak{Q} onto the sublattice of divisors of m in \mathfrak{Q} .

THEOREM 4.5. *If $a \rightarrow a^*$ and $b \sim a \pmod{m}$, then $b^* \sim a^*$, and conversely.*

Proof. $a \rightarrow a^*$ if and only if $a^* \sim (a, m)$ and $a \sim b \pmod{m}$ if and only if $(a, m) \sim (b, m)$.

THEOREM 4.6. *The residue classes A, B, \dots of \mathfrak{D} modulo m form a lattice with respect to the relation of division modulo m which is isomorphic with the lattice of the divisors of m in \mathfrak{D} if equivalent classes modulo m and equivalent divisors are not regarded as distinct.*

Proof. We assign to A the element $a^* \sim (a, m)$, a any element of A . (We may if we please make the correspondence entirely definite by replacing a^* by the ideal $a = ((a), (m)) = (a^*)$). Then since $a \equiv b \pmod{m}$ implies $a \sim b \pmod{m}$, a^* is, up to equivalence, independent of the particular element of A used in defining it. By theorem 4.5, $A \sim B \pmod{m}$ if and only if $a^* \sim b^*$ and by theorem 4.2, $A \supset B \pmod{m}$ if and only if $a^* \supset b^*$. The result then follows from theorem 4.4.

PASADENA, CALIFORNIA.

REFERENCES

- Morgan Ward, 1. *Duke Mathematical Journal*, vol. 3 (1937), pp. 627-636; 2. *Annals of Mathematics*, vol. 39 (1938), pp. 558-568.
 Morgan Ward-R. P. Dilworth, 1. *Proceedings of the National Academy of Sciences*, vol. 24 (1938), pp. 162-164; 2. *Transactions of the American Mathematical Society*.
 van der Waerden, 1. *Moderne Algebra*, vol. 1 (Berlin, 1930).

A CHARACTERIZATION OF DEDEKIND STRUCTURES*

MORGAN WARD

If Σ is a Dedekind structure,[†] then for any two elements A and B of Σ , the quotient structures $[A, B]/A$ and $B/(A, B)$ are isomorphic. (Dedekind [2], Ore [3].) I prove here a converse result.

THEOREM. *Let Σ be a structure in which for every pair of elements A and B , the quotient structures $[A, B]/A$ and $B/(A, B)$ are isomorphic. Then if either the ascending or descending chain condition holds in Σ , the structure is Dedekindian.*

This result is comparatively trivial if *both* the ascending and descending chain conditions hold. That some sort of chain condition is necessary may be seen by a simple example. Consider a structure Σ with an all element O_0 and a unit element E_0 built up out of three ordered structures Σ_1 , Σ_2 , Σ_3 meeting only at O_0 and E_0 , so that if $S_u \in \Sigma_u$, then

$$(S_u, S_v) = E_0, \quad [S_u, S_v] = O_0$$

for $u, v = 1, 2, 3, u \neq v$. Then if each Σ_i is a series of the type of the real numbers in the closed interval 0, 1, the quotient structures of any pair $[S_u, S_v]/S_u$, $S_v/(S_u, S_v)$ are obviously isomorphic. But Σ is clearly non-Dedekindian.

The theorem is of some interest in view of the generalizations Ore has given of his decomposition theorems in Ore [4].

It suffices to prove the result under the hypothesis that the descending chain axiom holds in Σ (Ore [3, p. 410]). We formulate this axiom as follows:

(β) *If for any two elements A and B of Σ ,*

$$A \triangleright X_1 \triangleright X_2 \triangleright X_3 \triangleright \dots \triangleright B$$

for an infinity of X_i in Σ , all the X_i are equal from a certain point on.

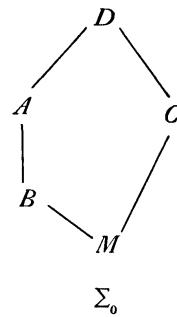
Our proof rests upon several lemmas which we collect here.

LEMMA 1. (Dedekind [2].) *Σ is a Dedekind structure if and only if Σ contains no substructure Σ_0 of order five which is non-Dedekindian.*

* Presented to the Society, April 15, 1939.

† We use the notation and terminology of Ore's fundamental paper, Ore [3], with the following two exceptions. (i) We write $A \triangleright B$, $B \subset A$ for Ore's $A \geqq B$, $B \leqq A$. (ii) If A is prime over B (Ore [3, p. 411]), we shall say " A covers B " or " B is covered by A " (Birkhoff [1]) and write $A > B$ or $B < A$.

The type of substructure in question is well known; its diagram is given in the figure. Since we utilize such substructures frequently in our proof, we shall introduce the notation $\{D, A, B, C, M\}$ for Σ_0 , writing the all element D and unit element M in the first and last



places in the symbol while the elements A and B where $A \triangleright B$ occupy the second and third places.

LEMMA 2. (Ore [3].) *If (β) holds in the structure Σ , then every set of elements of Σ which divide a fixed element A contains at least one minimal element dividing no other element of the set.*

LEMMA 3. *If (β) holds in the structure Σ , then for any two distinct elements A and C of Σ such that C divides A , there exists an element B such that C divides B and B covers A .*

For we need only pick a minimal element in the subset of all elements X such that $C \triangleright X \triangleright A$, $X \neq A$.

The following lemma is obvious:

LEMMA 4. *Let Σ be a structure in which*

$$(\epsilon) \quad [A, B]/A \cong B/(A, B)$$

for every A, B of Σ . Then $[A, B]$ covers A if and only if B covers (A, B) .

LEMMA 5. *Let Σ be a structure in which (ϵ) holds. Then if A covers B and M is any other element of Σ , either $[M, A] = [M, B]$ or $[M, A]$ covers $[M, B]$.*

For clearly $[M, A] \triangleright [M, B]$. Since $A \triangleright (A, [M, B]) \triangleright B$ and $A > B$, either $(A, [M, B]) = A$ or $(A, [M, B]) = B$. If $(A, [M, B]) = A$, then $[M, B] \triangleright A \triangleright [M, A]$, so that $[M, B] = [M, A]$. If $(A, [M, B]) = B$, then $A > (A, [M, B])$. Hence by Lemma 4, $[A, [M, B]] > [M, B]$. But since $A \triangleright B$,

$$[A, [M, B]] = [M, A].$$

Our final lemma is the dual of Lemma 5.

LEMMA 6. *Let Σ be a structure in which (ϵ) holds. Then if A covers B and M is any other element of Σ , either (M, A) equals (M, B) or (M, A) covers (M, B) .*

We shall prove our theorem indirectly. Assume that conditions (β) and (ϵ) hold in the structure Σ , but that Σ is non-Dedekindian. Then by Lemma 1, Σ contains a non-Dedekindian substructure

$$\Sigma_0 = \{D, A, B, C, M\}$$

of order five.*

We may assume that A covers B . For by Lemma 3, there exists an element N of Σ such that $A \triangleright N$, $N > B$. Thus

$$[A, C] \triangleright [N, C] \triangleright [B, C], \quad (A, C) \triangleright (N, C) \triangleright (B, C);$$

that is, $[N, C] = D$, $(N, C) = M$. Hence $\{D, N, B, C, M\}$ is a non-Dedekindian substructure where $N > B$.

We assume henceforth that A covers B . Since $[A, C] = D$, $(A, C) = M$, and $[B, C] = D$, $(B, C) = M$, $D/C \cong A/M$, and $D/C \cong B/M$ by (ϵ) . Hence $A/M \cong B/M$. But B lies in A/M and $A > B$. Since A corresponds to B under the isomorphism, *there exists an element in B/M covered by B .* Denote it by B_1 . Then

$$(1) \quad B > B_1 \triangleright M.$$

Since $B \triangleright B_1 \triangleright M$, $(B, C) \triangleright (B_1, C) \triangleright (M, C)$ or $(B_1, C) = M$. Consider next the union $D_1 = [B_1, C]$. Since $B > B_1$, by Lemma 5 either $[B, C] = [B_1, C]$ or $[B, C] > [B_1, C]$; that is, either $D = D_1$ or $D > D_1$.

If $D = D_1$, then on writing A_1 for B , we obtain a non-Dedekindian substructure $\{D_1, A_1, B_1, C, M\}$ in which $A_1 > B_1$.

Now assume that $D > D_1$. Clearly $[A, D_1] = [B, D_1] = D$. Consider the crosscut (B, D_1) . Since $B > B_1$, by Lemma 6, either $(B, D_1) = (B_1, D_1)$ or $(B, D_1) > (B_1, D_1)$. That is, since $B \triangleright (B, D_1)$ and $D_1 \triangleright B_1$, either $(B, D_1) = B_1$ or $(B, D_1) = B$. We must have $(B, D_1) = B_1$. For if $(B, D_1) = B$, then $D_1 \triangleright B$. Since $D_1 \triangleright C$, we would have $D_1 \triangleright [B, C]$, $D_1 = D$, contrary to the assumption $D > D_1$.

Consider next the crosscut $A_1 = (A, D_1)$. Since $A > B$, by Lemma 5 either $(A, D_1) = (B, D_1)$ or $(A, D_1) > (B, D_1)$; that is, either $A_1 = B_1$ or $A_1 > B_1$. We must have $A_1 > B_1$. For if $A_1 = B_1$, then $\{D, A, B, D_1, B_1\}$ is a non-Dedekindian substructure. But since $[A, D_1] = D$ and $(A, D_1) = B_1$, by (ϵ) $A/B_1 \cong D/D_1$. This isomorphism is impossible, for $A \triangleright B > B_1$ while $D > D_1$.

Finally, since $A \triangleright A_1 \triangleright C$ and $B \triangleright B_1 \triangleright C$, $(A_1, C) = (B_1, C) = M$

* The reader will find a structure diagram helpful in following the argument.

while $[A_1, C] = [B_1, C] = D_1$. Thus $\{D_1, A_1, B_1, C, M\}$ is a non-Dedekindian substructure of Σ in which $A_1 > B_1$.

We now replace Σ_0 in either case by $\Sigma_1 = \{D_1, A_1, B_1, C, M\}$ and obtain a non-Dedekindian substructure $\Sigma_2 = \{D_2, A_2, B_2, C, M\}$ where $A_2 > B_2$ and

$$(2) \quad B_1 > B_2 \supset M.$$

On repeating this reasoning, and combining (1), (2), . . . we obtain a chain

$$B > B_1 > B_2 > B_3 > \dots \supset M$$

of indefinite length in which all B_i are distinct, contradicting (β).

REFERENCES

1. G. Birkhoff, *On the combination of sub-algebras*, Proceedings of the Cambridge Philosophical Society, vol. 29 (1933), pp. 441–464.
2. R. Dedekind, *Über die von drei Moduln erzeugte Dualgruppe*, *Werke*, vol. 2, pp. 371–403.
3. O. Ore, *On the foundation of abstract algebra*, I, Annals of Mathematics, (2), vol. 36 (1935), pp. 406–437.
4. ———, *On the theorem of Jordon-Hölder*, Transactions of this Society, vol. 41 (1937), pp. 266–273.

CALIFORNIA INSTITUTE OF TECHNOLOGY

**NOTE ON THE GENERAL RATIONAL SOLUTION OF THE
EQUATION $ax^2 - by^2 = z^3$.***

By MORGAN WARD.

1. In a recent paper in this journal, E. Fogels (Fogels 1) has utilized the elements of algebraic number theory to determine all rational solutions of the diophantine equation

$$(1) \quad ax^2 - by^2 = z^3, \quad a, b \text{ rational, } \neq 0.$$

I show here that the underlying reason for the success of Fogel's method is an arithmetical relationship between the degrees of the left and right sides of (1). For consider the more general equation

$$(2) \quad a_0x^m + a_1x^{m-1}y + \cdots + a_my^m = z^n$$

where m, n are positive integers and a_0, \dots, a_m rational. The general rational solution of (2) may be immediately written down provided that we impose the following condition: *The degrees m and n are co-prime.*

In this case we may reduce (2) to the simple equation

$$(3) \quad Y^m = Z^n.$$

2. There are four types of rational solutions of (2) to consider; namely, (i) solutions with $z = 0$, (ii) solutions with $x = 0$, (iii) solutions with $y = 0$ and (iv) solutions with none of x, y, z zero.

The first three types are readily treated.

(i) If $z = 0$, the solution of (2) may be expressed in the form $x = tx'$, $y = ty'$. Here t is an arbitrary rational and x', y are either both zero or co-prime integers satisfying $a_0x'^m + \cdots + a_my'^m = 0$. Thus only a finite number of choices for x' and y' are possible.

(ii) If $x = 0$ and $a_m = 0$, then y is arbitrary, z is zero. If $a_m \neq 0$, then

* Received August 31, 1938.

(2) reduces to $a_m y^m = z^n$. Since m and n are co-prime, we may determine integers k and l such that

$$(4) \quad 1 + km = ln.$$

On letting $y = a^k m Y$, $z = a^l m Z$ (2) is reduced to (3).

(iii) If $y = 0$, (2) is either trivial or similarly reducible to (3).

(iv) Let x, y, z be a rational solution of (2) with $xyz \neq 0$. Then if we let $x = uy$, u is rational and not zero, and (2) becomes

$$y^m w = z^n, \quad w = a_0 u^m + a_1 u^{m-1} + \dots + a_m \neq 0.$$

As in type (ii), we let $y = w^k Y$, $z = w^l Z$. Then Y, Z are rational and non-zero and

$$(3) \quad Y^m = Z^n.$$

3. Equation (3) is a very special case of a type of diophantine system which I have already discussed in this journal. (Ward [1]). To solve (3), we let

$$Y = \prod p^\alpha, \quad Z = \prod p^\beta$$

where the products extends over all primes, and the α and β are integers having only a finite number of non-zero values. Then (3) yields the condition $m\alpha = n\beta$. Hence $\alpha = (n:m)y$, $\beta = (m:n)y$ where y is an integer, and $m:n$ denotes the residual $m/(m, n)$ of n with respect to m . (Ward [2]). Since m and n are co-prime, $n:m = n$, $m:n = m$. Thus

$$Y = v^n, \quad Z = v^m$$

where v is a rational number. On combining these results, we find that if x, y, z is any rational solution of (2) with $xyz \neq 0$, then there exist rationals u and v such that

$$(5) \quad \begin{aligned} x &= u(a_0 u^m + a_1 u^{m-1} + \dots + a_m)^k v^n, \\ y &= (a_0 u^m + a_1 u^{m-1} + \dots + a_m)^k v^n, \\ z &= (a_0 u^m + a_1 u^{m-1} + \dots + a_m)^l v^m. \end{aligned}$$

Here k and l are integers satisfying

$$(4) \quad 1 + km = ln.$$

Conversely, if u and v are rational and $a_0u^m + \dots + a_m \neq 0$, $uv \neq 0$, then (5) always gives a rational solution of (2) with $xyz \neq 0$.

4. In particular, let $m = 2$, $n = 3$, $a_0 = a$, $a_1 = 0$, $a_2 = -b$. (2) then reduces to (1), and we may take $k = l = 1$ in (3). The formulas (5) become

$$\begin{aligned}x &= u(au^2 - b)v^3 \\y &= (au^2 - b)v^3 \\z &= (au^2 - b)v^2\end{aligned}$$

If $a \neq 0$, we can make the reversible rational substitution $u = s/a$, $v = at$. We thus obtain

$$\begin{aligned}x &= as(s^2 - ab)t^3 \\y &= a^2(s^2 - ab)t^3 \\z &= a(s - ab)t^2.\end{aligned}$$

These are the formulas for the solution of (1) obtained by Fogels.

PASADENA, CALIFORNIA.

REFERENCES

- E. Fogels, 1. *American Journal of Mathematics*, vol. 60 (July, 1938), pp. 734-736.
M. Ward, 1. *American Journal of Mathematics*, vol. 55 (1933), pp. 67-76; 2. *American Journal of Mathematics*, vol. 59 (1937), pp. 921-926.

THE LATTICE THEORY OF OVA

BY MORGAN WARD AND R. P. DILWORTH¹

(Received December 21, 1938; revised March 24, 1939)

I. INTRODUCTION

1. In a series of previous papers,² we have developed the theory of residuated lattices; that is, lattices over which a multiplication and associated residuation may be defined with the same properties as in polynomial ideal theory. Here we reverse our procedure and start with a system closed under a single suitably restricted operation of multiplication (see section 3). Following E. T. Bell, (Bell 1), we call such a system an "ovum."³ By the adjunction of properly defined ideals of various kinds (distinguished sub-sets of the ovum), we imbed the ovum in a residuated lattice, incidentally generalizing many of the imbedding theorems of MacNeille 1. The Noether lattices introduced in W-D enables us to describe concisely the arithmetical behavior of ova. In particular, the recent results of A. H. Clifford in these Annals (Clifford 1) come under our general theory. An interesting new result is the following "fundamental theorem of the arithmetic of finite ova." *By the adjunction of a finite number of ideals, every finite ovum may be imbedded in a residuated lattice in which every element, and in particular the elements of the ovum, may be uniquely represented as a cross-cut of primary elements.*

2. The plan of this paper is as follows. After some set-theoretic preliminaries, we define and discuss in the third and fourth divisions of the paper two types of distinguished subsets of an ovum, its product ideals and ovoid ideals. (The reader is referred to the paper Clifford 2 in these Annals for the literature and history of ovoid ideals.) In the concluding division of the paper, we give the arithmetical theory of ovoid ideals, obtaining the following general result: *If the lattice of ovoid ideals is modular and if the ascending chain axiom holds, then all of the decomposition theorems of Emmy Noether for the ideals of commutative rings hold.*

3. We shall use the lattice terminology of our previous papers. If \mathfrak{S} is a lattice of elements A, B, \dots and unit element E over which a multiplication is

¹ Portions of this paper have been revised in accordance with suggestions of Dr. A. H. Clifford, who kindly read it in manuscript.

² The papers relevant to the present investigation are Ward 1, 2 and the joint paper Ward-Dilworth 1, which we cite here as W-D.

³ Bell does not postulate the existence of a unit in his general definition.

Other terms are "commutative groupoid" (G. Birkhoff 2), "semi-group" A. H. Clifford 2. For a recent discussion of finite ova, see Poole 1.

defined (Ward 1), we write $X \supset Y$, $Y \subset X$ for X contains Y and (X, Y) , $[X, Y]$, XY or $X \cdot Y$ for the union, cross-cut and product respectively of the elements X and Y .

Assume that \mathfrak{S} is completely closed relative to union; that is, every subset of elements of \mathfrak{S} has a union. Then if for every subset Ω of elements A of \mathfrak{S} and any fixed element B , the union of the set of elements BA is the product of B and the union of the A , we say that multiplication is "completely distributive" relative to union. It is easily shown that multiplication is completely distributive relative to union if and only if the union of the products of all pairs of elements of any two sets of \mathfrak{S} is the product of the unions of the sets.⁴ Complete distributivity is of importance because of the following theorem.

THEOREM 3.1. *Let \mathfrak{S} be a lattice which is completely closed relative to union over which a commutative and associative multiplication may be defined distributive with respect to union, and let the unit element of the lattice also be the unit with respect to multiplication. Then a necessary and sufficient condition that any two elements of \mathfrak{S} may have a residual is that multiplication be completely distributive relative to union.*

PROOF. The sufficiency of the condition is established in Ward 1. To prove the necessity, assume that every two elements of \mathfrak{S} have a residual: specifically, given A and B , there exists an element $R = A:B$ such that $A \supset RB$; $A \supset XB$ implies $R \supset X$. It is shown in Ward 1 how the ordinary properties of the residual then follow and in particular,

$$(i) \quad A:BC = (A:B):C \quad (ii) \quad A \supset B \text{ if and only if } A:B = E.$$

Now let Ω be any set of elements A of \mathfrak{S} , and B , a fixed element of \mathfrak{S} . Let U and V denote respectively the union of all A and of all BA . It suffices to show that $V = BU$. Since $U \supset A$, $BU \supset BA$ for $A \in \Omega$ (Ward 1). Hence $BU \supset V$. But $V \supset BA$, $A \in \Omega$. Hence by (ii) and (i), $E = V:BA = (V:B):A$ or $V:B \supset A$. Hence $V:B \supset U$ or $V \supset BU$, $V = BU$.

4. We understand by an "ovum" a set O of elements a, b, c, \dots over which a binary relation $x = y$ called "equality" and a binary operation xy called multiplication are well-defined subject to the following conditions: (i) Equality is an equivalence relation; (ii) O is closed under multiplication and multiplication is associative and commutative; (iii) O contains a unit e such that $ae = ea = a$, any a in O ; (iv) If $a = b$, then $ac = bc$, $ca = cb$ any c in O . In short, an ovum is a system satisfying all the usual postulates for an Abelian group save the existence of inverses.⁵

⁴ MacNeille 1 has an example showing that complete closure relative to union and distributivity of multiplication relative to union for finite sets does not imply complete distributivity.

⁵ The unit e may be dispensed with by strengthening slightly the conditions on the residual introduced later. The non-commutative case will be treated by R. P. Dilworth elsewhere.

For example, any lattice over which a multiplication is defined with the properties in Ward 1 is an ovum with respect to the multiplication whose unit element is the unit of the lattice.

If U and V are subsets of O , we denote by $U + V$ and $U \cap V$ their set-theoretic union and cross-cut. Here as usual if U and V have no elements in common, $U \cap V$ is the set-theoretic null class Z containing no elements of O but contained in every other subset.

If u lies in U , we write $u \in U$. If Ω is any class of subsets A of O , we write $\sum A$ for the set-theoretic union of the A in Ω . $U \supseteq V$, $V \subset U$ and $U = V$ denote set-theoretic inclusion and equality.

If U and V are any two subsets, their *set product* UV is by definition the set of all products uv , $u \in U$ and $v \in V$. If U consists of a single element u , we write uV for UV . It is clear that the subsets of O form an ovum with respect to the operation of multiplication so defined, and if $A \supseteq B$, then $AC \supseteq BC$ for any C . The following theorem is a direct consequence.

THEOREM 4.1. *The operation of multiplication of subsets is completely distributive with respect to set theoretic union.*

In particular $C(A + B) = CA + CB$ for any three sets A , B and C . On the other hand, $C(A \cap B) \neq CA \cap CB$ in general.

A set H is called a sub-ovum of O if $H^2 \subset H$. A sub-ovum is called "proper" if it contains the unit element e of O and the zero element z whenever the latter exists. Here z is defined by the property $az = z$ for every a of O .

Let \bar{O} be a proper sub-ovum of O , fixed throughout all that follows. An element a of O is said to "divide" an element b of O (relative to \bar{O}) if there exists an element c of \bar{O} such that $ac = b$. We write $a | b$. If $a | b$ and $b | a$, a and b are said to be equivalent (relative to \bar{O}); we write then $a \sim b$. The division relation $|$ partially orders O , and \sim is an equivalence relation. Moreover $e | a$ for every element a of \bar{O} , and if z exists, $a | z$ for every a of O .

II. THE PRODUCT IDEALS OF AN OVUM

5. The first type of distinguished subset of O which we shall consider is the product ideal.

DEFINITION 5.1. *A subset S' is called a product ideal (relative to \bar{O}) if $\bar{O}S' = S'$.*

If in addition $\bar{O} \supset S'$, S' is said to be integral. Clearly O itself is a product ideal. Hence given any subset A of O , there is a least product ideal A' containing it. We call A' the ideal generated by A . If A consists of a single element a , we write $A' = (a)$.

If the ovum contains a zero element z , then $z \in S'$ every S' and the ideal (z) is the set Z consisting of z alone. Hence $S' \supset Z$ for every product ideal S' . If O contains no zero element, we count the null set Z as a product ideal. It is easily seen that the product ideals of $O(\bar{O})$ are closed under the operations of set-theoretic cross-cut and union.

We denote the union and cross-cut of a set Ω by $\mu\Omega$ and $\kappa\Omega$ respectively. The following theorem is now evident:

THEOREM 5.1. *The set of all product ideals and the set of all integral product ideals of any ovum both form distributive lattices which are completely closed with respect to union and cross-cut.*

THEOREM 5.2. *The set of all integral product ideals of an ovum form a residuated lattice completely closed relative to union and cross-cut.*

PROOF. Since the union and cross-cut operations on ideals in \bar{O} are the set-theoretic operations on the ideals qua classes of elements, it is evident that the ideals form a completely closed distributive lattice. The postulates for a multiplication in a lattice are

M 1 *If \bar{O} contains A' , B' , then \bar{O} contains $A'B'$.*

M 2 *If $A' = B'$, then $A'C' = B'C'$.*

M 3 *$A'B' = B'A'$.*

M 4 *$(A'B')C' = A'(B'C')$.*

M 5 *$A'O' = A'$ any A' . (Here $O' = \bar{O}$).*

M 6 *$A'(B', C') = (A'B', A'C')$.*

These postulates are clearly all satisfied. We shall denote this lattice by \mathfrak{R} . We also have from theorems 3.1 and 4.1

M7 *\mathfrak{R} is completely closed with respect to union, and the product of the unions of any two classes of ideals of \mathfrak{R} is the union of the set-products of all pairs of elements in the classes.*

Hence (Ward 1) a residuation $X':Y'$ may be defined over \mathfrak{R} with the properties R 1-R 6 given in W-D, §4, so that the ideals of \bar{O} form a residuated lattice by definition.

It is impossible to prove that the lattice of *all* product ideals of O may be residuated, for the unit element O of the lattice is not the unit with respect to multiplication, so that M 5 is not satisfied. All the remaining postulates are satisfied. A similar situation occurs in defining the product of two modules of a ring of algebraic integers (Dedekind 1). M 5 is arithmetically important, as it assures that $A' \supseteq A'B'$.

If a is any element of \bar{O} , the product ideal (a) is clearly the set $a\bar{O}$ of all multiples of a in \bar{O} . We call (a) an (integral) principal ideal.

THEOREM 5.3. *If A' is an integral principal ideal and $A' \supseteq B'$, then there exists an integral ideal C' such that $A'C' = B'$.*

PROOF. By hypothesis, $A' = a\bar{O}$. Since $A' \supseteq B'$, every element of B' is of the form aq , where q lies in a certain fixed class Q of \bar{O} . Then

$$B' = \sum_q aq\bar{O} = \sum a\bar{O}q\bar{O} = a\bar{O} \sum q\bar{O} = A'C'$$

where C' is the ideal $\sum q\bar{O}$.

It follows from M 7 in the proof of theorem 5.5, and W-D, lemma 13.1, that we may take $C' = B':A'$.⁶

* There may be several ideals C' such that $A'C' = B'$.

6. It may be shown by simple examples that if the ovum \bar{O} contains an infinite number of non-equivalent elements, no chain conditions need be satisfied in \mathfrak{R} , or in other words integral product ideals are in general expressible only as unions of an infinite number of elements of \bar{O} . If however \bar{O} contains only a finite number of non-equivalent elements, then \mathfrak{R} is a finite lattice satisfying the following conditions:⁷

N 1. \mathfrak{R} is residuated.

N 2. The ascending chain condition holds in \mathfrak{R} .

D 3. Every element of \mathfrak{R} is the union of a finite number of principal ideals.

D 4. The principal ideals of \mathfrak{R} are closed under multiplication.

Hence by theorem 5.3 and theorem 14.2 of W-D, \mathfrak{R} is a Noether lattice. Since \mathfrak{R} is also a distributive lattice, we may state the following theorem.

THEOREM 6.1. *If \bar{O} contains only a finite number of principal product ideals, then every element of \bar{O} is expressible as a cross-cut of a finite number of primary product ideals in essentially one way only.*

If in particular O itself has only a finite number of elements, and we take $\bar{O} = O$, we have the "fundamental theorem of the arithmetic of finite ova" stated in the introduction.

III. THE OVOID IDEALS OF AN OVUM

7. The second type of distinguished subset of O which we shall consider is the ovoid ideal. There is little gain in defining division in O relative to a proper subovum \bar{O} , and for the remainder of the paper we identify \bar{O} with O as in Clifford 2.

DEFINITION 7.1. *Let A be any set of elements of O . The cross-cut of all the residuals $(s):(t)$ of principal product ideals $(s), (t)$ such that $(s):(t)$ contains A is called the ovoid ideal generated by A .*

We write $\alpha = (A)$ (Clifford 2). Evidently α is a product ideal containing both A and A' . It is easily shown that this definition is equivalent to the definition in Clifford 2. It seems to us somewhat easier to grasp.

O itself is an ovoid ideal \mathfrak{o} , and the ovoid ideals form a semi-ordered set with respect to the relation $(\mathfrak{x}) \supset (\mathfrak{y})$ of set-theoretic inclusion. We use small German letters for ovoid ideals.

As in part II, a special convention is made for the null ideal. If the ovum contains a zero element z , the set \mathfrak{z} consisting of the single element z is an ovoid ideal contained in every other ideal. If the ovum contains no zero element, we count the null set as an ovoid ideal \mathfrak{z} contained in every other.

The following properties of ovoid ideals are obvious from the definition:

$$(7.1) \quad (A) \supset A, \quad A \supset B \quad \text{implies} \quad (A) \supset (B), \quad ((A)) = (A).$$

LEMMA 7.1. (Clifford 2) *If the subset A consists of a single element a , the ovoid ideal (A) is the principal product ideal $(a) = aO$.*

⁷ The letters N 1, N 2, D 3, D 4 refer to the like-designated conditions in W-D.

THEOREM 7.1. *The set-theoretic cross-cut of any class of ovoid ideals is an ovoid ideal.*

PROOF. Let Ω be a class of ovoid ideals a , and let K be the set-theoretic cross-cut of the a . (K exists, since $a \supseteq \emptyset$). Then $a \in \Omega$ implies $a \supseteq K$. Hence by (7.1), $(a) \supseteq (K)$, $a \supseteq (K)$. Hence $K \supseteq (K)$, $K = (K)$.

We may now define the union of any set of ovoid ideals b as the cross-cut of the non-empty set Ω of all ideals a such that $b \supseteq a$, all b . It is easy to prove from (7.1):

LEMMA 7.2. (Clifford 2) *The union of any set of ovoid ideals is the ovoid ideal generated by their set theoretic sum.*

We may now state one of our fundamental theorems.

THEOREM 7.2. *The set of ovoid ideals of any ovum form a completely closed lattice relative to the relation of set-theoretic inclusion.*

8. We now pass to the multiplicative properties of the lattice of ovoid ideals. The set product of two ovoid ideals need not be an ovoid ideal. We accordingly define the product of two ovoid ideals to be the ideal generated by their set product. To distinguish this new product from the set product, we use a dot, writing

$$(8.1) \quad (A) \cdot (B) = ((A)(B)), \quad \text{or} \quad a \cdot b = (ab).$$

This multiplication is readily shown to satisfy postulates M 1-M 5 of section 5, where the unit element is the unit ideal o .

THEOREM 8.1. *The operation of multiplication of ovoid ideals is completely distributive with respect to union.*

PROOF. Let Ω be any set of ovoid ideals a , and let b be any fixed ovoid ideal. Let u be the union of the ideals a , and v the union of the ideals $b \cdot a$. Then by lemma 7.2 $u = (\sum a)$, $v = (\sum b \cdot a)$. We wish to show that $b \cdot u = v$. We need the following lemma due to A. H. Clifford: (Clifford 2).

LEMMA 8.1. *If A and B are any two subsets of O , then the product of the ovoid ideals which they generate is the ideal generated by their set product:*

$$(8.2) \quad (A) \cdot (B) = (AB).$$

By (8.2), $b \cdot u = (b \sum a) = (\sum ba)$ by theorem 4.1. But by lemma 7.2 $(\sum ba) = (\sum (ba)) = (\sum b \cdot a) = v$

It follows that M 7 and M 6 of section 5 are satisfied. Hence we have

THEOREM 8.2. *The set of all ovoid ideals of O form a completely closed residuated lattice.*

We denote this lattice by \mathfrak{S} .

If (a) and (b) are principal ovoid ideals, it is easily shown that $(a) \cdot (b) = (a)(b) = (ab)$. Hence we have

LEMMA 8.2. *The principal ovoid ideals of O are closed under multiplication, and form an ovum within the lattice \mathfrak{S} which is simply isomorphic with O .*

In W-D, an element a of a residuated lattice \mathfrak{S} was defined to be "principal" provided that $a \supset b$ if and only if there existed a lattice element c such that $ac = b$.

THEOREM 8.3. *Every principal ideal of the lattice of all ovoid ideals of an ovum is a principal element of the lattice.*

PROOF. Let $a = (a)$ and $a \supset b$. Consider the set C of all elements c such that $ac \in b$ and let $c = (C)$. Then $b = a \cdot c$. For since $b \supset aC$, $(b) \supset (aC)$ or $b \supset a \cdot c$. Since $a \supset b$ and $a = (a)$, if $b \in b$ then $b = ca$, $c \in O$. Hence $aC \supset b$ so that $(aC) \supset b$, $a \cdot c \supset b$, $a \cdot c = b$.

IV. THE ARITHMETICAL PROPERTIES OF OVA

9. We shall now consider the arithmetical properties of the lattice \mathfrak{S} . In W-D, we have called a lattice a "Noether lattice" if it satisfies the three conditions.

N 1. *The lattice \mathfrak{S} may be residuated.*

N 2. *The ascending chain condition holds in \mathfrak{S} .*

N 3. *Every irreducible of \mathfrak{S} is primary.*

In such a lattice the decomposition theorems first proved by Emmy Noether for the ideals of a commutative ring with chain condition hold. We also proved there that sufficient conditions⁸ that any lattice be a Noether lattice are N 1, N 2 and

D 2 \mathfrak{S} is modular.

D 3' *There exists a set \mathfrak{P} of principal elements of \mathfrak{S} such that every other element is the union of a finite number of elements of \mathfrak{P} .*

D 4' *The set \mathfrak{P} is closed under multiplication.*

In the present case, N 1 is satisfied by theorem 8.2, and D 4' is satisfied for \mathfrak{P} the principal ideals of \mathfrak{S} by lemma 8.2. Clifford has shown that N 2 implies D 3' (Theorem 8.4; Clifford 2, theorem 2.1). Hence we may state the fundamental result:

THEOREM 9.1. *The lattice of ovoid ideals of any ovum is a Noether lattice provided that*

N 2. *The ascending chain condition holds in \mathfrak{S} ,*

D 2. \mathfrak{S} is modular.

If we assume that \mathfrak{S} is distributive instead of modular, we have an analogue of theorem 6.1 on product ideals; namely

THEOREM 9.2. *If the lattice of ovoid ideals of an ovum satisfies the conditions*

N 2. *The ascending chain condition holds in \mathfrak{S} ,*

D 6. \mathfrak{S} is distributive,

then every element of the lattice, and in particular the principal ideals corresponding

⁸ The more restrictive conditions D 3 and D 4 quoted in section 6 are stated in W-D. But an examination of the proof of theorem 14.2 of W-D will show that D3' and D4' are sufficient.

to elements of the ovum, may be uniquely represented as a cross-cut of primary elements, each belonging to a different prime.

If we assume that every ovoid ideal is principal, then D 6 is satisfied by W-D theorem 16.2. Hence we may state:

THEOREM 9.3. *The conclusions of theorem 9.2 hold provided that the lattice of ovoid ideals satisfies the conditions*

N 2. *The ascending chain condition holds in \mathfrak{S} ,*

D 7. *Every ovoid ideal is principal.*

10. The two simplest types of distributive lattice are arithmetical lattices and semi-arithmetical lattices. An arithmetical lattice is one which is a direct product⁹ of simple chain lattices and in which N 2 holds. It is quite easy to show that the fundamental theorem of arithmetic¹⁰ holds in a lattice if and only if the lattice is arithmetical. Such lattices have been thoroughly investigated by F. Klein (Klein 1).

The notion of a semi-arithmetical lattice was introduced by one of us in a recent paper in these Annals. (Ward 2.) A semi-arithmetical lattice is a distributive lattice in which the ascending chain condition holds and in which every element may be uniquely represented as a cross-cut of irreducible elements *co-prime in pairs*. If the semi-arithmetical lattice is residuated, it follows that every element may be uniquely represented as a *product* of irreducible elements; for if a and b are coprime, their product equals their cross-cut. Conversely, it is not difficult to show that if every element of a lattice may be uniquely represented as a product of irreducible elements, co-prime in pairs, then the lattice is semi-arithmetical; in other words a residuated semi-arithmetical lattice is the most general type of lattice in which a unique multiplicative decomposition of elements may be defined.

We can therefore replace condition D 6 by conditions that \mathfrak{S} be semi-arithmetical or arithmetical to obtain still more special types of decomposition in \mathfrak{S} . The investigations of Clifford viewed from this standpoint give convenient sets of conditions that the lattice be arithmetical.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA.

REFERENCES

- | | |
|------------------|--|
| E. T. BELL | 1 Am. Math. Monthly 37 (1930) pp. 400-418. |
| GARRETT BIRKHOFF | 1 Bull. Am. Math. Soc. 40 (1934) pp. 613-619.
2 These Annals (2) 35 (1934) pp. 351-360. |
| A. H. CLIFFORD | 1 Bull. Am. Math. Soc. 40 (1934) pp. 326-330.
2 These Annals (2) 39 (1938) pp. 594-610. |

⁹ For the notion of a direct product of lattices, see Garrett Birkhoff 1.

¹⁰ Every lattice element is then uniquely representable as a cross-cut or product of co-prime powers of divisor free elements. (Klein 1.)

- | | |
|-------------------------------|--|
| R. DEDEKIND | 1 Dirichlet, <i>Vorlesungen über Zahlentheorie</i> , 4 th ed. |
| L. E. DICKSON | 1 Trans. Am. Math. Soc. 6 (1905) p. 205. |
| F. KLEIN | 1 Math. Annalen 106 (1932) pp. 114–134. |
| H. M. MACNEILLE | 1 Trans. Am. Math. Soc. 42 (1937) pp. 416–460. |
| A. R. POOLE | 1 Am. Math. Journ. 59 (1937) pp. 23–32. |
| M. WARD AND
R. P. DILWORTH | Trans. Am. Math. Soc. (reference later). |
| M. WARD | 1 Duke Math. Journ. 3 (1937) pp. 627–636.
2 These Annals (2) 39 (1938) pp. 558–568. |

A CHARACTERIZATION OF BOOLEAN ALGEBRAS

BY GARRETT BIRKHOFF AND MORGAN WARD

(Received January 9, 1939)

Introduction

When is a lattice a Boolean algebra—that is, isomorphic with a field of sets? The classical conditions are:¹ (1) The distributive law holds, (2) every element has a complement. Now it is well known² that (1) and (2) imply (3) no element has more than one complement. We are thus led to conjecture that (2) and (3) imply (1); in other words, that a necessary and sufficient condition that a lattice be a Boolean algebra is that each of its elements have a unique complement.

The only published result bearing on this question is G. Bergmann's³ theorem that the distributive law holds if and only if relative complements are unique; that is, if and only if given $a \leq x \leq b$, there exists one and only one y with $x \cap y = a, x \cup y = b$.

We prove here the truth of our conjecture for all complete atomistic lattices.⁴ These include lattices of finite length and of finite order. We do not know whether or not our conjecture is unrestrictedly true.

Exact statement of theorem

Let L be a complete lattice which is "atomistic" in the sense that if $O < a < I$, then $p_\alpha \leq a \leq q_\beta$ where p_α covers O and q_β is covered by I . Let us further define a "point" as an element p covering O .

THEOREM 1: *If each element of L has one and only one complement, then L is isomorphic with the Boolean algebra of all subsets of its points.*

THEOREM 2: *In order for L to be a Boolean algebra, it is necessary and sufficient that each element have one and only one complement.*

The second theorem follows from the first, and the known results stated in the introduction.

PROOF OF FIRST THEOREM. To each set S of points p_α , make correspond the join $x(S)$ of the p_α in S . Dually, associate with each set S of elements q_β covered by I , the meet $y(S)$ of the q_β in S . It will follow from generalized

¹ E. V. Huntington "Postulates for the algebra of logic," Trans. Am. Math. Soc. 5 (1904), pp. 288-309. His hypotheses (1) — (7) define lattices.

² See for example, A. N. Whitehead's "Universal Algebra" Cambridge (1898) p. 36. The result is due to R. Grassmann.

³ "Zur Axiomatik der Elementargeometrie" Monatschr. f. Math. u. Phys. 36 (1929), pp. 269-84.

⁴ The terminology of the present paper is that of G. Birkhoff's "Lattice theory and its applications" Bull. Am. Math. Soc. 44 (1938), pp. 793-800. By " a covers b ," we mean that $a > b$ while $a > x > b$ has no solution.

associativity, that $x(S \cup T) = x(S) \cup x(T)$ and $y(S \cup T) = y(S) \cap y(T)$. Again, the complement of $x(I)$ can contain no point, since $x(I)$ contains every point;⁵ hence it is O , and $x(I) = I$. Dually, $y(I) = O$.⁵

Again, given α, β , either $p_\alpha \leq q_\beta$, or $p_\alpha \cap q_\beta = O$ and $p_\alpha \cup q_\beta = I$ —that is, p_α and q_β are complementary. But not every q_β contains p_α , since $y(I) = O < p_\alpha$. Hence (by the existence of unique complements) a suitable subscript notation will make $p'_\alpha = q_\alpha$ and $p_\alpha \leq q_\beta$ if $\alpha \not\leq \beta$.

This notation will further identify subsets of p_α with subsets of q_α , and, since every $p_\alpha [\alpha \in S]$ is less than or equal to every $q_\beta [\beta \in S']$, it will make $x(S) \leq y(S')$. (Here S' denotes the set complementary to S .) From this important inequality we infer that

$$\begin{aligned} x(S) \cup y(S) &\geq x(S) \cup x(S') = x(S \cup S') = I, \\ x(S) \cap y(S) &\leq y(S') \cap y(S) = y(S \cup S') = O. \end{aligned}$$

Consequently $x(S)$ and $y(S)$ are complementary.

Also, $x(S) \cap x(S') \leq y(S') \cap y(S) = y(S \cup S') = O$ and $x(S) \cup x(S') = x(S \cup S') = I$; hence $x(S)$ and $x(S')$ are complementary. But since $x(S)$ and $x(S')$ are complementary, $x(S)$ contains no p_α not in S , distinct sets S determine distinct $x(S)$, and the partially ordered system of the $x(S)$ is isomorphic with the algebra of all subsets of the p_α .

It remains to show that every member a of L is an $x(S)$. But denote by S the set of $p_\alpha \leq a$. Evidently $x(S) \leq a$; moreover $a \cap x(S')$ will by the last paragraph contain no points; hence $a \cap x(S') = O$. On the other hand, $a \cup x(S') \geq x(S) \cup x(S') = I$; hence a is the unique complement $x(S)$ of $x(S')$, completing the proof.

HARVARD UNIVERSITY AND
CALIFORNIA INSTITUTE OF TECHNOLOGY.

⁵ We are letting I denote simultaneously: the biggest element in L , the set of all p_α , and the set of all q_β .

Chapter 14

1942

THE CLOSURE OPERATORS OF A LATTICE

BY MORGAN WARD

(Received January 29, 1940)

I. INTRODUCTION

1. If \mathfrak{S} is a lattice of elements A, B, \dots , the class of all operators of \mathfrak{S} (that is, one-valued functions $\phi X = \phi(X)$ on \mathfrak{S} to \mathfrak{S}) may be made into a lattice by defining the union δ and cross-cut κ of any set Φ of operators ϕ by¹

$$\delta X = (\cdots \phi X \cdots), \quad \kappa X = [\cdots \phi X \cdots], \quad \phi \in \Phi.$$

The union and cross-cut here are taken over all the values ϕX of the operators in Φ for any given X of \mathfrak{S} .

It is easily verified that the operators of \mathfrak{S} form a lattice in which $\phi \supseteq \psi$ if and only if $\phi X \supseteq \psi X$ for every X of \mathfrak{S} ; furthermore this lattice is closed, modular, or distributive according as \mathfrak{S} is closed, modular or distributive.²

The operator lattice of a lattice is a concept comparable in generality to the Boolean algebra of all subsets of a lattice. As in the algebra, it is certain distinguished sets of operators which are useful in investigating the given lattice rather than the operator lattice itself.

One obviously important distinguished type is the linear operator. An operator ϕ is said to be linear if for any subset \mathfrak{A} of elements A of \mathfrak{S} , it has one or more of the four properties

$$(1.1) \quad \begin{array}{ll} \text{(i)} & \phi(\cdots A \cdots) = (\cdots \phi A \cdots), \\ \text{(ii)} & \phi(\cdots A \cdots) = [\cdots \phi A \cdots], \\ & \text{(iii)} \phi[\cdots A \cdots] = [\cdots \phi A \cdots], \\ & \text{(iv)} \phi[\cdots A \cdots] = (\cdots \phi A \cdots). \end{array}$$

Here the unions and cross-cuts are taken over all the elements of \mathfrak{A} , and \mathfrak{A} is finite if \mathfrak{S} is not closed. Lattice homomorphisms and homomorphisms with respect to union with properties (i), (iii) and (ii) respectively are familiar examples. (Ore 1).

The linear operators and certain associated lattices are important in the study of residuated lattices (Ward-Dilworth 1) as I plan to show in detail elsewhere.³

¹ If \mathfrak{S} is not closed, Φ is assumed to contain only a finite number of operators. A lattice is said to be closed (or "complete" or "continuous") if it contains the union and cross-cut of any subset of elements in it.

² Chain conditions in \mathfrak{S} do not usually carry over to the operator-lattice.

³ The product $\phi\psi$ of two operators ϕ and ψ defined by $\phi\psi X = \phi(\psi(X))$ immediately gives us an associative multiplication over the operator lattice. On the other hand if B is any fixed element of a residuated lattice \mathfrak{S} , the operators μ and ρ defined by $\mu X = BX$, $\rho X = B:X$ have the linear properties $\mu(\cdots A \cdots) = (\cdots \mu A \cdots)$, $\rho(\cdots A \cdots) = [\cdots \rho A \cdots]$.

I have discussed elsewhere (Ward 2) a type of operator associated with a point lattice,⁴ which may be used to classify all such lattices of finite order.

2. I develop here the properties of a type of operator which is of fundamental importance in the study of certain imbedding problems of ring theory and semi-group theory.⁵ A typical problem of this class is to imbed a system I of elements over which a commutative and associative multiplication is defined in a residuated lattice \mathfrak{S} so as to preserve the multiplication in I and thus to study the arithmetical properties of I . (Clifford 2, Ward-Dilworth 2). The imbedding is effected by defining a suitable type of "ideal" (distinguished subset) of I in the Boolean algebra of its subsets.⁶ A closely related problem is to imbed a semi-ordered set in a closed lattice. (Mac Neille 1).

The "closure operators" introduced here enable us to view all these problems from a unified standpoint, and explain why in all extant theories of ideals as distinguished subsets, the cross-cut of two ideals is the set-theoretic cross-cut of their elements.

II. CLOSURE OPERATORS

3. Let \mathfrak{S} be a closed lattice. An operator ϕ of \mathfrak{S} is said to be a closure operator if it satisfies the following three conditions:⁷

- I 1. $A \supset B$ implies that $\phi A \supset \phi B$.
- I 2. $\phi \supset i$.
- I 3. $\phi^2 = \phi$.

Here i is the identity operator leaving every element of \mathfrak{S} unchanged.

If \mathfrak{T} is any set of elements T of \mathfrak{S} , it may be proved that every closure operator ϕ has the quasi-linear properties

$$(3.1) \quad \phi[\cdots \phi T \cdots] = [\cdots \phi T \cdots],$$

$$(3.2) \quad \phi(\cdots T \cdots) = \phi(\cdots \phi T \cdots), \quad T \in \mathfrak{T}.$$

No actual linearity is assumed.

THEOREM 3.1. *The cross-cut⁸ of any set of closure operators is again a closure operator.*

⁴ A lattice is called a point lattice if every element in it save the null element is a union of points. Here a point is any element covering the null element. Point lattices include important types of projective geometries, exchange lattices, and Boolean algebras.

⁵ For a discussion of these problems, the reader is referred to Clifford 1, 2 where references are given to the work of Prüfer and others.

⁶ Several definitions are usually possible. See Ward-Dilworth 2.

⁷ These axioms are satisfied by Kuratowski's closure operator over a Boolean algebra with points. (Kuratowski 1). But they are essentially weaker, as Kuratowski's operator is linear with respect to union. Compare also Birkhoff 1.

⁸ In general, no closure properties hold for the union and product of (closure) operators. It may be shown that if ϕ and ψ are operators, then (ϕ, ψ) is an operator if and only if $(\phi, \psi) = \phi\psi = \psi\phi$. Commutativity is thus a necessary condition for the union (ϕ, ψ) to be an operator. It is evidently a sufficient condition for the product $\phi\psi$ to be an operator.

PROOF. Let Φ be a set of closure operators ϕ , and let $\kappa = [\cdots \phi \cdots]$ be their cross-cut. We shall show that κ satisfies I 1, I 2, I 3.

I 1 is satisfied. For $A \supseteq B$ implies $\phi A \supseteq \phi B$ for every $\phi \in \Phi$. Hence $[\cdots \phi A \cdots] \supseteq [\cdots \phi B \cdots]$, $\kappa A \supseteq \kappa B$. I 2 is satisfied. For since $\phi A \supseteq A$ for every $\phi \in \Phi$, $[\cdots \phi A \cdots] \supseteq A$ or $\kappa \supseteq \iota$. I 3 is satisfied. For $K^2 A = [\cdots \phi \kappa A \cdots]$, $\phi \in \Phi$. Now $\phi \supseteq \kappa$. Hence $\phi A \supseteq \kappa A$, $\phi^2 A \supseteq \phi \kappa A$, $\phi A \supseteq \phi \kappa A$. Accordingly $\kappa \supseteq \kappa^2$. By I 1 and I 2, $\kappa^2 \supseteq \kappa$. Hence $\kappa^2 = \kappa$, completing the proof.

4. Let ϕ be a given closure operator, and let $\mathfrak{S}' = \phi \mathfrak{S}$ be the set of all its values $X' = \phi X$ in \mathfrak{S} . By formula (3.1) any subset \mathfrak{T}' of the X' is closed under cross-cut. We may express this fact by writing

$$(4.1) \quad [\cdots T' \cdots]_{\mathfrak{S}'} = [\cdots T' \cdots]_{\mathfrak{S}}, \quad T' \in \mathfrak{T}', \quad \mathfrak{T}' \subseteq \mathfrak{S}'.$$

If I is the unit element of \mathfrak{S} , then $I' = I$ divides all elements A' of \mathfrak{S}' . Hence for any subset \mathfrak{L}' of elements L' of \mathfrak{S}' , the class \mathfrak{K}' of all K' such that $K' \supseteq L'$ is non-empty. We define the union of the L' to be the cross-cut of the K' :

$$(4.2) \quad (\cdots L' \cdots)_{\mathfrak{S}'} = [\cdots K' \cdots]_{\mathfrak{S}'}, \quad L' \supseteq K' \text{ every } L' \text{ of } \mathfrak{L}'.$$

We obtain by a familiar argument:

THEOREM 4.1. *The set \mathfrak{S}' of values of a given closure operator forms a closed lattice within \mathfrak{S} with respect to the operations of union and cross-cut defined by (4.2) and (4.1).*

To each closure operator ϕ we may accordingly assign a lattice $\mathfrak{S}' = \phi \mathfrak{S}$. In particular, $\mathfrak{S} = \iota \mathfrak{S}$. We shall establish a converse result.

Let \mathfrak{S}' now denote a fixed subset of \mathfrak{S} closed under cross-cut and containing the unit element I . We make \mathfrak{S}' into a lattice within \mathfrak{S} by assigning to any subset \mathfrak{L}' of elements of \mathfrak{S}' as in (4.2) a union defined as the cross-cut of the set of all multiples of the elements of \mathfrak{L}' .

We next define an operator ϕ on \mathfrak{S} to \mathfrak{S}' as follows: If A is any element of \mathfrak{S} , then ϕA is the cross-cut of all elements B' of \mathfrak{S}' such that $B' \supseteq A$. Then ϕ is a closure operator, for I 1, I 2, I 3 are evidently satisfied. Furthermore, $\phi \mathfrak{S} = \mathfrak{S}'$.

We have thus established a one-to-one correspondence between the closure operators of \mathfrak{S} and subsets of \mathfrak{S} closed under cross-cut and containing I . The lattice $\mathfrak{S}' = \phi \mathfrak{S}$ and the operator ϕ will be said to belong to one another.

It is also easily proved from formula (3.2) that \mathfrak{S}' is a sublattice of \mathfrak{S} if and only if the closure operator belonging to \mathfrak{S}' is linear with respect to union.

THEOREM 4.2. *The closure operators of any closed lattice themselves form a lattice within the operator lattice of \mathfrak{S} .*

PROOF. Let Σ denote the set of all closure operators of \mathfrak{S} . By formula (3.1), the cross-cut of any set of such operators is again a closure operator. Furthermore the operator ω defined by $\omega A = I$, every A of \mathfrak{S} , is obviously a closure operator dividing every other closure operator. Hence we may define the union of any set Φ of such operators as the cross-cut of the non-empty set of closure operators containing every operator of Φ .

We may evidently define lattice operations on the set of all subsets \mathfrak{S}' of \mathfrak{S} closed under cross-cut and containing I by the rules

$$(4.3) \quad \begin{aligned} [\cdots \mathfrak{S}' \cdots] &= [\cdots \phi \cdots] \mathfrak{S}, \quad \phi \in \Phi, \quad \mathfrak{S}' = \phi \mathfrak{S} \subset \Phi \mathfrak{S} \\ (\cdots \mathfrak{S}' \cdots) &= (\cdots \phi \cdots) \mathfrak{S}. \end{aligned}$$

The lattices \mathfrak{S}' thus form a lattice simply isomorphic with the lattice Σ of closure operators. We shall return to these operations at the close of the next section.

5. Consider an operator ϕ belonging to a set consisting of two elements I and T of \mathfrak{S} . It follows from the previous theorems that ϕ is characterized by

$$(5.1) \quad \phi A = I \text{ if } T \not\supset A, \quad \phi A = T \text{ if } T \supset A, \quad A \text{ any element of } \mathfrak{S}.$$

We call ϕ the two-valued operator belonging to T . Since $\phi \mathfrak{S}$ is a sub-lattice of \mathfrak{S} , ϕ is linear with respect to union, as is directly evident from (5.1). It is easy to prove

THEOREM 5.1. *The ideal operator ϕ belonging to any set \mathfrak{S}' of elements of \mathfrak{S} which is closed under cross-cut and contains I is the operator cross-cut of all the two-valued operators belonging to elements of \mathfrak{S}' .*

If \mathfrak{T} is any set of elements T of \mathfrak{S} containing I , we obtain a lattice \mathfrak{S}' within \mathfrak{S} containing \mathfrak{T} by adjoining to \mathfrak{T} the cross-cuts of all sets of its elements. \mathfrak{S}' is evidently the smallest such lattice containing \mathfrak{T} . We call \mathfrak{S}' the imbedding lattice of \mathfrak{T} , and its corresponding closure operator the "imbedding operator" of \mathfrak{T} . We shall use the letter θ to denote an imbedding operator.

THEOREM 5.2. *If θ is the imbedding operator of a set \mathfrak{T} of elements of \mathfrak{S} containing I , then the value of θ for any element A of \mathfrak{S} is given by the formula*

$$(5.2) \quad \theta A = [\cdots T \cdots], \quad T \supset A, \quad T \in \mathfrak{T}.$$

PROOF. We have $\theta A = S'$ where S' lies in $\mathfrak{S}' = \theta \mathfrak{S}$. Hence S' is the cross-cut of a certain set of the T in \mathfrak{T} . Now since $\theta A \supset A$, every such T divides A . But since $\theta T = T$ if $T \in \mathfrak{T}$, $T \supset A$ implies that $T \supset \theta A = S'$. Hence (5.2) follows.

THEOREM 5.3. *Let ϕ and ψ be any two closure operators of \mathfrak{S} . Then $\phi \supset \psi$ if and only if the lattice belonging to ψ contains the lattice belonging to ϕ in the set-theoretic sense.*

PROOF. Assume that $\phi \supset \psi$ and let $A \in \phi \mathfrak{S}$. Then $\phi A = A$. By I 1, $\phi A \supset \psi A$. Hence $A \supset \psi A$. Therefore by I 2, $A = \psi A$ or $A \in \psi \mathfrak{S}$. Since ϕ and ψ are the imbedding operators of their respective lattices, the converse follows from Theorem 5.2.

The following corollaries are immediate:

COROLLARY 5.31. *Let θ be the imbedding operator belonging to any set \mathfrak{T} of elements of \mathfrak{S} containing I , and let ψ be any closure operator such that ψ leaves every element of \mathfrak{T} invariant. Then ψ divides θ .*

COROLLARY 5.32. *The imbedding operator of any set is the union of all closure operators which leave every element of the set invariant.*

COROLLARY 5.33. *The union operation on the lattices which belong to closure operators defined by (4.3) is the operation of taking the set-theoretic cross-cut of their elements.*

It is this correspondence between operator union and set-theoretic cross-cut which makes the ideal operators of importance in imbedding problems.

III. APPLICATIONS TO IMBEDDING PROBLEMS

6. Let I be a set of elements a, b, \dots semi-ordered with respect to a division relation $x | y$ and containing a unit element ι dividing every other element. The following problem has been considered by Mac Neille: (Mac Neille 1). To construct a closed lattice \mathfrak{S}' such that: (i) \mathfrak{S}' contains a subset of elements A', B', \dots which may be set in a one-to-one correspondence $x \leftrightarrow X'$ with a, b, \dots ; (ii) If $a \leftrightarrow A'$ and $b \leftrightarrow B'$, then

$$(6.1) \quad a | b \text{ in } I \text{ implies } A' \supset B' \text{ in } \mathfrak{S}'.$$

$$(6.2) \quad A' \supset B' \text{ in } \mathfrak{S}' \text{ implies } a | b \text{ in } I.$$

We call such a construction an "isomorphic imbedding" of the set I . If we do not require (6.2), we speak of a "homomorphic imbedding" of I .

We shall solve these problems by determining suitable ideal operators in the lattice \mathfrak{B} (Boolean algebra) of all subsets of I . In other words, we shall determine all ideal operators ϕ of \mathfrak{B} such that $\mathfrak{S}' = \phi\mathfrak{B}$ will be a suitable lattice.

Consider first the condition (6.1). Let $T = (t)$ be a subset of I consisting of the single element t . Since $T' = \phi T \supset T$, we must have $t \in \phi T$. But by (6.1), if $t | y$ in I , $\phi T \supset \phi(y)$. Hence if $t | y$, $y \in \phi T$. Thus (6.1) implies that ϕT must contain all elements y of I such that $t | y$.

For a homomorphic imbedding, no further conditions are imposed on the values of ϕT . But if the imbedding is isomorphic and $\phi T \supset \phi(X)$, then (6.2) requires that $t | x$. Hence ϕT must consist only of elements x of I such that $t | x$.

We let \mathfrak{T} denote the set of all $T' = \phi(t)$, $t \in I$ for any ideal operator ϕ . We call the elements of \mathfrak{T} the principal ideals of I .

It is evident from the preceding section that any ideal operator of \mathfrak{B} leaving every element of \mathfrak{T} invariant will solve our initial imbedding problem, and that the simplest of these operators is the imbedding operator of the set \mathfrak{T} itself; for its lattice $\theta\mathfrak{B}$ is the smallest lattice in the set-theoretic sense in which the imbedding can be made in \mathfrak{B} . The isomorphism between I and \mathfrak{T} with respect to division shows that this same minimal property of $\theta\mathfrak{B}$ will apply to any isomorphic imbedding of I in any closed lattice \mathfrak{S}' whatever; within the lattice \mathfrak{S}' there must lie a lattice simply isomorphic to $\theta\mathfrak{B}$. $\theta\mathfrak{B}$ is the lattice defined in Mac Neille 1 by "Dedekind cuts."

A similar situation occurs for homomorphic imbeddings. For a homomorphic imbedding, the "principal ideals" A', B', \dots which make up the set \mathfrak{T} are not

uniquely determined by the corresponding elements a, b, \dots of I ; for if $a \leftrightarrow A'$, A' may contain elements of I not divisible by a . But once the set \mathfrak{T} of principal ideals is chosen, the imbedding operator of I gives the smallest lattice in which the particular homomorphic imbedding can be performed.

7. If A is any subset of I , let A be the subset of all elements l such that $l \mid k$ for every k in A , and let A' be the subset of all elements a such that $l \mid a$ for every l in A . Then the operator

$$(7.1) \quad A' = \theta A$$

is the isomorphic imbedding operator of the set I discussed above. This result follows easily from Theorem 5.3. For a detailed discussion, the reader may consult Ward-Dilworth 2 or Clifford 1, to whom this definition of θ is originally due.⁹

CALIFORNIA INSTITUTE OF TECHNOLOGY.

REFERENCES

- | | |
|----------------------------|--|
| GARRETT BIRKHOFF | 1 Duke Math. Journal, 3 (1931) pp. 443-454. |
| A. H. CLIFFORD | 1 Bull. Am. Math. Soc. 40 (1934) pp. 326-330. |
| C. KURATOWSKI | 2 These Annals (2) 39 (1938) pp. 594-610. |
| H. M. MAC NEILLE | 1 Topologie 1, Warsaw (1933). |
| O. ORE | 1 Trans. Am. Math. Soc. 42 (1937) pp. 416-460. |
| M. WARD AND R. P. DILWORTH | 1 These Annals, (2) 36 (1935) pp. 406-437. |
| M. WARD | 1 Trans. Am. Math. Soc. vol. 45 (1939), pp. 335-354. |
| | 2 Unpublished. |

⁹ The identity of this operator and Mac Neille's operator was pointed out to me by Dr. A. H. Clifford in a letter. The definition (7.1) is used in Ward-Dilworth 2 to imbed any ovum (semi-group) in a residuated lattice of ideals.

Chapter 15

1945

¹ Kasner, "Conformal Classification of Analytic Arcs or Elements, Poincaré's Local Problem of Conformal Geometry," *Trans. Am. Math. Soc.*, **16**, 333–349 (1915). The theory of a pair of regular arcs, including the horn angle, is given in "Conformal Geometry," *Proceedings Cambridge International Congress Mathematicians*, 1912, and a paper appearing in *Scripta Mathematica*, 1945.

² Kasner and De Cicco, "The General Invariant Theory of Irregular Analytic Arcs or Elements," *Ibid.*, **51**, 232–254 (1942). Also in Publications of the Illinois Institute of Technology (1943).

³ See for regular curves Halhnen's dissertation 1878, and his collected works Vol. 2. Also Lane, "Projective Differential Geometry," Chicago Press, 1942.

EULER'S THREE BIQUADRATIC PROBLEM

BY MORGAN WARD

CALIFORNIA INSTITUTE OF TECHNOLOGY

Communicated March 19, 1945

1. Euler's problem of whether the sum of three biquadrates can be a biquadrate; that is, whether the diophantine equation

$$x^4 + y^4 + z^4 = w^4 \quad (1)$$

has any (non-trivial) integer solutions, has never been solved.¹ The problem is a hard one; indeed, a modern investigator has stated: "... it would be difficult to mention any other [problem] which has yielded so little to the efforts of those who have attempted its solution."

The most that is known to date is that there is no solution of (1) with³ $w < 1024$. I have recently proved that *there is no solution of (1) with*

$$w < 10,000. \quad (2)$$

This result makes it appear probable that there are no solutions of (1) whatever, especially since several closely allied soluble diophantine equations such as $x^4 + y^4 + z^4 + t^4 = w^4$, $x^4 + y^4 = w^4 + t^4$, $x^4 + 2y^4 + 2z^4 = w^4$ are known to have comparatively small solutions.⁴

2. The first step of the proof is to reduce the solution of (1) to the solution of another diophantine equation containing more variables but with the variables subjected to a number of restrictive conditions which it is unnecessary to state here:

$$u^4 + v^4 = 2\epsilon kl(e^8l^2 + 2^{18+8\sigma+2\epsilon}d^8k^2). \quad (3)$$

The old variables are easily expressed in terms of the new; for example,

$$w = 2^{4\sigma+9+\epsilon}d^4k + e^4l. \quad (4)$$

Equation (1) has a solution if and only if equation (3) has a solution with d, e, k, l, u and v positive integers. The exponent σ is a positive integer or zero, and the exponent ϵ is either zero or one.

The inequality (2) in conjunction with (4) immediately restricts σ, d, e, k and l to a finite number of choices; in fact,

$$\sigma \leq 1, d \leq 1, e \leq 9, k \leq 17 \text{ and } l \leq 9488. \quad (5)$$

3. The second step of the proof is to discuss (3) for each of the cases given by (5). The most difficult case turns out to be when $\sigma = 0, \epsilon = 1$ and $d = e = k = 1$. (3) then becomes

$$u^4 + v^4 = 2l(l^2 + 1024^2) \quad (6)$$

with

$$(i) \quad l < 8976.$$

The restrictions on the variables in (3) alluded to in Section 2 tell us that

(ii) Every prime factor of l and $l^2 + 1024^2$ is congruent to one modulo eight.

On considering (6) modulo 5 and modulo 13, we find that

$$(iii) \quad l \equiv 4 \pmod{5},$$

$$(iv) \quad l \equiv 3, 4, 5, 7, 10 \text{ or } 12 \pmod{13}.$$

The conditions (i)–(iv) reduce the possible choices of l to twenty-nine numbers: 289, 449, . . . , 8689.

The other cases lead to even fewer choices of l and the other variables in (5).

4. The third step of the proof is to dispose of the cases which survive after all conditions of the type (i)–(iv) just described have been applied. For example, in the case given by (6), we have to show by the composition formulae for products of sums of squares that $2l(l^2 + 1024^2)$ is not a sum of two biquadrates for twenty-nine numerical values of l . This last step is easily carried out, and the proof is complete.

5. The most laborious feature in the proof is the necessity for factoring several numbers greater than ten million, the extent of the present factor tables. For example, in the case discussed in Section 3, it is necessary to factor the number $l^2 + 1024^2$ not only in order that condition (ii) may be applied, but also in order to apply the final restrictions by composition of sums of squares. This work was performed with the aid of a calculating machine by the factor stencil method of D. N. Lehmer and J. D. Elder.⁵ Whenever the stencils indicated that the number was a prime, the fact was confirmed by D. H. Lehmer's⁶ method based on the converse of Fermat's theorem.

In order to insure accuracy, all the attendant numerical work and the algebra of determining the cases in step two was checked twice at different times. Complete details of the proof will appear elsewhere.

¹ In L. E. Dickson's *History of the Theory of Numbers*, vol. 2, p. 648—there is a statement that might lead one to infer that the impossibility of (1) was proved by A. Werebrusow (*L'Intérmédiaire des Mathématiciens*, 21, 161 (1914)). A fatal lacuna in Werebrusow's proof was pointed out by E. T. Bell (*Mathematics Student*, 4, 78 (1936)).

² Mordell, L. J., "The Present State of Some Problems in the Theory of Numbers," *Nature*, 121, 138 (1928).

³ Aubry, L., *Sphinx-Oedipe*, 7, 45–46 (March, 1912).

⁴ For example, we have Norrie's well-known result that

$$30^4 + 120^4 + 272^4 + 315^4 = 353^4.$$

⁵ Lehmer, D. N., and Elder, J. D., "Factor Stencils," Carnegie Institution, Washington (1939).

⁶ Lehmer, D. H., *Amer. Math. Monthly*, 43, 347–354 (1936).

ERRATUM

In the article, "Dominance Modification and Physiological Effects of Genes," by L. C. Dunn and S. Gluecksohn-Schoenheimer, *Proc. Nat. Acad. Sci.*, 31, 82 (1945), the formula in the middle of line 1, page 83, should read "138 Sd + ($\chi^2 = 5.26$, $p = 0.02$)" instead of "138 Sd + $X_{p=0.2}^{2-5.26}$."

Chapter 16

1948

MEMOIR ON ELLIPTIC DIVISIBILITY SEQUENCES.*

By MORGAN WARD.

I. Introduction.

1. By an elliptic divisibility sequence we mean a sequence of integers,

$$(h) : h_0, h_1, h_2, \dots, h_n, \dots$$

which is a particular solution of

$$(1.1) \quad \omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$

and such that h_n divides h_m whenever n divides m . Simple instances of such sequences are:

$$(1.2) \quad h_n = n;$$

$$(1.3) \quad h_n = (n/3)$$

where (n/p) is Legendre's symbol;

$$(1.4) \quad h_n = (-8/n)$$

where (d/n) is Kronecker's symbol.²

$$(1.5) \quad h_n = Q^{(1/2)-(n/2)} U_n$$

where $P = a + b$, $Q = ab$ and

$$(1.6) \quad U_n = (a^n - b^n)/(a - b)$$

is a polynomial in P and Q satisfying a linear recurrence of order two. This polynomial is one of the two³ fundamental numerical functions studied by Edouard Lucas in the first volume of this Journal (Lucas [1], [2]. See also Lucas [3]). Lucas continually emphasized the connections between his

* Received February 12, 1947.

¹ The case when the h are rational is not essentially more general.

² See Landau, *Vorlesungen*, I, p. 51. In the present case, $(-8/n) = 0$ if n is even and $(-8/n) = (-1)^{\lfloor n/4 \rfloor}$ if n is odd, where $\lfloor n/4 \rfloor$ denotes the greatest integer in $n/4$.

³ The other function $V_n = a^n + b^n$ does not lead to a solution of (1.1) despite Lucas' assertion to this effect (Lucas [1], p. 203). See Bell [1]. We assume that P and Q are chosen so that (1.6) is an integer; for example, P an integer and Q plus or minus one.

numerical functions and the trigonometric functions, and claimed to have made a remarkable generalization connecting numerical functions defined by a linear recurrence of order three or four with the elliptic functions. (See Bell [1] for a review and evaluation of Lucas' claims. Lucas apparently published nothing on the subject save scattered hints.)

Since (1.1) is the fundamental relation on which the real multiplication theory of elliptic functions rests,⁴ a systematic study of (h) -sequences should throw some light on Lucas' conjecture. In addition (h) -sequences are of arithmetical interest on their own account; they appear to be the simplest type of non-linear⁵ divisibility sequence, and yet most of the properties of Lucas' linear (U) -sequence carry over to them. The investigations which follow show conclusively that if any such generalization as Lucas conjectured exists, it must be looked for in the direction of the complex multiplication theory of elliptic functions. The arithmetical properties of elliptic divisibility sequences turn out to be quite different from those of numerical functions defined by linear recurrences or order greater than two.⁶

2. The main results of the memoir are as follows. We may confine ourselves to sequences in which $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 vanish.⁷

A solution of (1.1) satisfying these conditions is an elliptic divisibility sequence if and only if h_2 , h_3 , h_4 are integers and h_2 divides h_4 . Every such solution is uniquely determined by the initial values of h_2 , h_3 and h_4 and may be parameterized by elliptic functions provided that h_2 and h_3 are not zero.⁸ The invariants g_2 and g_3 of the associated \wp function are rational functions of h_2 , h_3 and h_4 .

Every divisibility sequence with $h_2 = 0$ is essentially equivalent to the solution (1.4) of the previous section and every rational solution of (1.1) with $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 zero is essentially equivalent to an integral elliptic divisibility sequence.

(h) reduces essentially to the solution (1.2) of Section 1 if and only if

⁴ $w_n = \sigma(nu)/\sigma(u)^{n^2}$ satisfies (1.1) where $\sigma(z)$ is the Weierstrass sigma function.

⁵ A divisibility sequence is said to be linear if it satisfies a linear recurrence relation. See Hall [1].

⁶ The theory of such functions was initiated by Carmichael. (Carmichael [1]). See also Ward [1] and the references given there.

⁷ If both h_2 and h_3 vanish, there exist integral solutions of (1.1) which are not divisibility sequences and which are not determined by any fixed number of initial values. These and other special sequences are discussed in Chapter VII.

⁸ If h_2 or h_3 is zero, h_n is trivially a product of powers of $\pm h_3$ or $\pm h_2$ and h_4 . (This case is discussed in Chapter VII).

g_2 and g_3 both vanish, and (h) reduces essentially to Lucas' solutions (1.5) if and only if neither g_2 nor g_3 vanishes, but the elliptic discriminant $g_2^3 - 27g_3^2$ vanishes.

An integer m is said to be a divisor of (h) if it divides some term h_k with $k > 0$. If m divides h_k but does not divide h_l when l divides k , then k is called a rank of apparition of m in (h) .⁹ Every prime p which does not divide both h_3 and h_4 has precisely one rank of apparition ρ , and (h) is periodic modulo p with period $\rho\tau$ where τ is a certain arithmetical function of p and (h) which can be exactly determined.¹⁰ Similar results hold for a composite modulus m .

If the least positive residues modulo m of the successive values U_0, U_1, U_2, \dots of any Lucas function are calculated, the pattern of residues exhibits interesting symmetries.¹¹ These symmetries extend to elliptic sequences, and find their ultimate explanation in the periodicity of the second kind of the Weierstrass sigma function.

3. The plan of the paper is sufficiently indicated by the chapter titles. We develop first those arithmetical properties of the sequences which can be proved without the use of elliptic functions; the important modular periodicity, however, depends on the elliptic function representation. Our conclusions regarding Lucas' conjectures are given in the final chapter.

The terminology describing the arithmetical properties of the elliptic sequences is chosen to agree with that used for linear sequences (Hall [1], Ward [2]). We use the standardized arithmetical notations of Landau's *Vorlesungen*; in particular, if a, b, \dots are integers or ideals, $a | b$ for "a divides b " and (a, b, \dots) for the greatest common divisor of a, b, \dots . We denote the least common multiple of a, b, \dots by $[a, b, \dots]$.

The results of elliptic function theory which are used in Chapter IV may be found in any standard text; the account of (1.1) in Halphen's Treatise is particularly complete, and many of his results may be restated as theorems about elliptic sequences.

⁹ This definition is due to M. Hall. See Hall [1].

¹⁰ In the terminology of the theory of linear recurrences, ρ is the "restricted period" of (h) modulo p . See Carmichael [1].

¹¹ Typical examples are given by the residues of the Fibonacci sequence 0, 1, 1, 2, 3, . . . for small integral moduli. See also the table of elliptic sequences modulo three in Section 7 of Chapter III.

II. Elementary Properties of Sequences.

4. We shall confine ourselves in the next five chapters to sequences whose first two initial values are zero and one. If in addition neither the third nor the fourth value vanishes, we call the sequence "general." Sequences which violate one or more of these restrictions are called "special," and are discussed in detail in Chapter VII. It turns out that the only sequences (h) which have any arithmetical interest satisfy the following conditions:

$$(4.1) \quad h_0 = 0, h_1 = 1; \text{ not both } h_2 \text{ and } h_3 \text{ zero.}$$

We call such sequences "proper." Proper sequences include as well as the general sequence, two special sequences in which either $h_2 = 0, h_3 \neq 0$ or $h_2 \neq 0, h_3 = 0$. We shall begin by proving the following basic theorem.

THEOREM 4.1. *Let (h) be a proper solution of (1.1) so that (4.1) holds and also*

$$(4.11) \quad h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \quad m \geq n \geq 1.$$

Then (h) is an elliptic divisibility sequence if and only if

$$(4.2) \quad h_2, h_3 \text{ and } h_4 \text{ are integers;}$$

$$(4.3) \quad h_2 \text{ divides } h_4.$$

Furthermore, the sequence (h) is uniquely determined by the three initial values h_2, h_3 and h_4 .

Proof. Assume first that

$$(4.31) \quad h_2 \neq 0.$$

Since the necessity of the conditions (4.2) and (4.3) is evident, assume conversely that (h) is a solution of (1.1) for which (4.1), (4.2), (4.3) and (4.31) all hold. We shall first prove by induction that all terms of (h) are integers and that h_2 divides h_{2n} . We then make a second induction to prove that (h) is a divisibility sequence; that is

$$(4.4) \quad h_r \text{ divides } h_s \text{ if } r \text{ divides } s.$$

A third and final induction shows that if n is greater than four, h_n is uniquely determined if h_0, h_1, \dots, h_{n-1} are uniquely determined.

We obtain the following important formulas from (4.11) on taking first $m = n + 1$, $n = n$ and then $m = n + 1$ and $n = n + 1$:¹²

$$(4.5) \quad h_{2n+1} = h_{n+2}h^3_n - h_{n-1}h^3_{n+1}, \quad n \geq 1.$$

$$(4.6) \quad h_{2n}h_2 = h_n(h_{n+2}h^2_{n-1} - h_{n-2}h^2_{n+1}), \quad n \geq 2.$$

We begin the first induction by assuming that

(α) h_0, h_1, \dots, h_{n-1} are integers;

(β) h_2 divides h_{2r} , $2r < n$; $n \geq 5$.

If n is odd, say $n = 2k + 1$, we conclude from (α) and (4.5) with $n = k$ that h_n is an integer. If n is even, say $n = 2k$, then $k \geq 3$ and (4.6) gives

$$(4.7) \quad h_nh_2 = h_k(h_{k+2}h^2_{k-1} - h_{k-2}h^2_{k+1}).$$

Since $k + 2 < 2k$ and the suffices $k \pm 2$, $k \mp 1$ are of opposite parity, $h_{k+2}h^2_{k-1} - h_{k-2}h^2_{k+1}$ is an integer divisible by h_2 . Hence h_n is an integer. But if k is even, h_k is divisible by h_2 and if k is odd, h^2_{k-1} and h^2_{k+1} are divisible by h^2_2 . Hence in either case h_n is divisible by h_2 . The first part of the theorem follows then by induction on n .

We prove (4.4) by a second induction. Assume that

(γ) $h_r | h_s$ provided that $r | s$ for $r \leq s < n$.

We observe that (γ) is true if $n \leq 5$. Hence we may assume that $n > 5$. Now consider h_n , and suppose that $n = uv$. We wish to show that $h_u | h_{uv}$ and it is evidently allowable to assume that $u \geq 2$ and $v \geq 2$.

Suppose first that $h_u \neq 0$. Then if v is even, (4.6) gives

$$h_{uv}h_2 = h_{uv/2}(h_{(uv/2)+2}h^2_{(uv/2)-1} - h_{(uv/2)-2}h^2_{(uv/2)+1}).$$

The parenthesis is divisible by h_2 . But by (γ), $h_u | h_{uv/2}$. Hence $h_u | h_v$.

If v is odd, u and uv are of the same parity. Hence on taking $m + n = uv$ and $m - n = u$ in (1.1) we obtain the relation

$$h_{uv}h_u = h_{m+1}h_{m-1}h^2_n - h_{n+1}h_{n-1}h^2_m$$

Since $m = u(v + 1)/2$ and $n = u(v - 1)/2$, we conclude from (γ) that the right side of this expression is divisible by h^2_u . Hence since $h_u \neq 0$, $h_u | h_{uv}$.

¹² As will be evident, if we define a sequence (h) recursively by (4.5) and (4.6) (taking $h_0 = 0$, $h_1 = 1$, $h_2 \neq 0$ and h_3, h_4 arbitrary) then conversely we obtain a solution of (1.1).

Now assume that $h_u = 0$. We shall need the following lemma which will be important in other connections. We shall postpone its proof until we have completed the proof of the theorem.

LEMMA 4.1. *Let (h) be any solution whatever of (1.1) with initial values $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 zero. Then if two consecutive terms of (h) vanish, all terms of (h) vanish beyond the third.¹³*

Since $h_u = 0$, $h_{u(v-1)}$ is zero by (γ) . Then on taking $m = uv$ and $n = u$ in (4.11), we obtain

$$h_{u(v+1)}h_{u(v-1)} = h_{uv+1}h_{uv-1}h^2_u = h_{u+1}h_{u-1}h^2_{uv}$$

Hence either $h_{uv} = 0$ or $h_{u+1}h_{u-1} = 0$ so that two consecutive terms of (h) vanish. Then by the lemma, $h_3 = h_4 = h_5 = \dots = h_{uv} = 0$. Hence in all cases, h_u divides h_{uv} . (4.4) now follows by induction on n in (γ) .

Finally, the unicity of (h) follows directly from the formulas (4.5) and (4.6) by a brief induction.

It remains to discuss the case when h_2 vanishes. Then $h_3 \neq 0$ and we shall prove in Theorem 23.1 of Chapter VII that the general term of (h) is as follows:¹⁴

$$(23.4) \quad h_n = \begin{cases} 0, & n \text{ even;} \\ (-1)^{\lceil n/4 \rceil} h_3^{(n^2-1)/8}, & n \text{ odd, } h_3 \neq 0. \end{cases}$$

Hence Theorem 4.1 holds in this special case, too, completing the proof.

The lemma is proved as follows. If two consecutive terms of (h) vanish, then two consecutive terms of smallest suffix vanish; let them be h_r and h_{r+1} . Then $r \geq 3$, and in the interval $0 < n < r$, not both h_n and h_{n+1} are zero. I say that $h_n \neq 0$ in this interval. For if $r = 3$, h_1 and h_2 are not zero. Assume then that $r > 3$, and $h_k = 0$. Then $2 \leq k \leq r-2$ and by the minimal property of r ,

$$(4.8) \quad h_{k-1}h_{k+1} \neq 0.$$

Now if $k < r/2$, choose l so that $l+k=r$ and take $m=l$ and $n=k$ in (4.11). Since $h_k = h_r = 0$, we obtain $-h_{k-1}h_{k+1}h^2_l = 0$. Hence by (4.8), $h_l = 0$. Now replace l by $l+1$. Since $h_{r+1} = h_k = 0$, we obtain

¹³ It is shown in Chapter VII that this lemma is not necessarily true if both h_2 and h_3 are zero. If, however, (h) is assumed to be a divisibility sequence, the vanishing of h_2 and h_3 entails the vanishing of all subsequent terms.

¹⁴ If $h_2 = 0$, $h_3 = 1$ we obtain the particular periodic solution $h_n = (-8/n)$ mentioned in the Introduction.

$-h_k h_{k+1} h^2_{l+1} = 0$. Hence $h_{l+1} = 0$. But $h_l = h_{l+1} = 0$ contradicts the minimal property of r . Next, if $k = r/2$, we take $l = k + 1$ and find that $h_{k+1} = 0$, contrary to (4.8). If $k > r/2$, we take $k + l = r$ and take $m = k$ and $n = l$ in (4.11), obtaining as before $h_l = 0$. Then replacing l by $l + 1$, we find $h_{l+1} = h_l = 0$ contradicting again the minimal property of r . Hence we may assume

$$(4.9) \quad h_r = 0, \quad h_{r+1} = 0, \quad h_n \neq 0, \quad 0 < n < r.$$

I say that $r = 3$. For if $r > 3$, $h_3 \neq 0$ by (4.9). Hence on taking $m + n = 2r - 3$ and $m - n = 3$ in (4.11), we obtain the relation

$$h_{2r-3} h_3 = h_{r+1} h_{r-1} h^2_{r-3} - h_{r-4} h_{r-2} h^2_r$$

where all the suffices are ≥ 0 . Hence by (4.9), $h_{2r-3} = 0$. But by (4.5) with $n = r - 2$,

$$0 = h_{2r-3} = h_r h^3_{r-2} - h_{r-3} h^3_{r-1} = -h_{r-3} h^3_{r-1}.$$

Hence either h_{r-1} or h_{r-3} is zero, contradicting (4.9).

But if $r = 3$, then $h_2 \neq 0$ but $h_3 = h_4 = 0$ and we find by a brief induction from (4.5) and (4.6) that $h_n = 0$ for $n \geq 3$. This completes the proof of the lemma.

5. An integer m is said to be a divisor of the sequence (h) if it divides some term with positive suffix. If m divides h_ρ but does not divide h_r if r divides ρ , then ρ is called a rank of apparition of m in (h) .

THEOREM 5.1. *An elliptic divisibility sequence admits every prime p as a divisor. Furthermore, p has at least one rank of apparition smaller than $2p + 2$.*

Proof. If none of $h_1, h_2, \dots, h_{p+1}, h_{p+2}$ is divisible by p , each of the p numbers

$$\frac{h_{r-1} h_{r+1}}{h_r^2}, \quad (r = 2, 3, \dots, p+1)$$

is congruent modulo p to one of the numbers $1, 2, \dots, p-1$. Hence at least two are congruent to one another; say

$$\frac{h_{n-1} h_{n+1}}{h_n^2} \equiv \frac{h_{m+1} h_{m-1}}{h_m^2} \equiv c \pmod{p}$$

when $2 \leq n < m \leq p+1$ and c is an integer. But then (4.11) gives the congruence

$$h_{m+n} h_{m-n} \equiv 0 \pmod{p}.$$

Since $m - n < p + 2$ and p is prime, h_{m+n} is divisible by p . Hence the smallest rank of apparition of p is at most $m + n$ and hence less than or equal to $2p + 1$. $2p + 1$ is the best upper bound possible. For if $p = 2$ and $h_0 = 0$, $h_1 = h_2 = h_3 = h_4 = 1$, then $\rho = 5$.

THEOREM 5.2. *Let p be a prime divisor of an elliptic sequence (h) , and let ρ be its smallest rank of apparition. Then if*

$$(5.1) \quad h_{\rho+1} \not\equiv 0 \pmod{p},$$

$$(5.2) \quad h_n \equiv 0 \pmod{p} \text{ if and only if } n \equiv 0 \pmod{\rho}.$$

Proof. By the definition of ρ ,

$$(5.3) \quad h_\rho \equiv 0 \pmod{p}, \quad h_r \not\equiv 0 \pmod{p}, \quad 0 < r < \rho.$$

Since (h) is a divisibility sequence h_ρ divides h_n if ρ divides n . Hence $h_n \equiv 0 \pmod{p}$ if $n \equiv 0 \pmod{\rho}$. We prove the converse by mathematical induction. Assume that (5.2) holds for $n < k$. We can clearly assume that $k \geq \rho + 2$. Consider h_k . If $h_k \not\equiv 0 \pmod{p}$, we cannot have $k \equiv 0 \pmod{\rho}$. Hence (5.2) will then hold for $n < k + 1$. If $h_k \equiv 0 \pmod{p}$, divide k by ρ and let the quotient be q and the remainder r :

$$(5.4) \quad k = q\rho + r, \quad 0 \leq r < \rho.$$

We shall show that the assumption that $r > 0$ in (5.4) leads to a contradiction. (5.2) then immediately follows by mathematical induction on k .

Assume then that $r > 0$ in (5.4). Then taking $m = q\rho$ and $n = r$ in (4.11) $h_{m+n} \equiv h_m \equiv 0$. Hence we obtain the congruence

$$h_{q\rho+1}h_{q\rho-1}h^2r \equiv 0 \pmod{p}.$$

Now $q\rho - 1 < k$ and $q\rho - 1$ is not divisible by ρ . Hence $h_{q\rho-1} \not\equiv 0 \pmod{p}$ by the hypothesis of the induction.

Also $h_r \not\equiv 0 \pmod{p}$ by (5.3). Hence since p is a prime,

$$h_{q\rho+1} \equiv 0 \pmod{p}.$$

If $q = 1$, (5.1) is contradicted. If $q = 2$, then on taking $m = \rho$ in (4.5), we find that $h_{q\rho+1} = h_{\rho+2}h^3\rho - h_{\rho+1}h^3\rho-1$. Hence

$$h_{\rho+1}h^3\rho-1 \equiv 0 \pmod{p}.$$

Since p is a prime, either $h_{\rho+1} \equiv 0 \pmod{p}$ or $h_{\rho-1} \equiv 0 \pmod{p}$, contradicting (5.1) or (5.3). Hence $q > 2$. Now take $m = (q - 1)\rho$ and

$n = \rho + 1$ in (1.2). Then $m - n > 0$ and since $h_{m+n} \equiv h_m \equiv 0 \pmod{p}$, we obtain the congruence

$$h_{(q-1)\rho+1} h_{(q-1)\rho-1} h^2_{\rho+1} \equiv 0 \pmod{p}.$$

But since $0 < (q-1)\rho - 1 < (q-1)\rho + 1 < qp + 1 \leq k$, $h_{(q-1)\rho-1}$, and $h_{(q-1)\rho+1}$ are incongruent to zero modulo p . Hence since p is a prime, $h_{\rho+1} \equiv 0 \pmod{p}$, contradicting (5.1). Hence r must be zero in (5.4), and the proof is complete.

6. The following theorem is a companion to Theorem 5.1.

THEOREM 6.1. *Let p be a prime divisor of an elliptic sequence (h) , and let ρ be its smallest rank of apparition. If*

$$(6.1) \quad h_{\rho+1} \equiv 0 \pmod{p}$$

then $\rho \leq 3$ and

$$(6.2) \quad h_n \equiv 0 \pmod{p}, \quad n \geq \rho.$$

Proof. By definition of ρ ,

$$(6.3) \quad h_\rho \equiv 0 \pmod{p}, \quad h_r \not\equiv 0 \pmod{p}, \quad 0 < r < \rho.$$

We shall show first that the assumption

$$(6.4) \quad \rho > 3$$

leads to a contradiction with (6.1) and (6.3). If (6.4) holds, $h_3 \not\equiv 0 \pmod{p}$. Taking $m + n = 2\rho - 2$ and $m - n = 3$ in (4.11), we obtain the relation

$$h_{2\rho-3} h_3 = h_{\rho+1} h_{\rho-1} h^2_{\rho-3} - h_{\rho-4} h_{\rho-2} h^2_{\rho}$$

where all the suffixes are ≥ 0 by (6.4). Thus since p is a prime,

$$h_{2\rho-3} \equiv 0 \pmod{p}.$$

Now taking $n = \rho - 2$ in the relation (4.5), we find that $h_{2\rho-3} = h_\rho h^2_{\rho-2} - h_{\rho-3} h^2_{\rho-1}$. Hence $h_{\rho-3} h^2_{\rho-1} \equiv 0 \pmod{p}$. Since p is a prime, either $h_{\rho-1}$ or $h_{\rho-3}$ is divisible by p contrary to (6.3). Hence $\rho \leq 3$. If $\rho = 2$, $h_{2n} \equiv 0 \pmod{p}$ since h_2 divides h_{2n} . Since $h_3 = 0$ by (6.1), $h_5 \equiv 0 \pmod{p}$ with $n = 2$. It is now easy to prove by induction from (4.5) that $h_{2n+1} \equiv 0 \pmod{p}$. Hence if $\rho = 2$, $h_n \equiv 0 \pmod{p}$, for $n \geq \rho$.

If $\rho = 3$, $h_2 \not\equiv 0 \pmod{p}$ and we easily prove from (4.5), (4.6) and $h_3 \equiv h_4 \equiv 0 \pmod{p}$ that $h_n \equiv 0 \pmod{p}$ for $n \geq 3$. This completes the proof of the theorem.

The following two theorems follow directly from Theorems 5.1 and 6.1.

THEOREM 6.2. *A necessary and sufficient condition that a prime p have exactly one rank of apparition in an elliptic sequence (h) is that p is not a common divisor of h_3 and h_4 .*¹⁵

THEOREM 6.3. *A necessary and sufficient condition that every prime have precisely one rank of apparition in an elliptic sequence (h) is that h_3 and h_4 have no common factor.*

The following theorem now follows from a known result: (Ward [3])

THEOREM 6.4. *If (h) is an elliptic sequence in which the initial values h_3 and h_4 are co-prime, then $(h_n, h_m) = h_{(m,n)}$.*

III. The Numerical Periodicity and Symmetry Modulo p of Sequences.

7. A sequence (s) of rational integers is said to be numerically periodic modulo m if there exists a positive integer π such that

$$(7.1) \quad s_{n+\pi} \equiv s_n \pmod{m}$$

for all sufficiently large n . If (7.1) holds for all n , then (s) is said to be purely periodic modulo m . The smallest such integer π for which (7.1) is true is called the period of (h) modulo m . All other periods are multiples of it.

We shall show in this chapter that any elliptic sequence is numerically periodic for any prime modulus and purely periodic for all primes which do not divide both h_3 and h_4 . The culminating result is the following theorem which shows precisely how the period and rank are connected.

THEOREM 11.1. *Let (h) be an elliptic divisibility sequence and p an odd prime whose rank of apparition ρ is greater than three. Let e be an integral solution of the congruence*

$$(11.1) \quad e \equiv h_2/h_{\rho-2} \pmod{p},$$

and let ϵ and κ be the exponents to which e and $h_{\rho-1}$ respectively belong modulo p . Then (h) is purely periodic modulo p , and its period π is given by the formula $\pi = \pi\rho$ where

$$(7.11) \quad \tau = 2^\kappa [\epsilon, \kappa].$$

¹⁵ Since h_2 divides h_4 , a common divisor of h_2 and h_3 is a common divisor of h_3 and h_4 .

Here $[\epsilon, \kappa]$ is the least common multiple of ϵ and κ and the exponent α is determined as follows:

$\alpha = +1$ if and only if ϵ, κ are both odd,

$\alpha = -1$ if and only if ϵ, κ are both even and both divisible by precisely the same power of 2;

$\alpha = 0$ in all other cases.

I have been unable to establish the numerical periodicity of (h) sequences by elementary means; that is, without the use of their elliptic function representation. It turns out that the two invariants g_2 and g_3 of the elliptic function associated with this representation are each expressible as a polynomial in h_2, h_3 and h_4 with integral coefficients divided by a product of powers of h_2, h_3 , two and three.¹⁶ The arithmetical consequences of the elliptic function representation do not therefore apply to the primes two and three, or more generally to any prime dividing h_2 or h_3 . We shall begin by discussing these exceptional primes.

There are eight *a priori* possible types of elliptic sequences modulo two distinguished by the possible residues of h_2, h_3 and h_4 modulo two. But since h_2 divides h_4 , sequences with $h_2 \equiv 0 \pmod{2}$ and $h_4 \equiv 1 \pmod{2}$ cannot occur. The six possibilities which are left are listed in the following table.

ELLIPTIC SEQUENCES MODULO TWO

Type Number	Residues of h_i modulo two						Rank ρ	Period π
	h_0	h_1	h_2	h_3	h_4	h_5		
1	0	1	0	0	0	0	2	1
2	0	1	1	0	0	0	3	1
3	0	1	0	1	0	1	2	2
4	0	1	1	0	1	1	3	3
5	0	1	1	1	0	1	4	4
6	0	1	1	1	1	0	5	5

Theorem 11.1 however is not true for the two types five and six for which ρ is greater than three. In both cases $\epsilon = \kappa = 1$ so that the formula (7.11) gives $\pi = 2\rho$ instead of $\pi = \rho$. Thus the restriction to odd primes is necessary.

The twenty-one possible types of sequences modulo three are listed below. In each case when the rank ρ is greater than three, ϵ and κ are listed and also the multiplier $\tau = 2^\alpha [\epsilon, \kappa]$. The ranks and periods were obtained by direct computation for each type from the formulas (4.5) and (4.6) taken modulo three. The table thus shows that Theorem 11.1 is true if $p = 3$.

¹⁶ See Chapter IV, Section 13, formulas (13.6) and (13.7).

ELLIPTIC SEQUENCES MODULO THREE

Type No.	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	Rank	Period	Exponents ϵ	κ	τ
1	0	1	0	0	0											2	1			
2	0	1	1	0	0											3	1			
3	0	1	2	0	0											3	1			
4	0	1	0	1	0	2	0	2								2	8			
5	0	1	0	2	0	1	0	2								2	4			
6	0	1	1	0	1	1	0	2	2	0	2	2				3	12			
7	0	1	1	0	2	2										3	6			
8	0	1	2	0	1	2										3	3			
9	0	1	2	0	2	1	0	2	1	0	1	2				3	12			
10	0	1	1	1	0	2	2	2								4	8	1	1	2
11	0	1	1	1	1	0	2	2	2	2						5	10	1	1	2
12	0	1	1	1	2	1	0	2	1	2	2	2				6	12	2	1	2
13	0	1	1	2	0	1	2	2								4	8	1	2	2
14	0	1	1	2	1	2	2	0	1	1	2	1	2	2		7	7	2	2	1
15	0	1	2	2	2	2	1	0	2	1	1	1	1	2		7	14	1	1	2
16	0	1	1	1	2	2	0									5	5	2	2	1
17	0	1	2	1	0	2	1	2								4	8	1	1	2
18	0	1	2	1	1	0	2	2	2	1	1					6	12	2	1	2
19	0	1	2	1	2	0										5	5	2	2	1
20	0	1	2	2	0	1	1	2								4	8	1	2	2
21	0	1	2	2	1	0	2	1	1	2	2					5	10	1	1	2

This table affords simple illustrations of the modular symmetry of sequences which was alluded to in the introduction. For example, consider type 14 and 15. For type 14, we have $h_{p-n} \equiv -h_n \pmod{3}$. For type 15, $h_{p-n} \equiv h_n \pmod{3}$; $h_{p+n} \equiv h_{p-n} \pmod{3}$. We shall see that for primes other than two and three, the origin of this symmetry is the periodicity of the second kind of the elliptic sigma functions.

Now consider primes which divide the initial values h_2 and h_3 . We have shown in Section 6 that primes which divide both h_3 and h_4 divide every subsequent term of (h) . We call such primes "null divisors" of (h) .¹⁷ If p is a null divisor, then (h) is numerically periodic modulo p with the period one.¹⁸ Since h_2 divides h_4 , primes which divide both h_2 and h_3 are

¹⁷ The terminology is borrowed from the theory of linear divisibility sequences. See Ward [2].

¹⁸ The first types listed in the tables of elliptic sequences modulo two and modulo three afford simple illustrations. If (h) is a null sequence modulo p , it appears to be very difficult to specify the exact power of p dividing h_n given only the initial values of (h) .

also null divisors. On excluding null divisors, we have as well as the “general case”

$$(7.3) \quad h_2 h_3 \not\equiv 0 \pmod{p},$$

two special cases:

$$(7.3) \quad h_2 \equiv 0 \pmod{p}, \quad h_3 \not\equiv 0 \pmod{p};$$

$$(7.4) \quad h_3 \equiv 0 \pmod{p}, \quad h_2 \not\equiv 0 \pmod{p}.$$

These cases are disposed of by the following theorem which is a simple consequence of the theorems on special sequences given in Chapter VII.

THEOREM 7.1. *If condition (7.3) holds, then*

$$h_{2n} \equiv 0 \pmod{p}, \quad h_{2n+1} \equiv (-1)^{\lfloor n/4 \rfloor} h_3^{(n^2-1)/8} \pmod{p}.$$

If condition (7.4) holds, then

$$h_{3n} \equiv 0 \pmod{p},$$

$$h_{3n+1} \equiv (-1)^{n(n-1)/2} h_2^{n(n-1)/2} h_4^{n(n+1)/2} \pmod{p},$$

$$h_{3n+2} \equiv -(-1)^{n(n+1)/2} h_2^{n(n+1)/2} h_4^{n(n-1)/2} \pmod{p}.$$

We see that in either case (h) is purely periodic modulo p . Its period depends in a simple way on the exponents to which its initial values belong modulo p .

8. The general case depends upon the following theorem which is proved in Chapter V, by the use of elliptic functions. All further developments in this chapter are obtained from this theorem by elementary means.

THEOREM 8.1. *Let p be a prime greater than three¹⁹ which divides neither h_2 nor h_3 . Then if ρ is its rank of apparition there exist two integers a and b such that*

$$(8.1) \quad h_{\rho-n} \equiv a^n b h_n \pmod{p}, \quad (n = 0, 1, 2, \dots, \rho).$$

If we calculate successively the least positive residues modulo p of the first ρ terms of (h) , the theorem states that there is a certain symmetry in the distribution of these residues. The theorems which follow not only lead to the proof of the periodicity of (h) modulo p , but also state symmetries in the pattern of least positive residues of successive blocks of ρ terms of (h) . The final result of these symmetries is to determine the residues modulo p of

¹⁹ The table of sequences modulo three shows that this theorem is also true if $p = 3$.

all terms of (h) in terms of the integers a and b of the theorem and the residues of the first $[\rho/2]$ terms. The next theorem shows how a and b may be determined modulo p .

THEOREM 8.2. *If a and b are the integers specified in Theorem 8.1 and if c is determined by the congruence*

$$(8.2) \quad ac \equiv 1 \pmod{p}$$

then the following congruences hold modulo p :

$$(8.3) \quad a \equiv h_{\rho-2}/h_2 h_{\rho-1}; \quad b \equiv h_2 h^2_{\rho-1}/h_{\rho-2}; \quad b \equiv h_{\rho-1} c.$$

$$(8.4) \quad a^\rho b^2 \equiv 1; \quad c^\rho \equiv b^2.$$

$$(8.5) \quad a^2 \equiv -h_{\rho-1}/h_{\rho+1}; \quad b^2 \equiv -h_{\rho+1} h_{\rho-1}.$$

Proof. Let n successively equal 1 and $\rho - 1$, in (8.1). We obtain:

$$(8.6) \quad h_{\rho-1} \equiv ab \pmod{p}$$

and ²⁰ $1 \equiv h_1 \equiv a^{\rho+1} b h_{\rho-1} \equiv a^\rho b^2$. (8.4) now follows and (8.6) and (8.2) imply that $b \equiv h_{\rho-1} c$ which is the last part of (8.3).

Next, put n equal to two in (8.1). Then

$$h_{\rho-2} \equiv a^2 b h_2 \equiv ah_{\rho-1}h_2 \pmod{p},$$

the last step following from (8.6). This result is equivalent to the first part of (8.3). The second part follows now by (8.6). It remains to prove (8.5). Consider $h_{\rho+1}$. Assume first that ρ is odd:

$$(8.7) \quad \rho = 2\sigma + 1 \geq 5.$$

Then on putting n equal to $\sigma + 1$ and σ in (4.6), we obtain

$$(8.8) \quad h_{\rho+1} = h_{\sigma+1} h_{\sigma+3} h^2_\sigma \cdots h_{\sigma+1} h_{\sigma-1} h^2_{\sigma+2},$$

$$(8.9) \quad h_{\rho-1} = h_\sigma h_{\sigma+2} h^2_{\sigma-1} \cdots h_\sigma h_{\sigma-2} h^2_{\sigma+1}.$$

But by (8.1) and (8.7), the following congruences hold modulo p :

$$h_{\sigma+1} \equiv a^\sigma b h_\sigma; \quad h_{\sigma+3} \equiv a^{\sigma-2} b h_{\sigma-2}; \quad h_\sigma \equiv a^{\sigma+1} b h_{\sigma+1};$$

$$h_{\sigma-1} \equiv a^{\sigma+1} b h_{\sigma+1}; \quad h_{\sigma+2} \equiv a^{\sigma-1} b h_{\sigma-1}.$$

²⁰ The modulus p will be omitted here and elsewhere when no confusion can arise.

On substituting these expressions into (8.8) and simplifying, (8.9) gives the congruence

$$(8.10) \quad h_{\rho+1} \equiv -a^{2\rho-2}b^4h_{\rho-1} \pmod{p}.$$

When ρ is even, this congruence may be shown to hold in essentially the same way.

Now by (8.2) and (8.4) Theorem 8.2, $a^{2\rho}b^4 \equiv 1 \pmod{p}$. Hence (8.10) implies that $h_{\rho+1} \equiv -a^{-2}h_{\rho-1} \pmod{p}$, and this congruence is equivalent to the first part of (8.5). The second part of (8.5) now follows by (8.6), completing the proof.

9. The theorems of this section give the fundamental symmetries of (h) modulo p .

LEMMA 9.1. *With the notation of Theorems (8.1) and (8.2), the following congruence is valid for all positive integers n :*

$$(9.1) \quad h_{\rho+n} \equiv -bc^n h_n \pmod{p}.$$

Proof. Assume first that $0 \leq n \leq \rho$. Since

$$h_{\rho+n}h_{\rho-n} = h_{\rho+1}h_{\rho-1}h_n^2 - h_{n+1}h_{n-1}h_\rho^2$$

and p divides h_ρ , we obtain from (8.5) the congruence $h_{\rho+n}h_{\rho-n} \equiv -b^2h_n^2 \pmod{p}$ or by (8.1), $h_{\rho+n}a^n b h_n \equiv -b^2h_n^2 \pmod{p}$. If $0 < n < \rho$, we may cancel bh_n . We then obtain (9.1) on multiplying by c^n . Since the cases $n = 0$ and $n = \rho$ are trivially satisfied, (9.1) is true for $0 \leq n \leq k\rho$ if k equals one.

We now proceed by induction on k . Suppose that (9.1) is true for $0 \leq n \leq k\rho$ and assume that $k\rho \leq n \leq (k+1)\rho$. Then since

$$h_{n+\rho}h_{n-\rho} = h_{n+1}h_{n-1}h_\rho^2 - h_{\rho+1}h_{\rho-1}h_n^2$$

and p divides h_ρ , we obtain from (8.5) the congruence

$$(9.2) \quad h_{n+\rho}h_{n-\rho} \equiv b^2h_n^2 \pmod{p}.$$

Now $0 \leq n - \rho \leq k\rho$. Hence by the hypothesis of the induction,

$$(9.3) \quad h_{n-\rho} \equiv -(a^{n-\rho}/b)h_n \pmod{p}.$$

Hence if $k\rho < n < (k+1)\rho$, (9.2) and (9.3) give the congruence $b^3h_n \equiv a^{n-\rho}h_{\rho+n} \pmod{p}$. Since $a^\rho b^2 \equiv 1$ by (8.4) and $a^n c^n \equiv 1$ by (8.1), this last congruence gives (9.1) on multiplication by $a^\rho c^n$. Since (9.1) holds

trivially for $n = k\rho$ or $n = (k + 1)\rho$, and has been proven true for $0 \leq n \leq \rho$, the induction is completed.

THEOREM 9.2. *Under the hypothesis of Lemma (9.1),*

$$(9.5) \quad h_{k\rho+n} \equiv (-1)^k c^{kn} b^{k^2} h_n \pmod{p}, \quad (k, n = 0, 1, 2, \dots).$$

Proof. (9.5) is true when $k = 1$ by Lemma 9.1. Its general validity follows directly by a brief induction on k .

10. We can now establish the numerical periodicity of (h) modulo p .²¹

THEOREM 10.1. *Let (h) be an elliptic divisibility sequence, and let p be any prime which divides neither h_2 nor h_3 . Let ρ be the rank of apparition of p in (h) , and let τ be the least positive integer such that*

$$(10.1) \quad (-b)^{\tau^2} \equiv 1, \quad c^\tau \equiv 1 \pmod{p}$$

when b and c are the integers specified in Theorems 8.1 and 8.2. Then (h) is purely periodic modulo p with period $\tau\rho$.

Proof. The proof of this theorem depends on the following lemma whose proof is left to the reader.

LEMMA 10.1. *If τ is defined as in Theorem 10.1 and if k is an integer such that*

$$(10.2) \quad (-b)^{k^2} \equiv 1, \quad c^k \equiv 1 \pmod{p}$$

then τ divides k .

We see from (10.1) and the congruence (9.5) of Theorem 9.1 that $\tau\rho$ is a period of (h) and (h) is purely periodic modulo p . Hence by Theorem 5.2, any other period π of (h) modulo p is a multiple of ρ ; say $\pi = k\rho$. But if $k\rho$ is a period, then on taking n equal to 1 and 2 in (9.5), we obtain the congruences

$$(-c)^{k^2} \equiv 1, \quad (-c)^k c^k b^{k^2} \equiv 1 \pmod{p}.$$

Since k and k^2 have the same parity, (10.2) follows. Hence, τ divides k , so that $\tau\rho$ divides π . This completes the proof of the theorem.

11. This section is devoted to the proof of the Theorem 11.1 quoted in Section 7 in which the integer τ was explicitly determined. We shall need the following arithmetical lemma whose proof we leave to the reader.

²¹ Periodicity for an arbitrary modulus m is an easy consequence. See Chapter VIII.

LEMMA 11.1. *Let p be an odd prime,²² d an integer prime to it, and belonging to the exponent δ modulo p . Then if δ is odd, there exists no integer x such that the congruence*

$$(11.2) \quad d^x \equiv -1 \pmod{p}$$

is satisfied. But if δ is even, (11.2) is satisfied if and only if x is an odd multiple of δ .

We observe first that the congruences (11.1) and (8.3) allow us to identify the integers c of Theorems 11.1 and 8.2. Since p is a prime, the congruence (8.4) implies that b is congruent to either plus or minus one. Assume that

$$(11.3) \quad b^\tau \equiv +1 \pmod{p}.$$

Then by (10.1), $(-b)^{\tau^2} \equiv (-1)^\tau \equiv 1 \pmod{p}$. Hence τ must be even. Now by (8.3), $b^\tau \equiv h^{\tau_{p-1}} c^\tau$. Since $c^\tau \equiv 1$ by (10.1), (11.3) gives

$$(11.4) \quad h^{\tau_{p-1}} \equiv 1 \pmod{p}.$$

Then by (11.1), (10.1),

$$(11.5) \quad e^\tau \equiv 1 \pmod{p}.$$

Let $\sigma = [\epsilon, \kappa]$ be the least common multiple of the exponents to which e and h_{p-1} belong modulo p . Then (11.4) and (11.5) imply that $\kappa \mid \tau$, $\epsilon \mid \tau$. Hence

$$(11.6) \quad \sigma \mid \tau.$$

On the other hand, $h^{\sigma_{p-1}} \equiv 1$ and $e^\sigma \equiv 1 \pmod{p}$. Hence by (11.1) and (8.3),

$$(11.7) \quad c^\sigma \equiv 1, \quad b^\sigma \equiv 1 \pmod{p}.$$

Now if σ is even, (11.7) implies that $c^\sigma \equiv 1$, $(-b)^\sigma \equiv 1 \pmod{p}$. Hence by Lemma 10.1, $\tau \mid \sigma$, so that by (11.6), $\tau = \sigma$.

σ is odd if and only if both ϵ and κ are odd. In this case (11.7) implies that $c^{2\sigma} \equiv 1$, $(-b)^{4\sigma} \equiv 1 \pmod{p}$. Hence by Lemma 10.1, $\tau \mid 2\sigma$. But τ is even and by (11.6), σ divides τ . Hence $\tau = 2\sigma$. This disposes of the first case of the theorem.

Assume now that

$$(11.8) \quad b^\tau \equiv -1 \pmod{p}.$$

Then by (8.3),

²² The lemma is false if $p = 2$.

$$(11.9) \quad h^{\tau_{p-1}} \equiv -1 \pmod{p},$$

and by (8.3) and (11.1)

$$(11.10) \quad e^{\tau} \equiv -1 \pmod{p}.$$

Now by Lemma 11.1, (11.9) and (11.10) imply that both κ and ϵ are even, and that τ is both an odd multiple of $\kappa/2$ and an odd multiple of $\epsilon/2$. But if σ now denotes $[\epsilon/2, \kappa/2]$,

$$(11.11) \quad \sigma \mid \tau.$$

Hence σ must be an odd multiple of both $\epsilon/2$ and $\kappa/2$. It follows that if (11.8) holds, both ϵ and κ must be even and both divisible by precisely the same power of two.

Assume, conversely, that the last mentioned conditions are satisfied. Then σ is an odd multiple of both $\epsilon/2$ and $\kappa/2$, so that by Lemma 11.1

$$h^{\sigma_{p-1}} \equiv -1, \quad e^{\sigma} \equiv -1 \pmod{p}.$$

But then by (11.1), (8.3) and (8.8)

$$c^{\sigma} \equiv 1, \quad b^{\sigma} \equiv -1 \pmod{p}.$$

Hence $(-b)^{\sigma^2} \equiv (-1)^{\sigma^2+\sigma} + 1$. Therefore by Lemma 10.1, $\tau \mid \sigma$. Hence by (11.11) $\tau = \sigma$. This completes the proof.

IV. The Representation of Elliptic Sequences by Elliptic Functions.

12. If (h) is a proper elliptic divisibility sequence, we have seen that if either h_2 or h_3 vanishes, the general term of the sequence becomes a simple product of powers, and the arithmetical properties of the sequence are patent. Consider now a general elliptic divisibility sequence so that the first five values of (h) are integers and

$$(12.0) \quad h_0 = 0, \quad h_1 = 1, \quad h_2 h_3 \neq 0; \quad h_2 \mid h_4.$$

We shall devote this chapter to the proof of the following fundamental result.

THEOREM 12.1. *If (h) is a general elliptic divisibility sequence, there exist two rational numbers g_2 and g_3 and a complex constant u such that if $\varphi(w; g_2, g_3)$ is the Weierstrass function with invariants g_2 and g_3 , then*

$$(12.1) \quad h_n = \psi_n(u) = \sigma(nu)/\sigma(u)^n.$$

Here $\sigma(w)$ is the Weierstrass sigma function.

Proof. Let (h) be a general elliptic divisibility sequence. Since $\psi_n(w)$ is always a solution of (1.1) and $\psi_0(w) = 0$, $\psi_1(w) = 1$, it suffices to show that we can determine g_2 , g_3 and u so that:

$$(12.2) \quad (\alpha) : \psi_2(u) = h_2; \quad (\beta) : \psi_3(u) = h_3; \quad (\gamma) : \psi_4(u) = h_4.$$

We quote for reference eight familiar formulas of elliptic function theory:

$$(12.3) \quad \psi_2(w) = -\wp'(w).$$

$$(12.4) \quad \psi_3(w) = 3\wp^4(w) - \frac{3}{2}g_2\wp^2(w) - 3g_3\wp(w) - \frac{1}{16}g_2^2.$$

$$(12.5) \quad \wp(2w) - \wp(w) = \frac{1}{4} \left(\frac{\wp''(w)}{\wp'(w)} \right)^2 - 3\wp(w)$$

$$(12.6) \quad \wp(3w) - \wp(w) = \wp'^2(w) (\wp'^4(w) - \psi_3(w)\wp''(w)) \div \psi_3^2(w).$$

$$(12.7) \quad \wp(2w) - \wp(w) = -\frac{\psi_1(w)\psi_3(w)}{\psi_2^2(w)}.$$

$$(12.8) \quad \wp(3w) - \wp(w) = -\frac{\psi_2(w)\psi_4(w)}{\psi_3^2(w)}.$$

$$(12.9) \quad \wp'^2(w) = 4\wp^3(w) - g_2\wp(w) - g_3.$$

$$(12.10) \quad \wp''(w) = 6\wp^2(w) - g_2/2.$$

From (12.10):

$$(12.11) \quad g_2 = 12\wp^2(w) - 2\wp''(w).$$

From (12.9) and (12.10):

$$(12.12) \quad g_3 = 2\wp(w) (\wp''(w) - 4\wp^2(w) - \wp'^2(w)).$$

13. Proof (Continued). Now assume that the conditions (12.2) (α), (β), (γ) can be satisfied. Then since $\psi_1(u) = 1$, (12.1), (12.3), (12.7) and (12.8) give:

$$(13.1) \quad \wp'(u) = -h_2,$$

$$(13.2) \quad \wp(2u) - \wp(u) = -h_3/h_2^2,$$

$$(13.3) \quad \wp(3u) - \wp(u) = -h_2h_4/h_3^2.$$

Now by (12.6), (13.3) and (13.1):

$$-h_2h_4/h_3^2 = h_2^2/h_3^2(h_2^4 - h_3\wp''(u)).$$

Hence solving for $\varphi''(u)$:

$$(13.4) \quad \varphi''(u) = (h_2^5 + h_4)/h_2 h_3.$$

Next, using (13.2), (12.5) and (13.1), (13.4):

$$-h_3/h_2^2 = \frac{1}{4} \{ (h_2^5 + h_4)/-h_2^2 h_3 \}^2 - 3\varphi(u).$$

Hence solving for $\varphi(u)$:

$$(13.5) \quad \varphi(u) = (h_4^2 + 2h_2^5 h_4 + 4h_2^2 h_3^3 + h_2^{10}) \div 12h_2^4 h_3^2.$$

Next, using (12.11), (13.5) and (13.4):

$$(13.6) \quad g_2 = (h_2^{20} + 4h_2^{15} h_4 - 16h_2^{12} h_3^3 + 6h_2^{10} h_4^2 - 8h_2^7 h_3^3 h_4 \\ + 4h_2^5 h_4^3 + 16h_2^4 h_3^6 + 8h_2^2 h_3^3 h_4^2 + h_4^4) \div 12h_2^8 h_3^4.$$

Finally, using (12.12), (13.5), (13.4) and (13.6):

$$(13.7) \quad g_3 = -(h_2^{30} + 6h_2^{25} h_4 - 24h_2^{22} h_3^3 + 15h_2^{20} h_4^2 - 60h_2^{17} h_3^3 h_4 \\ + 20h_2^{15} h_4^3 + 120h_2^{14} h_3^6 - 36h_2^{12} h_3^3 h_4^2 + 15h_2^{10} h_4^4 \\ - 48h_2^9 h_3^6 h_4 + 12h_2^7 h_3^3 h_4^3 + 64h_2^6 h_3^9 + 6h_2^5 h_4^5 \\ + 48h_2^4 h_3^6 h_4^2 + 12h_2^2 h_3^3 h_4^4 + h_4^6) \div 216h_2^{12} h_3^6.$$

(13.5), (13.6) and (13.7) are *necessary* conditions that the equations (12.2) hold. Now since by (12.1) neither h_2 nor h_3 is zero, we can start by defining g_2 , g_3 and u (13.6), (13.7) and (13.5). Then u is determined save for sign up to a period of $\varphi(u)$.

On combining (13.5) and (13.6), we find that

$$g_2 - 12\varphi^2(u) = -2(h_2^5 + h_4)/h_2 h_3.$$

Hence (13.4) follows from formula (12.11).

Now combining (13.7) with (13.5), (13.4) and (13.6), we obtain the formula

$$g_3 - 2\varphi(u) [\varphi''(u) - 4\varphi^2(u)] = -h_2^2.$$

Hence by formula (12.12), $\varphi'^2(u) = h_2^2$. We now choose the sign of u so that (13.1) is satisfied. u is now fixed up to a period of the φ function. But then (12.2) α follows immediately from formula (12.3).

Next, using (12.5) and substituting in it for $\varphi'(u)$, $\varphi''(u)$ and $\varphi(u)$ from (13.1), (13.4) and (13.5), we find that $\varphi(2u) - \varphi(u) = -h_3/h_2^2$.

Hence (12.2) β follows from (12.7), (12.2) and the fact that $\psi_1(u) = 1$.

Finally on substituting on the right of (12.6) for $p'(u)$, $p''(u)$ and $\psi_3(u)$, we find that $\varphi(3u) - \varphi(u) = -h_2h_4/h_3^2$.

Hence (12.2) γ follows from (12.8) and (12.2) α and β .

V. The Relationship Between the Numerical Periodicity of a Sequence and the Periodicity of the Corresponding Elliptic Functions.

14. We shall now prove Theorem 8.1 of Chapter III. Throughout this part of the paper, (h) denotes a fixed general elliptic sequence, and p a fixed prime greater than three dividing neither h_2 nor h_3 . For convenience of printing, the rank of apparition of p in (h) will be denoted by r , rather than by ρ as heretofore.

It follows from the results of Part IV that

$$(14.1) \quad h_n = \psi_n(u).$$

Furthermore g_2 , g_3 and $\varphi(u)$ are integers modulo p .

We commence by stating the results of elliptic function theory which we shall need.²³ If we regard w in $\psi_n(w)$ as a complex variable, $\psi_n(w)$ may be expressed in terms of the Weierstrass sigma function as follows:

$$(14.2) \quad \psi_n(w) = \sigma(nw)/\sigma(w)^{n^2}.$$

If 2ω is a period of the φ function, then with the usual notations of the theory of elliptic functions,

$$(14.3) \quad \sigma(w + 2\omega) = -e^{2\eta(w+\omega)}\sigma(w).$$

On the other hand, if $z = \varphi(w)$, $\psi_n(w)$ may be expressed as a polynomial in z , say $F_n(z)$, of the form

$$(14.4) \quad \psi_n(w) = F_n(z) = e_q \sum_{r=0}^q A_{q-r} z^r$$

where the degree q of $F_n(z)$ in z is $(n^2 - 1)/2$ or $(n^2 - 4)/2$, and e_q is 1 or $h_2/2$ according as n is odd or even. The coefficients A of $F_n(z)$ are polynomials in $g_2/4$ and g_3 with rational integral coefficients:

$$(14.5) \quad A_k = A_k(g_2/4, g_3), \quad k = 0, 1, \dots, q.$$

Hence each A_k is an integer modulo p . Furthermore A_k is homogeneous of degree k if g_2 is given the weight two and g_3 the weight three. In particular,

²³ See Fricke, *Die Elliptischen Funktionen . . . II*, Berlin, 1922, pp. 184-205.

$$(14.6) \quad A_0 = n,$$

$$(14.7) \quad A_1 = 0, \quad A_2 = bg_2/4, \quad A_3 = cg_3, \quad A_4 = dg_2^2/16$$

where b, c, d are integers depending of course on n .

It is also well known that if we consider the roots ζ of $F_r(z) = 0$ (where it will be recalled that r is the rank of apparition of p in (h)) then each ζ may be expressed in the form

$$(14.8) \quad \zeta = \varphi(2\omega/r)$$

where 2ω is some period of the φ function.

15. Let \mathfrak{R} denote the field obtained by adjoining all the roots of $F_r(z) = 0$ to the field of rationals, and let \mathfrak{p} denote any prime ideal divisor of p in \mathfrak{R} . By Theorem 5.1, the rank of apparition r of p is less than $2p + 2$. Hence either r is prime to p , or $r = p$, or $r = 2p$.

We shall assume that r is prime to p in this section. It follows from the results on $F_n(z)$ stated in the previous section, that all the roots ζ of $F_r(z) = 0$ are algebraic integers modulo p and that we have the congruence

$$h_r \equiv c_r \prod_{(\mathfrak{P})} (\varphi(u) - \zeta) \pmod{p}$$

where c_r is an integer prime to p . But by the definition of r , h_r is divisible by p . Hence we have the congruence in \mathfrak{R} : $\prod_{(\mathfrak{P})} (\varphi(u) - \zeta) \equiv 0 \pmod{\mathfrak{p}}$. Since \mathfrak{p} is a prime ideal, there must exist by (14.8) a period 2ω of the φ function such that

$$(15.1) \quad \varphi(u) \equiv \varphi(2\omega/r) \pmod{\mathfrak{p}}.$$

We deduce from (14.4) and (14.1) that

$$(15.2) \quad h_n \equiv \psi_n(2\omega/r) \pmod{\mathfrak{p}}$$

for $n = 0, 1, 2, \dots$

Consider now $\psi_{r-n}(2\omega/r)$ where $0 \leq n \leq r$. By formulas (14.2) and (14.3);

$$\begin{aligned} \psi_{r-n}(2\omega/r) &= \sigma(-2n\omega/r + 2\omega) \div \sigma(2\omega/r)^{r^2-2rn+n^2} \\ &= \alpha^n \beta \sigma(2n\omega/r) \div \sigma(2\omega/r)^n = \alpha^n \beta \psi_n(2\omega/r). \end{aligned}$$

Here $\alpha = e^{4\pi i \omega/r} \sigma(2\omega/r)^{2r}$, and $\beta = e^{2\pi i \omega} \div \sigma(2\omega/r)^{r^2}$, and we have used the fact that $\sigma(-w) = -\sigma(w)$. (15.2) now gives the congruences

$$(15.3) \quad h_{r-n} \equiv \alpha^n \beta h_n \pmod{\mathfrak{p}}.$$

Letting n equal one and two in (15.3), we see that $\alpha\beta$ and $\alpha^2\beta$ are congruent to rational integers modulo \mathfrak{p} . Hence α and β are congruent modulo \mathfrak{p} to two rational integers; say a and b . Thus (15.3) becomes

$$h_{r-n} \equiv a^n b h_n \pmod{\mathfrak{p}}.$$

Since all the Roman letters denote rational integers, we deduce that

$$h_{r-n} \equiv a^n b h_n \pmod{p}.$$

On replacing r by p , we obtain Theorem 8.1 for the case when the rank of apparition of the prime p is not p or $2p$.

16. It remains to discuss the more difficult case, when the rank of apparition r of p equals p or $2p$. It follows from the form of the coefficients A_k of $F_r(z)$, that if p divides both g_2 and g_3 , it divides every coefficient of $F_r(z)$. The converse is also true.

LEMMA 16.1. *A necessary and sufficient condition that p divide every coefficient of $F_p(z)$ or $F_{2p}(z)$ is that p divide both g_2 and g_3 . The rank of apparition of every such prime is p .*

Proof. We need only prove the necessity of the condition. Assume that $r = p$ and

$$A_k \equiv 0 \pmod{p}, \quad k = 0, 1, \dots, q = (p^2 - 1)/2.$$

Let \mathcal{G} denote the Galois field obtained by adjoining to the field of rationals the three roots e, e_2, e_3 of $4x^3 - g_2x - g_3 = 0$. Then with the usual notation, $e_i = \rho(\omega_i)$, ($i = 1, 2, 3$) where $2\omega_i$ is a period and $\omega_1 + \omega_2 + \omega_3 = 0$. The numbers e_i are integers modulo p since p is odd. Now let \mathfrak{p} be any prime ideal divisor of p in \mathcal{G} . Then by (14.2), (14.4) and our hypothesis on the A_h ,

$$(16.1) \quad \sigma(p\omega_i)/\sigma(\omega_i)^{p^2} = \psi_p(\omega_i) = e_q \sum_{r=0}^q A_{q-r} e_i^r \equiv 0 \pmod{p}.$$

On the other hand on writing $p = (2p - 1)/2 + 1$ and using the periodicity of the sigma function,

$$\sigma(p\omega_i) = (-1)^{(p-1)/2} e^{2\eta(p-1)/2(\omega_i + [(p-1)/2]\omega_i)} \sigma(\omega_i).$$

But

$$e^{2\eta\omega_i} = (e_i - e_j)^{1/4} (e_i - e_k)^{1/4} \sigma(\omega_i).$$

Hence

$$\sigma(p\omega_i) = (e_i - e_j)^{(p^2-1)/4} (e_i - e_k)^{(p^2-1)/4} \sigma(\omega_i)^{p^2}.$$

so that

$$\psi_p(\omega_i) = (e_i - e_j)^{(p^2-1)/4} (e_i - e_k)^{(p^2-1)/4}.$$

Hence by (16.1),

$$(e_i - e_j)^{(p^2-1)/4} (e_i - e_k)^{(p^2-1)/4} \equiv 0 \pmod{p}, \quad i, j, k = 1, 2, 3, i \neq j, i \neq k.$$

Since p is a prime ideal, we deduce that $e_1 \equiv e_2 \equiv e_3 \pmod{p}$. But then for every integer ξ of \mathcal{G} , $4\xi^3 - g_2\xi - g_3 \equiv 4(\xi - e_1)^3 \pmod{p}$. Hence

$$e_1 \equiv e_2 \equiv e_3 \pmod{p} \text{ so that } g_2 \equiv g_3 \equiv 0 \pmod{p}.$$

Since g_2 and g_3 are rational integers modulo p , it follows that $g_2 \equiv g_3 \equiv 0 \pmod{p}$. This completes the proof of the lemma for the case when $r = p$. The proof for the case when all the coefficients of $\psi_{2p}(w)$ are divisible by p is similar and will be omitted here.

17. In view of Lemma 16.1, we need consider only the case

$$(17.1) \quad h_r \equiv 0 \pmod{p}, \quad r = p \text{ or } r = 2p;$$

$$(17.2) \quad g_2 \text{ and } g_3 \text{ not both divisible by } p.$$

We first develop some simple arithmetical concepts which are needed in the proofs that follow. Let p be a prime ideal of an algebraic number field, and α any field element. Then the principal ideal $[\alpha]$ has a unique representation of the form $[\alpha] = p^{-a}bc^{-1}$ where b and c are integral ideals which are co-prime and also prime to p , and the exponent a is a rational integer. We call a "the index of α (modulo p)." α is said to be integral modulo p if and only if its index is negative or zero, and fractional modulo p if and only if its index is positive.

The following lemmas follow readily, and their proofs are left to the reader.

LEMMA 17.1. *If α is a fraction modulo p and β is an integer modulo p , $\alpha \pm \beta$ is a fraction with the same index as α , and the index of $\alpha\beta$ is not greater than that of α .*

LEMMA 17.2. *If $\alpha_1, \alpha_2, \dots, \alpha_k$ are fractions modulo p , the index of their product is the sum of the indices of the separate factors.*

LEMMA 17.3. *If $\alpha_1, \alpha_2, \dots, \alpha_k$ are fractions modulo p , the index of $(\phi - \alpha_1)(\phi - \alpha_2) \cdots (\phi - \alpha_k)$ is the same for all ϕ which are integers modulo p , and equals the sum of the indices of $\alpha_1, \alpha_2, \dots, \alpha_k$.*

18. We may now complete the proof of Theorem 8.1 as follows. With the notation of Section 16, let the roots of $F_r(z) = 0$ be $\zeta_1, \zeta_2, \dots, \zeta_q$. The leading coefficient of $F_r(z)$ is divisible by p but not by p^2 by formulas (14.4) and (14.6). Furthermore, there exists at least one coefficient A_k which is not divisible by p . Consequently, if \mathfrak{p} as before denotes a prime ideal divisor of p in the field \mathcal{R} , not all the roots ζ are integers modulo \mathfrak{p} . We shall now prove

LEMMA 18.1. *Not all the roots ζ of $F_r(z) = 0$ are fractions modulo \mathfrak{p} .*

Proof. Let ϕ denote a variable whose range is the set of all field elements of \mathcal{R} which are integers modulo \mathfrak{p} . Then if all the ζ are fractions, the index of $(\phi - \zeta_1)(\phi - \zeta_2) \cdots (\phi - \zeta_q)$ by Lemma 17.3 is a positive number independent of the choice of ϕ . But by formula (13.5), $z = \varphi(u)$ is an admissible value of ϕ , since \mathfrak{p} is prime to $6h_2h_3$. But by formulas (14.1) and (14.4),

$$(18.1) \quad h_r = F_r(z) = pl(z - \zeta_1)(z - \zeta_2) \cdots (z - \zeta_q)$$

where l is an integer depending on r but prime to p .

Now suppose that the highest power of \mathfrak{p} dividing p is the k -th. Then by (17.1), the index of the left side of (18.1) is at most $-k$. But by Lemma 17.2, the index of the right side of (18.1) is greater than $-k$. This contradiction establishes the lemma.

Now let $\zeta_1, \zeta_2, \dots, \zeta_s$ be the roots of $F_r(z) = 0$ which are integers modulo \mathfrak{p} , and $\zeta_{s+1}, \zeta_{s+2}, \dots, \zeta_q$ be the roots which are fractions modulo \mathfrak{p} . In view of what we have just proved, both these sets of roots are non-empty. Now re-write (18.1) as

$$h_r = pl[(z - \zeta_1) \cdots (z - \zeta_s)][(z - \zeta_{s+1}) \cdots (z - \zeta_q)].$$

The index of the right side is at most equal to the index $-k$ of p . But the index of $[(z - \zeta_{s+1}) \cdots (z - \zeta_q)]$ is positive. Consequently the index of $[(z - \zeta_1) \cdots (z - \zeta_s)]$ must be negative. But this implies that $(z - \zeta_1) \cdots (z - \zeta_s) \equiv 0 \pmod{\mathfrak{p}}$. Since \mathfrak{p} is a prime ideal and each term $z - \zeta_1, \dots, z - \zeta_s$ is an integer modulo \mathfrak{p} , there exists a ζ such that $\varphi(u) - z \equiv \zeta \pmod{\mathfrak{p}}$. Hence we obtain again from (14.8) the congruence (15.1) for a suitably chosen period 2ω of the φ -function. The remainder of the proof now follows exactly as in Section 15 for the case r prime to p .

VI. Equivalent Sequences. Singular Sequences and Their Representations by Circular Functions.

19. Two sequences (u) and (v) (which need neither be integral, nor solutions of (1.1)) are said to be “equivalent” if and only if there exists a constant $c \neq 0$ such that

$$u_n = c^{n^2-1} v_n, \quad (n = 0, 1, 2, \dots).$$

We write $(u) \sim (v)$ or $(u) = c(v)$ if it is desired to bring the constant c explicitly in evidence. \sim is evidently an equivalence relation in the technical sense. We shall show in Chapter VII that there are only four types of non-equivalent solutions of (1.1), of which the elliptic function and circular function solutions are the two most important. We shall continue the further development of the properties of equivalence in section twenty-one of this chapter.

Let (h) be a general elliptic sequence. We have seen in Chapter IV that there then exists an elliptic function $\varphi(w) = \varphi(w; g_2, g_3)$ whose invariants g_2 and g_3 are certain rational functions of the initial values of (h) , such that for a properly chosen value u of the complex variable w ,

$$(19.1) \quad h_n = \sigma(nu)/\sigma(u)^{n^2}.$$

By the “discriminant” of the sequence (h) we mean the discriminant of the corresponding φ -function:

$$(19.2) \quad \Delta = g_2^3 - 27g_3^2.$$

We write $\Delta = \Delta(h)$, or $\Delta = \Delta(h_2, h_3, h_4)$ if we wish to emphasize the dependence of Δ on the initial values of (h) .

If we substitute for g_2 and g_3 in (19.2) their expressions in terms of h_2 , h_3 and h_4 given by formulas (13.6) and (13.7), we find that

$$(19.3) \quad \begin{aligned} \Delta(h_2, h_3, h_4) = & 1/h_2^8 h_3^3 \{ h_4^4 + 3h_2^5 h_4^3 + (3h_2^8 + 8h_3^3)h_4^2 \\ & + h_2^7 (h_2^8 - 20h_3^3)h_4 + h_2^4 h_3^3 (16h_3^3 - h_2^8) \}. \end{aligned}$$

The sequence (h) is said to be “singular” if and only if its discriminant $\Delta(h)$ vanishes. We shall show that a sequence is singular if and only if it is essentially a Lucas function. The main step in the proof of this result is the following theorem:

THEOREM 19.1. *Necessary and sufficient conditions that a general elliptic*

sequence (h) be singular are that there exist integers r and s such that $rs(r^2 - s^2) \neq 0$ and

$$(19.4) \quad h_2 = r, \quad h_3 = s(r^2 - s^2), \quad h_4 = rs^3(r^2 - 2s^2).$$

20. This section is devoted to the proof of Theorem 19.1. We first prove that the conditions (19.4) are necessary for (h) to be singular. Assume then that (h) is a general elliptic sequence for which $\Delta(h)$ vanishes.

Since h_2 and h_3 are not zero and h_2 divides h_4 , it follows from (19.3) that if we let

$$(20.1) \quad u = h_2^4, \quad v = h_3^3, \quad w = h_4/h_2,$$

then Δ vanishes if and only if the diophantine equation

$$(20.2) \quad 16v^2 - (u^2 + 20uw - 8w^2)v + w(u + w)^3 = 0$$

has solutions of the form (20.1); that is, u a perfect fourth power and v a perfect cube.

If we solve (20.2) for v by the quadratic formula, we find that

$$(20.3) \quad 32v = u^2 + 20uw - 8w^2 \pm \sqrt{u(u - 8w)^3}.$$

Hence it is necessary that $u(u - 8w)$ be a square. But u is a square by (20.1). Hence we may write

$$(20.4) \quad u = l^2 = h_2^4,$$

$$(20.5) \quad u - 8w = m^2 = h_2^4 - 8h_4/h_2,$$

where l and m are integers. Then

$$(20.6) \quad w = (l^2 - m^2)/8.$$

We find from (20.4) and (20.6) that

$$\begin{aligned} u^2 + 2uw - 8w^2 &= \frac{1}{8}(27l^4 - 18l^2m^2 - m^4), \\ \sqrt{u(u - 8w)^3} &= lm^3. \end{aligned}$$

On substituting these expressions into (20.3) and multiplying by eight, we find that $256v = 27l^4 - 18l^2m^2 \pm 8lm^3 - m^4$.

The right hand side of this expression factors into $(l \pm m)(3l \mp m)^3$. Hence on multiplying by two and substituting h_3^3 for v , we obtain the formula

$$(20.7) \quad (8h_3)^3 = (2l \pm 2m)(3l \mp m)^3.$$

Hence $2l \pm 2m$ is the cube of an even integer, and we may write $2l \pm 2m = (2s)^3$ where s is an integer. Now $3l \mp m + 4s^3 = 4l$. Hence $3l \mp m$ in (20.7) is divisible by four. We thus have for integral s and q

$$(20.8) \quad l \pm m = 4s^3, \quad 3l \mp m = 4q,$$

and (20.7) becomes $(8h_3)^3 = (8sq)^3$. Hence

$$(20.9) \quad h_3 = sq$$

and on solving (20.8) for l and m , we find that

$$(20.10) \quad l = s^3 + q, \quad m = \pm(3s^3 - q).$$

On substituting these expressions for l and m into (20.6), we find that

$$(20.11) \quad h_4/h_2 = w = s^3(q - s^3).$$

Finally, (20.4) and (26.10) give

$$(20.12) \quad h_2^2 = s^3 + q.$$

Now let $h_2 = r$. Then by (20.12), $q = r^2 - s^3$. Then on substituting this expression for q into (20.9) and (20.11), we obtain the formulas (19.4). The accessory condition $rs(r^2 - s^3) \neq 0$ is needed to insure that (h) is general. The necessity of the conditions (19.4) is thus established.

The sufficiency of the conditions (19.4) is evident on retracing the steps of the proof of their necessity in reverse order. The sufficiency also follows directly by substituting into the formula (19.3) for $\Delta(h_2, h_3, h_4)$ the expressions for h_2 , h_3 and h_4 in terms of r and s . The result vanishes identically in r and s .

The following theorem may be proved by elementary algebra on substituting into the formulas (13.6) and (13.7) giving g_2 and g_3 the expressions for h_2 , h_3 and h_4 given in (19.4).

THEOREM 20.1. *If (h) is a singular elliptic sequence, then with the notation of Theorem 19.1,*

$$(20.13) \quad g_2 = 3\{(r^2 - 4s^3)/6s^2\}^2, \quad g_3 = -\{(r^2 - 4s^3)/6s^2\}^3.$$

Now if e , e_2 and e_3 denote as usual the roots of

$$(20.14) \quad 4z^3 - g_2z - g_3 = 0,$$

then $\Delta = 0$ if and only if two or more of the roots e_i are equal. Suppose that

$$(20.15) \quad \Delta = 0, \quad e_1 = e_2.$$

Then

$$(20.16) \quad e_3 = -2e_1$$

and

$$(20.17) \quad g_2 = 3e_3^2, \quad g_3 = e_3^3.$$

Hence we obtain the following corollary to Theorem 20.1:

THEOREM 20.2. *If (h) is a singular sequence, then the roots of (20.14) are*

$$-(r^2 - 4s^3)/6s^2, \quad (r^3 - 4s^3)/12s^2, \quad (r^2 - 4s^3)/12s^2.$$

Furthermore

$$(20.18) \quad g_2 = g_3 = 0 \quad \text{if and only if } r^2 = 4s^3.$$

In this case, $e_1 = e_2 = e_3 = 0$.

21. We shall now resume our discussion of the notion of equivalence of sequences introduced at the beginning of this chapter.

A sequence (α) of algebraic numbers is said to be “essentially integral” if it is equivalent to an integral sequence; that is, if there exists an algebraic number β other than zero such that $\beta^{n^2-1}\alpha_n$ is a rational integer for every n .

THEOREM 21.1. *If a sequence (u) is a particular solution of (1.1), so are all sequences equivalent to it. Furthermore, if (u) is general, so are all its equivalent sequences.*

THEOREM 21.2. *If an elliptic sequence (h) admits an elliptic function representation by means of $\varphi(w) = \varphi(w; g_2, g_3)$ and $(k) = c(h)$ is any equivalent sequence, then (k) admits an elliptic function representation by means of $\varphi(w') = \varphi(w'; g'_2, g'_3)$ where $w' = w/c$, $g'_2 = c^4 g_2$, $g'_3 = c^6 g_3$.*

Equivalence is thus the analogue of the φ -function homogeneity relation: $\varphi(w/c; c^4 g_2, c^6 g_3) = c^2 \varphi(w; g_2, g_3)$.

The proofs of these two theorems are almost immediate and are left to the reader.

THEOREM 21.3. *Every proper solution of (1.1) in rational numbers is essentially integral, and equivalent to an integral divisibility-sequence.*

Proof. Let (a) be a proper rational solution of (1.1) so that $a_0 = 0$, $a_1 = 1$ not both a_2, a_3 vanish and a_n is rational. If a_2 is zero, the theorem is

obvious from Lemma 4.1 of Chapter II, formula (4.13); for we may take c^8 equal to the denominator of a_3 . If a_2 is not zero, (a) is clearly uniquely determined by the initial values of a_2, a_3 and a_4 . Now we may write $a_2 = c_2/a, a_3 = c_3/a, a_4 = c_4/a$ where c_2, c_3, c_4 and a are integers and $c_2 \neq 0$. Then by Theorem 4.1, (b) is an equivalent integral divisibility sequence if $b_n = (c_2a)^{n^2-1}a_n$.

We may now prove a converse to Theorem 12.1 of Chapter IV.

THEOREM 21.4. *If the invariants g_2 and g_3 of the function $\varphi(w)$ are rational numbers and if u is such that $\varphi(u)$ is rational, then $a_n = \psi_n(u)$ is equivalent to an integral elliptic divisibility sequence.*

Proof. By (14.4), all the a_n are rational. But $\psi_n(w)$ satisfies (1.1). Hence the result follows from the previous theorem.

22. We shall resume the development of the properties of singular solutions by establishing the following theorem:

THEOREM 22.1. *Every singular elliptic sequence is equivalent either to the sequence*

$$(22.1) \quad 0, 1, 2, \dots, n, \dots$$

of the positive integers or to a Lucas sequence

$$(22.2) \quad U_0, U_1, U_2, \dots, U_n, \dots$$

where $U_n = (a^n - b^n)/(a - b)$, $Q = ab = 1$, and $P = a + b$ is in general, a quadratic irrationality.

Evidently such a Lucas sequence may be written in the form $U_n = \sin n\theta/\sin \theta$ for a suitably chosen complex number θ , and is hence parameterized by circular functions.

Proof. Let (h) be a singular elliptic divisibility sequence so that $\Delta(h) = 0$. Suppose first that $g_2 = g_3 = 0$. Then it follows from Theorem 20.2 that

$$(22.3) \quad r^2 = 4s^3$$

where r and s are the integers introduced in Theorem 19.1. But the diophantine relation (22.3) implies that there exists an integer c such that $r = 2c^3, s = c^2$. Then by (19.4), $h_2 = c^32, h_3 = c^83, h_4 = c^{15}4$.

Hence by Theorem 4.1, (h) is equivalent to the solution (22.1).

Now assume that not both g_2 and g_3 are zero. We first develop some lemmas.

LEMMA 22.1. *Let α and β be two distinct numbers neither of which is zero, and let $p = \alpha + \beta$, $q = \alpha\beta$, $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Then*

$$(22.4) \quad q^{(1-n)/2} u_n$$

is a solution of (1.1).

This lemma, as was mentioned in the introduction, is due to Lucas. We call (22.4) a "Lucas solution" of (1.1), or a "Lucas sequence."

In Lucas' arithmetical theory, p and q are rational integers so that a Lucas solution is not generally an integral sequence, although it is evidently equivalent to an integral sequence.

We may however restate the lemma of Lucas in a way which overcomes this defect and is more convenient for our purposes. Since neither α nor β is zero, we may let $a = \sqrt{\alpha/\beta}$ and $b = \sqrt{\beta/\alpha}$. Then $P = a + b = p/\sqrt{q}$ and $Q = ab = 1$ while $U_n = (a^n - b^n)/(a - b) = q^{(1-n)/2} u_n$. Hence we may state the following modification of Lemma 22.1.

LEMMA 22.2. *Every Lucas solution of (1.1) is of the form*

$$(22.5) \quad U_n = (a^n - b^n)/(a - b)$$

where $P = a + b$ and $Q = ab = 1$.

We shall assume that ²⁴ $P \neq 0$, as otherwise (U) is not general.

The initial values of the Lucas solution (22.5) with $Q = 1$ are

$$0, 1, P, P^2 - 1, P^3 - 2P.$$

On comparing these values with (19.4), we obtain the following result:

LEMMA 22.3. *A necessary and sufficient condition that a general ²⁵ elliptic sequence be a Lucas solution of (1.1) is that it be a singular solution with $r = P$ and $s = 1$.*

Now consider any singular sequence (h) with g_2 and g_3 not both zero. By Theorem 19.1,

$$(19.4) \quad h_2 = r, \quad h_3 = s(r^2 - s^3), \quad h_4 = rs^3(r^2 - 2s^3)$$

where r and s are integers and $rs(r^2 - s^3) \neq 0$.

²⁴ Lucas solutions of (1.1) with $P = 0$ are discussed in Chapter VII.

²⁵ Solutions with $h_2 = 0$, $h_3 \neq 0$ are equivalent to a Lucas solution. Solutions with $h_2 \neq 0$, $h_3 = 0$ are not generally Lucas solutions. See Chapter VII.

Now let $r = c^3P$, $s = c^2$. Then c is in general a quadratic irrationality. Hence P is in general a quadratic irrationality; namely

$$(22.6) \quad P = r\sqrt{s}/s^2.$$

Then (19.4) becomes

$$h_2 = c^3P, \quad h_3 = c^8(P^2 - 1), \quad h_4 = c^{15}(P^2 - 2).$$

Hence (h) is equivalent to a Lucas solution with P given by (22.6) and $Q = 1$. This completes the proof of Theorem 22.1.

VII. Special Sequences.

23. We have seen that any sequence (h) whose initial values satisfy the conditions

$$(23.1) \quad h_0 = 0, \quad h_1 = 1, \quad h_2 \neq 0, \quad h_3 \neq 0$$

may be parameterized by elliptic or circular functions. We discuss now the special sequences which arise when one or more of the conditions (23.1) are violated. Until further notice, (h) denotes a sequence of complex numbers satisfying (1.1), so that

$$(4.11) \quad h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \quad m \geq n \geq 1.$$

Sequences in which $h_1^2 \neq 1$ are uninteresting. For on first letting $m = 2$ and $n = 2$ in (4.11) and then letting $m = n$, $n = 1$; $n = n$, we obtain the relations

$$(23.2) \quad h_0h_2 = 0, \quad (h_1^2 - 1)h_{n+1}h_{n-1} = 0, \quad n \geq 1;$$

$$(23.3) \quad h_0h_{2n} = 0.$$

Now if $h_1^2 \neq 1$, then $h_{n+1}h_{n-1} = 0$. Hence since n is arbitrary, $h_{m+n}h_{m-n} = 0$ for $m \geq n \geq 1$. Since the integers $m + n$ and $m - n$ are of the same parity, there can be at most two non-vanishing terms in (h) and their suffices must be of opposite parity.

It is evident conversely that if k and l are any integers ≥ 0 , then $h_n = 0$, $n \neq k, n \neq k + 2l + 1$; h_k, h_{k+2l+1} arbitrary, defines a solution of (1.1).

We shall assume henceforth that $h_1^2 = 1$. There is no loss of generality in assuming then that $h_1 = 1$; for if h_n is a solution of (1.1), so is $(-1)^n h_n$.

We consider next solutions with $h_2 = 0$. We see from (23.2) that a sufficient condition that $h_2 = 0$ is that $h_0 \neq 0$. The simplest example of such

a solution is the Lucas sequence $h_n = \sin n\pi/2$, $n > 0$. This solution is periodic with period four and purely periodic if and only if $h_0 = 0$. The Kronecker symbol solution $(-8/n)$, mentioned in the introduction, equals $(-1)^{(n^2-1)/8} \sin n\pi/2$, and is hence essentially a Lucas solution, but of period eight instead of four. Evidently the fourth term of this solution is not zero. We shall now show that there is essentially no other such solution.

THEOREM 23.1. *Every solution (h) of (1.1) with $h_1 = 1$, $h_2 = 0$ and $h_3 \neq 0$ is equivalent to the Kronecker symbol solution, and is hence a Lucas solution; that is for $n > 0$,*

$$(23.4) \quad h_n = \begin{cases} 0 & n \text{ even} \\ (-1)^{\lceil n/4 \rceil} h_3^{(n^2-1)/8} & n \text{ odd.} \end{cases}$$

Proof. It is easily verified that $\lceil (2n+1)/4 \rceil \equiv n+1 + n(n+1)/2 \pmod{2}$. Hence an equivalent way of stating (23.4) is:

$$(23.5) \quad h_{2n} = 0, \quad h_{2n+1} = (-1)^{n+1} (-h_3)^{n(n+1)/2}, \quad (n = 1, 2, 3, \dots).$$

Now since (h) satisfies (4.11), we obtain on taking first $m = 2n$ and $n = 2$ and then $m = 2n - 2$ and $n = 3$ the two relations

$$(23.6) \quad h_{2n+2}h_{2n-2} = -h_1h_3h_{2n}, \quad n \geq 1.$$

$$(23.7) \quad h_{2n+1}h_{2n-5} = h_{2n-1}h_{2n-3}h_3^2, \quad n \geq 3.$$

Since h_2 vanishes, the first part of (23.5) follows by a brief induction from (23.6). Since $h_1 = 1$, we can calculate h_{2n+1} for $n = 2$ and $n = 3$ from (4.5): $h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3$.

We thus find that $h_5 = h_3^3$, $h_7 = -h_3^6$, so that (23.5) is true for $n \leq 3$. Its general validity now follows readily by an induction based on (23.7).

24. We next discuss solutions with vanishing fourth term. We see from (23.3) that if $h_0 \neq 0$, all terms of positive even suffix vanish. But since we are assuming that $h_1 = 1$, it follows by a brief induction based on (4.5) that all terms of odd suffix vanish save h_1 . Conversely

$$(24.1) \quad h_n = 0, \quad n > 1$$

is evidently a solution of (1.1) regardless of the values of h_0 and h_1 . We shall therefore assume henceforth that

$$(24.2) \quad h_0 = 0, \quad h_1 = 1, \quad h_3 = 0.$$

There exist an infinite number of essentially distinct solutions of (1.1) meeting these conditions. For let l denote a fixed odd number greater than one and define a numerical function of n and l , $\lambda_n = \lambda_n(l)$ as follows:

$$(24.3) \quad \begin{aligned} \lambda_n = & 0 \text{ if } n \not\equiv \pm 1 \pmod{l}; \\ & 1 \text{ if } n \equiv +1 \pmod{l}; \\ & -1 \text{ if } n \equiv -1 \pmod{l}. \end{aligned}$$

THEOREM 24.1. *If c is a constant and not zero then*

$$(24.4) \quad l_n = \lambda_n c^{1-n\lambda_n}$$

is a solution of (1.1) whose initial values satisfy the conditions of (24.2).

In particular, on taking $c = 1$, we see that λ_n itself satisfies (1.1).²⁶ If $l = 3$, λ_n reduces to the Legendre symbol solution ($n/3$) mentioned in the introduction. We see incidentally that (1.1) has integral periodic solutions with any preassigned odd period l ; but such a solution is a divisibility sequence only if $l = 3$.

Proof. The initial values given by formula (24.4) are evidently $l_0 = 0$, $l_1 = 1$ and $l_3 = 0$, so that (24.2) is satisfied. If we substitute l_n into the basic recurrence (4.11), the left hand side vanishes unless $m+n \equiv \pm 1 \pmod{l}$ and $m-n \equiv \pm 1 \pmod{l}$. Hence, since l is odd, there are only four cases when the left side of (4.11) is not zero; namely²⁷ (i) $m \equiv 1$, $n \equiv 0$; (ii) $m \equiv 0$, $n \equiv 1$; (iii) $m \equiv 0$, $n \equiv -1$; (iv) $m \equiv -1$, $n \equiv 0$.

Now of the two terms on the right hand side of (4.11), $l_{m+1}l_{m-1}l_n^2$ vanishes unless $m \equiv 0$ and $n \equiv \pm 1$, and $l_{n+1}l_{n-1}l_m^2$ vanishes unless $n \equiv 0$ and $m \equiv \pm 1$. Hence (4.11) is satisfied except, perhaps, in the four cases just listed. The following table lists the values of λ_m, \dots for each of the four cases and the computed values of the terms of (4.11) which result. A glance at these completes the proof.

TABLE OF VALUES OF (l)

Case	λ_m	λ_n	λ_{m+1}	λ_{m-1}	λ_{n+1}	λ_{n-1}	λ_{m+n}	λ_{m-n}	$l_{m+n}l_{m-n}$	$l_{m+1}l_{m-1}l_n^2$	$-l_{n-1}l_{n+1}l_m^2$
(i)	1	0	0	0	1	-1	1	1	c^{2-2m}	0	c^{2-2m}
(ii)	0	1	1	-1	0	0	1	-1	$-c^{2-2n}$	$-c^{2-2n}$	0
(iii)	0	-1	1	-1	0	0	-1	1	$-c^{2-2n}$	$-c^{2-2n}$	0
(iv)	-1	0	0	0	1	-1	-1	-1	c^{2+2m}	0	c^{2+2m}

²⁶ λ_n satisfies (1.1) if $l = 4$, but Theorem 24.1 is untrue in this case for c 's chosen arbitrarily.

²⁷ We suppress the modulus l when no confusion can arise.

25. We shall next show that the solutions (l) just investigated are essentially the only type of solution of (1.1) with fourth term zero.

THEOREM 25.1. *Every solution (h) of (1.1) with $h_0 = 0$, $h_1 = 1$ and $h_3 = 0$ either has all its other terms zero with at most one exception, or it is equivalent to a solution (l) of the type described in Theorem 24.1.*

Proof. Let (h) be a solution of (1.1) satisfying the conditions $h_0 = 0$, $h_1 = 1$ and $h_3 = 0$. Then (4.5) holds:

$$(4.5) \quad h_{2k+1} = h_{k+2}h_k^3 - h_{k-1}h_{k+1}^3, \quad k \geq 1.$$

If all terms of (h) with even suffixes vanish, we find by a brief induction based on (4.5) that all terms of (h) of odd suffix vanish save h_1 , and we have the trivial solution (24.1) again.

If not all terms of even suffix vanish, there is a first term which does not vanish. Consequently, there exists an odd integer l not less than three such that

$$(25.1) \quad h_0 = h_2 = \cdots = h_{l-3} = 0;$$

$$(25.2) \quad h_{l-1} \neq 0.$$

I say that

$$(25.3) \quad h_l = 0$$

and

$$(25.4) \quad h_n = 0 \quad \text{for } 1 < n < l-1 \quad \text{if } l > 3.$$

For (25.3) is true by hypothesis if $l = 3$. If $l > 4$, then (25.4) is true for even n by (25.1). Hence if (25.4) were false, there would exist an integer $k > 1$ such that $h_n = 0$ for $1 < n < 2k + 1 < l$ but $h_{2k+1} \neq 0$. However, by (4.5) $h_{2k+1} = 0$, since $1 \leq k-1 < k+2 < 2k+1$. This contradiction establishes (25.4). (25.3) now follows from (25.4) on taking n equal to $(l-1)/2$ in (4.5).

It may happen that $h_{l+1} = 0$. If so, it may be readily proved by induction that $h_n = 0$ for $n > l+1$.²⁸ It is evident that conversely, $h_0 = 0$, $h_1 = 1$, $h_n = 0$, $n \neq l+1$ gives a solution of (1.1). The first part of the theorem is thus established, and we may assume for the remainder of the proof that

$$(25.5) \quad h_{l+1} \neq 0.$$

²⁸ For odd n , we use (4.5) as a basis for the induction. For even n , we use the formula $h_{2k}h_{l-1} = h_{m+1}h_{m-1}h_m^2 - h_{n+1}h_{n-1}h_m^2$ obtained by letting $m = k + (l-1)/2$ and $n = k - (l-1)/2$ in (4.11).

I say that

$$(25.6) \quad h_n = 0 \quad \text{for } l+1 < n < 2l-1 \quad \text{if } l > 3;$$

$$(25.7) \quad h_{2l-1} = h_{l-1}h^3_{l+1}; \quad h_{2l} = 0; \quad h_{l+1} = -h_{l-1}h^3_{l+1}.$$

For if n is even, then by (4.11)

$$(25.8) \quad h_n h_{l-1} = h_{(n+l+1)/2} h_{(n+l-3)/2} h^2_{(n-l+1)/2} - h_{(n-l+3)/2} h_{(n-l-1)/2} h^2_{(n+l-1)/2}.$$

Now if $n = l+3$, $h_{(n-l+3)/2} = h_3 = 0$ and $h_{(n-l-1)/2} = h_2 = 0$. If $n > l+3$, then $1 < (n-l-1)/2 < (n-l+1)/2 < l/2 < l-1$. Hence $h_{(n-l+1)/2} = 0$ by (25.4). Hence $h_n = 0$ by (25.5). If n is odd, say $n = 2k+1$, $h_n = 0$ directly by (4.5) and (25.4). The first and third equations of (23.7) follow directly from (4.5), and the second equation follows from (25.8) on putting n equal to $2l$.

We can now prove that

$$(25.9) \quad h_n = a^{n^2-1} \lambda_n c^{1-n\lambda_n}$$

where

$$(25.10) \quad a = (-h_{l-1}h_{l+1})^{1/2l^2}, \quad c = (-h_{l-1})^{(2+l)/2l^2} h_{l+1}^{(2-l)/2l^2}.$$

Since $\lambda_n c^{1-n\lambda_n}$ is a special (l) solution, this step will complete the proof of the theorem.

If n is less than $2l+2$ and not congruent to ± 1 modulo l , (25.9) gives $h_n = 0$ in agreement with (25.4) and (25.6). It is readily seen that (25.9) also gives the values for h_{l+1} and h_{2l-1} already found.

We now proceed by induction. Suppose that we have proved that the formula (25.9) gives the solution (h) for $0 \leq n < m$, where we are entitled by what proceeds to assume that $m \geq 2l+2$. Since (h) satisfies (4.11), we obtain on taking n equal to l the relation

$$(25.11) \quad h_{m+l} h_{m-l} = -h_{l+1} h_{l-1} h^2_m.$$

Now if $m \not\equiv \pm 1 \pmod{l}$, then $h_{m-1} = 0$ by the hypothesis of the induction. Hence $h_m = 0$ unless $m \equiv \pm 1 \pmod{l}$. Hence by the definition of λ_n , (25.9) is true if $n = m$ and $m \not\equiv \pm 1 \pmod{l}$.

Now assume that $m \equiv \pm 1 \pmod{l}$. Then on replacing m by $m-l$ in (25.11) we obtain the formula

$$(25.12) \quad h_m = -h_{l-1} h_{l+1} h^2_{m-l} / h_{m-2l}.$$

For since $m \geq 2l+2$, we have $m-2l > 0$ and $h_{m-2l} \neq 0$ by the hypothesis of the induction. We may now evaluate h_m by substituting in (25.12) for h_{m-l} and h_{m-2l} from (25.9). But we obtain in this manner (25.9) with n

replaced by m . Thus we have shown that if (25.9) holds for $0 \leq n < m$, then it holds for $0 \leq n < m + 1$. Hence it is generally true by induction.

That conversely (25.9) is a solution of (1.1) is a trivial consequence of Theorem 24.1.

If we exclude from consideration the trivial solutions of (1.1) already discussed in which all except a finite number of terms are zero, we may summarize the results of Chapters IV, VI and the present sections as follows.

THEOREM 25.2. *Any non-trivial solution of*

$$(1.1) \quad \omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$

is equivalent to one of the following four solutions:

$$h_n = n; \quad h_n = \sin n\theta / \sin \theta; \quad h_n = \sigma(nu) / \sigma(u)^{n^2}; \quad h_n = \lambda_n c^{1-n\lambda_n}.$$

26. We have already remarked that the only non-trivial solutions of (1.1) with fourth term zero which can be divisibility sequences are those for which $l = 3$ so that h_3 is zero, but h_2 and h_4 are not zero. The formulas of Theorem 25.1 then give the general term of the sequence (h) .

The question arises whether or not such a solution can be parameterized by elliptic functions, so that with a proper choice of invariants, $h_n = \psi_n(u)$. But (Halphen, *Traité des fonctions elliptiques*, Part I (1886), p. 96) we have in the notation of Chapter IV,

$$\begin{aligned} h_2 &= \psi_2(u) = -\varphi'(u); \quad h_3 = \psi_3(u); \\ h_4 &= \psi_4(u) = \varphi'(u)(\varphi'^4(u) - \psi_3(u)\varphi''(u)). \end{aligned}$$

Consequently, if $h_3 = 0$, it is necessary that $h_4 = -h_2^5$ for such a parameterization to be possible. But if this condition is satisfied, h_n reduces to $(-h)^{(n^2-1)/2}(n/3)$, so that (h) is equivalent to the Legendre symbol solution $(n/3)$. Now the Legendre symbol solution is equivalent to $(n/3)(-1)^{1-(n/3)n}$; for $(-1)^{n^2-1} = (-1)^{1-(n/3)n} = (-1)^{n(n-(n/3))} = +1$ if n is not divisible by three. But $(n/3)(-1)^{1-(n/3)n}$ is the special λ_n solution for $l = 3$ and $c = -1$; and this is evidently expressible as the Lucas solution

$$U_n = (\sin 2n\pi/3) / (\sin 2\pi/3)$$

satisfying the recurrence $U_{n+2} = U_{n+1} - U_n$. We may thus state the following theorem.

THEOREM 26.1. *If (h) is an elliptic divisibility sequence with the initial values $0, 1, h_2, 0, h_4$ where $h_2 h_4 \neq 0$, then (h) cannot be parameterized in terms of elliptic functions unless $h_4 = -h_2^5$. If this condition is satisfied, (h) is equivalent to the Lucas solution $\sin(2n\pi/3) / \sin(2\pi/3)$.*

VIII. Periodic Sequences.

27. We shall determine in this chapter all periodic elliptic sequences other than the special periodic sequences (λ) already discussed in Section 24 of the preceding chapter. We shall be concerned here then with sequences (h) with $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 zero. By Lemma 4.1 of Chapter IV, if two consecutive terms of such a sequence vanish, then all terms vanish beyond the third, and we have the trivial solution $0, 1, h_2, 0, 0, 0, \dots$ of period one. It is easy to see conversely that this solution is the only one of period one. We shall now show that every other periodic sequence is purely periodic.

THEOREM 27.1. *Let $(h) : 0, 1, h_2, h_3, \dots$ be a solution of (1.1) in which no two consecutive terms vanish. Then if (h) is periodic, (h) is purely periodic.*

Proof. Since if h_2 is zero, h_3 is not zero, and the conditions for periodicity in this case are trivial, it suffices to show that if no two consecutive terms of (h) vanish, then the assumptions

$$(27.1) \quad h_{n+\kappa} = h_n, \quad n \geq a \geq 1, \quad \kappa \geq 2;$$

$$(27.2) \quad h_{a-1+\kappa} \neq h_{a-1};$$

$$(27.3) \quad h_2 \neq 0;$$

lead to a contradiction. (These conditions simply state that (h) becomes periodic with period $\kappa > 1$ after a non-periodic terms.)

We shall begin by showing that

$$(27.4) \quad h_\kappa = 0.$$

For, taking $m = a + \kappa - 1$ and $n = a + 1$ in the basic recursion (4.11), we obtain from (27.1), $h_{2a+2}h_\kappa = 0$. Hence either h_κ , or $h_{2a+2} = 0$. But if $h_{2a+2} = 0$, then on taking $m = 2a + 2 + \kappa$ and $n = \kappa$ in (4.11), we obtain $0 = h_{2a+1}h_{2a+3}h_\kappa^2$. Since neither h_{2a+1} nor h_{2a+3} can vanish, $h_\kappa = 0$.

We next show that

$$(27.5) \quad \text{Either } h_a = 0 \text{ or } h_{a+1} = 0.$$

For taking $m = a + \kappa$ and $n = a$ in (4.11) we find that

$$h_{2a}h_\kappa = h_{a+1}h_a^2(h_{a-1+\kappa} - h_{a-1}).$$

Hence (27.5) follows from (27.4) and (27.2). Since $h_2 \neq 0$, it follows from (27.5) and (4.6) that either $h_{2a} = 0$ or $h_{2a+2} = 0$. Hence

$$(27.6) \quad h_{2a+1} \neq 0.$$

We can now show that

$$(27.7) \quad h_{a+1} = 1, \quad h_{\kappa-1} = -1.$$

For taking $m = a + \kappa + 1$ and $n = a$ in (4.11) and reducing by (27.1) and (4.5), we find that $h_{2a+1}h_{\kappa+1} = h_{2a+1}$. Hence by (27.6), $h_{\kappa+1} = 1$. Next, taking $m = a + 1 + 2\kappa$ and $n = a$ in (4.11), we obtain the formula $h_{2a+1}h_{2\kappa+1} = h_{2a+1}$. Hence $h_{2\kappa+1} = 1$. But by (4.5), $h_{2\kappa+1} = -h_{\kappa-1}h^2_{\kappa+1}$, completing the proof of (27.7).

Next,

$$(27.8) \quad h_{a-1+\kappa} = 0.$$

For taking $m = a - 1 + \kappa$ and $n = \kappa$ in (4.11), we obtain by (27.4) and (27.7), $h_{a-1+2\kappa}h_{a-1} = h^2_{a-1+\kappa}$. Since by (27.1) and (27.2), $h_{a-1+2\kappa} = h_{a-1+\kappa} \neq h_{a-1}$, (27.8) follows.

Finally,

$$(27.9) \quad h_{a+1} = 0; \quad h_a \neq 0; \quad h_{a+2} \neq 0; \quad h_{a-1} \neq 0.$$

For by (27.5), either h_{a+1} or h_a equals zero. But $h_a = 0$ implies $h_{a+\kappa} = 0$ contrary to (27.8). Hence $h_{a+1} = 0$. Consequently $h_a \neq 0$ and $h_{a+2} \neq 0$; $h_{a-1} \neq 0$ by (27.2) and (27.8).

We may obtain a contradiction of (27.9) as follows. Take $m = a + 1 + \kappa$ and $n = a - 1 + \kappa$ in (4.11). Then $h_m = h_n = 0$ so that $h_{m+n}h_{m-n} = h_{2a}h_2 = 0$. Hence by (27.3), $h_{2a} = 0$. But by (4.6),

$$0 = h_{2a}h_2 = h_a(h_{a+2}h^2_{a-1} - h_a h^2_{a+1}) \text{ or } h_a h_{a+2}h^2_{a-1} = 0,$$

contradicting (27.9) and completing the proof of the theorem.

28. We have already shown the existence of periodic solutions of (1.1) with h_2 or h_3 zero of periods one, three, four, six and eight. The three theorems which follows are useful for deciding whether or not a given sequence is a periodic solution of (1.1). They may be proved either by mathematical induction or more briefly, by using the elliptic function representation theorem of Chapter IV.

THEOREM 28.1. *Let $(h) : 0, 1, h_2, h_3, \dots$ be a general solution of (1.1), so that neither h_2 nor h_3 is zero. Then any one of the following three sets of conditions is necessary and sufficient for (h) to be periodic with period κ :*

- | | | |
|-------|-------------------------|--|
| (i) | $h_{n+\kappa} = h_n$ | $(n = 0, 1, \dots, \kappa)$ |
| (ii) | $h_{\kappa-n} = -h_n$ | $(n = 0, 1, \dots, \kappa)$ |
| (iii) | $h_{\kappa/2+n} = -h_n$ | $(\kappa \text{ even}; n = 0, 1, \dots, \kappa/2)$ |

THEOREM 28.2. *Let $h_0, h_1, \dots, h_\kappa$ be a set of $\kappa + 1$ numbers satisfying the conditions (28.1) (ii) or (28.1) (iii), and also satisfying the basic recursion (4.11) for $m + n \leq \kappa$. Then if κ_n denotes the least positive residue of n modulo κ , and if h_n is defined to be h_{κ_n} for $n \geq 0$, then (h) is a periodic solution of (1.1) with period κ .*

THEOREM 28.3. *If (h) is any integral general elliptic sequence and if m is an integral modulus prime to both h_2 and h_3 , then the previous two theorems hold if the periodicity is understood to mean numerical periodicity modulo m and if the equalities in the conditions (26.1) are replaced by congruences modulo m .*

To illustrate the theorems, suppose that we start with the initial values $h_0 = 0, h_1 = 1, h_2 = b \neq 0, h_3 = 1$ and $h_4 = 0$ and compute from (4.5) and (4.6) $h_5 = -1, h_6 = -b, h_7 = -1$ and $h_8 = 0$. Then the nine numbers $0, 1, b, 1, 0, -1, -b, -1, 0$, satisfy (28.1) (ii) for $\kappa = 8$. They therefore define a periodic solution of (1.1) of period eight which is an elliptic divisibility sequence if b is an integer. It is easy to prove that any elliptic divisibility sequence with $h_2 h_3 \neq 0$ and $h_4 = 0$ is equivalent to this periodic solution.

Again, let us start with the initial values $h_0 = 0, h_1 = 1, h_2 = 1, h_3 = -1, h_4 = -1$. We find that $h_5 = 0$. Hence (28.1) (ii) is satisfied with $\kappa = 5$. If we start with the initial values $0, 1, b, b, 1$ we find that $h_5 = 0, h_6 = -1, h_7 = -b, h_8 = -b, h_9 = -1, h_{10} = 0$. Hence (28.1) (ii) is satisfied with $\kappa = 10$, and we have two periodic solutions of (1.1) of periods five and ten, respectively.

We shall show in the next section that there are essentially no other periodic elliptic sequences.

29. A sequence (h) will be called a “normal solution” of (1.1) if

$$(29.1) \quad h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \quad m \geq n \geq 1;$$

$$(29.2) \quad h_0 = 0, h_1 = 1; h_2, h_3, h_4 \text{ and } h_4/h_2 \text{ integers;}$$

$$(29.3) \quad (h_3 h_4) = 1.$$

By Theorem 6.1 of Chapter III, if (h) is normal

$$(29.4) \quad (h_n, h_{n+1}) = 1, \quad (n = 1, 2, 3, \dots)$$

and by Theorem 6.4,

$$(29.5) \quad (h_n, h_m) = h_{(n,m)}.$$

Every purely periodic elliptic divisibility sequence is normal, for if (h)

is purely periodic with period $\kappa \geq 2$, then $h_{2\kappa+1} = h_1 = 1$. Consequently $(h_3, h_4) = 1$ by Theorem 6.1.

Let (h) be any normal solution. Then if

$$(29.5) \quad h_\rho = 0 \quad \text{but} \quad h_n \neq 0, \quad 0 < n < \rho,$$

then (h) is said to be of rank ρ .

THEOREM 29.1. *If (h) is a normal solution of (1.1) of rank ρ , then (h) is purely periodic and its period is either ρ or 2ρ .*

Proof. Let $0 \leq n \leq \rho$, and take $m = n + \rho$ in (29.1). Then $h_{m+1}h_{m-1}h_n^2 = h_{n+1}h_{n-1}h_m^2$. But by (29.4), h_n is prime to $h_{n+1}h_{n-1}$. Hence h_n^2 divides h_m^2 . Similarly, h_m^2 divides h_n^2 . Hence $h_{n+\rho} = \pm h_n$, ($0 \leq n \leq \rho$), and it is easily shown that either the plus sign or the minus sign must be taken with every n according as $h_{\rho+1} = +1$ or $h_{\rho+1} = -1$. Hence by Theorem 28.1, (h) is purely periodic with period ρ or 2ρ .

THEOREM 29.2. *If (h) is purely periodic, its rank is less than six.*

In other words, integral periodic elliptic sequences can have only the periods 1, 2, 3, 4, 5, 6, 8 or 10. That each of these periods may actually occur has already been demonstrated. The proof of Theorem 29.2 rests on a series of lemmas which we establish in the next section. The proof of the theorem concludes the section and chapter.

30. LEMMA 30.1. *If (h) is any solution of (1.1) and $m \geq n \geq p > 0$, then*

$$(30.1) \quad h_{m+n}h_{m-n}h_p^2 = h_{m+p}h_{m-p}h_n^2 - h_{n+p}h_{n-p}h_m^2.$$

This result easily follows on substituting for $h_{m+p}h_{m-p}$ and $h_{n+p}h_{n-p}$ on the right of (30.1) their expressions obtained from (29.1).

LEMMA 30.2. *Let (h) be an elliptic divisibility sequence and h_r any non-vanishing term of (h) . Then if $k_n = h_{nr}/h_r$, ($n = 0, 1, 2, \dots$) (k) is an elliptic divisibility sequence. Furthermore if (h) is normal, so is (k) .*

For taking $p = r$, $m = mr$ and $n = nr$ in (30.1) and dividing by h_4^4 , we find that (k) satisfies (1.1). (k) is evidently integral and $k_0 = 0$, $k_1 = 1$ while k_4/k_2 is an integer. Hence (k) is an elliptic divisibility sequence. Now if (h) is normal, $(h_{3r}, h_{4r}) = h_r$ by (29.5). Hence $(k_3, k_4) = 1$ and (k) is normal.

LEMMA 30.3. *If p is a prime greater than five and (h) is normal, then h_p is never zero.*

Proof. Since p is a prime, if $h_p = 0$, (h) is of rank p and hence (h) is purely periodic with period p or $2p$ by Theorem 29.1. Since $(h_3, h_4) = 1$, (h) is purely periodic modulo three and hence p must be divisible by the rank of apparition of three in (h) . But it was shown in Chapter III that $\rho \leq 7$. Hence p equals seven. But if $h_7 = 0$, then $h_6 = \pm 1$ and $h_8 = \pm 1$ by (29.5). Hence $h_2 = \pm 1$, $h_4 = \pm 1$ and $h_3 = \pm 1$. Since $h_5 = h_4h_2^3 - h_3^3 \neq 0$, $h_5 = \pm 2$. But then $h_7 = h_5h_3^3 - h_2h_4^3 = \pm 2 \pm 1 \neq 0$. This contradiction completes the proof of the lemma.

LEMMA 30.4. *If ρ is the rank of (h) , then ρ can contain no prime factor other than two, three or five.*

For if p is any prime factor of ρ , write $\rho = pq$. Then $h_q \neq 0$ by the definition of rank. Hence if $k_n = h_{nq}/h_q$, (k) is a normal sequence of rank p by Lemma 30.2. Hence by Lemma 30.3, p equals two, three or five.

LEMMA 30.5. *Let (h) be a normal sequence of rank ρ . Then ρ is not equal to any one of the following numbers:*

$$(30.2) \quad 6, 8, 9, 10, 15, 25.$$

The proof proceeds by examination of cases; it suffices to give two examples. Suppose that $\rho = 6$. Then $h_5 = \pm 1$, $h_n \neq 0$, $0 < n < 6$ and $h_6h_2 = h_3(h_5h_2^2 - h_4^2) = 0$. Hence $h_5 = \pm 1$, $h_4 = \pm h_2$. But $h_5 = h_4h_2^3 - h_3^3$. Hence one or the other of the diophantine equations $X^4 = 1 + Y^3$, $X^4 + 1 = Y^3$ must have non-zero integral solutions. But it is easily seen that neither has non-zero integral solutions. Hence $\rho \neq 6$.

Now suppose that $\rho = 10$. Then $h_9 = \pm 1$, so $h_3 = \pm 1$, and since $h_{50} = 0$, $h_{49} = \pm 1$ so $h_7 = \pm 1$. Now $0 = h_{10}h_2 = h_5(h_7h_4^2 - h_3h_6^2)$. Hence $h_4^2 = h_6^2$, $h_3 = \pm 1$, $h_6 = \pm h_4$. Next, $h_6h_2 = h_3(h_5h_2^2 - h_4^2)$. Hence $h_4 | h_2$, $h_4 = \pm h_2$. But then $h_6h_2 = \pm h_2^2 = h_3h_2^2(h_5 - 1)$. Hence $h_5 - 1 = \pm 1$, and since $h_5 \neq 0$, $h_5 = 2$. But $h_9 = h_6h_4^3 - h_3h_5^3$. Hence $\pm 1 = \pm h_4^4 = 8$ or $h_4^4 = 7$ or 9 which is impossible. Hence $\rho \neq 10$. The other cases may be disposed of similarly.

LEMMA 30.6. *Let (h) be a normal sequence of rank ρ . Then ρ is not divisible by any one of the numbers (30.2).*

For let m be any one of the numbers (30.2) and assume that $\rho = lm$,

$l \geq 1$. Then $h_l \neq 0$ and $k_n = h_{ln}/h_l$ defines a normal sequence (k) of rank m contrary to Lemma 30.5.

Proof of Theorem 29.2. Let (h) be normal of rank ρ . By Lemma 30.4, the only prime factors of ρ are two, three and five and by Lemma 30.6, ρ is not divisible by $2^2, 3^2, 5^2$ or $2 \times 3, 2 \times 5, 3 \times 5$. Hence ρ must equal two, three, four or five.

IX. Conclusion: Lucas' Conjecture.

31. The results obtained in Chapters VI and VII make it clear that the only solutions of (1.1) that can be related to solutions of linear recurrences of order three or four are the general elliptic function solutions. Now the arithmetical behavior of a sequence of integers $(W): W_0, W_1, W_2, \dots$ defined recursively by

$$W_{n+3} = PW_{n+2} + QW_{n+1} + RW_n$$

or

$$W_{n+4} = PW_{n+3} + QW_{n+2} + RW_{n+1} + TW_n$$

P, Q, R, T fixed integers, is well known. (Carmichael [1], Ward [1].) First of all, such a sequence is only exceptionally a divisibility sequence (Hall [1], Ward [2]), and if it is a divisibility sequence, the rank of any prime p in it divides $p(p^3 - 1)$ or $p(p^4 - 1)$ according as the recursion is of order three or four. Since there exist elliptic sequences in which the rank of every prime is five and since there are an infinite number of primes p such that $p^3 - 1$ is not divisible by five, no direct connection with recurrences of order three seems possible. In particular, there cannot exist a formula $h_n = K^{a_n} W_n$ analogous to Lucas' $h_n = q^{(1-n)/2} U_n$.

If (h) is singular and hence essentially a Lucas function, the rank of apparition of any prime in (h) may be shown to divide $p(p^4 - 1)$. But this is not true if (h) is non-singular. For consider the sequence with the initial values 0, 1, 1, 1, 5. We find that $h_5 = 4$, $h_6 = -21$, and $h_7 = -121$. Hence the rank of apparition of the prime 11 is 7. But $11 \cdot (11^4 - 1) = 2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 61$ is not divisible by 7.

If (W) is not a divisibility sequence, the prospects are even worse, for two consecutive terms of such a sequence may be divisible by a prime p without having almost all terms of (W) divisible by p , contrary to Theorem 6.1.

Although the analogy between an elliptic sequence (h) and a Lucas sequence (U) is a close one, I should like to point out in concluding one

very significant difference. For a Lucas sequence, (and more generally for any linear divisibility sequence) it is possible to name in advance terms which will certainly be divisible by a given prime p ; for example U_{p+1} for the Lucas function proper. Consequently, the rank of apparition of p is arithmetically restricted since it must divide either $p - 1$ or $p + 1$. But for the general elliptic sequence (h) , computational experiments disclose no such simple arithmetical connections between a prime and its rank of apparition; it appears to be impossible to name in advance a particular h_k which will be divisible by a given prime p .

CALIFORNIA INSTITUTE OF TECHNOLOGY.

BIBLIOGRAPHY

E. T. Bell.

- [1] *Bulletin of the American Mathematical Society*, vol. 29 (1923), pp. 401-406.

R. D. Carmichael.

- [1] *Quarterly Journal of Mathematics* vol. 48 (1920), pp. 343-372.

M. Hall.

- [1] *American Journal of Mathematics*, vol. 38 (1936), pp. 577-584.

E. Lucas.

- [1] and [2] *American Journal of Mathematics*, vol. 1 (1878), pp. 184-240; 289-321.

M. Ward.

- [1] *Transactions of the American Mathematical Society*, vol. 33 (1931), pp. 153-165.

- [2] *Ibid.*, vol. 44 (1938), pp. 68-86.

- [3] *Bulletin of the American Mathematical Society*, vol. 42 (1936), pp. 843-845.

Chapter 17

1949

The slopes of the two tangents of inflection are given by the expression

$$q \pm \left(\frac{-2p}{3} \right)^{3/2}.$$

If the slope of one inflection tangent is zero, then the slope of the other is $2q$.

MATHEMATICAL NOTES

EDITED BY E. F. BECKENBACH, University of California
and Institute for Numerical Analysis of the National Bureau of Standards

Material for this department should be sent directly to E. F. Beckenbach, University of California, Los Angeles 24, California.

A GENERALIZED INTEGRAL TEST FOR CONVERGENCE OF SERIES

MORGAN WARD, California Institute of Technology

The following useful generalization of the familiar Maclaurin-Cauchy integral test for convergence of real series deserves to be better known. It is apparently due to G. H. Hardy,* who made a redundant hypothesis on $f(t)$. The integrals may be taken either in the sense of Riemann or in the sense of Lebesgue.

THEOREM. *Let $f(t)$ be a complex-valued function of the real variable in the interval $1 \leq t < \infty$, such that $f'(t)$ exists and is integrable to $f(t)$ over any finite interval $1 \leq t \leq T$. Then if $\int_1^\infty f'(t)dt$ is absolutely convergent, the series $\sum_1^\infty f(n)$ and the integral $\int_1^\infty f(t)dt$ converge and diverge together.*

Proof: By Abel's partial summation formula, we have

$$\sum_{r=1}^n a_r b_r = A_n B_n - \sum_{r=1}^{n-1} A_r (b_{r+1} - b_r),$$

where $A_r = a_1 + a_2 + \dots + a_r$, ($r = 1, 2, \dots, n$).

Let $s_n = \sum_{r=1}^n f(r)$. Then on taking $a_r = 1$ and $b_r = f(r)$ in the summation formula, we find that

$$s_n = nf(n) - \sum_{r=1}^{n-1} r(f(r+1) - f(r)).$$

Now if $[t]$ denotes as usual the greatest integer in t , then

* G. H. Hardy: Proc. London Math. Soc. (2), vol. 9, 1910, pp. 126-144.

$$r(f(r+1) - f(r)) = \int_r^{r+1} [t]f'(t)dt.$$

Also

$$nf(n) - 1 \cdot f(1) = \int_1^n \frac{d}{dt} (tf(t))dt,$$

or

$$nf(n) = f(1) + \int_1^n f(t)dt + \int_1^n tf'(t)dt.$$

On substituting these expressions into the formula for s_n , simplifying and transposing, we obtain the formula

$$s_n - \int_1^n f(t)dt = f(1) + \int_1^n (t - [t])f'(t)dt.$$

Now $|(t - [t])f'(t)| < |f'(t)|$. Hence the infinite integral $\int_1^\infty (t - [t])f'(t)dt$ is convergent, and

$$(1) \quad \lim_{n \rightarrow \infty} \left(s_n - \int_1^n f(t)dt \right) \text{ exists.}$$

Now assume that the integral $\int_1^\infty f(t)dt$ is convergent. Then $\lim_{n \rightarrow \infty} \int_1^n f(t)dt$ exists. Hence by (1), $\lim_{n \rightarrow \infty} s_n$ exists; that is, the series $\sum_1^\infty f(n)$ is convergent.

The converse result is a little more troublesome. Assume that $\sum_1^\infty f(n)$ converges. Then

$$(2) \quad \lim_{n \rightarrow \infty} f(n) = 0,$$

and by (1),

$$(3) \quad \lim_{n \rightarrow \infty} \int_1^n f(t)dt \text{ exists.}$$

Now $f(T) = f(1) + \int_1^T f'(t)dt$. But since $\int_1^\infty f'(t)dt$ converges, $\lim_{T \rightarrow \infty} \int_1^T f'(t)dt$ exists. Hence $\lim_{T \rightarrow \infty} f(T)$ exists, so that by (2),

$$(4) \quad \lim_{t \rightarrow \infty} f(t) = 0.$$

Now

$$\begin{aligned} \left| \int_1^T f(t)dt - \int_1^{[T]} f(t)dt \right| &= \left| \int_{[T]}^T f(t)dt \right| \leq \max_{[T] \leq t \leq T} |f(t)| (T - [T]) \\ &< \max_{t \geq [T]} |f(t)|. \end{aligned}$$

Hence by (4)

$$\lim_{T \rightarrow \infty} \left(\int_1^T f(t) dt - \int_1^{[T]} f(t) dt \right) = 0.$$

But

$$\lim_{T \rightarrow \infty} \int_1^{[T]} f(t) dt$$

exists by (3). Hence $\lim_{T \rightarrow \infty} \int_1^T f(t) dt$ exists; that is $\int_1^\infty f(t) dt$ is convergent.

As an example, suppose that $f(t) = t^{-1} e^{-i\mu \log t}$, μ real. Then $f'(t) = O(1/t^2)$ and the conditions of the theorem are met. But

$$\int_1^T f(t) dt = \frac{i}{\mu} (e^{-i\mu \log T} - 1).$$

Hence $\int_1^\infty f(t) dt$ diverges. Therefore $\sum_1^\infty 1/n^{1+i\mu}$ diverges.

Again, suppose that $f(t) = e^{it\alpha\theta}/n^\beta$, where α and θ are real, and $R1 \beta > \alpha > 0$, $\theta \neq 0$. Then $f'(t)$ is continuous and of order $t^{-1-\mu}$, where $\mu = R1 \beta - \alpha$, in the range $1 \leq t < \infty$. Hence the conditions of the theorem are met. Now the infinite integral $\int_1^\infty f(t) dt$ is easily seen to converge on making the change of variable $s = t^\alpha$. Hence the infinite series $\sum_1^\infty e^{in\alpha\theta}/n^\beta$ converges. In particular then, if β is real, we see that the two real series

$$\sum_1^\infty \frac{\cos n^\alpha \theta}{n^\beta} \quad \text{and} \quad \sum_1^\infty \frac{\sin n^\alpha \theta}{n^\beta}$$

both converge if $\beta > \alpha > 0$ and $\theta \neq 0$.

The ordinary integral test is included as a special case if we use Lebesgue integrals; for if $f(t)$ is real, continuous and tends to zero steadily, $f'(t)$ exists almost everywhere and $f(t) = \int_1^t f'(s) ds + f(1)$. Since $|f'(t)| = -f'(t)$, the hypotheses of the theorem are evidently satisfied.

GEOMETRY OF THE SQUARE ROOT OF THREE

C. S. OGILVY, Trinity College, Hartford, Conn.

That the diagonal of a square is incommensurable with its side and the quotient is representable by the continued fraction

$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots$$

is easy to prove geometrically. The corresponding fact that the altitude of an equilateral triangle and half its side are incommensurable and the quotient representable by

type $\alpha_{2,4}$ is indecomposable; $\alpha_{2,8}$ has, apart from order, the unique decomposition into indecomposable factors:

$$\alpha_{2,8} = \alpha_{1,2} \times \alpha_{2,4};$$

and finally $\alpha_{2,12}$ has two different decompositions into indecomposable factors:

$$\alpha_{2,12} = \alpha_{2,6} \times \alpha_{1,2} = \alpha_{2,4} \times \alpha_{1,3}.$$

Thus the last example shows that the refinement theorems 4.7 and 4.8, as well as the unique factorization theorem 4.9, of Jónsson and Tarski cannot be extended to algebras which have an idempotent element but not a zero element. The problem whether the cancellation theorem 4.10 can be extended to such algebras still remains open.

UNIVERSITY OF CALIFORNIA

NOTE ON A PAPER BY C. E. RICKART

R. P. DILWORTH AND MORGAN WARD

In a recent issue of this Bulletin,¹ C. E. Rickart proves the following two theorems:

THEOREM 1. *Any one-to-one multiplicative mapping of a Boolean ring onto an arbitrary ring is necessarily additive.*

THEOREM 3. *Any one-to-one meet preserving mapping of a distributive lattice onto a distributive lattice is also join preserving.*

We should like to point out that both of these theorems are simple consequences of the following well known principle of lattice theory:

Any one-to-one mapping of one lattice onto another lattice which preserves order both ways is a lattice isomorphism.

Now a one-to-one meet preserving mapping of one lattice onto another preserves order both ways; for if x and x' denote corresponding elements,

$$a \geqq b \Leftrightarrow a \cap b = b \Leftrightarrow a' \cap b' = b' \Leftrightarrow a' \geqq b'.$$

CALIFORNIA INSTITUTE OF TECHNOLOGY

Received by the editors September 20, 1948.

¹ Vol. 54 (1948) pp. 758-764.

Chapter 18

1950

ARITHMETICAL PROPERTIES OF THE ELLIPTIC POLYNOMIALS
ARISING FROM THE REAL MULTIPLICATION
OF THE JACOBI FUNCTIONS.*

By MORGAN WARD.

I. Introduction.

1. In a previous paper in this JOURNAL,¹ referred to hereafter as "M," I have made a detailed investigation of the arithmetical properties of the sequence of polynomials (ψ) ,

$$\psi_n = \psi_n(\varphi(u); g_2, g_3), \quad (n = 0, 1, 2, \dots)$$

associated with the real multiplication of the Weierstrass φ function when $\varphi(u)$, g_2 and g_3 are given fixed rational values. If the elliptic discriminant $g_2^3 - 27g_3^2$ vanishes, (ψ) reduces essentially to Lucas' well-known linear sequence (U) ,

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \quad (n = 0, 1, 2, \dots).$$

I study here the arithmetical properties of the four polynomials A_n , B_n , C_n , and D_n associated with the real multiplication of Jacobi's sn , cn , and dn .²

Here each of A_n, \dots, D_n is a polynomial in $sn^2 u$ and k^2 with rational integral coefficients. Consequently, if we substitute for $sn^2 u$ and k^2 two fixed algebraic numbers, we obtain four sequences of algebraic numbers (A) , (B) , (C) and (D) . The arithmetical properties of these elliptic sequences are the subject of this investigation. If k^2 is zero or one, the four sequences reduce essentially to Lucas' sequences (U) and (V) , where $V_n = \alpha^n + \beta^n$.

2. To give an idea of the type of results obtained, choose fixed rational integral values x_0 and a_0 for $sn^2 u$ and k^2 . Then the four elliptic sequences consist exclusively of rational integers. Each sequence is numerically periodic modulo m for any modulus m , but only the sequence (B) is an elliptic

* Received January 28, 1949.

¹ See the reference Ward [1] at the close of this paper.

² If n is an odd integer

$$sn_{n+1}u/sn_nu = B_n/A_n, \quad cn_{n+1}u/cn_nu = C_n/A_n, \quad dn_{n+1}u/D_n/A_n$$

with similar formulas when n is even.

divisibility sequence in the sense of M. The only primes whose laws of apparition present new features of interest are those dividing neither $2a_0(1 - a_0)$ nor $x_0(1 - x_0)(1 - a_0x_0)$. Let p be such a prime, and let its rank of apparition in the divisibility sequence (B) be ρ , so that $B_n \equiv 0 \pmod{p}$ if and only if $n \equiv 0 \pmod{\rho}$. Then if ρ is odd, p divides no term of (A) , (C) or (D) . But if ρ is even, it appears as a divisor of precisely one of the sequences (A) , (C) and (D) . Suppose for example that it is a divisor of (C) . Then no term of (A) or (D) is divisible by p , and $C_n \equiv 0 \pmod{p}$ if and only if n is an odd multiple of $\rho/2$.

The laws of repetition and apparition for powers of primes in (A) , (B) , (C) and (D) are easily reduced to the corresponding laws for (B) which in turn are corollaries of the results in Ward [2] for elliptic divisibility sequences.

3. The plan of the paper is sufficiently clear from the chapter titles. Accounts of the elliptic polynomials A_n, \dots, D_n , are given in Krause [1] and Fricke [2]; but there are errors in the formulas given in these works. Although the properties of the Al functions³ on which we base the theory were very completely worked out in Weierstrass [1], most of the formulas which we utilize are most simply obtained by transformation from the corresponding σ or θ function formulas.

II. Properties of Weierstrass *AL* Functions.

4. The multiplication theory of the Jacobian elliptic functions is most conveniently developed in terms of certain modified θ functions, the Al functions of Weierstrass (Weierstrass, [1]). These may be defined as follows: Let v be a complex variable, $q = e^{\pi i \tau}$ with $\text{Im } \tau > 0$, $u = 2Kv$, where K is the complete elliptic integral. The Jacobi theta functions are then

$$\begin{aligned}\Theta(u) &= \theta_0(v) = \sum_{-a}^{+a} (-1)^m q^{m^2} e^{2m\pi iv}, \\ H(u) &= \theta_1(v) = -i \sum_{-a}^{+a} (-1)^m q^{(m+\frac{1}{2})^2} e^{(2m+1)\pi iv} \\ H_1(u) &= \theta_2(v) = \sum_{-a}^{+a} q^{(m+\frac{1}{2})^2} e^{(2m+1)\pi iv}, \\ \Theta_1(u) &= \theta_3(v) = \sum_{-a}^{+a} q^{m^2} e^{2m\pi iv}.\end{aligned}$$

³ The functions were named by Weierstrass in honor of Abel who was the first to consider them.

If we write θ_a for $\theta_a(0)$ and θ_0 for $\theta_0(0)$, then Weierstrass Al functions may be defined by

$$(4.1) \quad \begin{aligned} Al_1(u) &= \theta_3/\theta_0\theta_2 \exp(-\frac{1}{2}v^2\theta''_0/\theta_0)\theta_1(v), \\ Al_\alpha(u) &= 1/\theta_\alpha \exp(-\frac{1}{2}v^2\theta''_0/\theta_0)\theta_\alpha(v), \end{aligned} \quad (\alpha = 0, 2, 3).$$

Note that $Al_1(u)$ is odd and $Al_2(u)$, $Al_3(u)$ and $Al_0(u)$ even. Also

$$(4.11) \quad Al_1(0) = 0, \quad Al_\alpha(0) = 1, \quad (\alpha = 0, 2, 3).$$

sn , cn and dn have particularly simple expressions in terms of the Al s; namely

$$(4.2) \quad snu = Al_1(u)/Al_0(u), \quad cnu = Al_2(u)/Al_0(u), \quad dnu = Al_3(u)/Al_0(u).$$

The relationship to the Weierstrass σ functions is also very simple; namely if $w = \omega u/K$, then

$$(4.3) \quad \begin{aligned} Al_1(u) &= (e_1 - e_3)^{\frac{1}{2}} e^{e_3 w^2/2} \sigma(w); & Al_3(u) &= e^{e_3 w^2/2} \sigma_2(w); \\ Al_2(u) &= e^{e_3 w^2/2} \sigma_1(w); & Al_0(u) &= e^{e_3 w^2/2} \sigma_3(w). \end{aligned}$$

For the lemniscate case, $e_3 = 0$ and the Al functions are essentially the σ functions.

The fundamental three-terms sigma identity becomes

$$(4.4) \quad \begin{aligned} & Al_1(u + u_1)Al_1(u - u_1)Al_1(u_2 + u_3)Al_1(u_2 - u_3) \\ & + Al_1(u + u_2)Al_1(u - u_2)Al_1(u_3 + u_1)Al_1(u_3 - u_1) \\ & + Al_1(u + u_3)Al_1(u - u_3)Al_1(u_1 + u_2)Al_1(u_1 - u_2) = 0. \end{aligned}$$

5. We next introduce four new functions $K_{an}(u)$ of u and n by the definition

$$(5.1) \quad K_{an} = Al_\alpha(nu)/Al_0(u)^n, \quad (n = 0, 1, 2, \dots; \alpha = 0, 1, 2, 3).$$

Evidently

$$(5.2) \quad snnu = K_{1n}/K_{0n}, \quad cnnu = K_{2n}/K_{0n}, \quad dnnu = K_{3n}/K_{0n}.$$

The first three initial values of the four sequences (K_a) are as follows:

TABLE I. Initial values of K_{an} .

α/n	0	1	2
0	1	1	$1 - k^2 sn^4 u$.
1	0	snu	$2snu \ cnu \ dnu$.
2	1	cnu	$1 - 2sn^2 u + k^2 sn^4 u$.
3	1	dnu	$1 - 2k^2 sn^2 n + k^2 sn^4 u$.

There are twenty-four addition formulas for the products $Al_\alpha(u+v) \times Al_\beta(u-v)$ obtainable by simple transformations from the corresponding formulas for $\theta_\alpha(u+v)\theta_\beta(u-v)$ or by suitably specializing (4.4). If in these formulas we replace u by nu and v by mu and divide by $Al_0(u)^{2(n^2+m^2)}$, we obtain on using (5.1) twenty-four addition formulas for the products $K_{\alpha n+m}K_{\beta n-m}$. It is sufficient to quote here a few such formulas as examples:

TABLE II. Addition formulas for $K_{\alpha n}$.

$$\begin{aligned}
 (i) \quad & K_{0n+m}K_{0n-m} = K_{0n}^2 K_{0m}^2 - k^2 K_{1n}^4 K_{1m}^2. \\
 & \cdot \quad \cdot \quad \cdot \quad \cdot \\
 (v) \quad & K_{1n+m}K_{1n-m} = K_{1n}^2 K_{0m}^2 - K_{0n}^2 K_{1m}^2. \\
 & \cdot \quad \cdot \quad \cdot \quad \cdot \\
 (xix) \quad & K_{0n+m}K_{1n-m} = K_{0n}K_{1n}K_{2m}K_{3m} - K_{2n}K_{3n}K_{0m}K_{1m}. \\
 & \cdot \quad \cdot \quad \cdot \quad \cdot \\
 (xxiv) \quad & K_{2n+m}K_{3n-m} = K_{2n}K_{3n}K_{2m}K_{3m} - k'^2 K_{0n}K_{1n}K_{0m}K_{1m}.
 \end{aligned}$$

In formula (xxiv), k'^2 is the complementary modulus $1-k^2$.

If we take $m=\pm n$ or $m=n$ and $n=n+1$ in the addition formulas, we obtain a set of over forty "duplication formulas" which it is also unnecessary to give in detail; the two formulas so obtained from (i) and (xix) suffice as examples:

$$(5.3) \quad K_{12n+1}K_{11} = K_{1n+1}^2 K_{0n}^2 - K_{0n+1}^2 K_{1n}^2,$$

$$(5.4) \quad K_{12n} = 2K_{0n}K_{1n}K_{2n}K_{3n}.$$

As noted in Krause [1], the duplication formulas allow many results about the algebraic form of the polynomials $K_{\alpha n}$ to be proved by mathematical induction from the initial values given in Table I; the results in the next section are easily obtained in this manner.

III. The Four Elliptic Polynomials.

6. If we write

$$\begin{aligned}
 (6.1) \quad & K_{0n}(u) = A_n(sn^2 u; k^2) & n \text{ odd or even}; \\
 & snuB_n(sn^2 u; k^2) & n \text{ odd}; \\
 & K_{1n}(u) = & \\
 & \quad snu cnu dnuB_n(sn^2 u; k^2) & n \text{ even}; \\
 & \quad cnucnuC_n(sn^2 u; k^2) & n \text{ odd};
 \end{aligned}$$

$$\begin{aligned}
K_{2n}(u) &= \\
&\quad C_n(sn^2u; k^2) && n \text{ even;} \\
&\quad dnuD_n(sn^2u; k^2) && n \text{ odd;} \\
K_{3n}(u) &= \\
&\quad D_n(sn^2u; k^2) && n \text{ even;}
\end{aligned}$$

then (Krause [1], pp. 159-162, Fricke [2], Chapter 2) A_n , B_n , C_n and D_n are polynomials in sn^2u and k^2 with rational integral coefficients. It is convenient to let

$$(6.2) \quad x = sn^2u, \quad a = k^2.$$

Then

$$(6.3) \quad K_{1n}(u) = \begin{cases} (x)^{\frac{1}{2}}B_n(x; a), & n \text{ odd;} \\ (x(1-x)(1-ax))^{\frac{1}{2}}B_n(x; a), & n \text{ even;} \end{cases}$$

with similar formulas for K_{0n} , K_{2n} and K_{3n} .

We shall refer to A_n , B_n , C_n and D_n as the "elliptic polynomials of order n ." If we let

$$(6.4) \quad \alpha_n = \begin{cases} (n^2 - 1)/2, & n \text{ odd,} \\ n^2/2, & n \text{ even,} \end{cases} \quad \beta_n = \begin{cases} (n^2 - 1)/2 & n \text{ odd,} \\ (n^2 - 4)/2 & n \text{ even,} \end{cases}$$

then A_n , C_n and D_n are of degree α_n in x and B_n is of degree β_n in x .

7. There are a number of transformation formulas for the elliptic polynomials (Krause [1], Chapter III, Fricke [1], [2]) which are of arithmetical importance. These arise either by increasing u in the Al and K_n functions by the quarter periods K , iK' and $K + iK'$ or by performing the fundamental substitutions $\tau \rightarrow \tau + 1$, $\tau \rightarrow -1/\tau$ of the modular group on the four Al functions. It suffices here to develop one formula of each type by way of example.

Weierstrass showed that

$$\begin{aligned}
Al_0(u + K) &= 1/k'^{\frac{1}{2}} e^{\lambda(u^2 - (u+K)^2)} Al_3(u), \\
Al_3(u + 2K) &= e^{\lambda(u^2 - (u+K)^2)} Al_3(u),
\end{aligned}$$

where we have written λ for $(K - E)/2K$.

It easily follows that if n is odd,

$$Al_0(u + nK) = 1/k'^{\frac{1}{2}} e^{\lambda(u^2 - (u+nK)^2)} Al_3(u).$$

Hence

$$\begin{aligned} K_{0n}(u+K) \\ = Al_0(nu+nK)/Al_0(u+K)^{n^2} = k'^{(n^2-1)/2}(Al_3(nu)/Al_3(u))^{n^2}. \end{aligned}$$

On multiplying both sides of this expression by $dnu^{n^2} = (Al_3(u)/Al_0(u))^{n^2}$, we find that

$$(7.1) \quad dnu^{n^2}K_{0n}(u+K) = k'^{(n^2-1)/2}K_{3n}(u).$$

Now $sn(u+K) = cn u / dnu$. Hence the substitution of $u+K$ for u induces the substitution of $(1-x)/(1-ax)$ for $x = sn^2 u$. Therefore we obtain from (7.2) on substituting for K_{an} their expressions in terms of A_n and D_n the transformation formula

$$(1-ax)^{\alpha_n} A_n((1-x)/(1-ax)) = (1-a)^{\alpha_n/2} D_n(x) \quad n \text{ odd.}$$

The following sets of transformation formulas are obtained by proceeding systematically in this manner.

8. The modular transformation $\tau \rightarrow -1/\tau$ is simply Jacobi's imaginary transformation $u \rightarrow iu$, $k \rightarrow k'$. Now Weierstrass⁴ showed that

$$\begin{aligned} Al_3(iu; k') &= e^{u^2/2} Al_3(u; k) \\ Al_0(iu; k') &= e^{u^2/2} Al_2(u; k) \end{aligned}$$

Hence

$$K_{3n}(iu; k') = Al_3(niu; k')/Al_0(iu; k')^{n^2} = Al_3(nu; k)/Al_2(u; k)^{n^2}$$

or

$$(8.1) \quad K_{3n}(iu; k') = cn u^{-n^2} K_{3n}(u; k).$$

But since $sn(iu, k') = isn(u, k) / cn(u, k)$, Jacobi's imaginary transformation induces the transformation

$$(8.2) \quad x \rightarrow -x/(1-x), \quad a \rightarrow 1-a$$

on x and a .

Now $K_{3n} = (1-ax)^{\frac{1}{2}} D_n$ or D_n according as n is odd or even, and (8.2) throws $\sqrt{1-ax}$ into $(1-ax)^{\frac{1}{2}}/1-x$. Hence on substituting into (8.1) and using the abbreviation α_n for $(n^2-1)/2$ or $n^2/2$ we obtain the formula

$$(1-x)^{\alpha_n} D_n(x/(x-1); 1-a) = D_n(x; a).$$

The formulas listed below were obtained by systematically combining

⁴ Weierstrass [1], page 20.

TABLE III. Transformation formulas.

<i>n odd</i>	<i>n even</i>
$(1 - ax)^{a_n} A_n((1 - x)/(1 - ax)) = (1 - a)^{a_n/2} D_n(x) ;$	$= (1 - a)^{a_n/2} A_n(x)$
$(1 - ax)^{\beta_n} B_n((1 - x)/(1 - ax)) = (-1)^{(n-1)/2} (1 - a)^{\beta_n/2} C_n(x) ;$	$= (-1)^{(n-2)/2} (1 - a)^{\beta_n/2}(x)$
$(1 - ax)^{a_n} C_n((1 - x)/(1 - ax)) = (-1)^{(n-1)/2} (1 - a)^{a_n/2} B_n(x) ;$	$= (-1)^{n/2} (1 - a)^{a_n/2} C_n(x)$
$(1 - ax)^{a_n} D_n((1 - x)/(1 - ax)) = (1 - a)^{a_n/2} A_n(x) ;$	$= (1 - a)^{a_n/2} D_n(x)$
$(\sqrt{ax})^{a_n} A_n(1/ax) = (-1)^{(n-1)/2} B_n(x) ;$	$= (-1)^{n/2} A_n(x)$
$(\sqrt{ax})^{\beta_n} B_n(1/ax) = (-1)^{(n-1)/2} A_n(x) ;$	$= (-1)^{(n-2)/2} B_n(x)$
$(\sqrt{ax})^{a_n} C_n(1/ax) = D_n(x) ;$	$= C_n(x)$
$(\sqrt{ax})^{a_n} D_n(1/ax) = C_n(x) ;$	$= D_n(x)$
$(1 - x)^{a_n} A_n((1 - ax)/(a - ax)) = ((1 - a)/a)^{a_n/2} C_n(x) ;$	$= (-1)^{n/2} ((1 - a)/a)^{a_n/2} A_n(x)$
$(1 - x)^{\beta_n} B_n((1 - ax)/(a - ax)) = (-1)^{(n-1)/2} ((1 - a)/a)^{\beta_n/2} D_n(x) ;$	$= ((1 - a)/a)^{\beta_n/2} B_n(x)$
$(1 - x)^{a_n} C_n((1 - ax)/(a - ax)) = ((1 - a)/a)^{a_n/2} A_n(x) ;$	$= (-1)^{n/2} ((1 - a)/a)^{a_n/2} C_n(x)$
$(1 - x)^{a_n} D_n((1 - ax)/(a - ax)) = (-1)^{(n-1)/2} ((1 - a)/a)^{a_n/2} B_n(x) ;$	$= ((1 - a)/a)^{a_n/2} D_n(x).$

the two transformations $\tau \rightarrow -1/\tau$ and $\tau \rightarrow 1 + \tau$; the latter transformation induces the transformation

$$(8.3) \quad x \rightarrow (x - ax)/(1 - ax), \quad a \rightarrow a/(a - 1)$$

on x and a .

TABLE IV. Transformation formulas.

$$\begin{aligned} A_n(x; a) &= (1 - ax)^{\alpha_n} D_n((x - ax)/(1 - ax); a/(a - 1)) \\ &= (1 - x)^{\alpha_n} C_n(x/(x - 1); 1 - a), \\ &= (1 - ax)^{\alpha_n} C_n(ax/(ax - 1); (a - 1)/a) = A_n(ax; 1/a) \\ &= (1 - x)^{\alpha_n} D_n((ax - x)/(1 - x); 1/(1 - a)). \\ B_n(x; a) &= (1 - ax)^{\beta_n} B_n((x - ax)/(1 - ax); a/(a - 1)) \\ &= (1 - x)^{\beta_n} B_n(x/(x - 1); 1 - a), \\ &= (1 - ax)^{\beta_n} B_n(ax/(ax - 1); (a - 1)/a) = B_n(ax; 1/a) \\ &= (1 - x)^{\beta_n} B_n((ax - x)/(1 - x); 1/(1 - a)). \\ (8.4) \quad C_n(x; a) &= (1 - ax)^{\alpha_n} C_n((x - ax)/(1 - ax); a/(a - 1)) \\ &= (1 - x)^{\alpha_n} A_n(x/(x - 1); 1 - a), \\ &= (1 - ax)^{\alpha_n} D_n(ax/(ax - 1); (a - 1)/a) = D_n(ax; 1/a) \\ &= (1 - x)^{\alpha_n} A_n((ax - x)/(1 - x); 1/(1 - a)). \\ D_n(x; a) &= (1 - ax)^{\alpha_n} A_n((x - ax)/(1 - ax); a/(a - 1)) \\ &= (1 - x)^{\alpha_n} D_n(x/(x - 1); 1 - a), \\ &= (1 - ax)^{\alpha_n} A_n(ax/(ax - 1); (a - 1)/a) = C_n(ax; 1/a) \\ &= (1 - x)^{\alpha_n} C_n((ax - x)/(1 - x); 1/(1 - a)). \end{aligned}$$

We finally tabulate for later reference the first few initial values of the four elliptic sequences.

TABLE V. Initial values.

n	0	1	2	3
A_n	1	1	$1 - ax^2$	$1 - 6ax^2 + 4a(1 + a)x^3 - 3a^2x^4$
B_n	0	1	2	$3 - 4(1 + a)x + 6ax^2 - a^2x^4$
C_n	1	1	$1 - 2x + ax^2$	$1 - 4x + 6ax^2 - 4a^2x^3 + a^2x^4$
D_n	1	1	$1 - 2ax + ax^2$	$1 - 4ax + 6ax^2 - 4ax^3 + a^2x^4$

The transformation formulas of Tables III and IV may all be proved without function theory by mathematical induction from the duplication formulas and the initial values in Table V.

IV. Elliptic Divisibility Sequences in Domains of Integrity.

9. In \mathcal{M} , the functional equation

$$(9.1) \quad \omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$

was solved completely over the ring of rational integers and over the field of all complex numbers. It is necessary for the purposes of this paper to extend certain theorems of \mathcal{M} to solutions of (9.1) over more general rings.

Let \mathcal{R} denote a domain of integrity; (commutative ring with a unit and no divisors of zero). \mathcal{R} may be a field; in any event we denote its quotient field by \mathcal{F} , and for brevity refer to \mathcal{R} as a ring. We are interested in solutions of (9.1) over \mathcal{R} and over \mathcal{F} . We lay down the following definitions:

A particular solution

$$(h) : h_0, h_1, h_2, \dots, h_n, \dots$$

of (9.1) will be said to belong to \mathcal{R} (to \mathcal{F}) if all its terms belong to \mathcal{R} (to \mathcal{F}). If a and b belong to \mathcal{R} , we say that a divides b in \mathcal{R} if there exists an element c of \mathcal{R} such that $ac = b$. We write: $a | b (\mathcal{R})$.

In particular, if \mathcal{R} is a field, and $b \neq 0$, $a | b (\mathcal{R})$ for every $a \neq 0$.

If m is an ideal of \mathcal{R} , $a \equiv b (m)$ means as usual $a - b$ is contained in m .

If p is a maximal ideal of \mathcal{R} , the quotient ring \mathcal{R}/p is a field. If this field is finite its order is a power of a certain rational prime p . We denote the order by $Np = p^f$ and call p the (rational) prime belonging to p .

Definition 9.1. A solution of (9.1) is said to be “regular over \mathcal{F} ” if it belongs to \mathcal{F} and if

$$(9.2) \quad h_0 = 0, \quad h_1 = 1, \quad h_2, h_3 \text{ not both zero.}$$

Definition 9.2. A solution (h) of (9.1) is said to be “a divisibility sequence over \mathcal{R} ” if it belongs to \mathcal{R} and if

$$(9.3) \quad h_r | h_s (\mathcal{R}) \quad \text{whenever } r | s.$$

Let (h) belong to \mathcal{R} , and let m be an ideal of \mathcal{R} . m is called a divisor of (h) if it contains at least one term h_{n_0} of the sequence (h) with $n_0 > 0$. n_0 is called a “place of apparition” of m in (h) . If in addition $h_r \not\equiv 0 \pmod{m}$ for every proper divisor r of n_0 , then n_0 is called a rank of apparition of m in (h) .

10. The proofs of the theorems which follow are by mathematical

induction with the exception of the proof of Theorem 10.7 which uses the Dirichlet box principle. In any event they are almost word for word the same as corresponding theorems in M for the special cases when \mathcal{R} is the ring of rationals or the complex field. We shall accordingly cite the corresponding results in M for the details of proof.

THEOREM 10.1. *Let (h) be a sequence satisfying the following three conditions:*

$$(10.1) \quad (h) \text{ is a regular solution of (9.1) over } \mathfrak{F},$$

$$(10.2) \quad h_2, h_3 \text{ and } h_4 \text{ belong to } \mathcal{R},$$

$$(10.3) \quad h_2 \mid h_4 (\mathcal{R}).$$

Then (h) is a divisibility sequence over \mathcal{R} uniquely determined by its initial values h_2 , h_3 and h_4 .

Proof. M, Theorem 4.1. Chapter II.

THEOREM 10.2. *Under the hypotheses of Theorem 10.1,*

$$(10.4) \quad h_n = P_n(h_2, h_3, h_4),$$

where P_n is a polynomial in h_2 , h_3 , h_4 with rational integral coefficients and such that for any element a of \mathfrak{F}

$$(10.5) \quad P_n(a^3h_2, a^6h_3, a^{15}h_4) = a^{n^2-1}P_n(h_2, h_3, h_4).$$

Proof. M, Theorem 4.1. Chapter II.

THEOREM 10.3. *If (k) is any regular solution of (9.1) over \mathfrak{F} and a any non-zero element of \mathfrak{F} , then (l) is also a regular solution over \mathfrak{F} , where*

$$l_n = a^{n^2-1}k_n, \quad (n = 0, 1, 2, \dots).$$

THEOREM 10.4. *If (k) is any regular solution of (1.1) over \mathfrak{F} , then there always exists an element a of \mathfrak{F} and a regular solution (h) of (9.1) over \mathcal{R} satisfying conditions (10.1), (10.2) and (10.3) such that*

$$k_n = a^{n^2-1}h_n, \quad (n = 0, 1, 2, \dots).$$

Proof. M, Theorems 21.1, 21.3.

THEOREM 10.5. *Let (k) be a regular solution of (1.1) over \mathfrak{F} with $k_2 \neq 0$. Then if two consecutive terms of (k) are zero, all terms vanish beyond the third.*

THEOREM 10.6. *Let (h) be a solution of (1.1) over \mathcal{R} with $h_0 = 0$ and $h_1 = 1$ (but not necessarily a regular solution). Then if (h) is a divisibility sequence over \mathcal{R} and two consecutive terms of (h) vanish, all terms of (h) vanish beyond the third.*

Proof. M, Lemma 4.1.

It is shown in M that the hypothesis that (h) is a divisibility sequence in Theorem 10.6 is necessary for the truth of the theorem when (h) is not regular; that is, when both h_2 and h_3 are zero.

THEOREM 10.7. *Let (h) be an elliptic divisibility sequence over \mathcal{R} , and let \mathfrak{p} be a prime ideal of \mathcal{R} whose quotient ring \mathcal{R}/\mathfrak{p} is of finite order $N\mathfrak{p}$. Then \mathfrak{p} is a divisor of (h) , and has a rank of apparition r in (h) less than $2(N\mathfrak{p} + 1)$.*

Proof. M, Theorem 5.1.

It is shown in M that the upper limit $2(N\mathfrak{p} + 1)$ is the best possible for the rank of \mathfrak{p} in (h) .

V. The Laws of Apparition of Prime Ideals in Elliptic Sequences.

11. The connection between the results of Chapter IV and the elliptic polynomials is made by the following theorem.

THEOREM 11.1. *If u_0 is neither a zero nor a pole of snu and if*

$$(11.1) \quad h_n = K_{1n}(u_0)/K_{11}(u_0) = K_{1n}/K_{11} \quad (n = 0, 1, 2, \dots)$$

then the sequence (h) is a solution of the functional equation

$$(9.1) \quad \omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$

over the complex field.

Proof. Let l, m and n be fixed integers. Take $u = 0$, $u_1 = lu_0$, $u_2 = mu_0$ and $u_3 = nu_0$ in the basic three-term identity (4.4), and divide by the non-zero quantity $Al_0(u_0)^2(l^2+m^2+n^2)$. Then we obtain on substitution, from (5.1) the formula

$$K_{1l}^2 K_{1m+n} K_{1m-n} + K_{1m}^2 K_{1n+l} K_{1n-l} + K_{1n}^2 K_{1l+m} K_{1l-m} = 0.$$

Now $K_{11} = snu_0 \neq 0$. Hence on letting $l = 1$ and dividing by K_{11}^4 , we obtain from (11.1) the formula

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2;$$

for $K_{1l-m} = -K_{1m-l}$.

We shall now assign to x and to a algebraic integer values x_0 and a_0 . Let \mathfrak{F}_1 be the field $F[x_0, a_0]$ obtained by adjoining x_0 and a_0 to the rational field F , and let \mathcal{R}_1 be the ring of integers of \mathfrak{F}_1 . Let \mathfrak{F} be the field $F[x_0^{\pm}, 1 - x_0^{\pm}, 1 - a_0x_0^{\pm}]$, and \mathcal{R} the ring of integers of \mathfrak{F} . Clearly $\mathcal{R} \supseteq \mathcal{R}_1$, $\mathfrak{F} \supseteq \mathfrak{F}_1$, and every ideal of either ring has a finite norm. We shall use German letters to denote either ideals of \mathcal{R} or of \mathcal{R}_1 , and let \mathfrak{p} denote as usual a prime ideal, and p the corresponding rational prime.

The four elliptic sequences (A) , (B) , (C) and (D) belong to \mathcal{R}_1 while the four sequences (K_x) , ($x = 0, 1, 2, 3$) belong to \mathcal{R} .

Let u_0 be chosen in a period parallelogram so that⁵

$$sn u_0 = (x_0)^{\frac{1}{2}}.$$

Then

$$(11.2) \quad h_n = \begin{cases} B_n(x_0, a_0), & n \text{ odd}, \\ ((1-x_0)(1-a_0x_0))^{\frac{1}{2}}B_n(x_0, a_0), & n \text{ even}. \end{cases}$$

Hence the initial values of (h) are

$$\begin{aligned} h_0 &= 0, & h_1 &= 1, & h_2 &= 2((1-x_0)(1-a_0x_0))^{\frac{1}{2}}, \\ h_3 &= B_3(x_0, a_0), & h_4 &= ((1-x_0)(1-a_0x_0))^{\frac{1}{2}}B_4(x_0, a_0). \end{aligned}$$

Now by direct calculation or from Table III,

$$(11.3) \quad B_3(1; a_0) = -(1-a_0)^2, \quad B_3(1/a_0; a_0) = -(1-a_0/a_0^2)^2.$$

Hence h_2 and h_3 both vanish if and only if $x_0 = 1$ and $a_0 = 1$. Also $h_4 = 2h_2A_2C_2D_2$ by formula (5.4). Hence $h_2 \mid h_4$ (\mathcal{R}).

Thus the sequence (h) satisfies all the hypotheses of Theorem 10.1. We may consequently state

THEOREM 11.1. *Unless both x_0 and a_0 are unity, the sequence (h) defined by*

$$(11.2) \quad h_n = B_n(x_0; a_0), \quad n \text{ odd}; \\ = ((1-x_0)(1-a_0x_0))^{\frac{1}{2}}B_n(x_0; a_0), \quad n \text{ even}$$

is an elliptic divisibility sequence over the ring \mathcal{R} . Every prime ideal \mathfrak{p} of \mathcal{R} is a divisor of (h) . Furthermore, if \mathfrak{p} does not divide both h_3 and h_4 then \mathfrak{p} has a unique rank of apparition ρ in (h) such that

$$(11.4) \quad h_n \equiv 0 \pmod{\mathfrak{p}} \quad \text{if and only if } n \equiv 0 \pmod{\rho}.$$

⁵ Two choices of u_0 are possible; for definiteness let u_0 be chosen with smallest imaginary part; if u_0 is real, with smallest real part.

If \mathfrak{p} does divide both h_3 and h_4 , it divides every subsequent term of (h) by Theorem 10.5. We call such primes “null divisors” of (h) .

12. Let \mathfrak{p} be a null divisor of (h) . Then

$$(12.1) \quad B_3(x_0; a_0) \equiv 0 \pmod{\mathfrak{p}},$$

$$((1 - x_0)(1 - a_0x_0))^{\frac{1}{2}}B_4(x_0; a_0) \equiv 0 \pmod{\mathfrak{p}}.$$

We first consider the case when \mathfrak{p} divides both B_3 and B_4 . Then the two polynomials $B_3(x, a_0)$ and $B_4(x, a_0)$ have a common root in the field $\mathcal{R}_1/\mathfrak{p}$. Hence their resultant must vanish in this field. Now this resultant is found to have the value $2^{20}a_0^4(1 - a_0)^9$. Hence either $a_0 \equiv 0$, $a_0 \equiv 1$ or $2 \equiv 0 \pmod{\mathfrak{p}}$.

$a_0 \not\equiv 0 \pmod{\mathfrak{p}}$. For if $a_0 \equiv 0$, then by Table V, $B_3(x_0, a_0) \equiv 3 - 4x_0$ and $B_4(x_0, a_0) \equiv 4 - 8x_0 \pmod{\mathfrak{p}}$. But the congruences $3 - 4x_0 \equiv 4 - 8x_0 \equiv 0 \pmod{\mathfrak{p}}$ are impossible.

If $a_0 \equiv 1 \pmod{\mathfrak{p}}$, then $x_0 \equiv 1 \pmod{\mathfrak{p}}$. For by Tables IV and V,

$$\begin{aligned} B_3(x_0, a_0) &\equiv (1 - x_0)^3(3 - x_0) \\ B_4(x_0, a_0) &\equiv 4(1 - x_0)^5(1 + x_0) \end{aligned} \pmod{\mathfrak{p}}$$

if $a_0 \equiv 1$. Hence if $x_0 \not\equiv 1 \pmod{\mathfrak{p}}$, we must have $3 - x_0 \equiv 2 + 2x_0 \equiv 0 \pmod{\mathfrak{p}}$ but $1 - x_0 \not\equiv 0 \pmod{\mathfrak{p}}$, which is impossible.

Now finally if $2 \equiv 0 \pmod{\mathfrak{p}}$ but $a_0 \not\equiv 1 \pmod{\mathfrak{p}}$, since $B_4(x_0; a_0) \equiv 0 \pmod{2}$ and $B_3(x_0; a_0) \equiv (1 - a_0x_0^2)^2 \pmod{2}$ we must have $1 - a_0x_0^2 \equiv 0 \pmod{\mathfrak{p}}$. Hence since $a_0 \not\equiv 1 \pmod{\mathfrak{p}}$,

$$((1 - x_0)(1 - a_0x_0))^{\frac{1}{2}} \not\equiv 0 \pmod{\mathfrak{p}}.$$

If on the other hand $((1 - x_0)(1 - a_0x_0))^{\frac{1}{2}} \equiv 0 \pmod{\mathfrak{p}}$, it is easily shown that the previous case $a_0 \equiv x_0 \equiv 1 \pmod{\mathfrak{p}}$ must hold. We have thus proved

THEOREM 12.1. *The only prime ideal null divisors of (h) are primes dividing $2(1 - a_0)$. Necessary and sufficient conditions that \mathfrak{p} be a null divisor are that either*

$$\begin{aligned} a_0 &\equiv 1 \text{ and } x_0 \equiv 1 \pmod{\mathfrak{p}} \text{ or} \\ 2 &\equiv 0 \text{ and } a_0x_0^2 \equiv 1 \pmod{\mathfrak{p}} \text{ but} \\ a_0 &\not\equiv 1 \text{ and } x_0 \not\equiv 1 \pmod{\mathfrak{p}}. \end{aligned}$$

In the lemniscate case, for example when $a_0 = -1$, the only null divisors are divisors of two for which $x_0 \equiv 1 \pmod{\mathfrak{p}}$. Hence if x_0 is an even rational integer, there are no null divisors.

13. We may classify the prime ideals of both \mathcal{R} and \mathcal{R}_1 into three categories:

- I. Ideals dividing $2a_0(1 - a_0)$.
- II. Ideals dividing $x_0(1 - x_0)(1 - a_0x_0)$.
- III. Ideals dividing neither $2a_0(1 - a_0)$ nor $x_0(1 - x_0)(1 - a_0x_0)$.

Ideals of the first and second categories will be called irregular; they include all null divisors, and are usually finite in number. Ideals of the third category will be called regular. In this section, we shall determine their laws of apparition in the elliptic sequences (A), (B), (C) and (D).

THEOREM 13.1. *No regular prime ideal can divide any two of A_n , B_n , C_n and D_n for the same value of n . Common divisors of $A_n, B_n; A_n, C_n; \dots, C_n, D_n$ are always null divisors of the sequence (B).*

Proof. Suppose, for example, that for a certain fixed value of n

$$A_n \equiv 0 \pmod{\mathfrak{p}} \text{ and } B_n \equiv 0 \pmod{\mathfrak{p}}, \quad \mathfrak{p} \text{ regular.}$$

Then $K_{0n} \equiv 0 \pmod{\mathfrak{p}}$ and $K_{1n} \equiv 0 \pmod{\mathfrak{p}}$. Hence by the duplication formulas (5.3) and (5.4),

$$K_{12n} = K_{11}K_{12n+1} \equiv 0 \pmod{\mathfrak{p}}$$

so that $K_{11}h_{2n} = K_{12n}^2 \equiv 0 \pmod{\mathfrak{p}}$ by formula (11.1). But $K_{11}^2 = sn^2u_0 - x_0 \not\equiv 0 \pmod{\mathfrak{p}}$. Hence \mathfrak{p} divides two consecutive terms of the elliptic divisibility sequence (h). Therefore by Theorems 11.1, 10.5 and 12.2, $h_3 \equiv h_4 \equiv 0 \pmod{\mathfrak{p}}$, $2(1 - a_0) \equiv 0 \pmod{\mathfrak{p}}$, contrary to the hypothesis that \mathfrak{p} is regular.

It can be shown from the duplication formulas that a similar contradiction ensues if it is assumed that any other pair from A_n , B_n , C_n and D_n is divisible by \mathfrak{p} .

14. For regular prime ideals, the rank ρ of \mathfrak{p} in (h) and in (B) is evidently the same. Hence if \mathfrak{p} is regular,

$$(14.1) \quad B_n \equiv 0 \pmod{\mathfrak{p}} \quad \text{if and only if } n \equiv 0 \pmod{\rho},$$

where ρ is a fixed positive integer depending only on \mathfrak{p} and B_3 and B_4 .

THEOREM 14.1. *Let \mathfrak{p} be a regular prime ideal. Then if the rank of apparition of \mathfrak{p} in (B) is odd, \mathfrak{p} is not a divisor of (A), (C) or (D).*

Proof. Let \mathfrak{p} be regular. Then $B_n \equiv 0 \pmod{\mathfrak{p}}$ if and only if $K_{1n} \equiv 0 \pmod{\mathfrak{p}}$; similarly A_n , C_n or D_n are divisible by \mathfrak{p} only if K_{0n} , K_{2n} or K_{3n} are divisible by \mathfrak{p} . Suppose that \mathfrak{p} is of odd rank ρ in (B) and a divisor

of (A) , for example. Then there exists a term A_k of (A) such that $A_k \equiv 0 \pmod{p}$. Now by the duplication formula (5.4),

$$(14.2) \quad K_{2k} \equiv 2K_{0k}K_{1k}K_{2k}K_{3k}.$$

Hence by the preceding remarks, $B_{2k} \equiv 0 \pmod{p}$ so that $p \mid 2k$ by (14.1). Therefore $p \mid k$ so that $A_k \equiv B_k \equiv 0 \pmod{p}$ contrary to Theorem 13.1. In like manner, p cannot be a divisor of (C) or (D) .

THEOREM 14.2. *Let p be a regular prime ideal of even rank of apparition in (B) . Then p is a divisor of precisely one of the three sequences (A) , (C) and (D) . If p is a divisor of (C) , then $C_n \equiv 0 \pmod{p}$ if and only if n is an odd multiple of $p/2$, with similar results if p is a divisor of (A) or (D) .*

Proof. Let p and ρ satisfy the hypothesis of the theorem. Then by the duplication formula (5.4)

$$K_{1\rho} \equiv 2K_{0(\rho/2)}K_{1(\rho/2)}K_{2(\rho/2)}K_{3(\rho/2)} \pmod{p}.$$

Hence since $B_\rho \equiv 0 \pmod{p}$ and p is regular, precisely one of $A_{\rho/2}$, $B_{\rho/2}$, $C_{\rho/2}$, $D_{\rho/2}$ is divisible by p . Evidently, $B_{\rho/2} \not\equiv 0 \pmod{p}$. Assume that $C_{\rho/2} \equiv 0 \pmod{p}$ so that p is a divisor of (C) . Then p is not a divisor of (A) or (D) . For if for example $D_k \equiv 0 \pmod{p}$, then by the duplication formula (14.2), $B_{2k} \equiv 0 \pmod{p}$. Hence $p \mid 2k$, $p/2 \mid k$ and $B_k \equiv 0 \pmod{p}$ contrary to Theorem 13.1. In precisely the same way we can show that $A_k \not\equiv 0 \pmod{p}$, and that if $C_k \equiv 0 \pmod{p}$, then k must be an odd multiple of $p/2$. It remains to prove the converse of this last statement. Consider then any term C_k of the sequence (C) in which k is a multiple of $p/2$. Then $2k$ is a multiple of p . Hence by (14.1) and (14.2)

$$0 \equiv 2A_kB_kC_kD_k \pmod{p}.$$

Now either B_k or C_k must be divisible by p but not both, by what we have already proved. If k is an even multiple of $p/2$, it is a multiple of p , so that $B_k \equiv 0$ and $C_k \not\equiv 0 \pmod{p}$. But if k is an odd multiple of $p/2$, it is not a multiple of p . Consequently, $B_k \not\equiv 0 \pmod{p}$, so that $C_k \equiv 0 \pmod{p}$, completing the proof for regular divisors of (C) . The proof for divisors of (A) or (D) is precisely similar.

15. It remains to discuss the laws of apparition of the irregular prime ideals of categories I and II in Section 13. Since the elliptic polynomials have rational integral coefficients, if p is a prime ideal dividing a_0 say, we have $A_n(x; a_0) \equiv A_n(x; 0) \pmod{p}$. Consequently the arithmetical behavior of the sequences modulo p is given immediately by the algebraic behavior of the elliptic polynomials in the following five singular cases:

$$(15.1) \quad (\text{i}) \ a = 0; \quad (\text{ii}) \ a = 1; \quad (\text{iii}) \ x = 0; \quad (\text{iv}) \ x = 1; \quad (\text{v}) \ ax = 1.$$

Here the first two cases apply to all prime ideals of category I save divisors of two, while the last three cases apply to prime ideals of category II. We discuss the former two cases in this section, and the latter three in Section 16.

Case 15.1 (i) $a = 0$.

Then $k^2 = 0$ and snu becomes $\sin u$, cnu becomes $\cos u$ and dnu becomes one. Thus if

$$U_n = U_n(x) = (\alpha^n - \beta^n)/(\alpha - \beta) \quad V_n = V_n(x) = \alpha^n + \beta^n$$

are the Lucas functions of the quadratic equation $t^2 - 2t\sqrt{1-x} + 1$ where

$$(15.2) \quad x = \sin^2 u,$$

then we readily find that

$$\begin{aligned} A_n(x; 0) &= D_n(x; 0) = 1; \\ B_n(x; 0) &= \sin nu / \sin u = U_n(x), & n \text{ odd}, \\ &= \sin nu / (\sin u \cos u) = 2U_n(x)/V_1(x), & n \text{ even}; \\ C_n(x; 0) &= \cos nu / \cos u = V_n(x)/V_1(x), & n \text{ odd} \\ &\cos nu = V_n(x)/2, & n \text{ even}. \end{aligned}$$

We thus obtain the following theorem:

THEOREM 15.1. *If \mathfrak{p} is a prime ideal of the first category dividing a_0 , then*

$$\begin{aligned} A_n &\equiv D_n \equiv 1 \pmod{\mathfrak{p}} \\ B_n &\equiv U_n, \quad n \text{ odd}; \quad \equiv 2U_n/V_1, \quad n \text{ even}; \\ C_n &\equiv V_n/V_1, \quad n \text{ odd}; \quad \equiv \frac{1}{2}V_n, \quad n \text{ even}. \end{aligned}$$

Here $U_n = U_n(x_0)$ and $V_n = V_n(x_0)$ are the Lucas functions of the quadratic equation $t^2 - 2(1-x_0)^{\frac{1}{2}}t + 1 = 0$.

Case 15.1 (ii). $a = 1$.

Then $k^2 = 1$ and snu becomes $\tanh u$, while cnu and dnu become $\operatorname{sech} u$. Now by the transformation formulas of Table IV,

$$\begin{aligned} A_n(x; 1) &= (1-x)^{\alpha n} C_n(x/(x-1); 0) \\ B_n(x; 1) &= (1-x)^{\beta n} B_n(x/(x-1); 0) \\ C_n(x; 1) &= (1-x)^{\alpha n} A_n(x/(x-1); 0) \\ D_n(x; 1) &= (1-x)^{\alpha n} D_n(x/(x-1); 0). \end{aligned}$$

Hence if we let $u = ir$, then $x = -\tan^2 r$ and $x/(x-1) = \sin^2 r$. Therefore, by the results of case (i),

$$\begin{aligned} A_n(x; 1) &= \sec r^{n^2} \cos nr = (2/V_1)^{n^2} V_n/2^6 \\ &= \sec r^{n^2-3} (\sin nr / \sin r) = (2/V_1)^{n^2-3} U_n, && n \text{ even} \\ B_n(x; 1) &= \sec r^{n^2-1} (\sin nr / \sin r) = (2/V_1)^{n^2-1} U_n, && n \text{ odd} \\ C_n(x; 1) &= D_n(x; 1) = \sec r^{2a_n} = (2/V_1)^{2a_n}. \end{aligned}$$

Here $U_n = U_n(x/(x-1))$, $V_n = V_n(x/(x-1))$ are the Lucas functions of the quadratic equation $t^2 - 2t/(1-x)^{\frac{1}{2}} + 1 = 0$.

We thus obtain the following theorem:

THEOREM 15.2. *If \mathfrak{p} is a prime ideal of the first category dividing $1 - a_0$, then*

$$\begin{aligned} A_n &\equiv (2/V_1)^{n^2} V_n/2; \\ B_n &\equiv \begin{cases} (2/V_1)^{n^2-1} U_n, & n \text{ odd}, \\ (2/V_1)^{n^2-3} U_n, & n \text{ even}; \end{cases} \\ C_n &\equiv D_n \equiv \begin{cases} (2/V_1)^{n^2-1}, & n \text{ odd}, \\ (2/V_1)^{n^2}, & n \text{ even}. \end{cases} \end{aligned}$$

Here $U_n = U_n(x_0/(x_0-1))$, $V_n = V_n(x_0/(x_0-1))$ are the Lucas functions of the quadratic equation $t^2 - 2t/(1-x_0)^{\frac{1}{2}} + 1 = 0$.

For prime ideals of the first category dividing two, a special discussion must be made as in the case of the rational field for the prime two treated in M, pages 40-41. We shall not pursue the matter further here.

16. Consider now prime ideals of the second category. We may confine ourselves to ideals which are not also of the first category; for ideals of both categories are either null divisors of (B) or else are already covered by the results of Section 15. A prime ideal of this character is easily shown to divide precisely one of the algebraic numbers x_0 , $1 - x_0$ or $1 - a_0 x_0$. Clearly then $A_n(x_0, a_0)$ is congruent to either $A_n(0, a_0)$, $A_n(1, a_0)$ or $A_n(1/a_0, a_0)$, with similar results for B_n , C_n and D_n .

By the results of Table IV, we find that

⁶ For example, $A_3(x; 1) = (1 - x^3)(1 + 3x)$ by direct calculation from Table V. On the other hand, the formula for $n = 3$ becomes $A_3(x; 1) = \sec r^6 (\cos 3r / \cos r)$. Now $\cos 3r / \cos r = 4 \cos^2 r - 3 = [1 + 3(-\tan^2 r)] / \sec^2 r$ and $\sec^2 r = 1 - (-\tan^2 r)$. Hence $A_3(x; 1) = (1 - (-\tan^2 r))^3 (1 + 3(-\tan^2 r))$; checking, since $x = -\tan^2 r$.

	<i>n</i> odd	<i>n</i> even
$A_n(0) =$	1	1
$B_n(0) =$	n	n
$C_n(0) =$	1	1
$D_n(0) =$	1	1
$A_n(1) =$	$(1-a)^{(n^2-1)/4}$	$(1-a)^{n^2/4}$
$B_n(1) =$	$(-1)^{(n-1)/2}(1-a)^{(n^2-1)/4}$	$(-1)^{n/2}(1-a)^{(n^2-4)/4}$
$C_n(1) =$	$(-1)^{(n-1)/2}(1-a)^{(n^2-1)/4}n$	$(-1)^{n/2}(1-a)^{n/4}$
$D_n(1) =$	$(1-a)^{(n^2-1)/4}$	$(1-a)^{n^2/4}$
$A_n(1/a) =$	$((1-a)/a)^{(n^2-1)/4}$	$(-1)^{n/2}((1-a)/a)^{n^2/4}$
$B_n(1/a) =$	$(-1)^{(n-1)/2}((1-a)/a)^{(n^2-1)/4}$	$((1-a)/a)^{(n^2-4)/4}n$
$C_n(1/a) =$	$((1-a)/a)^{(n^2-1)/4}$	$(-1)^{n/2}((1-a)/a)^{n^2/4}$
$D_n(1/a) =$	$(-1)^{(n-1)/2}((1-a)/a)^{(n^2-1)/4}n$	$((1-a)/a)^{(n^2-4)/4}$

We deduce the following theorems from these results.

THEOREM 16.1. *Let \mathfrak{p} be a prime ideal of the second category which is not of the first category. Then \mathfrak{p} never divides the sequence (A). Furthermore \mathfrak{p} divides (B), (C) or (D) according as $x_0 \equiv 0$, $1-x_0 \equiv 0$ or $1-a_0x_0 \equiv 0 \pmod{\mathfrak{p}}$. Its rank of apparition in every case is p , where p is the rational prime which \mathfrak{p} divides.*

THEOREM 16.2. *Under the hypotheses of the preceding theorem, if \mathfrak{p} divides (C), it does not divide (D), and its rank of apparition in (B) is $2p$. Furthermore, $C_n \equiv 0 \pmod{\mathfrak{p}}$ if and only if n is an odd multiple of p . Similar results hold for divisors of (D).*

17. If we compare the results of Sections 15 and 16 for irregular prime ideals, we see that the laws of apparition are the same for all ideals save null divisors, and that the laws of apparition for (A), (C) and (D) essentially generalize Lucas' law of apparition for (V), and in a sense explain it. Furthermore, the laws of apparition for ideals of the field \mathcal{F}_1 are precisely the same as for the field \mathcal{F} . If in particular then x_0 and a_0 are rational integers, the four elliptic sequences are sequences of rational integers, and the ideals become ordinary primes. It is of some interest to note that the Lucas sequences associated with the primes of the first category in this case involve quadratic irrationalities, and are of the type studied in Lehmer's thesis. (D. H. Lehmer [1])

VI. Conclusion. The Laws of Repetition.

18. We conclude the paper by giving the laws of repetition for powers of primes in rational integral elliptic sequences. The extension to arbitrary algebraic integral sequences is easy, but will not be discussed here.

Assume then that x_0 and a_0 are rational integers. We need consider only regular primes p not dividing $2a_0(1-a_0)x_0(1-x_0)(1-a_0x_0)$. Let p be such a prime. Then p is odd. Assume that p divides (D) , and that its rank in (B) is 2ρ . Then the rank of p in (D) is ρ , and p does not divide (A) or (C) , by the results of Chapter IV. Consequently by the duplication formula (5.4) if p^k is the highest power of p dividing $B_{2\rho}$, it is also the highest power of p dividing D_ρ . Now since (B) is essentially the elliptic divisibility sequence (h) so far as regular primes are concerned, the law of repetition of powers of p in (B) follows from the results in Ward [2] for elliptic divisibility sequences; namely, if $l \leq k$, the rank of apparition of p^l in (B) is 2ρ , and if $l \geq k$, the rank is $2p^{l-k}\rho$. Now p is odd, and the only terms of (D) divisible by p are odd multiples of ρ . Hence since $D_n \equiv 0 \pmod{p^l}$ if and only if $B_{2n} \equiv 0 \pmod{p^l}$, we can state the following theorem:

THEOREM. *Let x_0 and a_0 be rational integers, and p a regular prime of rank ρ in (D) . Furthermore, let p^k be the highest power of p dividing D_ρ . Then the rank of apparition ρ^* of p^l in (D) is ρ or $p^{l-k}\rho$ according as $l \leq k$ or $l \geq k$. Furthermore $D_n \equiv 0 \pmod{p^l}$ if and only if n is an odd multiple of ρ^* .*

Precisely similar results hold for prime divisors of (A) or (C) . For the Lucas functions, these results become Lucas' law of repetition for primes in (V) .

CALIFORNIA INSTITUTE OF TECHNOLOGY.

BIBLIOGRAPHY

- R. Fricke, 1. *Die elliptischen Funktionen und ihre Anwendungen*, vol. 1, Leipzig (1916).
- 2. Vol. 2, Leipzig (1922).
- M. Krause, 1. *Theorie der doppelperiodischen Funktionen*, Leipzig (1895).
- D. H. Lehmer, 1. "An extended theory of Lucas' functions," *Annals of Mathematics*, Ser. 2, vol. 31 (1930), pp. 419-448.
- M. Ward, 1. "Memoir on elliptic divisibility sequences," *American Journal of Mathematics*, vol. 70 (1948), pp. 31-74.
- 2. "The law of repetition of primes in an elliptic divisibility sequence," *Duke Mathematical Journal*, vol. 15 (1948), pp. 941-946.
- K. Weierstrass, 1. *Werke*, vol. 1, Berlin (1894), pp. 1-49.

possesses an approximate functional equation, cf. reference 1, where this last result was used in connection with the mean value of $\zeta(s)$ on the critical line. The case $k = 1$ is due to Wigert.

It seems very difficult to establish corresponding results for

$$f_k(x, y) = \sum_{n=1}^{\infty} d_k(n) V_k(n^2 x^2) e^{iny} \quad (5)$$

¹ Bellman, R., "Wigert's Approximate Functional Equation and the Riemann Zeta-Function," *Duke Math. J.*, **16**, 547–552 (1949).

² Hardy, G. H., "On Dirichlet's Divisor Problem," *Proc. Lond. Math. Soc.*, **15**, 1–20 (1916).

³ Hardy, G. H., "Some Multiple Integrals," *Quart. J. Math.*, **39**, 357–375 (1908).

⁴ Maass, H., "Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletschen Reihen durch Funktionalgleichungen," *Math. Ann.*, **121**, 141–183 (1949).

⁵ Siegel, C. L., "Über die analytische Theorie der quadratischen Formen," *Ann. Math.*, **136**, 527–606 (1935).

ARITHMETICAL PROPERTIES OF POLYNOMIALS ASSOCIATED WITH THE LEMNISCATE ELLIPTIC FUNCTIONS

BY MORGAN WARD

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE, PASADENA

Communicated by H. S. Vandiver, April 18, 1950

1. I have studied elsewhere the arithmetical properties of certain polynomials associated with the real multiplication of elliptic functions.¹ Such polynomials include as a special case the function $U_n = (a^b - b)_n / (a - b)$ first systematically studied by Lucas² and Sylvester³ when expressed as a polynomial in $P = a + b$ and $Q = ab$.

I have recently investigated the polynomials associated with the simplest type of complex multiplication of elliptic functions; namely, the so-called lemniscate case for which the period ratio τ has the value $i = \sqrt{-1}$ and the Weierstrass invariant g_3 is zero.

In the account which follows, the small greek letters $\alpha, \epsilon, \lambda, \mu, \nu$ and π will be used for elements of the ring G of Gaussian integers. $\bar{\alpha}$ and $N\alpha$ denote the conjugate and norm of α in G . α is said to be odd, oddly even or totally even according as $N\alpha$ is congruent to one, two or zero modulo 4. The letter ϵ is reserved for denoting any one of the four units $\pm 1, \pm i$ of the ring G .

2. Let u be a complex variable, and $\wp(u)$ the Weierstrass \wp -function formed with the invariants $g_2 = 4w$, $g_3 = 0$. Let $E\mu = E\mu(u)$ equal 1,

$\sqrt{\wp(u)}$ or $\wp'(u)$ according as μ is odd, oddly even or totally even. Finally let

$$\Psi_\mu = \Psi_\mu(u) = \sigma(\mu u)/\sigma(u)^{N\mu} \quad (1)$$

where $\sigma(u)$ is the Weierstrass sigma function. Then $\Psi_\mu \div E_\mu$ is an even elliptic function with the same periods as $\wp(u)$. More specifically,

$$\Psi_\mu(u) = E_\mu(u)P_\mu(z, w) \quad (2)$$

where

$$P_\mu = P_\mu(z, w) = \sum_{r=0}^q \pi_r z^{q-2r} w^r \quad (3)$$

is a polynomial in $z = \wp(u)$ and $w = \frac{g_2}{4}$ whose coefficients π_r are Gaussian integers with $\pi_0 = \mu$. The degree q of P_μ in z depends in a simple way on $N\mu$. The arithmetical properties of these polynomials were the object of the investigation; (3) is the elliptic function analog of the cyclotomic polynomial $\frac{z^n - 1}{z - 1}$ associated with Lucas' U_n .

3. The arithmetical properties of the polynomials P_μ closely parallel the properties of Lucas' U_n . The main new feature of interest (not occurring in the real multiplication case) is a genuine double numerical periodicity when the free variables z and w are given fixed values in G , and the residues of the resulting sequence in G are considered for moduli in G . Indeed Lucas claimed in his fundamental paper and elsewhere to have discovered doubly periodic numerical functions connected with the elliptic functions, but he apparently published nothing on this subject.⁴

The Lucas polynomial U_n may be defined as the solution of a simple difference equation with prescribed initial values. The function Ψ_μ may be similarly defined as a solution of the difference equation

$$\Omega_\mu + , \Omega_\mu - , = \Omega_\mu + _1 \Omega_\mu - _1 \Omega_\nu^2 - \Omega_\nu + _1 \Omega_\nu - _1 \Omega_\mu^2 \quad (4)$$

with prescribed initial values; in particular, $\Psi_0 = 0$ and $\Psi_\epsilon = \epsilon$. (A table of the corresponding initial values of P_μ for small $N\mu$ is given at the close of the paper.)

Consequently, just as in the real multiplication case,⁵ the polynomials P_μ may be defined purely algebraically as modified solutions of (4). On using this algebraic definition in conjunction with the function-theoretic definitions (1) and (2), the following results were obtained.

(i) *If z, w are indeterminates, the correspondence $\nu \rightarrow P_\mu(z, w)$ is a mapping of the ring G into the polynomial ring $G(z, w)$ which preserves*

division; that is ν divides μ in G implies that P_ν divides P_μ in $G(z, w)$. Furthermore,

$$P_\epsilon = \epsilon, \quad P_{\epsilon\mu} = \epsilon P_\mu, \quad P_{\bar{\mu}} = \bar{P}_\mu.$$

Therefore if μ is a rational integer, all the coefficients π_r of P_μ are rational integers, and P_μ reduces to the polynomial of the real multiplication case studied in reference 1.

Let z_0, w_0 be fixed rational integers. Then $h_\nu = P_\nu(z_0, w_0)$ is a Gaussian integer and the correspondence $\nu \rightarrow h_\nu$ is a mapping of G into itself preserving division. Let π from now on denote a fixed Gaussian prime. An integer λ is called a zero of h_ν modulo π if $h_\lambda \equiv 0 \pmod{\pi}$ and a rank of apparition of π in $\{h_\nu\}$ if $h_\lambda \equiv 0 \pmod{\pi}$ but $h_\mu \not\equiv 0 \pmod{\pi}$ for μ any proper divisor of λ .

(ii) *If π is odd, the zeros of the prime π in $\{h_\nu\}$ form an ideal m which is never the zero ideal.* Furthermore if λ is any rank of apparition of π in $\{h_\nu\}$, m is the principal ideal determined by λ .

(iii) *If π is an odd complex Gaussian prime, then⁶*

$$P_\mu(z, w) \equiv P_\mu(0, w) \pmod{\pi}.$$

(iv) *The sequence $\{h_\nu\}$ becomes numerically periodic modulo π . The moduli of its periods is contained in the ideal m of its zeros modulo π .*

(v) *Given a specific term h_λ of $\{h_\nu\}$, the only odd primes π which can have rank of apparition λ in $\{h_\nu\}$ are either divisors of λ , or primes for which the polynomial $P_\lambda(z, w)$ splits completely into linear factors or completely into quadratic factors in the residue class ring $G(z, w)/(\pi)$. Such primes lie in arithmetical progressions whose common constant difference is a function of λ alone.⁷*

(v) generalizes the well-known result of Lucas and Sylvester that if P and Q are rational integers, all primitive prime divisors of U_l are either divisors of l or of the form $kl \pm 1$.

The first few polynomials P_μ are as follows: $P_0 = 0$, $P_1 = 1$, $P_i = i$, $P_{1+i} = 1+i$, $P_2 = 2$, $P_3 = 3z^4 - 6wz^2 - w^2$, $P_{1+2i} = (1+2i)z^2 - w$, $P_{3+i} = (3+i)z^4 - 2(1+3i)wz^2 + (3+i)w^2$. All the remaining P_μ can be calculated from the recursion (4) and the relations $P_\mu = \bar{P}_\mu$, $P_{\epsilon\mu} = \epsilon P_\mu$.

Qualitatively similar results hold for the polynomials associated with any complex multiplication of $\mathcal{O}(u)$.⁸

A more complete account of these and other results with proofs will be published elsewhere.

¹ *Am. J. Math.*, **70**, 31–74 (1948). Various algebraic properties of these polynomials are developed in Halphen's treatise on elliptic functions.

² *Ibid.*, 1, 184–240, 289–321 (1878).

³ *Ibid.*, 2, 357–380 (1879).

⁴ In particular, Lucas stated to C. A. Laisant that there was a remarkable connection between his doubly periodic numerical functions and Fermat's last theorem. See Bell, E. T., *Bull. Am. Math. Soc.*, **29**, 401–406 (1923). The crux of the matter is to understand what Lucas meant by "double periodicity." Since the modules of the ring of Integers are all principal ideals, no numerical function of the rational integer n can be doubly periodic. The simplest case in which double periodicity in the usually understood sense can occur is for numerical functions over the ring of Gaussian integers.

⁵ See Chapter V of reference 1.

⁶ Due to Eisenstein for the Jacobian lemniscate polynomials and used by him to prove the biquadratic reciprocity law. See his *Math. Abb.*, third paper or *J. Math. (Crelle)*, **30**, 184–187 (1846).

⁷ This result follows from Abel's theorem that the Galois group of the equation $P_\mu(z, w) = 0$ in z is commutative and of order q .

⁸ The equi-harmonic case when the period ratio τ is a complex cube root of unity and the invariant g_2 vanishes is being studied in detail by Lincoln K. Durst.

Chapter 19

1951

A CLASS OF SOLUBLE DIOPHANTINE EQUATIONS

By MORGAN WARD

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE, PASADENA

Communicated by E. T. Bell, November 21, 1950

1°. Let R be a commutative ring with a unit element, $F(x)$ a homogeneous polynomial of degree n in t indeterminates x_1, x_2, \dots, x_t with coefficients in R . Let I denote the subring of the coefficients of $F(x)$ in R ; that is, the smallest ring containing all of them. We consider the existence of solutions of the diophantine equation

$$F(x) = z^m \quad (1)$$

in R or in I . Here z is an indeterminate and m is a given positive integer.

If y_1, y_2, \dots, y_t are t new indeterminates and if there exist $t + 1$ polynomials $Q(y); P_i(y)$, ($i = 1, \dots, t$), with coefficients in R (or in I) such that

$$F(P(y)) = Q(y)^m \quad (2)$$

identically in the y , (1) will be said to have a t -parameter family of solutions in R (or in I).

2°. THEOREM. If m is prime to the degree n of $F(x)$, then the diophantine equation (1) always has a t -parameter family of solutions in both in R and in I .

For assume that m is prime to n . If m is less than n , write r for m . Then integers k and l exist uniquely determined by n and r such that

$$kn + 1 = lr, \quad 0 < k < r, \quad 0 < l < n.$$

Define polynomials $P(y); Q(y)$ by

$$P_i(y) = y_i F(y)^k, \quad (i = 1, \dots, t); \quad Q(y) = F(y)^l.$$

Then the coefficients of the $P(y)$ and $Q(y)$ lie in I . Since $F(x)$ was assumed to be homogeneous of degree n , (2) holds identically in the y with m equal to r .

If m is greater than n , divide m by n and let the quotient be q and the remainder r . Then if m is prime to n ,

$$m = qn + r, \quad 0 < r < n, \quad r \text{ prime to } n.$$

With $k, l, P(y)$ and $Q(y)$ as before, let

$$y_i^* = y_i F(y)^k \quad (i = 1, \dots, t).$$

Then $F(y^*) = Q(y)^r$. Hence if

$$\begin{aligned} P_i^*(y) &= y_i^* Q(y)^q \quad (i = 1, \dots, t) \\ Q^*(y) &= Q(y), \end{aligned}$$

then $F(P^*(y)) = Q^*(y)^m$ identically in the y . Since the polynomials $P^*(y)$ and $Q^*(y)$ have their coefficients in I , the proof is complete.

3°. The most interesting case of this theorem is when I is the ring of ordinary integers. For example the diophantine equation

$$x^n + y^n = z^m$$

has a two parameter family of integral solutions for every m prime to n ; the diophantine equation

$$x^4 + y^4 + z^4 = z^m$$

has a three-parameter family of integral solutions for every odd m , and so on. Many other special cases occur in the literature.¹

4°. The family \mathfrak{M} of solutions of (1) in R consists of vectors $[\xi; \eta] = [\xi_1, \xi_2, \dots, \xi_t; \eta]$ of the form

$$\begin{aligned} \xi &= P(\alpha), & \eta &= Q(\alpha) & m < n, \\ \xi &= P^*(\alpha), & \eta &= Q^*(\alpha) & m > n. \end{aligned}$$

Here α stands for t arbitrarily chosen elements $\alpha_1, \dots, \alpha_t$ of R or of I . If the α are such that $F(\alpha) = 0$, we obtain the trivial zero solution of (1) and this is evidently the only solution of the family \mathfrak{M} with $\eta = 0$ if R has zero radical. In any event the solutions of (1) in R with $z = 0$ are entirely independent of the choice of m .

5°. If R is a field, it is easy to show that every solution $[\kappa, \lambda]$ of (1) in R with $\lambda \neq 0$ is of the form

$$\kappa_i = \theta^a \xi_i \quad (i = 1, 2, \dots, t); \quad \lambda = \theta^b \eta.$$

Here $[\xi; \eta]$ belongs to the family \mathfrak{M} , a and b are positive integers depending only on m and n , while θ is a field element depending only on λ . Thus in this case, \mathfrak{M} gives essentially all solutions of (1) with $z \neq 0$.

6°. The situation is quite different for the solutions \mathfrak{M} in I if I is a domain of integrity. \mathfrak{M} by no means exhausts the possible solutions of (1) in I ; in fact the components ξ, η of any \mathfrak{M} solution will usually have common factors in I . For example, if I is the ring of integers, the diophantine equation

$$x_1^2 x_2 + x_1 x_2^2 = z^m$$

has a two-parameter family of integral solutions $[\xi_1, \xi_2, \eta]$ for every odd prime m other than three. But the existence of a single integral solution with ξ_1, ξ_2 co-prime [other than the trivial solutions $(1, 0; 1), (0, 1; 1)$] would disprove Fermat's last theorem.

¹ Dickson, *History of the Theory of Numbers*, Vol. 1.

Chapter 20

1954

THE MAXIMAL PRIME DIVISORS OF LINEAR RECURRENCES

MORGAN WARD

1. Introduction. Let

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

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

$$(1.1) \quad \Omega_{n+r} = P_1 \Omega_{n+r-1} + P_2 \Omega_{n+r-2} + \dots + P_r \Omega_n,$$

where $P_1, P_2, \dots, P_r \neq 0$ are integers, and the initial values W_0, W_1, \dots, 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 $W_k, W_{k+1}, \dots, W_{k+s-1}$, 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

$$(1.2) \quad f(z) = z^r - P_1 z^{r-1} - \dots - P_r,$$

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.

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 $\alpha_1, \alpha_2, \dots, \alpha_r$, so that its discriminant D is not zero.

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

$$(2.1) \quad W_n = \beta_1 \alpha_1^n + \dots + \beta_r \alpha_r^n$$

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 i th row and j th 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

$$(2.2) \quad \beta_1 \dots \beta_r D = \Delta(W) \neq 0.$$

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

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

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

$$\gamma_i = w(\alpha_i) \quad (i = 1, 2, \dots, r).$$

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

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

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

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

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

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

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

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

$$(3.1) \quad \alpha_1^n \equiv \alpha_2^n \equiv \dots \equiv \alpha_r^n \pmod{p}$$

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

$$(3.2) \quad W_{n+\rho} \equiv CW_n \pmod{p}, \quad C \not\equiv 0 \pmod{p},$$

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

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

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

$$L_1 = L_2 = \dots = L_{r-2} = 0, \quad L_{r-1} = 1.$$

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

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

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 , 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

$$(4.1) \quad \Lambda(W) = DP, \Delta(W).$$

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) .*

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

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

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, \dots, T_{r-1} all divisible by p . Consequently, p divides every term of (T) ; in other words the congruences

$$(5.1) \quad W_{n+k} \equiv CL_n \pmod{p}$$

$$(5.2) \quad C \not\equiv 0 \pmod{p}$$

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

$$(5.3) \quad p = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_s$$

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

$$(5.4) \quad \alpha_1^n \equiv \alpha_2^n \equiv \dots \equiv \alpha_r^n \pmod{\mathfrak{p}_j}$$

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), $\rho = \rho_j$ ($j = 1, 2, \dots, s$).*

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

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

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

$$\sum_{i=1}^r (\gamma_i \alpha_i^k - C) \frac{\alpha_i^n}{f'(\alpha_i)} \equiv 0 \pmod{p_j} \quad (n = 0, 1, \dots, r-1).$$

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

$$(5.6) \quad \gamma_1 \alpha_1^k \equiv \gamma_2 \alpha_2^k \equiv \dots \equiv \gamma_r \alpha_r^k \equiv C \not\equiv 0 \pmod{p_j}.$$

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 p_j of p in the root field of $f(z)$.*

Now let ρ_j be the restricted period of $f(x)$ modulo p_j , and σ_j the restricted period of $g(x)$ modulo p_j ; that is, σ_j is the smallest positive value of n such that

$$\gamma_1^n \equiv \gamma_2^n \equiv \dots \equiv \gamma_r^n \pmod{p_j}.$$

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_j th 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

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

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

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

Here α as before is any root of $f(z)$, γ is an integer of the root field \mathfrak{N} of $f(z)$, C is a rational integer, p any prime ideal of \mathfrak{N} 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 p , writing (6.2) for example as $\gamma \alpha^k \equiv C$. $\gamma \equiv \text{Int}$ means there exists a rational integer g such that p divides $\gamma - g$. Clearly

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

$\gamma \equiv Pr(\alpha)$ means γ is congruent modulo p to a power of α . $ex(\gamma)$ means the exponent to which γ belongs modulo 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

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

Let

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

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

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

Proof: Evidently ν divides $\sigma\delta$. Let $(\nu, p - 1) = t$ so that $\nu = \nu_0t$ 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

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

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

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

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 $l \geq 0$, $\gamma^{p-1} \equiv \alpha^l$.

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

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

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 $\gamma^{\sigma(p-1)} \equiv 1$, $\text{ex}(\gamma^{p-1})$ divides σ . Hence $\text{ex}(\gamma^{p-1})$ divides $rx(\alpha)$ or $\text{ex}(\gamma^{p-1})$ divides $\text{ex}(\alpha)$ 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 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 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 p divides the restricted period of γ modulo 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 , 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,

$$(7.1) \quad \gamma\alpha^k \equiv C \not\equiv 0 \pmod{\mathfrak{p}_j}.$$

Here k may depend on j .

Now raise the congruence (7.1) successively to the p, p^2, \dots, 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

$$\alpha_i \equiv \alpha^{p^{i-1}} \pmod{p} \quad (i = 1, 2, \dots, r).$$

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

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

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.

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

CYCLOTOMY AND THE CONVERSE OF FERMAT'S THEOREM

MORGAN WARD, California Institute of Technology

The following theorem of A. Hurwitz [1] was stated without proof in answer to a question raised by E. B. Escott [2] regarding a test for the primality of the Fermat numbers 2^k+1 (k a power of two) stated without proof by E. Lucas in his *Theorie des Nombres* [3].

HURWITZ'S THEOREM: *Let $Q_n(x)$ denote the cyclotomic polynomial of order n and degree $\phi(n)$. Then n is a prime number if there exists an integer a such that*

$$(1) \quad Q_{n-1}(a) \equiv 0 \pmod{n}.$$

This theorem is a simple consequence of the converse of Fermat's theorem. For let n be greater than one. Then the factorization of $x^{n-1}-1$ into its irreducible factors over the rational field is

$$(2) \quad x^{n-1} - 1 = \prod_{d|n-1} Q_d(x).$$

Here the product extends over all distinct divisors d of $n-1$.

The discriminant $\pm(n-1)^{n-1}$ of $x^{n-1}-1$ is prime to n . Consequently if d and d' are distinct divisors of $n-1$, the resultant of $Q_d(x)$ and $Q_{d'}(x)$ is always prime to n . Hence for any integer a and any proper divisor d of $n-1$, the three numbers $Q_{n-1}(a)$, $Q_d(a)$ and n are co-prime.

Now assume that the congruence (1) is satisfied. By what precedes, $Q_d(a)$ is prime to n for every proper divisor d of $n-1$. But by (2)

$$\begin{aligned} a^{n-1} - 1 &\equiv \prod_{k|n-1} Q_k(a) \equiv 0 \pmod{n}, \\ a^d - 1 &= \prod_{k|d} Q_k(a) \not\equiv 0 \pmod{n}, \quad d | n-1; d < n-1. \end{aligned}$$

Therefore n is a prime by the converse of Fermat's theorem. (For this converse see for example, O. Ore, *Number Theory*, Chapter XIV.)

For example, $Q_2(a)=a+1\equiv 0 \pmod{3}$ for $a=2$; $Q_6(a)=a^2-a+1\equiv 0 \pmod{7}$ for $a=3$. Hence 3 and 7 are primes. But the most interesting application of the theorem is that made by Hurwitz himself to the case when $n=2^k+1$ so that $Q_{n-1}(x)=x^{(n-1)/2}+1$; namely $n=2^k+1$ is a prime number if and only if there exists an integer a such that $a^{(n-1)/2}\equiv -1 \pmod{n}$. For $a=3$, this result is the test quoted by Lucas and used extensively by him and by other arithmeticians for investigating particular Fermat numbers.

References

1. A. Hurwitz, *Mathematische Werke*, vol. 2, page 747.
2. *Intermédiaire des Math.*, vol. II, 1896, pp. 80 and 214.
3. Lucas published proofs elsewhere, but the test is due to T. Pepin. For a history and references to other proofs see Dickson, *History of the Theory of Numbers*, vol. 1, Chap. XV.

Chapter 21

1955

THE INTRINSIC DIVISORS OF LEHMER NUMBERS

BY MORGAN WARD

(Received March 15, 1954)

1. Introduction

A prime p is called an intrinsic divisor of the Lucas number $L_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ where $\alpha + \beta$ and $\alpha\beta$ are integers, if p divides L_k but does not divide L_n for $0 < n < k$. It is well known [1], [2], [8], page 283, that if α and β are themselves integers, L_k always has an intrinsic divisor unless $\alpha = \pm 2$, $\beta = \pm 1$, $k = 6$.

The question of the existence of intrinsic divisors when α and β are real but not necessarily integers was studied some time ago in these Annals by R. D. Carmichael [3], and again quite recently by C. G. Lekkenkerker [6]. In this paper, I study the intrinsic divisors of D. H. Lehmer's generalization of the Lucas numbers [5] in which merely $(\alpha + \beta)^2$ and $\alpha\beta$ are required to be integers, again under the assumption that α and β are real. The method of attack goes back in principle to Sylvester [7], page 607, and is powerful enough to furnish a complete answer. Nothing appears to be known about the intrinsic divisors of Lucas or Lehmer numbers when α and β are complex.

Let L and M be integers, with L and $K = L - 4M$ positive and $M \neq 0$. Then the roots α and β of the polynomial

$$f(z) = z^2 - (L)z + M$$

are real. Let

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

Then P_n is an integer. The sequence

$$(P): P_0 = 0, P_1 = 1, P_2 = 1, \dots, P_n, \dots$$

gives the Lehmer numbers associated with $f(z)$. For brevity, we call (P) and P_n "real" when α and β are real.

The subscript k of P_k is called its index; p is an intrinsic divisor of P_k if $P_k \equiv 0 \pmod{p}$, $P_n \not\equiv 0 \pmod{p}$ for $0 < n < k$. (P) is called "exceptional" if it contains terms P_k of index greater than two with no intrinsic divisors; any such k is called an exceptional index. Let

$$(1.1) \quad R = \begin{cases} |4LM|, & M \text{ negative}; \\ |4KM|, & M \text{ positive}. \end{cases}$$

Then our results are as follows:

THEOREM 1.1. *A real Lehmer sequence can only be exceptional if R is less than*

sixteen. A term of a real Lehmer sequence always has an intrinsic divisor if its index is greater than eighteen.

THEOREM 1.2. *There are only three exceptional real Lehmer sequences. The associated polynomials are $z^2 - z - 1$, $z^2 - (5)^{\frac{1}{2}}z + 1$ and $z^2 - 3z + 2$. The exceptional indices for the first two sequences are six, twelve, eighteen, and for the last sequence, six.*

The last case is the exception discovered by A. S. Bang [1]; in the first case, the Lehmer numbers are the Fibonacci numbers $0, 1, 1, 2, 3, \dots$ and in the second case, they are simply related to the Fibonacci numbers.

2. Elementary properties of Lehmer numbers

We collect here various properties of the Lehmer numbers given in Lehmer's Thesis [5] which are needed in what follows.

We may assume that L and M are co-prime. For if $(L, M) = D > 1$ then $L = DL'$, $M = DM'$ with $(L', M') = 1$. But if we let $\alpha = (D)^{\frac{1}{2}}\alpha'$, $\beta = (D)^{\frac{1}{2}}\beta'$ then α', β' are real when α and β are real and $(\alpha' + \beta')^2 = L'\alpha'\beta' = M'$ are co-prime integers. Furthermore if P'_n is the Lehmer number corresponding to α' and β' , then $P_n = D^{\frac{1}{2}(n-1)}P'_n$ so that P_n and P'_n have the same intrinsic divisors. We may assume that L is positive; for if we let $\alpha = i\alpha'$, $\beta = i\beta'$ the signs of L and M are changed, and P_n is multiplied by ± 1 . Since α and β are to be real, we have:

$$(2.1) \quad L > 0, \quad K = L - 4M > 0, \quad M \neq 0, \quad L, M \text{ co-prime.}$$

Carmichael [3] has shown by simple examples that if α and β are complex, there may be many exceptional indices.

Let n be an integer greater than two and let

$$(2.2) \quad Q_n(z, w) = \prod_{\substack{1 \leq r \leq n \\ (r, n) = 1}} (z - e^{2\pi ir/n}w)$$

be the homogeneous cyclotomic polynomial of degree $\phi(n)$. We call the sequence

$$(Q): Q_0 = 0, Q_1 = 1, Q_2 = 1, \dots, Q_n = Q_n(\alpha, \beta), \dots$$

the cyclotomic numbers associated with the Lehmer numbers (P) . Q_n is an integer, and

$$(2.3) \quad P_n = \prod_{d|n} Q_d$$

where the product is extended over all divisors d of n . (P) is a divisibility sequence; that is, if n divides m , then P_n divides P_m .

The "rank" of a prime p in (P) is the least positive value k of the index n such that $P_n \equiv 0 \pmod{p}$. If p divides M , it divides no term of (P) save P_0 and we assign to it rank zero. Otherwise k exists, and divides $p - (k/p)$. The basic property of the rank of a prime may be stated as follows:

LEMMA 2.1. *Every prime number p has a rank $k \geq 0$ in (P) such that p divides P_n if and only if k divides n .*

Consider next the ranks of powers of a prime. Clearly powers of p can only divide terms whose indices are multiples of k . Let

$$(2.4) \quad p^t \parallel P_k, t \geq 1; P_n \not\equiv 0 \pmod{p} \quad 0 < n < k.$$

That is, p^t exactly divides P_k and $P_k \div p^t$ is prime to p . Assume that $P_n \equiv 0 \pmod{p}$ and let $p^r \parallel n/k, r \geq 0$.

LEMMA 2.2. *Under the hypotheses just given, p^{r+t} exactly divides P_n .*

3. The divisors of the cyclotomic numbers

A prime p which divides Q_n is called an extrinsic or intrinsic divisor according as it does or does not divide some Q_m of positive index less than n . Evidently p is an intrinsic divisor of Q_n if and only if p is an intrinsic divisor of P_n . Furthermore, if p is an extrinsic divisor of Q_n , p divides Q_d where d is a proper divisor of n . In the lemmas that follow, p is a fixed prime with positive rank k in (P) , satisfying condition (2.4).

LEMMA 3.1. *Under the hypotheses just given, for every positive exponent r , p exactly divides $Q_{p^r k}$.*

PROOF. We make an induction on r . First, let $r = 1, n = pk$. Then by (2.3),

$$(3.1) \quad P_n = Q_n P_k Q', \quad Q' = \prod Q_d$$

where the product is extended over all proper divisors d of n which are not divisors of k . If the product is empty, we take $Q' = 1$.

Then $(Q', p) = 1$. For otherwise p divides some Q_d , and hence the corresponding P_d . But then by Lemma 2.1, $k \mid d$ contrary to $d \nmid k, d \mid pk, d < pk$.

Now $p^t \parallel P_k$ and $p^{t+1} \parallel P_n$ by Lemma 2.2. Hence (3.1) implies that $p \parallel Q_n$.

Assume that the lemma is true for $n = pk, \dots, p^{r-1}k$ and let $n = p^r k$. Then by (2.3),

$$P_n = Q_n P_k Q_{pk} Q_{p^{2k}} \cdots Q_{p^{r-1}k} Q', \quad Q' = \prod Q_d$$

where the product is now extended over all divisors d of n which neither divide k nor are of the form $p^s k$ with $1 \leq s \leq r$. Then $(Q', p) = 1$ as in the case $r = 1$. By Lemma 2.2, $p^{t+r} \parallel P_n$. But $p^t \parallel P_k$ and by the hypothesis of the induction, $p \parallel Q_{p^s k}, 1 \leq s \leq r - 1$. Hence $p \parallel Q_n$, which completes the proof.

LEMMA 3.2. *With the previous hypotheses, let $P_n \equiv 0 \pmod{p}$ so that $n = kqp^r$ with $r \geq 0$ and q prime to p . Then if q is greater than one, p does not divide Q_n .*

PROOF. As in the previous proof,

$$P_n = Q_n P_k Q_{pk} \cdots Q_{p^{r-1}k} Q'$$

where Q' is an integer. By Lemma 2.2, if $p^t \parallel P_k$, then $p^{t+r} \parallel P_n$ and by Lemma 3.1, $p \parallel Q_{p^s k} (s = 1, \dots, r)$. Hence Q_n is prime to p .

The following two lemmas are easy consequences of these results.

LEMMA 3.3. *An extrinsic prime divisor of Q_n divides it to the first power only.*

LEMMA 3.4. *A sufficient condition that P_n have an intrinsic prime divisor is that $|Q_n| > n$.*

4. Inequalities for the cyclotomic numbers

We next derive some inequalities for $|Q_n|$ which enable us to use Lemma 3.4 to prove the existence of intrinsic divisors.

If $n \geq 3$ and $\varepsilon = e^{2\pi i/n}$, then by (2.2)

$$Q_n^2 = \prod (\alpha - \varepsilon^r \beta) \prod (\alpha - \varepsilon^{-r} \beta) = \prod (\alpha^2 + \beta^2 - \alpha \beta (\varepsilon^r + \varepsilon^{-r})).$$

Here and later the products are extended over all positive integers r less than n and prime to it. Hence

$$Q_n^2 = \prod (L - 4M \cos^2 r\pi/n) = \prod (K + 4M \sin^2 r\pi/n).$$

Note also that by (2.2)

$$\prod 4 \sin^2 r\pi/n = \prod (1 - \varepsilon^r)(1 - \varepsilon^{-r}) = Q_n^2(1, 1) \geq 1,$$

$$\prod 4 \cos^2 r\pi/n = \prod (-1 - \varepsilon^r)(-1 - \varepsilon^{-r}) = Q_n^2(-1, 1) \geq 1.$$

Now if R is defined as in (1.1) of the introduction,

$$\begin{aligned} L - 4M \cos^2 r\pi/n &> R^{\frac{1}{2}} |\cos r\pi/n| && \text{if } M < 0; \\ K + 4M \sin^2 r\pi/n &> R^{\frac{1}{2}} |\sin r\pi/n| && \text{if } M > 0. \end{aligned}$$

Hence in either case, we obtain the inequality

$$(4.1) \quad |Q_n| > R^{\frac{1}{2}\phi(n)}.$$

Since $R \geq 4$, Lemma 3.4 gives us

THEOREM 4.1. *A sufficient condition that the Lehmer number of index n has an intrinsic divisor is that*

$$(4.2) \quad 2^{\frac{1}{2}\phi(n)} \geq n.$$

We next determine for what n this inequality is satisfied.

LEMMA 4.1. *If $n \geq 2 \cdot 10^9$, then*

$$(4.3) \quad \phi(n) > \frac{n}{\log n}.$$

PROOF. Since

$$(4.4) \quad \phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

it suffices to show that

$$-\log \prod_{p|n} \left(1 - \frac{1}{p}\right) < \log \log n, \quad \text{for } n \geq 2 \cdot 10^9.$$

But by a familiar procedure (Hardy and Wright [4], Chap. 22)

$$-\log \prod_{p|n} \left(1 - \frac{1}{p}\right) < \sum_{p|n} \frac{1}{p} + \frac{1}{2} < \sum_{p \leq \log n} \frac{1}{p} + \frac{1}{\log \log n} \frac{1}{2}.$$

But by summation by parts and the trivial inequality $\pi(x) < 2x/\log x$,

$$\sum_{p \leq x} \frac{1}{p} < \frac{2}{\log x} + 2 \log \log x - 2 \log \log 2,$$

so that

$$\begin{aligned} -\log \prod_{p|n} \left(1 - \frac{1}{p}\right) &< 2 \log \log \log n + \frac{3}{\log \log n} + \frac{1}{2} - 2 \log \log 2 \\ &< \log \log n \end{aligned}$$

since n is large.

LEMMA 4.2. If $1 \leq n < 2 \cdot 10^9$, then

$$(4.5) \quad \phi(n) > \frac{n}{6}.$$

PROOF. The product of the first nine primes is greater than $2 \cdot 10^9$. Hence any number $n < 2 \cdot 10^9$ has at most eight prime factors. Therefore (4.4) gives

$$\phi(n) \geq n \prod_{2 \leq p \leq 19} \left(1 - \frac{1}{p}\right) = .171n > \frac{1}{6}n.$$

It follows from Lemma 4.1 that the inequality $2^{\frac{1}{6}\phi(n)} > n$ is true for large n . It also holds for $75 \leq n < 2 \cdot 10^9$ by Lemma 4.2; for in that range, $n > 12 \log n / \log 2$ so that (4.5) implies that $\frac{1}{2}\phi(n) \log 2 > \log n$.

Finally, by examining the tabulated values of $\phi(n)$, the inequality $2^{\frac{1}{6}\phi(n)} \geq n$ is found to be true for $30 < n < 75$, failing for $n = 30$ and numerous smaller indices. Hence we have proved

THEOREM 4.2. A real Lehmer number P_n always has at least one intrinsic prime divisor provided that its index n is greater than thirty.

5. Intrinsic divisors of Lehmer numbers of low index

It remains to discuss the Lehmer numbers of index thirty or less. The first seven cyclotomic numbers are:

$$(5.1) \quad \begin{aligned} Q_0 &= 0, & Q_1 &= 1, & Q_2 &= 1, & Q_3 &= L - M, & Q_4 &= L - 2M, \\ & & & & & & Q_5 &= L^2 - 3ML + 3M^2, & Q_6 &= L - 3M. \end{aligned}$$

Hence

$$(5.2) \quad Q_8 = Q_4(Q_4 + 4M) + M^2, \quad Q_{10} = Q_5 - 2MQ_4, \quad Q_{12} = Q_4^2 - 3M.$$

The conditions $L, K > 0$, $M \neq 0$ and $(L, M) = 1$ easily give

LEMMA 5.1. P_3 , P_4 and P_6 always have intrinsic divisors. P_6 has an intrinsic divisor prime to L unless $L = 5$, $M = 1$, $K = 1$; $L = 1$, $M = -1$, $K = 5$; or $L = 9$, $M = 2$, $K = 1$.

In the first two cases $R = 4$ and $P_6 = 8 = 4P_3$ or $2P_3$. In the third case, $R =$

8 and $P_6 = 63 = LP_3$. This is the exception $\alpha = 2, \beta = 1$ mentioned in the introduction.

The following table lists all indices n between 3 and 31 for which $4^{\frac{1}{\phi(n)}}$ is less than n (so that Theorem 4.1 is inapplicable) along with the corresponding values of $\phi(n)$ and $R^{\frac{1}{\phi(n)}}$ for $R \leq 16$. The entry for $R^{\frac{1}{\phi(n)}}$ is listed only if it is smaller than n ; otherwise, it is starred, and has an intrinsic divisor by the inequality (4.1) and Lemma 3.4.

TABLE OF POSSIBLE EXCEPTIONAL INDICES

	$n = 4$	5	6	8	9	10	12	14	16	18	20	24	30
R	$\phi(n) = 2$	4	2	4	6	4	4	6	8	6	8	8	8
4	2	4	2	4	8	4	4	8	16	8	16	16	16
8	$R^{\frac{1}{\phi(n)}} = 2.8$	*	2.8	8	*	8	8	*	*	*	*	*	*
12	3.5	*	3.5	*	*	*	12	*	*	*	*	*	*
16	4	*	4	*	*	*	*	*	*	*	*	*	*

Since the entries for $R = 16$ beyond $n = 6$ are all starred, Theorem 2.1 follows from Lemma 5.1 and Theorem 4.2. We also observe that if $16 > R > 4$, then 8, 10 and 12 are the only possible exceptional indices. These are disposed of by the following lemmas.

LEMMA 5.2. *If $R = 8$ or 12, then twelve is not an exceptional index.*

PROOF. Since $(L, M) = 1$ we see from the list of Q 's in (5.1) that $(Q_3, M) = (Q_4, M) = (Q_6, M) = 1$. Also $Q_4 = Q_3 - M = Q_6 + M$. Hence by (5.2) $(Q_{12}, Q_6) = (Q_{12}, Q_3) = (-2M^2, Q_3) = (2, Q_3) = 1$ or 2 and $(Q_{12}, Q_4) = (-3M^2, Q_4) = (3, Q_4) = 1$ or 3.

Since $|Q_n| \geq 8$ if neither 2 nor 3 are divisors of Q_{12} , Q_{12} has an intrinsic divisor ≥ 5 . If either 2 or 3 are intrinsic divisors of Q_{12} , there is nothing to prove. Finally if both 2 and 3 are extrinsic divisors of Q_{12} they are the only extrinsic divisors, and by Lemma 3.3 $2 \parallel Q_{12}, 3 \parallel Q_{12}$. Hence the quotient $Q_{12}/6$ is an integer greater than one and prime to Q_3, Q_4, Q_6 . Therefore in every case Q_{12} has an intrinsic divisor.

The next lemma may be proved similarly.

LEMMA 5.3. *If $R = 8$, then eight and twelve are not exceptional indices.*

There remains then only the two cases when $R = 4$; namely $L = 1, M = -1$ and $K = 5$ or $L = 5, M = 1$ and $K = 1$.

In the first case, the Lehmer numbers are simply the well known Fibonacci numbers $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots$. By direct computation, $F_6 = 2^3, F_{12} = 2^4 3^2, F_{18} = 2^3/17^2$ are the only exceptional Fibonacci numbers of index less than thirty-one.

In the second case, $P_n = F_n$ when n is even. But all possible exceptional indices are even. Hence again 6, 12 and 18 are the only exceptional indices. This argument completes the proof of Theorem 1.2 of the introduction.

In closing, note that our results immediately apply to the associated Lehmer numbers (S) defined by

$$S_n = \begin{cases} (\alpha^n + \beta^n) & n \text{ even;} \\ (\alpha^n + \beta^n)/(\alpha + \beta) & n \text{ odd.} \end{cases}$$

For $S_n = P_{2n}/P_n$.

CALIFORNIA INSTITUTE OF TECHNOLOGY

REFERENCES

- [1] A. S. BANG, *Taltheoretiske Undersogelser*, Tidsskrift fur Mat. (5), 4 (1886), pp. 130–132.
- [2] G. D. BIRKHOFF and H. S. VANDIVER, *On the integral divisors of $a^n - b^n$* , Ann. of Math. (2), 5 (1904), pp. 173–180.
- [3] R. D. CARMICHAEL, *On the numerical factors of arithmetic forms*, Ann. of Math., 15 (1913–1914), pp. 30–70.
- [4] G. H. HARDY and E. M. WRIGHT, *The Theory of Numbers*, Oxford, 1938.
- [5] D. H. LEHMER, *An extended theory of Lucas' functions*, Ann. of Math., 31 (1930), pp. 419–448.
- [6] C. G. LEKKENKERKER, *Prime factors of the elements of certain sequences of integers*, Proc. Amsterdam Akad. A 56, no. 3 (1953), pp. 265–280.
- [7] J. J. SYLVESTER, *Collected Mathematical Papers*, 4, Cambridge University Press, 1912.
- [8] K. ZSIGMONDY, *Zur theorie der Potenzreste*, Monatshefte Math. Phys., 3 (1892), pp. 265–284.

ON THE NUMBER OF VANISHING TERMS IN AN INTEGRAL CUBIC RECURRENCE

MORGAN WARD, California Institute of Technology

Introduction. Let

$$(T): T_0, T_1, T_2, \dots, T_n, \dots$$

be an integral cubic recurrence; that is, the initial values T_0, T_1, T_2 of (T) are integers and

$$T_{n+3} = PT_{n+2} - QT_{n+1} + RT_n \quad (n = 0, 1, \dots).$$

Here P, Q and R are fixed integers and $R \neq 0$. The polynomial

$$f(z) = z^3 - Pz^2 + Qz - R$$

and the recurrence (T) are said to be associated. If

$$g(z) = T_0z^2 + (T_1 - PT_0)z + (T_2 - PT_1 + QT_0),$$

then for $|z|$ sufficiently large,

$$g(z)/f(z) = \sum_1^{\infty} T_{n-1}z^{-n}$$

is a generating function for (T) .

The two most interesting cases are when $g(z) = df(z)/dz$ and $g(z) = 1$; we denote the corresponding recurrences by (S) and (H) .

If $f(z)$ has distinct roots u, v, w , then S_n is simply the Newtonian sum of the n th powers of the roots, while H_{n+2} as a symmetric function is the homogeneous product sum of the roots of degree n [4]:

$$S_n = u^n + v^n + w^n, \quad H_{n+2} = \sum u^{r_1}v^{r_2}w^{r_3}.$$

Here the second sum is extended over all non-negative integers r_i such that $r_1+r_2+r_3=n$. (H) is of particular importance in the algebra of recurring sequences [1], [2]; the corresponding recurrences of order two are the well known Lucas functions [3].

An integer $k \geq 0$ is called a "zero" of the recurrence (T) if $T_k=0$. For example, 0 and 1 are zeros of (H) . We determine here the maximum number of possible zeros of (T) when its associated polynomial has integral roots subject to a restriction to be described presently.

Prior work on this problem has been confined to the cases when $f(z)$ has complex roots and $R=\pm 1$ [6], [7] or when $(T)=(S)$ and $P=0$ [8]. There is an important general result of Kurt Mahler's [5] in this connection. Let us call both (T) and its polynomial $f(z)$ "degenerate" or "nondegenerate" according as the ratio of any pair of different roots of $f(z)$ is, or is not, a root of unity.

Mahler showed that if (T) is non-degenerate, $|T_n|$ tends to infinity with n . Hence

The total number of zeros of any non-degenerate recurrence (T) is finite.

We prove here the following more precise result.

THEOREM 1. *If the associated polynomial of an integral cubic recurrence is both non-degenerate and has integral roots which are co-prime in pairs, then at most three terms of the recurrence can vanish.*

The exact determination of the number of zeros of a given recurrence (T) under these hypotheses may be very difficult. For example, it is easy to see that (S) can have at most one zero; but the assertion that if $S_1 \neq 0$, (S) has no zeros is essentially Fermat's last theorem. On the other hand, it follows from the results of this paper that the sequence (T) with initial values $T_0=0$, $T_1=1$ and $T_2=0$ has no other zeros.

The plan of the paper is sufficiently indicated by the section headings. In the conclusion we mention some unsolved problems concerning the zeros of (H) suggested by the investigation.

2. Preliminary lemmas. We denote the roots of $f(z)$ by u , v and w . Then u , v and w are integers co-prime in pairs with distinct absolute values, since $f(z)$ is non-degenerate.

The general term T_n of (T) is of the form

$$(2.1) \quad T_n = Uu^n + Vv^n + Ww^n$$

where U , V , W are rational and different from zero, since (T) is of order three. Consequently, k and l are zeros of (T) if and only if

$$(2.2) \quad \begin{aligned} Uu^k + Vv^k + Ww^k &= 0 \\ Uu^l + Vv^l + Ww^l &= 0. \end{aligned}$$

On solving (2.2) for the ratios $U:V:W$, we obtain

LEMMA 2.1. *If k and l are distinct integers and $l > k \geq 0$, a necessary and sufficient condition that k and l be zeros of (T) is that U , V and W of formula (2.1) satisfy the conditions*

$$\frac{Uu^k}{w^{l-k} - v^{l-k}} = \frac{Vv^k}{u^{l-k} - w^{l-k}} = \frac{Ww^k}{v^{l-k} - u^{l-k}}.$$

We note for future use two simple corollaries of this result.

LEMMA 2.2. *If $T_0=0$, then a necessary and sufficient condition that $T_n=0$ for $n > 0$ is that*

$$(2.3) \quad \frac{U}{w^n - v^n} = \frac{V}{u^n - w^n} = \frac{W}{v^n - u^n}.$$

LEMMA 2.3. If $T_0=0$ and if $l>k>0$, then a necessary condition that $T_l=T_k=0$ is that

$$(2.4) \quad \frac{w^k - v^k}{w^l - v^l} = \frac{u^k - w^k}{u^l - w^l} = \frac{v^k - u^k}{v^l - u^l}.$$

LEMMA 2.4. Let t be a real variable and n any real number greater than one. Then the function $(t^n-1)/(t+1)$ increases steadily if $t>0$ and $(t^n+1)/(t+1)$ increases steadily if $t>1$.

For the derivatives of the functions are positive under the stated conditions.

LEMMA 2.5. Let r and s be co-prime integers and k and l positive integers. Then

$$(2.5) \quad (r^k - s^k, r^l - s^l) = r^d - s^d \quad \text{where } d = (k, l).$$

Here (x, y) denotes the greatest common divisor of the integers x and y .

For denote the left side of (2.5) by m . Since d divides k and l , $r^d - s^d$ divides $r^k - s^k$ and $r^l - s^l$. Consequently, $r^d - s^d$ divides m . It suffices then to show that m divides $r^d - s^d$.

Since m divides $r^k - s^k$, it is prime to both r and s . Hence there exists a positive integer t with the property that m divides $r^t - s^t$ but m does not divide $r^n - s^n$ if $0 < n < t$. Then m divides $r^n - s^n$ if and only if t divides n . For let $n = 2qt \pm c$, where $0 \leq c < t$ and let $a = qt$, $b = qt \pm c$. Then if $b \geq a$, $r^n - s^n = (r^a - s^a)(r^b - s^b) + (rs)^a(r^c - s^c)$, and if $a \geq b$, $r^n - s^n = (r^a - s^a)(r^b - s^b) - (rs)^b(r^c - s^c)$. In either case, since m divides $r^n - s^n$ and $r^a - s^a$ and is prime to r and s , the minimal property of t is contradicted unless $c = 0$ or $c = t$.

Now m divides both $r^k - s^k$ and $r^l - s^l$. Hence t divides both k and l . Therefore, t divides d , and m divides $r^d - s^d$, completing the proof.

3. Recurrences with three zeros. Let (T) be a recurrence with $T_0=0$ and at least two other zeros, k and l . We may assume that

$$(3.1) \quad 0 < k < l, \quad T_n \neq 0, \quad 0 < n < k.$$

Then by Lemma 2.3, the equalities (2.4) must hold. Let $d = (k, l)$. Since u, v and w are co-prime in pairs, if we divide the numerator and denominator of each of the fractions in (2.4) by the corresponding integers $w^d - v^d$, $u^d - w^d$ and $v^d - u^d$, we obtain by Lemma 2.5 three equal fractions in their lowest terms. Hence corresponding numerators and denominators must be equal up to sign; that is

$$(3.2) \quad \begin{aligned} \frac{w^k - v^k}{w^d - v^d} &= \pm \frac{u^k - w^k}{u^d - w^d} = \pm \frac{v^k - u^k}{v^d - u^d}, \\ \frac{w^l - v^l}{w^d - v^d} &= \pm \frac{u^l - w^l}{u^d - w^d} = \pm \frac{v^l - u^l}{v^d - u^d}. \end{aligned}$$

Consider now the equalities

$$(3.3) \quad \frac{w^n - v^n}{w - v} = \pm \frac{u^n - w^n}{u - w} = \pm \frac{v^n - u^n}{v - u}, \quad n \geq 1.$$

Observe that each of the equalities (3.2) may be put into this form by letting $u' = u^d, v' = v^d, w' = w^d$, taking n equal to k/d or l/d and then dropping the primes.

Let a, b and c be the absolute values of u, v and w respectively. We may evidently assume that

$$(3.4) \quad w = c > b > a > 0; \quad v = \pm b, \quad u = \pm a.$$

For changing the signs of all the roots of $f(z)$ merely multiplies T_n by $(-1)^n$. There are four cases according to the choices of sign of u and v .

Case	Roots of $f(z)$			Equalities (3.3)
	u	v	w	
1	a	b	c	$\frac{c^n - b^n}{c - b} = \frac{c^n - a^n}{c - a} = \frac{b^n - a^n}{b - a}$
2	$-a$	b	c	$\frac{c^n - b^n}{c - b} = \frac{c^n - (-a)^n}{c + a} = \frac{b^n - (-a)^n}{b + a}$
3	a	$-b$	c	$\frac{c^n - (-b)^n}{c + b} = \frac{c^n - a^n}{c - a} = \frac{b^n - (-a)^n}{b + a}$
4	$-a$	$-b$	c	$\frac{c^n - (-b)^n}{c + b} = \frac{c^n - (-a)^n}{c + a} = \frac{b^n - a^n}{b - a}$

Both case 1 and case 2 are impossible if $n > 1$. In case 1, this statement is evident, since $c > b > a > 0$. In case 2, if $n > 1$, we have

$$\frac{c^n \pm a^n}{c + a} = \frac{b^n \pm a^n}{b + a}.$$

Now let $c = ax$ and $b = ay$. Then

$$\frac{x^n \pm 1}{x + 1} = \frac{y^n \pm 1}{y + 1} \quad \text{with } x > y > 1 \text{ and } n > 1$$

contradicting Lemma 2.4.

Both cases 3 and 4 are impossible if n is even. For assume n is even. Then $n > 1$, and in case 3 we have

$$\frac{b^n - a^n}{b + a} = \frac{c^n - a^n}{c - a}.$$

But $(b^n - a^n)/(b + a) < (b^n - a^n)/(b - a) < (c^n - a^n)/(c - a)$ since $c > b > a > 0$.

In case 4, we have

$$\frac{c^n - b^n}{c + b} = \frac{c^n - a^n}{c + a}.$$

Hence if $b = cx$ and $a = cy$, then

$$\frac{1 - x^n}{1 + x} = \frac{1 - y^n}{1 + y} \quad \text{with } 1 > x > y > 0.$$

But by Lemma 4, $(1 - t^n)/(1 + t)$ steadily decreases if $t > 0$.

We now apply these results to the equalities (3.2) in accordance with the remark following (3.3). First, d must be odd. For if d is even, u^d, v^d, w^d are positive, and case 1 applies; that is, $n = 1$ so that $k = d$ and $l = d$ contrary to (3.1). Since n must be odd, k and l must both be odd. Hence $w^k - v^k$ and $w^d - v^d$ are of like sign. Therefore, the first equality (3.2) may be written as

$$\frac{w^k - v^k}{w^d - v^d} = \frac{u^k - w^k}{u^d - w^d} = \frac{v^k - u^k}{v^d - u^d}.$$

But since $T_0 = T_k = 0$, this equality and lemma 2.2 imply that

$$\frac{U}{w^d - v^d} = \frac{V}{u^d - w^d} = \frac{W}{v^d - u^d}.$$

Hence $T_d = 0$ by Lemma 2.2. But $0 < d \leq k$. Hence $d = k$ by condition (3.1). We have thus proved:

THEOREM 2. *Let (T) be an integral cubic recurrence whose associated polynomial is non-degenerate and has integral roots which are co-prime in pairs, and assume that the first two zeros of (T) are 0 and k . Then if k is even, (T) has no other zeros. If k is odd, any other zero of (T) must be an odd multiple of k .*

It follows immediately that the recurrence with initial values 0, 1, 0 has no other zeros. On the other hand, the recurrence (H) of the introduction has $H_3 = P = 0$ if $u + v + w = 0$. Hence there exist recurrences with three zeros.

4. Proof of Theorem 1. We will now use Theorem 2 to give a proof by contradiction of Theorem 1. Let (T) and $f(z)$ satisfy the hypotheses of the theorem, and suppose (T) has more than three zeros. Let the first four zeros of (T) be k_1, k_2, k_3, k_4 , so that $0 \leq k_1 < k_2 < k_3 < k_4$.

The recurrence (T') defined by $T'_n = T_{n+k_1}$ is associated with $f(z)$ and its first three zeros are 0, $k_2 - k_1$, and $k_3 - k_1$. Both $k_2 - k_1$ and $k_3 - k_1$ are odd by Theorem

2. Hence their difference $k_3 - k_2$ is even. The recurrence (T'') defined by $T''_n = T_{n+k_2}$ is associated with $f(z)$ and its first three zeros are 0, $k_3 - k_2$, and $k_4 - k_2$. But $k_3 - k_2$ is even, contradicting Theorem 2.

5. Conclusion. It follows from Theorem 2 that if (T) has three zeros, say k_1 , k_2 and k_3 , then $d = k_2 - k_1$ is odd and the zeros lie in a recurrence (T^*) defined by $T_n^* = T_{k_1+n d}$ whose associated polynomial $f^*(z)$ has for its roots the d th powers of the roots of $f(z)$. Since the initial values of (T^*) are 0, 0, and T_2^* , $T_n^* = T_2^* H_n^*$ where (H^*) is the recurrence associated with $f^*(z)$ discussed in the introduction. We are thus led to consider the zeros of the recurrence (H) .

We have seen that H_3 can vanish. The next possibility is that $H_6 = 0$, giving the diophantine equation

$$(5.1) \quad (u + v + w)(u^2 + v^2 + w^2) + uvw = 0.$$

Trivial solutions of (5.1) evidently violate our hypotheses on $f(z)$. Whether or not (5.1) has non-trivial solutions appears to be unknown. The more general question of whether H_{2n+1} can vanish when $n > 1$ appears to be of a difficulty comparable to the Fermat problem for the recurrence (S) .

The simplest case when $(T) \neq (H)$ would have three zeros would be when $d = 3$ and $k_3 = k_1 + 5d$ making $H_6^* = 0$. The related diophantine equation is obtained from (5.1) by replacing u, v, w by their cubes. It would imply then that the diophantine system

$$u^3 + v^3 + w^3 = 4^\epsilon s^3, \quad u^6 + v^6 + w^6 = 2t^3, \quad \epsilon = 0 \text{ or } 1,$$

has a non-trivial solution, which appears unlikely.

It is tempting to conjecture in view of these remarks that under our hypotheses on $f(z)$, (H) is the *only* recurrence which can have more than two zeros. It follows of course from Lemma 2.2 that there exist recurrences (T) with arbitrarily assigned zeros k and l . But it may be shown by simple examples that neither Theorem 1 or Theorem 2 is true if we change our hypotheses on the roots of $f(z)$.

References

1. E. T. Bell, Notes on recurring series of the third order, *Tohoku Math. Journal*, vol. 24, 1924, pp. 168–184.
2. L. E. Dickson, *History of the Theory of Numbers*, vol. 1, pp. 407–411.
3. Eduard Lucas, *Theorie des Nombres*, Paris, 1891, Chapter 18.
4. P. A. MacMahon, *Combinatory Analysis*, vol. 1, Cambridge, 1915, page 3.
5. Kurt Mahler, Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, *Proc. Amsterdam Acad.*, vol. 38, 1935, pp. 50–60.
6. C. L. Siegel, Über die Koeffizienten in der Taylorschen Entwicklung rationaler Funktionen, *Tohoku Journal*, vol. 20, 1921, pp. 26–31.
7. Morgan Ward, Note on an arithmetical property of recurring series, *Math. Zeitschr.*, vol. 39, 1934, pp. 211–214.
8. Morgan Ward, On the vanishing of the sum of the N th powers of the roots of a cubic equation, *This MONTHLY*, vol. 41, 1934, pp. 313–316.

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

BY
MORGAN WARD

1. Introduction. Let

$$(W): \quad W_0, W_1, W_2, \dots, W_n, \dots$$

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

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

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

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

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, \dots 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,

$$(3.1) \quad W_n = A\alpha^n + B\beta^n + C\gamma^n$$

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

$$(3.2) \quad \alpha^{\rho_k} \equiv \beta^{\rho_k} \equiv \gamma^{\rho_k} \equiv g \pmod{p^k}$$

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

$$(3.3) \quad W_{n+\rho} \equiv gW_n \pmod{p}.$$

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 $W_0, \dots, W_{\rho-1}$ of (W) .*

If $W_n \equiv 0 \pmod{p}$, $0 \leq n < \rho$, 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 $g \not\equiv 0 \pmod{p}$ such that

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

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

$$(3.5) \quad w_n = w_r.$$

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 $b \geq 0$ 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 $\alpha^r, \beta^r, \gamma^r$. 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 p_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

$$(4.1) \quad (W_0, W_1, W_2) = 1.$$

We may then classify the primes with respect to the sequence (W) in three ways: first by whether or not they divide the integer $R\Delta(W)$; 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 $R\Delta(W)$ 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

$$(4.2) \quad \alpha \equiv \beta \equiv \gamma \equiv a \pmod{p}$$

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

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

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

$$(5.1) \quad \alpha^\rho = a + p\alpha_0, \quad \beta^\rho = a + p\beta_0, \quad \gamma^\rho = a + p\gamma_0.$$

Here $\alpha_0, \beta_0, \gamma_0$ 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 $0 \leq t < \rho$ and by the congruence (3.3), all other multiples of p appear in subsequences (W') of order ρ ,

where $W'_n = W_{np+t}$. 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+p}, W_{t+2p}) , then $w_{np+t} = v_n + c$. Here v_n is the p -adic value of V_n .

The characteristic polynomial of (V) $f_p(z) = (z - \alpha^p)(z - \beta^p)(z - \gamma^p)$ 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 $l \geq 1$ such that

$$(5.2) \quad \alpha - a = p^l \alpha_0, \quad \beta - a = p^l \beta_0, \quad \gamma - a = p^l \gamma_0$$

where $\alpha_0, \beta_0, \gamma_0$ 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

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

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*

$$(5.4) \quad g(z) = Hz^2 + Kz + M$$

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

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

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

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

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

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

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 $\Delta(W) \equiv 0 \pmod{p}$. 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,*

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

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*

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

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 $t_0 = 0$, $t_1 = n_0$, \dots , $t_k = n_0 + n_1 p + \cdots + n_{k-1} p^{k-1}$, \dots 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

$$(6.1) \quad \alpha - a = p\alpha_0, \quad \beta - a = p\beta_0, \quad \gamma - a = p\gamma_0$$

where a is an integer prime to p ; $\alpha_0, \beta_0, \gamma_0$ 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 $\alpha_0, \beta_0, \gamma_0$ 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

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

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

$$T_k^{(i)} = P_0 T_k^{(i)} - Q_0 T_k^{(i)} + R_0 T_k^{(i)}$$

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 ≥ 0 and if $W_t^{(r)}$ is defined by*

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

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

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

are integers. Furthermore $p^2 W_t^{(r)}$ 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 $p^2 W_t^{(r)}$ 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

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

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):

$$\begin{aligned} W_{xp^k+t} &= \sum_{\alpha} A\alpha^t \alpha^{xp^k} = \sum_{\alpha} A\alpha^t (a + p\alpha_0)^{xp^k} = \sum_{\alpha} \sum_r A\alpha^t \binom{xp^k}{r} a^{xp^k-r} p^r \alpha_0^r \\ &= \sum_r \sum_{\alpha} A\alpha^t \binom{xp^k}{r} a^{xp^k-r} p^r \alpha_0^r = \sum_r \binom{xp^k}{r} a^{xp^k-r} p^r W_t^{(r)}. \end{aligned}$$

Hence we may write

$$(6.6) \quad W_{xp^k+t} = \sum_1 + \sum_2$$

where

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

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

$$\begin{aligned} \sum_1 &= a^{xp^k} W_t + xp^k a^{xp^k-1} (W_{t+1} - aW_t) \\ &\quad + \frac{xp^k(xp^k-1)}{1 \cdot 2} (W_{t+2} - 2aW_{t+1} + a^2W_t). \end{aligned}$$

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

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

Now consider the summation \sum_2 . By Lemma 6.2, the numbers $p^2 W_t^{(r)}$ 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 $3 \leq r < p$, $\theta \geq k+1$ 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 $r \geq p$, 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 $\sum r_n \geq 1$, and the p -adic value of the denominator of

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

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

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

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

since $p \geq 5$. 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,

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

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 $\chi(p) \neq 0$, and let n_0 be one of its ranks of apparition. Then by Lemma 5.1,

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

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 $k \geq 1$. 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

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

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

Since $a \not\equiv 0 \pmod{p}$, it follows that as x runs through a complete residue system modulo p , so does $U_k + x a^{t_k} g'(t_1)$. 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 $t_{k-1} + n_k p^k$, 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 $k \geq 1$.

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 $0 \leq t_0 < p$ and $W_n \equiv 0 \pmod{p}$ if and only if $n \equiv t_0 \pmod{p}$. Hence

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

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

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

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

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

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), $w_n \geq 2$ 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),

$$\alpha' - a' = p^2 \alpha'_0, \quad \beta' - a' = p^2 \beta'_0, \quad \gamma' - a' = p^2 \gamma'_0$$

where $\alpha'_0, \beta'_0, \gamma'_0$ are algebraic integers of \Re . 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 preceding Theorem 5.1. Hence since

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

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 $q \geq 1$. 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 $q \geq l$, or q even, and less than l . Hence assume that $q = 2r < l$, and consider the congruences

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

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

$$\mu = m_0 + m_1 p + m_2 p^2 + \dots$$

with convergents $\mu_0 = 0$; $\mu_k = m_0 + m_1 p + \dots + m_{k-1} p^{k-1}$, $k \geq 1$, with the property that the p -adic value of $2Hn + K$ is exactly k if and only if

$$(7.4) \quad n \equiv \mu_k \pmod{p^k}, \quad n \not\equiv \mu_{k+1} \pmod{p^{k+1}}.$$

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 $q \geq l$ 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 $q \geq l$, 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 $(W) \supset (W') \supset (W'') \dots$. 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

$$(8.1) \quad \alpha^p = a + p^l \alpha_0, \quad \beta^p = a + p^l \beta_0, \quad \gamma^p = a + p^l \gamma_0, \quad l \geq 1,$$

where a is prime to p and $\alpha_0, \beta_0, \gamma_0$ 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

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

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 $\mathfrak{R} \pmod{p^l}$, but not $\pmod{p^{l+1}}$. 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 $\pmod{p^{l+1}}$, 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 Φ_{pt} denote its numerical value when $R^2 L_{p-1}^2 W_t$, $4RL_p W_{t+p}$, and W_{t+2p} each divided by (W_t, W_{t+p}, W_{t+2p}) 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 $(\Phi_{p,t} | p)$.

If $\chi_t = 0$, let ϕ_{pt} denote the p -adic value of Φ_{pt} . 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 $W'_n = W_{n+p+t}$. 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 $0 < c \leq b$.*

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

Consider next the regular null divisors of (W) , that is the $r \geq 1$ distinct prime factors p_1, p_2, \dots, 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

$$(9.1) \quad P = p^k P_0, \quad Q = p^l Q_0, \quad R = p^m R_0$$

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

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

Then we shall prove in the following section

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

$$(W'_x) \quad (x = 0, 1, \dots, c - 1)$$

all satisfying the same recurrence and such that

- (i) *The regular null divisors of each recurrence are precisely p_1, p_2, \dots, p_{r-1} ;*
- (ii) *If $n = ct + x$, $0 \leq x < c$, 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

$$(10.1) \quad k' = k - s \geq 0, \quad l' = l - 2s \geq 0, \quad m' = m - 3s \geq 0.$$

There are several cases to discuss.

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

Case 2. $s \geq 1$; 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

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

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

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

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

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 $W'_0 = p^{2s} W_0$, $W'_1 = p^s W_1$, $W'_2 = W_2$. 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, \dots, 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 $k' \geq 1$, $m' \geq 2$. 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 $l' \geq m'$, $2m'$, $k' \geq m'$. Hence $d' = m'/3$, $s' = 0$ and Case 4 following will apply to (W') .

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

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

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

Hence $k' \geq 1$, $l' = 2$, and $m' \geq 4$. 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

$$A'_x = A\alpha^x, \quad B'_x = B\beta^x, \quad C'_x = C\gamma^x, \quad x = 0 \text{ or } 1,$$

and let

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

Then if $n = 2t+x$, $0 \leq x \leq 1$, $t = [n/2]$ 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') have the same regular null divisors.

Since, for each sequence (W) , $s' = a' = 1$ the results of Case 1 give $W'_{xt} = p^{t-2} W_x^*$ where sequences (W_x^*) have p_1, \dots, 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 $n = 2t+x$, $0 \leq x \leq 1$, then

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

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

In Case 4, if $m = 2$, then $k \geq 1, l \geq 2$ but if $m = 1, k \geq 1, l \geq 1$. 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 non-zero 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

$$(1.2) \quad f(z) = z^3 - Pz + Qz - R$$

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 $W_{n+8} = RW_n$ 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 polynomial 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

$$(11.1) \quad W_q^6 \equiv 1 \pmod{q}.$$

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 $R\Delta\Delta(W) \not\equiv 0 \pmod{13}$ 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 $(W) \pmod{13}$, we obtain 1, 2, 3, 2, 3, 5, 0, 10, 4, 7, 2, 0; 1, 2, 3, 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, . . . 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 $(W) \pmod{13^2}$ 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

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

(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 arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Amsterdam Acad. vol. 38 (1935) pp. 50–60.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.

THE MAPPINGS OF THE POSITIVE INTEGERS INTO THEMSELVES WHICH PRESERVE DIVISION

MORGAN WARD

1. Introduction, First Theorem. Let L denote the lattice of the integers $0, 1, 2, \dots$ partially ordered by division. We study here mappings

$$\phi: \phi_0, \phi_1, \phi_2, \dots, \phi_n = \phi(n), \dots$$

of L into itself which preserve division; that is,

- (i) If n divides m , then ϕ_n divides ϕ_m .

Since ϕ_1 divides every ϕ_n and every ϕ_n divides ϕ_0 , we lose little generality by assuming

- (ii) $\phi_0 = 0, \phi_1 = 1$.

Any mapping with properties (i) and (ii) will be called a divisibility sequence on L .

A mapping ϕ is said to be of “*positive character*” if

- (iii) $\phi_n > 0$ for $n > 0$.

A divisibility sequence of positive character will be called a *normal sequence* or *normal mapping* of L .

In many instances, we are interested in the occurrence of multiples of some assigned modulus m among the terms of a normal sequence ϕ . If $\phi_r \equiv 0 \pmod{m}$ for some $r > 0$, we call m a *divisor* of ϕ and r a “*place of apparition*” of m in ϕ . If in addition $\phi_s \not\equiv 0 \pmod{m}$ for every proper divisor s of r , r is called a “*rank of apparition*” of m in ϕ . If m is not a divisor of ϕ , we assign to it the rank of apparition zero, which is consistent with the definitions.

It follows that every modulus m has at least one rank of apparition in ϕ . If each modulus has exactly one rank of apparition, we say that ϕ “*admits a rank function*”. Indeed if the rank of m in ϕ is denoted by $\rho(m)$ then ρ is a divisibility sequence. Furthermore

- (iv) $\phi_n \equiv 0 \pmod{m}$ if and only if $n \equiv 0 \pmod{\rho_m}$.

Under this condition, multiples of any integer m if they appear at all in ϕ are regularly spaced as in the identity mapping $i(n) = n$.

Normal sequences are of common occurrence in number theory; the totient function and its various generalizations [3, chap. 5] is a

familiar example. For other examples and generalizations see [3, chap. 17], [4], [6], [9], [10].

Normal sequences with property (iv) are of considerable arithmetical interest, and special instances, notably the Lucas sequences [6] have been intensively studied [1], [5].

We study here general properties of all divisibility sequences and in particular develop necessary and sufficient conditions that a normal sequence shall admit a rank function. Our first main result is as follows.

THEOREM 1. *A necessary and sufficient condition that a normal mapping ϕ admit a rank function is that it have the following property:*

$$(v) \quad \phi(pn) \succ \phi(qn) = \phi(n) \quad p, q \text{ any distinct primes.}$$

Here we are using the lattice notation explained in § 3; the left side of (v) is the greatest common divisor of $\phi(pn)$ and $\phi(qn)$.

2. Further Results, Second Theorem. Our other results are formulated in terms of the notion of the “generator” of a normal sequence. Let

$$(2.1) \quad n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

be the prime factorization of any positive integer n of L . Define a new mapping ψ of L by $\psi(0)=0$, $\psi(1)=1$ and

$$(2.2) \quad \psi(n) = \phi(n) \div \bigcap_{1 \leq i \leq k} \phi\left(\frac{n}{p_i}\right), \quad n > 1.$$

Then ψ is called the generator of ϕ . It has properties (ii) and (iii), but not in general property (i). It is shown in § 5 that formula (2.2) may be inverted to express ϕ in terms of ψ thus:

$$(2.3) \quad \phi(n) = \bigcap_{(c)} \prod_{1 \leq i \leq r} \psi(c_i).$$

Here (c) : $1=c_1, c_2, \dots, c_{r-1}, c_r=n$ is a complete chain of divisors of n in the lattice L , c_i covering c_{i+1} for $i=1, 2, \dots, r-1$. The indicated least common multiple \bigcap of the products $\prod \psi(c_i)$ is to be extended over all such chains (c) of divisors of n .

For example, if $n=12$, there are three complete chains: 1, 2, 4, 12; 1, 2, 6, 12 and 1, 3, 6, 12. Thus (2.3) becomes

$$\phi(12) = \psi(1)\psi(2)\psi(4)\psi(12) \cap \psi(1)\psi(2)\psi(6)\psi(12) \cap \psi(1)\psi(3)\psi(6)\psi(12).$$

Conversely, it turns out that if we start off with a mapping ψ of positive character with $\psi_0=0$, $\psi_1=1$ and define ϕ by (2.3), then ϕ is a

normal mapping, and ψ is its generator. The relationships between arithmetical properties of ϕ and ψ are developed in §§ 6 and 7.

If ϕ is of positive character, we may define a new numerical function ζ by the Dedekind-Möbius inversion formulas [2, p. 61]

$$(2.4) \quad \zeta(n) = \prod_{d \mid n} \phi\left(\frac{n}{d}\right)^{\mu(d)}; \quad \phi(n) = \prod_{d \mid n} \zeta(d).$$

Here μ as usual is the Möbius function.

ζ is uniquely determined by ϕ , but does not define a mapping of L because $\zeta(n)$ is not necessarily an integer. If $\zeta(n)$ is an integer for every n , ϕ is evidently a normal sequence; we call ζ in this case the “Dedekind generator” of ϕ .

THEOREM 2. *If ϕ is a normal sequence, then a necessary and sufficient condition that ϕ admit a rank function is that its Dedekind generator should exist, and be equal to its ordinary generator.*

The best known instance of this theorem is when ϕ is the Lucas sequence $\phi_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ where $p = \alpha + \beta$, $q = \alpha\beta$ are co-prime integers chosen so that $|pq| > 1$; $|p^2 - 4q| > 0$. Then ψ is the Sylvester [7] cyclotomic sequence

$$\psi_n = \prod_{\substack{1 \leq r \leq n \\ r \nmid n}} \left(\alpha - e^{2\pi i \frac{r}{n}} \beta \right).$$

3. Notations. We use whenever convenient the standard notations of lattice algebra for arithmetical division and its associated operations over L considered as a distributive residuated lattice [8], [11]. We thus write $a \sqsupseteq b$, $a \not\sqsupseteq b$ and $a \sqsupset b$ for “ a divides b ”, “ a does not divide b ” and “ a properly divides b ”. If neither $a \sqsupseteq b$ nor $b \sqsupseteq a$, we say a and b are “non-comparable”. If $a \sqsupseteq b$ and $a \sqsupset x \sqsupset b$ implies either $a = x$ or $b = x$ we say “ a covers b ”.

$a \sqcup b$, $a \sqcap b$ and ab stand respectively for the greatest common divisor (g.c.d.), least common multiple (l.c.m.), and product of a and b . If a_1, a_2, \dots, a_k are k given integers of L , we write $\sqcup a_i$, $\sqcap a_i$ and $\prod a_i$ for their g.c.d., l.c.m. and product suppressing the range of i where no confusion can arise.

If $x * y$ denotes any one of the three operations $x \sqcup y$, $x \sqcap y$ or xy in L , and ϕ is any mapping of L , we say that ϕ is “ $*$ -factorable” if $\phi(x * y) = \phi(x) * \phi(y)$ whenever $x \sqcup y = 1$ and “completely $*$ -factorable” if $\phi(x * y) = \phi(x) * \phi(y)$ for every x, y . The star-product of two mappings ϕ and θ is defined as usual by $(\phi * \theta)_n = \phi_n * \theta_n$.

In proofs we use when convenient \Rightarrow and \Leftrightarrow for "implies", and "implies and is implied by". We use without specific mention the familiar formulas [12]

$$\begin{aligned} b \cup a_i &= \cup ba_i, & b \cap a_i &= \cap ba_i, \\ b \cup 0 &= b \cap 1 = b; & b \cup 1 &= 1, & b \cap 0 &= 0. \end{aligned}$$

4. Divisibility Sequences, Binary Sequences. Let ϕ be any divisibility sequence; that is, a mapping of L with properties (i) and (ii) of the introduction. Define $\alpha_0 = \beta_0 = 0$ and

$$\begin{aligned} \alpha_n &= \phi_n, & \beta_n &= 1 & \text{if} & \quad \phi_n \neq 0 \\ \alpha_n &= \bigcap_{\substack{x \geq n \\ \phi_x \neq 0}} \phi_x, & \beta_n &= 0 & \text{if} & \quad \phi_n = 0. \end{aligned}$$

Then α and β are divisibility sequences, and $\phi = \alpha\beta$. Furthermore α is a normal mapping of L , while β consists exclusively of zeros and ones. We call β a "binary (divisibility) sequence".

We may immediately obtain a binary sequence from any divisibility sequence by reducing each term modulo 2. More generally, if m is any modulus, we may obtain from the divisibility sequence ϕ a binary sequence θ which describes the distribution of multiples of m in ϕ by letting $\theta_n = 0$ or 1 according as $\phi \equiv 0$ or $\phi \not\equiv 0 \pmod{m}$. The sequences obtained in this manner from linear divisibility [12] or elliptic divisibility sequences [13] are usually periodic.

Again, if E is any subset of L with the properties that 0 is not in E and if x is in E , so is every divisor of x , then the characteristic function of E is evidently a binary sequence. A simple example is the set of square-free integers; the characteristic function is μ^2 .

Let β be any binary sequence. If $\beta_k = 0$, k is called a zero of β . If in addition $\beta_d \neq 0$ for $d \supset k$, k is called a prime zero of β . The prime zeros of β evidently form a multiplicative basis for the set of all zeros of β . Perhaps the most interesting property of this basis is expressed by the following theorem whose proof is left to the reader.

THEOREM. *The zeros of a binary divisibility sequence have a finite basis if and only if the sequence is periodic. The period of the sequence is then the l.c.m. of the prime zeros of its basis.*

5. The Generator of A Normal Sequence. From now on, all mappings considered are of positive character. Let ψ be any such mapping with $\psi_0 = 0$, $\psi_1 = 1$ and define a new mapping ϕ by means of formula (2.3) and $\phi_0 = 0$, $\phi_1 = 1$. Then ϕ is evidently normal. Hold n fixed, and let (2.1) be its prime decomposition. Each complete chain

$$(c): \quad 1=c_1, c_2, \dots, c_{r-1}, c_r=n; \quad c_i \text{ covers } c_{i+1}$$

in the sublattice of all divisors of n is of the same length $r=a_1+a_2+\dots+a_k+1$, while c_{r-1} is one of the k elements n/p_i which cover n . We may accordingly group the chains into k mutually exclusive classes C_i by putting into class C_i all chains (c) with $c_{r-1}=n/p_i$. But any chain of class C_i consists of a complete chain of divisors of n/p_i plus the fixed element $c_r=n$. Hence formula (2.3) may be written

$$\phi_n = \bigcap_{C_i} \bigcap_{(c')} (\psi_{c'_1} \cdots \psi_{c'_{r-1}}) \psi_n$$

where the inner l.c.m. is taken over all complete chains (c') of divisors of n/p_i . Thus by (2.3) again

$$\phi_n = \bigcap_i \phi(n/p_i) \psi(n) = \psi(n) [\phi_{n/p_1} \cap \cdots \cap \phi_{n/p_k}].$$

Therefore ψ is the generator of ϕ as defined in formula (2.2).

Conversely, if we define ψ by (2.2), we find by direct calculation that (2.3) holds for small n . We therefore proceed by induction and assume that (2.3) is true for all integers less than n , and hence in particular for the k integers n/p_i which cover n .

On transforming the right side of (2.3) as in the first part of this proof, we obtain by (2.2) and the hypothesis of the induction

$$\bigcap_{(c)} \prod_i \psi_{c_i} = \bigcap_{C_i} \prod_i \psi_{c'_i} \psi_n = \bigcap_i (\phi_{n/p_i} \psi_n) = \psi_n \bigcap_i \phi_{n/p_i} = \phi_n.$$

Thus the formulas (2.2) and (2.3) are equivalent.

6. Factorable sequences. Various factorability properties of normal sequences may be elegantly stated as properties of its generator. We postpone the consideration of g.c.d. factorability until the next section, since it is intimately connected with the existence of a rank function. We omit proofs of the results stated here, since we merely wish to show the importance of the notion of a generator.

Either of the following two conditions is necessary and sufficient for a normal sequence ϕ with generator ψ to be product-factorable:

$$(6.1) \quad \phi_n = \prod_{p^t \mid n} \psi_{p^t}.$$

Here the product is extended over all prime powers p^t dividing n .

$$(6.2) \quad \psi_{nm} = \psi_n \cup \psi_m \quad n, m \text{ co-prime.}$$

A necessary and sufficient condition for ϕ to be l.c.m.-factorable is that

$$(6.3) \quad \psi_n = 1, \quad n \text{ not a power of a prime.}$$

Any one of the following three sets of conditions are necessary and sufficient for ϕ to be completely product factorable:

$$(6.4) \quad \psi(mn) = \psi(m \cap n) = \psi(m) \cup \psi(n), \quad n, m > 1.$$

$$(6.5) \quad \psi(mn) = \psi(m) \cup \psi(n) \quad \text{if } m, n \text{ are co-prime}$$

and $\psi(p^a) = \psi(p)$ for every prime p .

$$(6.6) \quad \psi(n) = \psi(p_1, \dots, p_k) = \phi(p_1)\phi(p_2), \dots, \phi(p_k).$$

Here as in (2.1), p_1, p_2, \dots, p_k are the distinct prime factors of n .

7. G.C.D. factorable mappings. A mapping ϕ is said to be *completely g.c.d. factorable* if it has the property

$$(vi) \quad \phi(n \cup m) = \phi(n) \cup \phi(m).$$

Every such mapping evidently preserves division.

LEMMA 7.1. (Ward [14]): *Conditions (iv) and (vi) are equivalent for normal mappings of L ; that is, a normal mapping admits a rank function if and only if it is completely g.c.d. factorable.*

Proof. Assume that ϕ is a normal mapping satisfying Condition (iv). Let $\rho = \rho(k)$ be the rank of $k = \phi_n \cup \phi_m$ in ϕ . Then ρ is positive. Also $k \supseteq \phi_n$, $\phi_m \Rightarrow \rho \supseteq n$, $m \Rightarrow \rho \supseteq n \cup m \Rightarrow k \supseteq \phi(n \cup m)$. But by (i),

$$n \cup m \supseteq n, m \Rightarrow \phi_{n \cup m} \supseteq \phi_n, \phi_m \Rightarrow \phi_{n \cup m} \supseteq k.$$

Hence $\phi_{n \cup m} = \phi_n \cup \phi_m$ and (iv) implies (vi).

Conversely, let ϕ be a normal mapping with property (vi), and let k be any modulus. If k is not a divisor of ϕ , the rank of k is zero, and (iv) is satisfied. If k is a divisor of ϕ , let ϕ_r be the first term with positive index r which k divides. By (i),

$$n \equiv 0 \pmod{r} \Rightarrow \phi_n \equiv 0 \pmod{k}.$$

Assume conversely that $\phi_n \equiv 0 \pmod{k}$. Then by (vi), $\phi_{n \cup r} \equiv 0 \pmod{k}$. But $0 < n \cup r \leq r$. Hence $n \cup r = r$ or $n \equiv 0 \pmod{r}$. In other words,

$$\phi_n \equiv 0 \pmod{k} \Rightarrow n \equiv 0 \pmod{r}.$$

Hence r is the rank of k in ϕ . Since k was arbitrary, (vi) implies (iv), which completes the proof.

The factorability condition on ϕ may be replaced by an equivalent condition on its generator ψ .

LEMMA 7.2 *A normal mapping ϕ admit a rank function if and*

only if its generator ϕ satisfies the condition

$$(vii) \quad \phi(n) \cup \phi(m) = 1 \quad n, m \text{ non-comparable.}$$

Proof. Assume that ϕ is normal, and admits a rank function, but that (vii) is false. Then there exist integers n, m and a prime q such that

$$(7.1) \quad \phi(n) \equiv \phi(m) \equiv 0 \pmod{q}, \text{ but } n \nmid m, m \nmid n.$$

By formula (2.2),

$$(7.1) \Rightarrow \phi(n) \equiv \phi(m) \equiv 0 \pmod{q}.$$

Suppose that q^a exactly divides $\phi(n)$ and q^b exactly divides $\phi(m)$. We may evidently assume that $b \geq a$. Let r be the rank of q^a in ϕ . Then since $n \equiv m \equiv 0 \pmod{r}$, we have $n \cup m \equiv 0 \pmod{r}$. But if (2.1) gives the factorization of n so that p_1, p_2, \dots, p_k are its distinct prime factors, then

$$(7.2) \quad \phi(n/p_i) \not\equiv 0 \pmod{q^a}, \quad 1 \leq i \leq k.$$

For in the contrary case, $\phi(n) \equiv 0 \pmod{q}$ and (2.2) together imply

$$\phi(n) \equiv \phi(n) \cap_i \phi\left(\frac{n}{p_i}\right) \equiv 0 \pmod{q^{a+1}}$$

which is a contradiction.

Now

$$(7.2) \Rightarrow n/p_i \not\equiv 0 \pmod{r} \quad i = 1, 2, \dots, k.$$

But $n \equiv 0 \pmod{r}$. Hence $n = r$ and $n \supseteq n \cup m \supseteq m$ contradicting (7.1). Therefore (iv) implies (vii).

Assume conversely that ϕ is normal with generator ψ satisfying (vii). To show that ϕ then admits a rank function, it will suffice to prove that *every prime power q^a has a unique rank of apparition in ϕ .* If q^a is not a divisor of ϕ then it has the unique rank zero. If q^a is a divisor of ϕ then there exists a positive index r such that

$$(7.3) \quad \phi_r \equiv 0 \pmod{q^a}, \quad \phi_n \not\equiv 0 \pmod{q^a}, \quad 0 < n < r.$$

To prove that r is the rank of q^a in ϕ , it will suffice to show that if $\phi_n \equiv 0 \pmod{q^a}$ then $n \equiv 0 \pmod{r}$. This we do by contradiction. For otherwise, there exists a least positive $n > r$ such that $\phi_n \equiv 0 \pmod{q^a}$, but n, r noncomparable. Evidently, $\phi_r \equiv 0 \pmod{q}$. Hence $\phi_n \not\equiv 0 \pmod{q}$ by Condition (vii). But then formula (2.2) implies that $\phi(n/p_i) \equiv 0 \pmod{q^a}$ for some prime divisor p_i of n . Therefore, by the minimal

choice of n , either $r \supseteq n/p_i$ or $n/p_i \supseteq r$. In the first case, $r \supset n$. In the second case $n/p_i \leq r$ so that by (7.3), $n/p_i = r$ and $r \supset n$. In either case $r \supset n$ is contradicted. Hence (vii) implies (iv), which completes the proof of the lemma.

8. Proof of Theorem 1. In view of Lemma 7.1, the proof of Theorem 1, requires only the demonstration that if ϕ is normal, Condition (v) implies Condition (vi); for $pn \cup qn = n$ so that the implication (vi) \Rightarrow (v) is trivial. Note also that (v) is essentially a weakening of (vi), since it amounts to asserting (vi) only in the special case when $n \cup m$ covers both n and m .

Let ϕ be normal, and s a fixed positive integer. Then the normal mapping θ defined by

$$(8.1) \quad \theta(n) = \phi(sn)/\phi(s), \quad n=0, 1, 2, \dots$$

is called a subsequence of ϕ . The following lemma is an easy consequence of this definition.

LEMMA 8.1. *If ϕ is normal, and has the property (v), then so has every subsequence of ϕ .*

LEMMA 8.2. *If ϕ is normal, and has the property (v), then ϕ is g.c.d. factorable; that is*

$$(viii) \quad \phi(n) \cup \phi(m) = 1 \quad \text{if } n \cup m = 1.$$

Note that by (ii), (viii) is a special case of (vi); the proof is by induction on the number of prime factors of n and m . First if n and m are distinct primes p and q , then (viii) follows from (v) on taking $n=1$.

Suppose that $n=p$ and m is the product of $l \geq 2$ primes, $m=q_1, q_2, \dots, q_l$ where the q_i are distinct from p but not necessarily distinct from one another. Assume that (viii) has been proved for $n=p$ and m a product of $l-1$ primes. Now take $p=p$, $q=q_l$ and $n=m/q_l$ in (v). Then

$$\phi(pm/q_l) \cup \phi(m) = \phi(m/q_l).$$

Now

$$q_l \not\supset p \Rightarrow p \supset pm/q_l \Rightarrow \phi(p) \supset \phi(pm/q_l).$$

Consequently,

$$\phi(p) \cup \phi(m) = \phi(p) \cup \phi(pm/q_l) \cup \phi(m) = \phi(p) \cup \phi(m/q_l) = 1$$

by the hypothesis of the induction. Hence (viii) is true if n is a prime number.

Next assume that $n=p_1p_2 \cdots p_k$ is the product of $k \geq 2$ primes p_i distinct from all the primes q_j dividing m so that $n \cup m = 1$, and also assume that (viii) has been proved for n a product of $k-1$ primes. Now apply (v) with $p=p_k$, $q=q_1$ and $n=nm/p_kq_1$. Thus

$$\phi(nm/q) \cup \phi(nm/p) = \phi(nm/pq).$$

Now

$$\begin{aligned} n \supseteq nm/q &\Rightarrow \phi(n) \supseteq \phi(nm/q) \Rightarrow \phi(n) \cup \phi(nm/p) = \phi(n) \cup \phi(nm/q) \cup \phi(nm/p) \\ &= \phi(n) \cup \phi(nm/pq) = \phi(n) \cup \phi(nm/pq_1). \end{aligned}$$

Repeat this argument replacing m successively by

$$m/q_1, m/q_1q_2, \dots, m/q_1q_2 \cdots q_t = 1$$

and leaving n and p unchanged; we find that

$$\begin{aligned} \phi(n) \cup \phi(nm/p) &= \phi(n) \cup \phi(nm/pq_1) \\ &= \phi(n) \cup \phi(nm/pq_1q_2) = \dots = \phi(n) \cup \phi(n/p) = \phi(n/p). \end{aligned}$$

But

$$\begin{aligned} m \supseteq nm/p &\Rightarrow \phi(m) \supseteq \phi(nm/p) \Rightarrow \phi(n) \cup \phi(m) = \phi(n) \cup \phi(nm/p) \cup \phi(m) \\ &= \phi(n/p) \cup \phi(m) = 1 \end{aligned}$$

by the hypothesis of the induction. Hence (viii) is true for every n prime to m , completing the proof of Lemma 8.2.

Theorem 1 may now be proved as follows: Let ϕ be a normal mapping satisfying (v) and let both n and m be positive, since (vi) is trivially satisfied if n or m is zero. Let $s=n \cup m$. Then $n=n's$, $m=m's$ with $n' \cup m'=1$. Consider the subsequence θ of ϕ defined by (8.1). By Lemma 8.1, θ has property (v). Hence Lemma 8.2 implies

$$\begin{aligned} \theta(n') \cup \theta(m') &= 1 \Rightarrow \phi(n)/\phi(s) \cup \phi(m)/\phi(s) = 1 \\ &\Rightarrow \phi(n) \cup \phi(m) = \phi(s) = \phi(n \cup m). \end{aligned}$$

Hence (v) implies (vi), completing the proof of Theorem 1.

9. Proof of second theorem—necessity. Assume that ϕ is normal, and admits a rank function, and let ψ be its generator. We shall show that

$$(ix) \quad \phi_n = \prod_{d \mid n} \psi_d$$

so that ψ is the Dedekind generator of ϕ . The proof is based on a consequence of Dedekind's cross-classification principle [2]; namely

LEMMA 9.1. *If a_1, a_2, \dots, a_k are positive integers, then*

$$a_1 \cap a_2 \cap \cdots \cap a_k = \prod a_1 \amalg (a_1 \cup a_2 \cup a_3) \cdots \div \prod (a_1 \cup a_2) \amalg (a_1 \cup a_2 \cup a_3 \cup a_4) \cdots$$

This result is a generalization of the familiar formula $a_1 \cap a_2 = a_1 a_2 \div a_1 \cup a_2$ and is perhaps easiest proved by showing that the highest powers of p dividing both sides of the formula are the same.

On applying the result to formula (2.2), we obtain

$$\begin{aligned} \psi(n) &= \phi(n) \div \left[\phi\left(\frac{n}{p_1}\right) \cap \phi\left(\frac{n}{p_2}\right) \cap \cdots \cap \phi\left(\frac{n}{p_k}\right) \right] \\ &= \phi(n) \prod \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right) \right) \prod \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right) \cup \phi\left(\frac{n}{p_3}\right) \cup \phi\left(\frac{n}{p_4}\right) \right) \cdots \\ &\quad \div \prod \phi\left(\frac{n}{p_1}\right) \prod \left(\phi\left(\frac{n}{p_1}\right) \cup \phi\left(\frac{n}{p_2}\right) \cup \phi\left(\frac{n}{p_3}\right) \right) \cdots \end{aligned}$$

Now since ϕ admits a rank function, ϕ is completely g.c.d. factorable by Lemma 7.1. Therefore the formula above may be written

$$\begin{aligned} \psi(n) &= \phi(n) \prod \phi\left(\frac{n}{p_1 p_2}\right) \prod \phi\left(\frac{n}{p_1 p_2 p_3 p_4}\right) \cdots \\ &\quad \div \prod \phi\left(\frac{n}{p_1}\right) \prod \phi\left(\frac{n}{p_1 p_2 p_3}\right) \cdots \\ &= \prod_{d \mid n} \phi\left(\frac{n}{d}\right)^{\mu(d)} \end{aligned}$$

where μ is the Möbius function. Hence (ix) follows by the Dedekind inversion formula, completing the proof of the necessity.

10. Proof of second theorem—sufficiency. Now assume that ϕ is normal, and that its Dedekind generator exists and equals its ordinary generator; that is, Condition (ix) is satisfied. We shall show that

$$(vi) \quad \psi(n) \cup \psi(m) = 1. \quad n, m \text{ non-comparable.}$$

Hence it will follow from Lemma 7.2 that (ix) is a sufficient condition for ϕ to admit a rank function.

Assume n, m non-comparable. Then if $l = n \cap m$, $n \lessdot l$ and $m \lessdot l$. Let q_1, q_2, \dots, q_s be the distinct prime factors of l , and let p be any prime p^{a_p}, p^{b_p} the highest powers of p dividing $\phi(n)$ and $\psi(n)$ respectively.

Now by formula (2.2),

$$\phi_l = \psi_l [\phi_{l/q_1} \cap \cdots \cap \phi_{l/q_s}].$$

Hence $a_l = b_l + a_{l/q}$, where $a_{l/q}$ is the largest of $a_{l/q_1}, \dots, a_{l/q_s}$. But by (ix), $a_l = \sum_{d \mid l} b_d$. Hence $b_d = 0$ unless $d = l$ or $d \supseteq l/q$.

Not both b_n and b_m are positive. For since $n \supset l$ and $m \supset l$, in the contrary case $n \supseteq l/q$ and $m \supseteq l/q$ by the remark above. But then $l = n \cap m \supseteq l/q$ so that $q=1$, contrary to q a prime.

It follows that p does not divide both $\psi(n)$ and $\psi(m)$. Since p was an arbitrarily chosen prime, (v) follows, which completes the proof of Theorem 2.

In closing, note that it follows from Theorem 2 and Lemma 7.2 that if ϕ has the Dedekind generator ζ (that is,

$$\zeta(n) = \prod \phi(n/a)^{\mu(a)}$$

is an integer for every n); then a necessary and sufficient condition that ϕ should admit a rank function is that its Dedekind generator satisfy the condition $\zeta(n) \cup \zeta(m) = 1$ if n, m are non-comparable.

REFERENCES

1. R.D. Carmichael, *On the numerical factors of the arithmetic forms*, Ann. Math. (2), **15** (1913–14), 30–70.
2. R. Dedekind, *Werke*, Vol. 1, Brunswick (1930).
3. L.E. Dickson, *History*, Vol. 1, Washington (1919).
4. M. Hall, *Divisibility sequences of the third order*, Amer. J. Math., **58** (1936), 577–84.
5. D.H. Lehmer, Thesis: *On an extended theory of Lucas functions*, Ann. Math. (2), **31** (1930), 419–48.
6. E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–240; 289–321.
7. J.J. Sylvester, *On certain ternary cubic form equations*, Amer. J. Math., **2** (1879), 357–83.
8. Morgan Ward and R.P. Dilworth, *Residuated lattices*, Trans. Amer. Math. Soc., **45** (1939), 335–50.
9. Morgan Ward, *Arithmetical properties of sequences in rings*, Ann. Math. (2), **39** (1938), 210–19.
10. ———, *Arithmetical properties of polynomials associated with the lemniscate elliptic functions*, Proc. Nat. Acad. Sci., **36** (1950), 359–62.
11. ———, *Residuated distributive lattices*, Duke Math. J., **6** (1940), 641–51.
12. ———, *Linear divisibility sequences*, Trans. Amer. Math. Soc., **41** (1937), 276–86.
13. ———, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J., **15** (1948), 941–46.
14. ———, *Note on divisibility sequences*, Bull. Amer. Math. Soc., **42** (1936), 843–45.

CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA

Chapter 22

1959

TESTS FOR PRIMALITY BASED ON SYLVESTERS CYCLOTOMIC NUMBERS

MORGAN WARD

Introduction. Lucas, Carmichael [1] and others have given tests for primality of the Fermat and Mersenne numbers which utilize divisibility properties of the Lucas sequences (U) and (V); in this paper we are concerned only with the first sequence;

$$(U): U_0, U_1, U_2, \dots, U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \dots .$$

Here α and β are the roots of a suitably chosen quadratic polynomial $x^2 - Px + Q$, with P and Q coprime integers. (For an account of these tests, generalizations and references to the early literature, see Lehmer's Thesis [2]).

I develop here a test for primality of a less restrictive nature which utilizes a divisibility property of the Sylvester cyclotomic sequence [3]:

$$(Q) : Q_0 = 0, Q_1 = 1, Q_2, \dots, Q_n = \prod_{\substack{1 \leq r \leq n \\ (r, n)=1}} (\alpha - e^{\frac{2\pi ir}{n}}\beta), \dots$$

Here α and β have the same meaning as before. (U) and (Q) are closely connected [4]; in fact

$$(1.1) \quad U_n = \prod_{d|n} Q_d .$$

The divisibility property is expressed by the following theorem proved in § 3 of this paper.

THEOREM. *If m is an odd number dividing some cyclotomic number Q_n whose index n is prime to m , then every divisor of m greater than one has the same rank of apparition n in the Lucas sequence (U) connected with (Q).*

Here the rank of apparition or rank, of any number d in (U) means as usual the least positive index x such that $U_x \equiv 0 \pmod{d}$.

The following primality test is an immediate corollary.

Primality test. *If m is odd, greater than two, and divides some cyclotomic number Q_n whose index n is both prime to m and greater than the square root of m , then m is a prime number except in two trivial cases: $m = (n-1)^2$, $n-1$ a prime greater than 3, or $m = n^2 - 1$ with $n-1$ and $n+1$ both primes.*

Received January 14, 1959.

The primality tests of Lucas and Carmichael are the special case when $n = m \pm 1$ is a power of two (which allows Q_n to be expressed in terms of V_n) with $X^2 - Px + Q$ suitably specialized.

2. Notations. We denote the rational field by R , and the ring of rational integers by I . The polynomial

$$(2.1) \quad f(x) = x^2 - Px + Q, \quad P, Q, \text{ in } I \text{ and co-prime}$$

is assumed to have distinct roots α and β .

We denote the root field of $f(x)$ by \mathcal{A} and the ring of its integers by \mathcal{I} . Thus \mathcal{A} is either R itself, or a simple quadratic extension of R .

Let p be an odd prime of I , and \mathfrak{p} a prime ideal factor of p in \mathcal{I} . Every element ρ of \mathcal{A} may be put in the form $\rho = \alpha/a$ with α in \mathcal{I} and a in I . The totality of such ρ with $(a, p) = 1$ forms a subring \mathcal{I}_p of \mathcal{A} . Evidently $\mathcal{A} \supset \mathcal{I}_p \supset \mathcal{I} \supseteq I$. If we extend \mathfrak{p} into \mathcal{I}_p in the obvious way, we obtain a prime ideal \mathfrak{P} . The homomorphic image of \mathcal{I}_p modulo \mathfrak{P} is a field, \mathcal{F}_p . We denote the mapping of \mathcal{I}_p onto \mathcal{F}_p by (\mathfrak{P}) .

Let $F_n(z)$ denote the cyclotomic polynomial of degree $\phi(n)$. $F_n(z)$ has coefficients in I , and if n is greater than one, then (Lehmer [2], Carmichael [1])

$$(2.2) \quad Q_n = \beta^{\phi(n)} F_n\left(\frac{\alpha}{\beta}\right),$$

Furthermore

$$(2.3) \quad z^n - 1 = \prod_{d|n} F_d(z).$$

3. Proof of theorem. Let m be an odd number greater than one which divides some term of (Q) whose index n is prime to m , so that

$$(3.1) \quad Q_n \equiv 0 \pmod{m}, \quad (n, m) = 1.$$

Throughout the next three lemmas, p stands for a fixed prime factor of m .

LEMMA 1. *If \mathfrak{p} is any ideal factor of p in \mathcal{I} , then*

$$(3.2) \quad (Q, p) = (\alpha, \mathfrak{p}) = (\beta, \mathfrak{p}) = (1).$$

Proof. It suffices to prove that $(Q, p) = (1)$. Assume the contrary. Then $(p, P) = 1$. Since $U_1 = 1$ and $U_{x+2} = PU_{x+1} - QU_x \equiv PU_{x+1} \pmod{p}$, it follows by induction that $U_n \not\equiv 0 \pmod{p}$. Then by (1.1), $Q_n \not\equiv 0$

(mod p). But p divides m so that by (3.1) $Q_n \equiv 0$ (mod p) a contradiction.

LEMMA 2. *The rank of apparition of p in (U) is n .*

Proof. Since $U_n \equiv 0$ (mod p), p has a positive rank of apparition in (U) , r say. Then r divides n . But by (1.1), $U_r = \prod_{d|n} Q_d$. Hence $Q_d \equiv 0$ (mod p) for some d dividing both r and n . Clearly, if $d = n$, then $r = n$ and we are finished. Assume that d is less than n .

The number $\alpha/\beta = \alpha^2/Q$ is in \mathcal{I}_p by Lemma 1. Let τ be its image in \mathcal{F}_p under the mapping (Ψ) . Then by (2.2) and Lemma 1 $F_n(\tau) = F_d(\tau) = 0$ in \mathcal{F}_p . Consequently the resultant of the polynomials $F_n(z)$ and $F_d(z)$ is zero in \mathcal{F}_p . Therefore its inverse image under the mapping is in Ψ . But this resultant is evidently in I . Therefore it must be divisible by p . But by formula (2.3), since $d < n$ the resultant of $F_n(z)$ and $F_d(z)$ must divide the discriminant $\pm n^{n-1}$ of $z^n - 1$. Thus $n \equiv 0$ (mod p) so that $(n, m) \equiv 0$ mod p which contradicts (3.1) and completes the proof.

LEMMA 3. *The rank of apparition in (U) of any positive power of p which divides m is n .*

Proof. Let p^k divide m , $k \geq 1$ and let the rank of p^k in (U) be r . Now $U_n = \prod_{d|n} Q_d \equiv 0$ (mod p^k). But by Lemma 2, each Q_d with $d < n$ is prime to p . Hence r must equal n .

The theorem proper now follows easily. For let m' be any divisor of m other than one. By Lemma 3, every prime power dividing m' has rank of apparition n in (U) . But the rank of apparition of m' in (U) is the least common multiple of the ranks of the prime powers of maximal order dividing m' . (Carmichael [1]). Hence m' also has rank of apparition n in (U) .

4. Proof of primality test. Assume that (3.1) holds for some n greater than \sqrt{m} . If m is not a prime, it has a prime factor $\leq \sqrt{m}$. Let p be the smallest such factor, and let

$$(4.1) \quad m = pq, \quad q \geq 3.$$

Then p has rank n in (U) by Lemma 3. But by a classical result of Lucas, $U_{p \pm 1} \equiv 0$ (mod p). Hence n divides $p \pm 1$. If n is less than $p + 1$, $\sqrt{m} < p \leq \sqrt{m}$, a contradiction. Hence $n = p + 1$. If $p = \sqrt{m}$, then $m = (n - 1)^2$ and $n - 1$ is a prime. Since m is odd, $n \geq 4$. This is the first trivial case.

If $p < \sqrt{m}$, then $q \geq p + 2$ and $m \geq p(p + 2)$. But if $m > p(p + 2)$,

then $n^2 > m \geq (p+1)^2 = n^2$, a contradiction. Hence $m = p(p+2)$ where $p+2$ has no prime factor smaller than p . Hence $p+2$ is a prime and $m = n^2 - 1$ with both $n-1$ and $n+1$ primes. This is the second trivial case. In every other case then, m must be a prime.

5. Conclusion. The two trivial cases can actually occur. For if $P = 22$ and $Q = 3$, then $Q_6 = \alpha^2 - \alpha\beta + \beta^2 = P^2 - 3Q = 475$. Hence $Q_6 \equiv 0 \pmod{25}$ and $25 = (6-1)^2$. Again, if $P = 17$ and $Q = 3$, then $Q_6 = 280$. Hence $Q_6 \equiv 0 \pmod{35}$ and $35 = 6^2 - 1 = 5 \times 7$. It is worth noting that these trivial cases cannot occur if α and β are rational integers. (See [1], Theorem XII and remark.)

To illustrate the theorem, note that if $P = 2$ and $Q = 1$, $Q_9 = 73$. Since $\sqrt[3]{73} < 9$ and $(9, 73) = 1$, 73 is a prime. But for $P = 3$ and $Q = 1$, $Q_9 = 91$. But $9 < \sqrt[3]{91}$ so the test is inapplicable. As a matter of fact, 91 is the product of two primes. Evidently the test may be extended to cover such a case. That is, if $Q_n \equiv 0 \pmod{m}$, $(n, m) = 1$ and $n > \sqrt[3]{m}$, m will usually be either a prime, or the product of two primes.

REFERENCES

1. R. D. Carmichael, *On the numerical factors of arithmetic forms*, Ann. of Math., **15** (1913-14), 30-70.
2. D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. **31** (1930), 419-448.
3. J. J. Sylvester, *On certain ternary cubic form equations*, Amer. J. Math. **2** (1879), 357-83.
4. Morgan Ward, *The mappings of the positive integers into themselves which preserve division*, Pacific J. Math. **5** (1955), 1013-1023.

CALIFORNIA INSTITUTE OF TECHNOLOGY

Chapter 23

1960

THE CALCULATION OF THE COMPLETE ELLIPTIC INTEGRAL OF THE THIRD KIND

MORGAN WARD, California Institute of Technology

1. Introduction. The difficulty of computing an elliptic integral of the third kind is well known; even a computation of the complete integral

$$(1.1) \quad \int_0^{4\pi} \frac{d\phi}{(1 + \nu \sin^2 \phi) \sqrt{(1 - k^2 \sin \phi)}}$$

for numerical values of its parameters ν and k is a time-consuming operation. Apparently it is only very recently that any systematic tabulation has been made. I develop here a very efficient way to compute this integral when the parameters ν and k are real. The procedure is well adapted to a digital computer, and is so easily programmed that no tables should be necessary in the future.

When ν is zero, the procedure reduces to Gauss' method for computing the complete elliptic integral of the first kind by the use of Landen's transformation. However no knowledge of elliptic functions or integrals is required for the developments which follow. Any reader who has had a first course in function theory can easily understand the proofs.

2. The computation procedure. The process of computation is iterative, but takes slightly different forms according as the parameter ν is positive or negative. We let $\nu = \epsilon \mu^2$, $\epsilon = \pm 1$.

If $\epsilon = +1$, we speak of the positive case; if $\epsilon = -1$, of the negative case. In either case, we denote the integral (1.1) by $L(\mu, k)$. If $\mu = 0$, the integral reduces to the complete integral of the first kind. We denote it then by $L(k)$:

$$(2.1) \quad L(k) = \int_0^{4\pi} \frac{d\phi}{\sqrt{(1 - k^2 \sin^2 \phi)}}.$$

The parameters μ and k are assumed to be real, and

$$(2.2) \quad 0 \leq k < 1, \quad 0 \leq \mu \quad \text{if } \epsilon = 1; \quad 0 \leq \mu < 1 \quad \text{if } \epsilon = -1.$$

Write for brevity

$$(2.3) \quad k' = \sqrt{(1 - k^2)}, \quad \mu' = \sqrt{(1 + \epsilon \mu^2)},$$

and let $k^* = (1 - k')/(1 + k')$ and $\mu^* = \mu k / \{(1 + \mu')(1 + k')\}$. We shall prove in Section 4 of this paper that

$$(2.4) \quad L(\mu, k) = \frac{2}{1 + k'} \mu'^{-1} (2L(\mu^*, k^*) - L(k^*)).$$

Now $k^* = k^2/(1 + k')^2 < k^2$ so that if we iterate (2.4), the successive values of μ and k obtained tend rapidly to zero. Since $L(0, 0) = L(0) = \frac{1}{2}\pi$, the following procedure suggests itself for obtaining an approximation $A(\mu, k)$ to $L(\mu, k)$.

First step. Compute k_1, \dots, k_r and μ_1, \dots, μ_r by the formulas

$$(2.5) \quad \mu_1 = \mu, \quad k_1 = k; \quad k_{n+1} = \frac{1 - k_n'}{1 + k_n'}, \quad \mu_{n+1} = \frac{\mu_n k_n}{(1 + \mu_n')(1 + k_n')}.$$

The algorithm is continued until k_{r+1} and μ_{r+1} are sufficiently small. More specifically for $n = 1, 2, \dots, r$, let

$$(2.6) \quad K_n = \prod_{s=1}^n 2/(1 + k_s'), \quad M_n = \prod_{s=1}^n \mu_s'^{-1},$$

and let

$$(2.7) \quad E_n = \begin{cases} 2^n K_n M_n k_{n+1}^2 & \text{in the positive case;} \\ 2^n K_n M_n (\mu_{n+1} + \frac{1}{2} k_{n+1}^2) & \text{in the negative case.} \end{cases}$$

We require that E_r be negligible.

Second step. Compute the approximations $A(\mu_{r+1}, k_{r+1})$, $A(\mu_r, k_r)$, $A(\mu_{r-1}, k_{r-1})$, $\dots, A(\mu_1, k_1) = A(\mu, k)$ and $A(k_{r+1}), A(k_r), A(k_{r-1}), \dots, A(k_1)$ by the formulas

$$(2.8) \quad \begin{aligned} A(\mu_{r+1}, k_{r+1}) &= A(k_{r+1}) = \frac{1}{2}\pi, \\ A(\mu_n, k_n) &= \frac{2}{1 + k_n'} \frac{1}{\mu_n'} (2A(\mu_{n+1}, k_{n+1}) - A(k_{n+1})), \\ A(k_n) &= \frac{2}{1 + k_n'} A(k_{n+1}), \quad n = r, r-1, \dots, 1. \end{aligned}$$

Third step. Take $A(\mu, k)$ as an approximation to $L(\mu, k)$; the error in doing so is negligible, for

$$(2.9) \quad 0 < L(\mu, k) - A(\mu, k) < E_r.$$

It will be observed that the first two steps of the computation are iterative processes very well adapted to a digital computer or even to an ordinary desk calculator.

3. The rapidity of convergence. The convergence of the process is extremely rapid. It is evident from (2.2) and (2.5) that if μ and k are positive, then $0 < k_{n+1} < k_n^2$ and $0 < \mu_{n+1} < \frac{1}{2}(\mu_n^2 + k_n^2)$. We shall show later that if $0 < k_t, \mu_t < \frac{2}{3}$ and $n \geq 1$, then

$$(3.1) \quad 0 < k_{n+t} < (\frac{1}{3}k_t)^{2^n}, \quad 0 < \mu_{n+t} < \mu_t(\frac{1}{3}k_t)^{2^{n-1}}.$$

We shall also show that if $0 < k_n, \mu_n < .1$, then

$$(3.2) \quad 2/(1 + k_n') = 1 + \theta_n(\frac{1}{4}k_n^2), \quad 1/\mu_n' = 1 - \epsilon\phi_n(\frac{1}{2}\mu_n^2),$$

with $1 < \theta_n < 1.006$, $1 < \phi_n < 1.008$.

It follows from (3.2) that the infinite products $K = \prod_1^\infty \{2/(1+k_n')\}$, $M = \prod_1^\infty (1/\mu_n')$, converge and, from (3.1), that the partial products M_r and K_r in the error term E_r change very little as r increases when μ_r and k_r are small. It is also evident from the inequalities (3.1) that E_r may be made arbitrarily small by choosing r large enough; that is, the procedure converges in the usual sense. The following numerical data for the negative case illustrate the rapidity of convergence.

The data is taken from a systematic computation of E_r to twenty places for μ and k ranging independently over the values .1, .2, . . . , .8, .9. The computation was programmed for the California Institute Datatron by Mr. George W. Logemann, and the complete results will be given elsewhere. Evidently the most unfavorable case is when $\mu = k = .9$. Mr. Logemann found that $E_3 = .000174$, . . . , $E_4 = .00000 00000 5197$, . . . , $E_6 < 10^{-18}$. We conclude then that four or five iterations will suffice for most ordinary purposes.

4. Derivation of the iterative formula. We here derive formula (2.4) on which the computation procedure rests.

The functions $(1 + \epsilon\mu^2 \sin^2 \phi)^{-1}$ and $(1 - k^2 \sin^2 \phi)^{-1/2}$ may evidently be expanded in Fourier series which converge uniformly to them in the closed interval $[-\pi, \pi]$. Let these expansions be

$$(4.1) \quad \frac{1}{1 + \epsilon\mu^2 \sin^2 \phi} = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos n\phi,$$

$$(4.2) \quad \frac{1}{\sqrt{1 - k^2 \sin^2 \phi}} = \frac{1}{2}b_0 + \sum_{n=1}^{\infty} b_n \cos n\phi.$$

Then

$$(4.3) \quad b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} \frac{\cos n\phi d\phi}{\sqrt{1 - k^2 \sin^2 \phi}}.$$

It will be shown at the close of this section that $a_{2n+1} = 0$ and that

$$(4.4) \quad a_{2n} = 2\mu'^{-1}\epsilon^n \cdot \{\mu/(1 + \mu')\}^{2n}.$$

Thus by (4.1)

$$\begin{aligned} & \frac{1}{(1 + \epsilon\mu^2 \sin^2 \phi)\sqrt{1 - k^2 \sin^2 \phi}} \\ &= \mu'^{-1} \left(\frac{1}{\sqrt{1 - k^2 \sin^2 \phi}} + 2 \sum_1^{\infty} \epsilon^n \left(\frac{\mu}{1 + \mu'} \right)^{2n} \frac{\cos 2n\phi}{\sqrt{1 - k^2 \sin^2 \phi}} \right). \end{aligned}$$

The series on the right is uniformly convergent with respect to ϕ . Hence integrating term-wise over $[-\pi, \pi]$ we obtain from (2.1) and (4.3) the formula

$$(4.5) \quad L(\mu, k) = \frac{1}{4}\pi\mu'^{-1} \left(b_0 + 2 \sum_1^{\infty} \epsilon^n \{ \mu/(1+\mu') \}^{2n} b_{2n} \right).$$

We next obtain another expression for the coefficients b_{2n} in this series. Let $w=\phi+i\zeta$ be a complex variable. Then there exists a positive number δ depending on k alone such that $\Delta(w)=(1-k^2 \sin^2 w)^{-1/2}$ is regular in the strip $|\operatorname{Im} w|<\delta$. Since $\Delta(w)$ is also periodic with period 2π in the whole plane, it is representable everywhere in the strip by the Fourier series

$$(4.6) \quad \Delta(w) = \frac{1}{2}b_0 + \sum_1^{\infty} b_n \cos nw,$$

with the b_n given by formula (4.3). From now on, we confine ourselves to the rectangle $|\operatorname{Re} w| \leq \pi$, $|\operatorname{Im} w| < \delta$.

Let T stand for the mapping of the w -plane induced by letting $z=e^{iw}$. Then T transforms the rectangle above into a circular ring R in the z plane: $R = \{z \mid 0 < r < |z| < R\}$, where $e^{-\delta} = r < 1 < R = e^{\delta}$. Furthermore if

$$(4.7) \quad F(z) = T\Delta(w),$$

then $F(z)$ is regular in R . But $T \cos nw = \frac{1}{2}(z^n + z^{-n})$. Hence if we let $b_{-n} = b_n$, we have by (4.6) and (4.7) the Laurent expansion of $F(z)$ in R : $F(z) = \sum_{n=-\infty}^{\infty} \frac{1}{2}b_n z^n$.

Consequently by Laurent's theorem,

$$(4.8) \quad b_n = \frac{1}{\pi i} \int_{\Gamma} z^{n-1} F(z) dz, \quad n = 0, 1, \dots.$$

Here Γ is the unit circle described once counterclockwise. Now let

$$(4.9) \quad k = \sin \frac{1}{2}\beta, \quad 0 \leq \beta < \pi.$$

Then we find from (4.7) after a little algebra that

$$(4.10) \quad F(z) = \frac{2 \csc \frac{1}{2}\beta z}{\sqrt{(z^2 + \tan^2 \frac{1}{4}\beta)(z^2 + \cot^2 \frac{1}{4}\beta)}}.$$

Hence the only singularities of $F(z)$ within Γ are branchpoints of order two at $z = \pm i \tan \frac{1}{4}\beta$. Join these points by a cut along the axis of imaginaries. Then the contour Γ in (4.8) may be shrunk down to a path consisting of two small circles about the branch points and the two sides of the cut. If the radius of each of these circles is ρ , their contribution to the line integral is of order $\sqrt{\rho}$. If therefore we set $z = i \tan \frac{1}{4}\beta \sin \phi$ along the cut and pass to the limit by letting ρ tend to zero, we find that

$$b_n = \frac{4}{\pi} i^n \csc \frac{1}{2}\beta \int_{-\frac{1}{2}\pi}^{\frac{1}{2}\pi} \frac{\sin^n \phi \tan^{n+1} \frac{1}{4}\beta d\phi}{\sqrt{(1 - \tan^4 \frac{1}{4}\beta \sin^2 \phi)}}.$$

Hence b_n is zero when n is odd, and when n is even,

$$(4.11) \quad b_{2n} = \frac{8}{\pi} \frac{(-k^*)^n}{1+k'} \int_0^{\frac{1}{2}\pi} \frac{\sin^{2n} \phi \, d\phi}{\sqrt{(1-k^{*2} \sin^2 \phi)}}.$$

Here we have written k^* for $\tan^2 \frac{1}{4}\beta$ and replaced the multiplier $\csc \frac{1}{2}\beta \tan \frac{1}{4}\beta$ by $(1+\cos \frac{1}{2}\beta)^{-1}$ which equals $(1+k')^{-1}$ by (4.9) and (2.3). We easily find from the same formulas that

$$(4.12) \quad k^* = (1-k')/(1+k').$$

(4.11) is the new expression for b_{2n} which we were seeking. Introduce it into the series (4.5) for $L(\mu, k)$, and let

$$(4.13) \quad \mu^* = \frac{\mu}{1+\mu'} \sqrt{k^*} = \frac{\mu}{1+\mu'} \frac{k}{1+k'}.$$

Then (4.5) becomes

$$(4.14) \quad L(\mu, k) = \frac{2\mu'^{-1}}{1+k'} \left(\int_0^{\frac{1}{2}\pi} \frac{d\phi}{\sqrt{(1-k^{*2} \sin^2 \phi)}} + 2 \sum_1^\infty (-\epsilon)^n \mu^{*2n} \int_0^{\frac{1}{2}\pi} \frac{\sin^{2n} \phi}{\sqrt{(1-k^{*2} \sin^2 \phi)}} \right).$$

Now the series $(1-k^* \sin^2 \phi)^{-1/2} + 2 \sum_1^\infty (-\epsilon \mu^{*2})^n \sin^{2n} \phi (1-k^* \sin^2 \phi)^{-1/2}$ is uniformly convergent in ϕ , and is essentially a geometric progression whose sum may be written

$$\frac{2}{(1+\epsilon \mu^{*2} \sin^2 \phi) \sqrt{(1-k^{*2} \sin^2 \phi)}} - \frac{1}{\sqrt{(1-k^{*2} \sin^2 \phi)}}.$$

Hence on integrating term-wise from 0 to $\frac{1}{2}\pi$ and comparing it with (4.14) and the integral of its sum with (1.1) and (2.1), we obtain the iteration formula (2.4), with the values of k^* and μ^* given in Section 2.

It remains to verify the values given for the Fourier coefficients a_n in the series (3.1) for $(1+\epsilon \mu^2 \sin^2 \phi)^{-1}$. Let $\mu = \tan \frac{1}{2}\alpha$, $0 \leq \alpha < \pi$, in the positive case; $\mu = \sin \frac{1}{2}\alpha$, $0 \leq \alpha < \pi$, in the negative case. Then we find that

$$T(1+\epsilon \mu^2 \sin^2 \phi)^{-1} = \begin{cases} 4 \cot^2 \frac{1}{2}\alpha z^2 [(z^2 - \tan^2 \frac{1}{4}\alpha)(z^2 - \cot^2 \frac{1}{4}\alpha)]^{-1} & \text{if } \epsilon = +1, \\ 4 \csc^2 \frac{1}{2}\alpha z^2 [(z^2 + \tan^2 \frac{1}{4}\alpha)(z^2 + \cot^2 \frac{1}{4}\alpha)]^{-1} & \text{if } \epsilon = -1. \end{cases}$$

This result may be written

$$T(1+\epsilon \mu^2 \sin^2 \phi)^{-1} = \frac{4\mu^{-2} z^2}{(z^2 - \epsilon \tan^2 \frac{1}{4}\alpha)(z^2 - \epsilon \cot^2 \frac{1}{4}\alpha)}.$$

Hence by analogy with (4.8)

$$a_n = \frac{4\mu^{-2}}{\pi i} \int_{\Gamma} \frac{z^{n+1} dz}{(z^2 - \epsilon \tan^2 \frac{1}{4}\alpha)(z^2 - \epsilon \cot^2 \frac{1}{4}\alpha)}.$$

Thus by the residue theorem a_n equals $8\mu^{-2}$ times the sum of the residues of the integrand at its two poles $\pm \sqrt{\epsilon} \tan \frac{1}{4}\alpha$ within Γ . On evaluating these residues, we find that $a_{2n+1}=0$ and that a_{2n} has the value stated in (4.4), so that the proof is complete.

5. Proofs of the basic inequalities. The inequalities (3.1) are proved as follows. We have $k_{t+1} = (1 - k_t')/(1 + k_t') = k_t^2/(1 + k_t')^2$. Hence $k_{t+1} < \frac{1}{3}k_t^2$ if and only if $1 + k_t' > \sqrt{3}$. This works out to $k_t^2 < \sqrt{(3 + 2\sqrt{3})} = .681$. Hence: *If $k_t < \frac{2}{3}$, then $k_{t+1} < \frac{1}{3}k_t^2$.* This statement is the case $n=1$ of the inequality (3.1) for k_{t+n} . The general inequality follows by an easy induction. The inequality for μ_{t+n} is proved similarly.

To prove that (3.2) is valid, assume that $0 < k_n < .1$. Then

$$\frac{2}{1 + k_n'} = \frac{2(1 - k_n')}{1 - k_n'^2} = \frac{2}{k_n^2} \sqrt{(1 - k_n^2)}.$$

Now on expanding the function $1 - \sqrt{(1 - x)}$, $0 < x < 1$ by Taylor's theorem with remainder and then substituting k_n^2 for x , we obtain the formulas

$$\frac{2}{1 + k_n'} = \theta_n(\frac{1}{4}k_n), \quad \theta_n = 1 + \frac{1}{2}k_n^2 + \frac{5}{16} \frac{k_n^4}{(1 - \theta k_n^2)^{7/2}}, \quad 0 < \theta < 1.$$

Hence

$$1 < \theta_n < 1 + \frac{1}{2}(.01) + \frac{5}{16} \frac{.0001}{(.99)^{7/2}} < 1.006.$$

The formula for μ_n' in (3.2) is proved in a similar fashion.

We preface the proof of the inequality (2.9) by two lemmas.

LEMMA 5.1. *If $0 < \mu, k < .1$, then*

$$(5.1) \quad 0 < L(\mu, k) - \frac{1}{2}\pi < \frac{4}{5}k^2 \quad \text{if } \epsilon \text{ is positive,}$$

$$(5.2) \quad 0 < L(\mu, k) - \frac{1}{2}\pi < \frac{4}{5}(\mu^2 + \frac{1}{2}k^2) \quad \text{if } \epsilon \text{ is negative.}$$

Proof. By Taylor's theorem with remainder, where $0 < \theta < 1$,

$$\begin{aligned} (1 - k^2 \sin^2 \phi)^{-1/2} &= 1 + \frac{1}{2}k^2 \sin^2 \phi + \frac{3}{8} k^4 \frac{\sin^4 \phi}{(1 - \theta k^2 \sin^2 \phi)^{5/2}} \\ &> 1 + \frac{1}{2}k^2 \left(1 + \frac{3}{4} \frac{k^2}{(1 - k^2)^{5/2}}\right) \sin^2 \phi. \end{aligned}$$

Since $k < .1$,

$$1 + \frac{3}{4} \frac{k^2}{(1 - k^2)^{5/2}} < 1 + \frac{3}{4} \frac{.01}{(.99)^{5/2}} = 1.0077.$$

Hence

$$(5.3) \quad \frac{1}{(1 - k^2 \sin^2 \phi)^{1/2}} < 1 + \alpha(\tfrac{1}{2}k^2) \sin^2 \phi, \quad \alpha = 1.0077.$$

Similarly

$$\frac{1}{1 - \mu^2 \sin^2 \phi} < 1 + \beta\mu^2 \sin^2 \phi, \quad \beta = 1.01031.$$

Therefore

$$\begin{aligned} 0 &< \frac{1}{(1 - \mu^2 \sin^2 \phi)\sqrt{(1 - k^2 \sin^2 \phi)}} - 1 \\ &< \tfrac{1}{2}\alpha k^2 \sin^2 \phi + \beta\mu^2 \sin^2 \phi + \alpha\beta(\tfrac{1}{2}\mu^2 k^2) \sin^4 \phi. \end{aligned}$$

On integrating these inequalities from 0 to $\frac{1}{2}\pi$ we obtain when ϵ is negative the inequality

$$0 < L(\mu, k) - \tfrac{1}{2}\pi < \tfrac{1}{8}\pi\alpha(1 + \tfrac{3}{8}\beta\mu^2)(\tfrac{1}{2}k^2) + \tfrac{1}{4}\pi(1 + \tfrac{3}{16}k^2\alpha)\mu^2.$$

The coefficients of $\frac{1}{2}k^2$ and μ^2 turn out to be .79446 and .794996 which are both less than $\frac{4}{5}$. This completes the proof of the inequality (5.2).

If ϵ is positive, it follows from (5.3) that

$$L(\mu, k) - \tfrac{1}{2}\pi < L(k) - \tfrac{1}{2}\pi - (\tfrac{1}{2}\alpha k^2)(\tfrac{1}{4}\pi).$$

Since $\tfrac{1}{4}\alpha\pi < \tfrac{4}{5}$, (5.1) follows, completing the proof of the lemma.

LEMMA 5.2. If

$$\begin{aligned} A(\mu_n, k_n) &= \frac{2\mu_n'^{-1}}{1 + k_n'} (2a(\mu_{n+1}, k_{n+1}) - A(k_{n+1})), \\ A(k_n) &= \frac{2}{1 + k_n'} A(k_{n+1}), \end{aligned}$$

for $n = 1, 2, \dots$, then

$$(5.2) \quad \begin{aligned} L(\mu, k) - A(\mu, k) &= 2^n M_n K_n (L(\mu_{n+1}, k_{n+1}) - A(\mu_{n+1}, k_{n+1})) \\ &\quad - \sum_{s=1}^n 2^{s-1} M_s K_s (L(k_{s+1}) - A(k_{s+1})), \end{aligned}$$

where K_n and M_n are given for all n by (2.6).

Proof. We know by the iteration formula that for all n ,

$$L(\mu_n, k_n) = \frac{2}{1 + k_n'} \mu_n'^{-1} (2L(\mu_{n+1}, k_{n+1}) - L(k_{n+1}),$$

$$L(k_n) = \frac{2}{1+k'_n} L(k_{n+1}).$$

Hence since $\mu = \mu_1$ and $k = k_1$,

$$\begin{aligned} L(\mu, k) - A(\mu, k) &= \frac{2}{1-k'_n} \mu_1'^{-1}(2L(\mu_2, k_2) - L(k_2)) - \frac{2}{1+k'_1} \mu_1'^{-1}(2A(\mu_2, k_2) - A(k_2)) \\ &= 2K_1 M_1(L(\mu_2, k_2) - A(\mu_2, k_2)) - K_1 M_1(L(k_2) - A(k_2)). \end{aligned}$$

Hence (5.2) is true when $n=1$. But it is easy to show that if it is true for n , it is true for $n+1$. Hence it is true for all n by mathematical induction. Now

$$\begin{aligned} L(k_{n+1}) &= \frac{2}{1+k'_{n+1}} \frac{2}{1+k'_{n+2}} \cdots \frac{2}{1+k'_n} L(k_{n+1}), \\ A(k_{n+1}) &= \frac{2}{1+k'_{n+1}} \frac{2}{1+k'_{n+2}} \cdots \frac{2}{1+k'_n} A(k_{n+1}). \end{aligned}$$

Hence (5.2) may be written

$$(5.3) \quad \begin{aligned} L(\mu, k) - A(\mu, k) &= 2^n K_n M_n (L(k_{n+1}) - A(k_{n+1})) \\ &\quad - K_n \left(\sum_{s=1}^n 2^{s-1} M_s \right) (L(k_{n+1}) - A(k_{n+1})). \end{aligned}$$

Now suppose that $A(k_{n+1}, \mu_{n+1}) = A(k_{n+1}) = \frac{1}{2}\pi$. Then if ϵ is positive, $L(\mu_{n+1}, k_{n+1}) < L(k_{n+1})$. Hence when ϵ is positive, we obtain from (5.3) the inequalities.

$$\begin{aligned} L(\mu, k) - A(\mu, k) &< 2^n K_n M_n (L(k_{n+1}) - \frac{1}{2}\pi) \\ &> K_n \left(2^n M_n - \sum_{s=1}^n 2^{s-1} M_s \right) (L(k_{n+1}, \mu_{n+1}) - \frac{1}{2}\pi). \end{aligned}$$

Now $M_1 < M_2 < \cdots < M_n$. Hence $\sum_{s=1}^n 2^{s-1} M_s < 2^n M_n$. Hence $L(\mu, k) - A(\mu, k)$ is positive from the second inequality. And by the first inequality and Lemma 5.1, it is less than $2^n K_n (\frac{2}{3} k_{n+1}^2)$.

If ϵ is negative, $L(\mu_{n+1}, k_{n+1}) > L(k_{n+1})$. Hence we obtain from (5.3) the inequalities

$$\begin{aligned} L(\mu, k) - A(\mu, k) &> K_n \left(2^n M_n - \sum_{s=1}^n 2^{s-1} M_s \right) (L(k_{n+1}) - \frac{1}{2}\pi) > 0, \\ L(\mu, k) - A(\mu, k) &< 2^n K_n M_n (L(\mu_{n+1}, k_{n+1}) - \frac{1}{2}\pi) \\ &< 2^n K_n M_n \frac{4}{3} (\mu_{n+1}^2 + \frac{1}{2} k_{n+1}^2), \end{aligned}$$

by Lemma 5.1, and this completes the proof of the inequality (2.9).

In conclusion, it is worth noting that the method may evidently be extended

to compute a complete integral of the third kind of the form

$$\int_0^{\frac{1}{2}\pi} \frac{d\phi}{(1 + \nu \sin^2 \phi) \sqrt{(1 + k^2 \sin^2 \phi)}}$$

for ν and k real and ν greater than -1 .

ANALYTICAL EXPRESSIONS AND ELEMENTARY FUNCTIONS

MARLOW SHOLANDER, Carnegie Institute of Technology

The title is very nearly meaningless. When Professor Ritt discusses integration in finite terms an elementary function is one (a not too elementary) thing. In common classroom usage it is another—roughly, any differentiable function frequently used by Euler. When an author presents us with an analytic expression for a function, the expression usually has little or nothing to do with analytic functions in any strict sense. The adjective has become a synonym for “nonverbal”. As examples we give*

$$\operatorname{sgm} \sin^2 \frac{(n-1)!+1}{n} \pi \quad \text{and} \quad \operatorname{sgm} \sin^2 \frac{(n-1)!^2}{n} \pi,$$

characteristic functions for the sets of nonprime and prime integers. The spirit of the formula constructing game is clear. Its rules are not.

Consider $[x]$,† the characteristic of x regarded as a logarithm, the greatest integer not greater than x . We find

$$[x] = x - \frac{1}{2} + (1/\pi) \tan^{-1} \cot \pi x \quad x \neq 0, \pm 1, \pm 2, \dots$$

How do we fill in the gaps at integral x ? Using limits is too much like hunting quail with an elephant gun. It's difficult to find functions which are not expressible as limits of limits.

The admission of one simple additional function somehow seems more sporting. Logical candidates are null $x = \lim_{n \rightarrow \infty} (1 + |x|)^{-n}$, the characteristic function of the set (0) , or $\operatorname{sgm} x = \lim_{n \rightarrow \infty} x^{1/(2n+1)} = x / (|x| + \text{null } x)$. Thus, for $T(x) = (2/\pi) \sin^{-1} \sin \frac{1}{2}\pi x \operatorname{sgm} \cos \frac{1}{2}\pi x$, we have $[x] = x - \max(T(x), T(x+1))$. Even this procedure may be circumvented if we adopt the convention that an expression meaningless for $x=a$, but suitably defined in a neighborhood, defines $f(a) = \frac{1}{2}\{f(a-) + f(a+)\}$. Then $\operatorname{sgm} x = x / |x|$ and $T(x) = (2/\pi) \tan^{-1} \tan \frac{1}{2}\pi x$.

It is interesting to see how far one may go with modest assumptions. If we agree $\cos x$, $\cos^{-1} x$, x , and real constants are “common” functions of x and

* Cf. Louis Brand, Advanced Calculus, New York, 1955, p. 84.

† Cf. Arthur Porges, An analytical expression for $[X]$, this MONTHLY, vol. 66, 1959, pp. 706-707.

Chapter 24

1961

THE PRIME DIVISORS OF FIBONACCI NUMBERS

MORGAN WARD

1. Introduction. Let

$$(U) : U_0, U_1, U_2, \dots, U_n, \dots$$

be a linear integral recurrence of order two; that is,

$$U_{n+2} = PU_{n+1} - QU_n (n = 0, 1, \dots).$$

P, Q integers, $Q \neq 0$; U_0, U_1 , integers. It is an important arithmetical problem to decide whether or not a given number m is a divisor of (U) ; that is, to find out whether the diophantine equation

$$(1.1) \quad U_x = my, \quad m \geq 2$$

has a solution in integers x and y . Our information about this problem is scanty except in the cases when it is trivial; that is when the characteristic polynomial of the recursion has repeated roots, or when some term of (U) is known to vanish.

If we exclude these trivial cases, there is no loss in generality in assuming that m in (1.1) is a prime power. It may further be shown by p -adic methods [7] that we may assume that m is a prime. Thus the problem reduces to characterizing the set \mathfrak{P} of all the prime divisors of (U) . \mathfrak{P} is known to be infinite [6], and there is also a criterion to decide a priori whether or not a given prime is a member of \mathfrak{P} , [2], [6], [7]. But this criterion is local in character and tells little about \mathfrak{P} itself.

I propose in this paper to study in detail a special case of the problem in the hope of throwing light on what happens in general. I shall discuss the prime divisors of the Fibonacci numbers of the second kind:

$$(G) : 2, 1, 3, 4, 7, \dots, G_n, \dots$$

These and the Fibonacci numbers of the first kind

$$(F) : 0, 1, 1, 2, 3, 5, \dots, F_n, \dots$$

are probably the most familiar of all second order integral recurrences; (F) and (G) have been tabulated out to one hundred and twenty terms by C. A. Laisant [3].

2. Preliminary classification of primes. Let R denote the rational field and $\mathcal{R} = R(\sqrt{5})$ the root field of the characteristic polynomial

Received April 14, 1960.

$$(2.1) \quad f(x) = x^2 - x - 1$$

of (F) and (G) . Then if α and β are the roots of $f(x)$ in \mathcal{R} ,

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad G_n = \alpha^n + \beta^n, \quad (n = 0, 1, 2, \dots).$$

If p is any rational prime, by its rank of apparition in (F) or rank, we mean the smallest positive index x such that p divides F_x . We denote the rank of p by ρ_p or ρ . Its most important properties are: $F_n \equiv 0 \pmod{p}$ if and only if $n \equiv 0 \pmod{\rho}$; $p - (5/p) \equiv 0 \pmod{\rho}$. Here $(5/p)$ is the usual Legendre symbol.

The following consequence of (2.1) and the formula $F_{2n} = F_n G_n$ is well known.

LEMMA 2.1. *p is a divisor of (G) if and only if the rank of apparition of p in (F) is even.*

The formula

$$(2.2) \quad G_n^2 - 5F_n^2 = (-1)^n 4$$

gives more information. For if $p \equiv 1 \pmod{4}$, and p divides (G) , (2.2) implies that $(5/p) = 1$. On the other hand if $p \equiv 3 \pmod{4}$, p must divide (G) . For otherwise Lemma 2.1 and formula (2.2) with $n = \rho_p$ imply $(-1/p) = 1$.

On classifying the primes according to the quadratic characters of 5 and -1 modulo p , they are distributed into eight arithmetical progressions $20n + 1, 20n + 3, 20n + 7, 20n + 9, 20n + 11, 20n + 13, 20n + 17, 20n + 19$. By the remarks above, only primes of the form $20n + 1$ and $20n + 9$ for which both -1 and 5 are quadratic residues need be considered; the following lemma disposes of all others.

LEMMA 2.2. *p is a divisor of (G) if $p \equiv 3 \pmod{4}$; that is if $p \equiv 3, 7, 11, 19 \pmod{20}$. p is a non-divisor of (G) if $p = 1 \pmod{4}$ and $p \equiv 2$ or $3 \pmod{5}$; that is if $p \equiv 13, 17 \pmod{20}$.*

3. Further classification criteria. Let \mathfrak{Q} denote the set of all primes having both 5 and -1 as quadratic residues; that is primes of the $20n + 1$ or $20n + 9$. For the remainder of the paper all primes considered belong to \mathfrak{Q} . Let \mathfrak{P} denote the subset of divisors of (G) and $\mathfrak{P}^* = \mathfrak{Q} - \mathfrak{P}$ the complementary set of non-divisors of (G) . We shall derive criteria to decide whether p belongs to \mathfrak{P} or to \mathfrak{P}^* .

If p is any element of \mathfrak{Q} , we may write

$$(3.1) \quad p \equiv 2^k + 1 \pmod{2^{k+1}}, \quad p - 1 = 2^k q, \quad q \text{ odd}; \quad k \geq 2.$$

We shall call k the (dyadic) order of p . Thus primes of order two are of the forms $40n + 21$ and $40n + 29$, primes of order three, of the form $80n + 9$ and $80n + 41$ and so on. The difficulty of classifying p as a divisor or non-divisor of (G) increases rapidly with its order.

Let R_p denote the finite field of p elements. For every $p \in \mathfrak{P}$, the characteristic polynomial (2.2) splits in R_p :

$$(3.2) \quad x^2 - x - 1 = (x = a)(x - b), a, b \in R_p .$$

If we represent the elements of R_p by the least positive residues of p , then by a classical theorem of Dedekind's, the factorization of p in the root-field \mathcal{R} of $f(x)$ is given by

$$(3.3) \quad p = qq', q = (p, \alpha - a), q' = (p, \alpha - b) .$$

Here q and q' are conjugate prime ideals of \mathcal{R} of norm p .

Now assume $p \in \mathfrak{P}^*$; then rank ρ of p divides q in (3.1). Consequently $F_q \equiv 0 \pmod{p}$, so that $\alpha^q \equiv \beta^q \pmod{q}$ in \mathcal{R} . But then $\alpha^{2q} \equiv \alpha^q \beta^q \equiv (-1)^q \equiv -1 \pmod{q}$ so that $\alpha^{2q} \equiv -1 \pmod{q}$. But then $\alpha^{2q} \equiv -1 \pmod{p}$ in R . Conversely, assume that $\alpha^{2q} \equiv -1 \pmod{p}$. Then in \mathcal{R} , $\alpha^{2q} \equiv -1 \pmod{q}$ or $\alpha^{2q} \equiv (\alpha\beta)^q \pmod{q}$, $(\alpha - \beta)\alpha^q F_q \equiv 0 \pmod{q}$. But $(\alpha - \beta, q) = (\alpha, q) = (1)$ in \mathcal{R} . Hence $F_q \equiv 0 \pmod{q}$ so that $F_q \equiv 0 \pmod{p}$ in R . Thus the rank of p in (F) must divide q and is consequently odd. Hence $p \in \mathfrak{P}^*$.

It follows that $p \in \mathfrak{P}^*$ if and only if $\alpha^{2q} \equiv -1$ in R_p . Since $(ab)^{2q} = (-1)^{2q} = +1$ in R_p , it is irrelevant which root of $f(x) = 0$ in R_p we choose for a . An equivalent way of stating this result is that $p \in \mathfrak{P}^*$ if and only if $\alpha^{4q} \equiv 1 \pmod{p}$ but $\alpha^{2q} \not\equiv 1 \pmod{p}$.

For ease of printing, let

$$[u/p]_n = (u/k)_{2^n}$$

denote the 2^n ic character of u modulo p . Thus $[u/p]_1$ is an ordinary quadratic character, $[u/p]_2$ or $(u/p)_4$ a biquadratic character and so on. The result we have obtained may be stated as follows:

THEOREM 3.1. *Let p be any prime of order $k \geq 2$. Then if a is a root of $x^2 - x - 1$ in the finite field R_p , a necessary and sufficient condition that p belong to \mathfrak{P}^* is*

$$(3.3) \quad [a/p]_{k-1} = -1 .$$

There is another useful way of stating this result. Let

$$(3.4) \quad g(x) = f(x^{2^{k-2}}) = x^{2^{k-1}} - x^{2^{k-2}} - 1 .$$

Assume that $p \in \mathfrak{P}$. Then each of the equations

$$x^{2^{k-2}} = a, \quad x^{2^{k-2}} = b$$

where a, b are the roots of $f(x)$ in R_p , has 2^{k-2} roots in R_p . If c is any one of these roots, it follows from (3.4) that c is a root of $g(x)$. Hence the polynomial $g(x)$ splits completely in R_p . On the other hand since neither of the equations

$$x^{2^{k-1}} = a, \quad x^{2^{k-1}} = b$$

has a root in R_p , $g(x^2)$ has no roots in R_p . Evidently, by Theorem 3.1, these splitting conditions imply conversely that $p \in \mathfrak{P}^*$. Hence

THEOREM 3.2. *Necessary and sufficient conditions that p belong to \mathfrak{P}^* are that the polynomial $g(x)$ defined by (3.4) splits completely into linear factors modulo p , but the polynomial $g(x^2)$ has no linear factor modulo p .*

For example, assume that $p \equiv 5 \pmod{8}$ so that $k = 2$. Then $g(x) = f(x)$ so the first condition of Theorem 3.2 is always satisfied. Since $g(x^2) = x^4 - x^2 - 1$ we may state the following corollary.

COROLLARY 3.1. *If p is of order two, $p \in \mathfrak{P}$ if and only if the polynomial $x^4 - x^2 - 1$ is completely reducible modulo p .*

In like manner if $p \equiv 1 \pmod{8}$ so that $k \geq 2$, we may state the following corollary

COROLLARY 3.2. *If p is of order three or more, a sufficient condition that $p \in \mathfrak{P}$ is that the polynomial $x^4 - x^2 - 1$ is not completely reducible modulo p .*

Now let

$$(3.5) \quad p = u^2 + 4v^2$$

be the representation of p as a sum of two squares. Either u or v is divisible by 5.

LEMMA. *The polynomial $x^4 - x^2 - 1$ splits completely in R_p if and only if in the representation (3.5) either $u \equiv \pm 1 \pmod{5}$ or $v \equiv \pm 1 \pmod{5}$.*

Proof. Since $x^4 - x^2 - 1 = ((2z^2 - 1)^2 - 5)/4$, $x^4 - x^2 - 1$ always splits into quadratic factors in R_p . But if i denotes an element of R_p whose square is $p - 1$, then $x^4 - x^2 - 1 = (z^2 + i)^2 - (1 + 2i)z^2$. Hence a necessary and sufficient condition that $x^4 - x^2 - 1$ split completely in R_p is that $1 + 2i = ((-1)(-1 - 2i))$ be a square in R_p .

Now let \mathfrak{T} denote the ring of the Gaussian integers, and let $p = (u + 2iv)(u - 2iv)$ be the decomposition of p into primary factors in \mathfrak{T} .

(Bachmann [1]). Then $u - 2iv$ is a prime ideal of norm p so that the residue class ring $\mathfrak{T}/(u - 2iv)$ is isomorphic to R_p . Now $-1 - 2i$ is primary in \mathfrak{T} . Also since $p \equiv 1 \pmod{4}$, -1 is a quadratic residue of $u - 2iv$. Hence $1 + 2i$ is a square in R_p if and only if $-1 - 2i$ is a quadratic residue of $u - 2iv$ in \mathfrak{T} . By the quadratic reciprocity law in \mathfrak{T} , (Bachmann [1])

$$\left(\frac{-1 - 2i}{u - 2iv}\right) = \left(\frac{u - 2iv}{-2 - 2i}\right) = \left(\frac{u + v}{-1 - 2i}\right).$$

Now either u or v must be divisible by $-1 - 2i$. But $(-1 - 2i)$ is a prime ideal in \mathfrak{T} of norm five. Therefore $-1 - 2i$ is a quadratic residue of $u - 2iv$ if and only if $u \equiv 0, v \equiv 1, 4 \pmod{5}$ or $v \equiv 0, u \equiv 1, 4 \pmod{5}$. This completes the proof of the lemma.

On combining the results of Corollaries 3.1 and 3.2 into the lemma, we obtain

THEOREM 3.3. *Let p be congruent to 5 modulo 8. Then a necessary and sufficient condition that $p \in \mathfrak{P}$ is that in the representation (3.5) of p as a sum of two squares, either $u \equiv \pm 1 \pmod{5}$ or $v \equiv \pm 1 \pmod{5}$. If p is congruent to 1 modulo 8, a sufficient condition that $p \in \mathfrak{P}$ is that $u \equiv \pm 2 \pmod{5}$ or $v \equiv \pm 2 \pmod{5}$.*

4. Applications of the criteria. The theorems of § 3 classify unambiguously all primes of \mathfrak{Q} either into \mathfrak{P} or into \mathfrak{P}^* . But in the absence of workable reciprocity laws beyond the biquadratic case, they tell us little more than Lemma 2.1 for primes of order greater than three; that is, primes of the forms $160n + 9$ or $160n + 81$. However the theorems may be extended so as to give useful information about primes of any order by utilizing the following elementary properties of the character symbol $[u/p]_k$:

$$(4.1) \quad \begin{aligned} [uv/p]_k &= [u/p]_k[v/p]_k \\ [u^2/p]_k &= [u/p]_k^2 = [u/p]_{k-1} \\ [u/p]_k = 1 &\text{ implies } [u/p]_n = 1 \text{ for } 1 \leq n \leq k-1. \end{aligned}$$

From (4.1) (iii) and Theorem 3.1 we immediately obtain.

THEOREM 4.1. *If p is of order $k \geq 3$, then a necessary condition that p belong to \mathfrak{P}^* is that*

$$(4.2) \quad [a/p]_n = 1 \quad (n = 1, 2, \dots, k-2).$$

COROLLARY 4.1. *A sufficient condition that p belong to \mathfrak{P} is that (4.2) be false for some $n \leq k-2$.*

Now suppose that a solution $x = c$ of the congruence $c^2 \equiv a \pmod{p}$ is known, p of order four or more. Then by (4.1) (ii) and the theorem just proved we obtain.

THEOREM 4.2. *If p is of order $k \geq 4$, then a necessary condition that p belong to \mathfrak{P}^* is that*

$$(4.4) \quad [c/p]_n = 1, \quad (n = 1, 2, \dots, k-3).$$

A necessary and sufficient condition that p belong to \mathfrak{P}^ is that*

$$(4.5) \quad [c/p]_{k-2} = -1.$$

There is a method for obtaining a , the root of (2.1) modulo p , which leads to another useful criterion for primes of low order. For every prime p of \mathfrak{D} there exists a unique representation in the form

$$(4.6) \quad p = r^2 - 5s^2, \quad 0 < r, \quad 0 < s < \sqrt{4p/5}.$$

(Uspensky [5]). If this representation is known, a is easily shown to be the least positive solution of the congruence

$$(4.7) \quad 2sa \equiv (r+s) \pmod{p}.$$

By using property (4.1) (i) of the character symbol and Theorem 3.1, we see that

$$[2s/p]_{k-1} = -[(r+s)/p]_{k-1}$$

is a necessary and sufficient condition that p belong to \mathfrak{P}^* .

If $k = 2$, the criterion becomes $(2s/p) = -((r+s)/p)$. But since $p \equiv 5 \pmod{8}$ and $p = r^2 - 5s^2$, r is odd and $s = 2s'$ where s' is odd. Hence by the reciprocity law for the Jacobi symbol, $(2s/p) = (s'/p) = (p/s') = (r^2/s') = +1$. Hence $p \in \mathfrak{P}^*$ if and only if $((r+s)/p) = -1$. But $((r+s)/p) = ((r^2 - 5s^2)/(r+s)) = (-4s^2/(r+s)) = (-1/(r+s)) = (-1)^{(r+1)/2}$ since $s \equiv 2 \pmod{4}$. We have thus proved

THEOREM 4.3. *If p is of order two, so that p is of the form $40n + 21$ or $40n + 29$, then p belongs to \mathfrak{P} or to \mathfrak{P}^* according as r in the representation (4.6) is congruent to three or one modulo 4.*

Now if $k > 2$, $p \equiv 1 \pmod{8}$ so that r in the representation (4.6) is odd. Hence using the corollary to Theorem 4.1 with $n = 1$ and the results established in the proof of Theorem 4.3, we obtain

THEOREM 4.4. *If p is of order greater than two, p belongs to \mathfrak{P} if r in the representation (4.6) is congruent to one modulo 4.*

To illustrate, suppose that $p = 101$. Then $p \equiv 5 \pmod{8}$ so that

Theorem 3.3 is applicable. Since $101 = 1^2 + 4 \cdot 5^2$, $101 \in \mathfrak{P}$. Also $101 = 11^2 - 5 \cdot 2^2$ and $11 \equiv 3 \pmod{4}$. Hence $101 \in \mathfrak{P}$ by Theorem 4.3. In fact we find from Laisant's table that $G_{50} = 12586269025 = 101 \times 124616525$.

Again, there are seven primes in \mathfrak{Q} less than one thousand of order greater than three; namely 241, 401, 449, 641, 769, 881 and 929. But only two of these need be discussed; Theorem 3.3 assigns 241, 449, 641, 881 and 929 to \mathfrak{P} . For $241 = 15^2 + 4 \cdot 2^2$, $449 = 7^2 + 4 \cdot 10^2$, $641 = 25^2 + 4 \cdot 2^2$, $881 = 25^2 + 4 \cdot 8^2$ and $929 = 23^2 + 4 \cdot 10^2$. There remain 401 and 729. Now $401 \equiv 17 \pmod{32}$. Hence $k = 4$. Since $112^2 - 112 - 1 = 31 \times 401$, $a = 112$. Hence by Theorem 3.1, $401 \in \mathfrak{P}^*$ if and only if $[112/401]_3 = -1$. Now using the idea in Theorem 4.2, $112 = 2^4 \times 7$ and $85^2 \equiv 7 \pmod{401}$. Hence $[112/401]_3 = [85/401]_2$. But $(85/401) = -1$. Hence $401 \in \mathfrak{P}$. This conclusion is easily checked. For $401 - 1 = 25 \cdot 16$ and by Laisant's table, $F_{25} = 75025 \not\equiv 0 \pmod{401}$. Hence $401 \in \mathfrak{P}$ by Lemma 2.1.

Finally $769 \equiv 257 \pmod{512}$ so that $k = 8$. Using Jacobi's Canon, $a = 43$, $\text{ind } a = 500 \not\equiv 0 \pmod{64}$ so that $769 \in \mathfrak{P}$. Indeed $769 - 1 = 3 \cdot 256$ and $F_3 = 2$. Hence $769 \in \mathfrak{P}$ by Lemma 2.1.

We have shown incidentally that every prime $p < 1000$ in \mathfrak{Q} of order greater than three is a divisor of (G) .

5. Conclusion. The methods of this paper may be easily extended to obtain information about the prime divisors of the Lucas or Lehmer [4] numbers of the second kind $\alpha^n + \beta^n$ where α and β now are the roots of any quadratic polynomial $x^2 - \sqrt{P}x + Q$ with P, Q integers, $Q(P - 4Q) \neq 0$. It is worth noting that just as in the special case $P = 1, Q = -1$ investigated here, there will be arithmetical progressions whose primes cannot be characterized as divisors or non-divisors by their quadratic or biquadratic characters alone.

In the absence of any criterion like Lemma 2.1 for a prime divisor of an arbitrarily selected recurrence (U) , it seems difficult to characterize the divisor of (U) in any general way. It would be interesting to make a numerical study of several recurrences (U) to endeavor to find out whether the two Lucas sequences $0, 1, P, \dots$ and $2, P, P^2 - 2Q, \dots$ and their translates are essentially the only ones for which a global characterization of the divisors is possible.

REFERENCES

1. Paul Bachmann, *Kreistheilung*, Leipzig (1921), 150–185.
2. Marshall Hall, *Divisors of second order sequences*, Bull. Amer. Math. Soc., **43** (1937), 78–80.
3. C. A. Laisant, *Les deux suites Fibonacci fondamentales*, Enseignement Math., **21** (1920), 52–56.
4. D. H. Lehmer, *An extended theory of Lucas functions*, Annals of Math., **31** (1930), 419–448.

5. J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, New York (1939), 358–359.
6. Morgan Ward, *Prime divisors of second order recurrences*, Duke Math. Journal **21** (1954), 607–614.
7. ———, *The linear p -adic recurrence of order two*, Unpublished.

CALIFORNIA INSTITUTE, PASADENA.

Chapter 25

1962

THE LINEAR p -ADIC RECURRENCE OF ORDER TWO

Dedicated to Hans Rademacher
on the occasion of his seventieth birthday

BY
MORGAN WARD

I. Introduction and summary of results

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

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

defined by

$$(1.1) \quad W_{n+2} = PW_{n+1} - QW_n \quad (n = 0, 1, 2, \dots)$$

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

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

$$(1.2) \quad w_n = \phi(W_n) \quad (n = 0, 1, 2, \dots).$$

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

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

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

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

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

2. Let

$$(2.1) \quad f(z) = z^2 - Pz + Q$$

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

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

Received August 31, 1960.

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

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

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

If we represent ν in the canonical form

$$\nu = \sum_0^\infty a_n p^n, \quad 0 \leq a_i < p,$$

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

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

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

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

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

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

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

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

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

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

II. Reduction to integral sequences

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

Let $\phi(P) = a$ and $\phi(Q) = b$, so that $P = p^a U$, $Q = p^b V$, where U and V are units. Also let $W_0 = p^{w_0} U'_0$, $W_1 = p^{w_1} U'_1$ where U'_0 and U'_1 are units. Finally, let

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

where c and d are integers at our disposal. Then

$$W'_{n+2} = p^{a-c} UW'_{n+1} - p^{b-2c} VW'_n \quad (n = 0, 1, \dots),$$

and

$$W'_0 = p^{w_0-d} U'_0, \quad W'_1 = p^{w_1-d-c} U'_1.$$

We choose c so that $a - c$ and $b - 2c$ shall be nonnegative and as small as possible. Then if $d = \text{Min}\{w_0, w_1 - c\}$, W'_0 and W'_1 are integers, and at least one is a unit. Evidently the value function of (W) is known as soon as the value function of the integral recurrence (W') is determined.

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

$$a - c = \frac{1}{2}((2a - b) + (b - 2c)) \geq \frac{1}{2}(b - 2c),$$

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

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

and we choose $c = a$.

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

$$W'_{n+2} = P' W'_{n+1} - Q' W'_n,$$

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

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

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

The two subsequences

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

of (W') both satisfy the recurrence

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

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

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

$$(5.1) \quad W'_n = \Gamma\gamma^n + \Delta\delta^n$$

where Γ and Δ are both integers of R .

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

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

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

Case 1. p odd, Q and P units;

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

III. Properties of the root field

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

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

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

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

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

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

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

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

$$(6.1) \quad u = \zeta \psi.$$

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

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

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

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

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

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

$$(7.2) \quad \phi(\log \psi) = \phi(\psi - 1) > 0.$$

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

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

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

and

$$(7.3) \quad e^{\log \psi} = \psi.$$

We shall make repeated use of the elementary formulas

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

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

$$(7.4) \quad \log \psi^\nu = \nu \log \psi.$$

(7.2) and (7.3) give the useful lemma

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

$$(7.5) \quad \phi(\log \psi^\nu) = \phi(\nu \log \psi) = \phi(\psi^\nu - 1) = \phi(\nu) + \phi(\psi - 1).$$

IV. The zeros mod p of integral recurrences

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

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

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

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

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

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

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

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

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

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

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

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

V. The rank function for ordinary primes

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

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

The general term of (W) may be written

$$(9.1) \quad W_n = (A\alpha^n - B\beta^n)/(\alpha - \beta),$$

where

$$(9.2) \quad A = W_1 - W_0\beta, \quad B = W_1 - W_0\alpha$$

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

$$AB = \Phi(W_1, W_0).$$

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

$$(9.3) \quad A/B = \rho_2 \psi_2.$$

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

$$(9.4) \quad \beta/\alpha = \rho_1 \psi_1.$$

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

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

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

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

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

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

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

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

and r divides $p - 1$.

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

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

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

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

fined by

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

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

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

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

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

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

We may thus state

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(10.1) \quad (\beta/\alpha)^r = \psi_1, \quad A/B = \psi_2, \quad \phi(\log \psi_2) \geq \phi(\log \psi_1).$$

Consequently

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

is an integer of \mathfrak{R}_p .

LEMMA 10.1. *ν is an integer of R_p .*

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

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

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

which completes the proof.

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

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

Hence by formulas (9.6) and (10.1),

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

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

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

We have thus proved the following result:

THEOREM 10.1. *Under the hypotheses:*

(i) *(W) is integral and its associated polynomial $z^2 - Pz + Q$ has unit coefficients and distinct roots,*

(ii) *p is not a discriminantal divisor,*

(iii) *$W_0 \equiv 0 \pmod{p}$, $W_1 \not\equiv 0 \pmod{p}$,*

(iv) *$w_0 = \phi(W_0) \geq l_r = \phi(L_r)$,*

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

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

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

Here ν is the p -adic integer

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

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

VI. The value function for discriminantal divisors

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

$$(11.1) \quad \beta/\alpha = \psi_1,$$

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

$$(11.2) \quad A/B = \psi_2.$$

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

$$(11.3) \quad \nu = (\log \psi_2)/(\log \psi_1)$$

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

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

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

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

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

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

- (i) $W_1^2 - PW_1W_0 + QW_0^2$ is a unit of R_p , and either
- (ii) p is a discriminantal divisor of $z^2 - Pz + Q$, or
- (iii) p is ordinary, and $(W_1 - \beta W_0)/(W_1 - \alpha W_0)$ is a unit in \mathfrak{R}_p whose order divides the order of the unit β/α .

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

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

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

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

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

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

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

VII. The determination of a sequence by its zeros

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

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

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

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

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

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

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

$$(12.1) \quad A/B = \psi_1, \quad AB = 1.$$

Now let

$$W_n = (A\alpha^n - B\beta^n)/(\alpha - \beta) \quad (n = 0, 1, \dots).$$

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

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

VIII. Polar sequences

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

$$(13.1) \quad W_{n+1} V_{n+1} - (P/2)(W_{n+1} V_n + W_n V_{n+1}) + QW_n V_n = 0.$$

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

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

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

Let

$$W_n = (A\alpha^n - B\beta^n)/(\alpha - \beta), \quad V_n = (\Gamma\alpha^n - \Delta\beta^n)/(\alpha - \beta),$$

and as in Section 9, let

$$(13.2) \quad \beta/\alpha = \rho_1 \psi_0, \quad A/B = \rho_2 \psi_2, \quad \Gamma/\Delta = \rho_3 \psi_3,$$

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

$$(13.3) \quad (\beta/\alpha)^r = \psi_0^r = \psi_1.$$

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

$$(13.4) \quad \begin{aligned} \Phi(W_1, W_0) &= AB, & \Phi(V_1, V_0) &= \Gamma\Delta, \\ \Psi(W_1, W_0; V_1, V_0) &= A\Delta + B\Gamma. \end{aligned}$$

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

$$(13.5) \quad \rho_2 = -\rho_3, \quad \psi_2 = \psi_3.$$

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

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

$$(13.6) \quad V_n = C(A^n + B^n)$$

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

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

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

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

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

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

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

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

It follows from formula (13.6) that

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

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

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

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

$$\begin{aligned} v_n &= 0 && \text{if } n \not\equiv r/2 \pmod{4}, \\ v_n &= \phi(2\nu - (2n - r)/2r) + l_r && \text{if } n \equiv r/2 \pmod{r}. \end{aligned}$$

REFERENCES

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

Bibliography

- [1] Lehmer, D. (1993). *The Mathematical Work of Morgan Ward*. Mathematics of Computation, 61(203), 307-311.