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),

$$\psi_n = \psi_n(\wp(u); g_2, g_3), \qquad (n = 0, 1, 2, \cdots)$$

associated with the real multiplication of the Weierstrass $\wp$ function when $\wp(u)$, 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),

$$U_n = (\alpha^n - \beta^n)/(\alpha - \beta), \qquad (n = 0, 1, 2, \cdots).$$

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 $A_n, \cdots, D_n$ is a polynomial in sn^2u and k^2 with rational integral coefficients. Consequently, if we substitute for sn^2u 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^2u 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

$$snnu/snu = B_n/A_n, \quad cnnu/cnu = C_n/A_n, \quad dnu = D_n/A_n$$

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 $A_n, \cdots, D_n$, 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 functions [3] 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 $\operatorname{Im} \tau > 0$, $u = 2Kv$, where K is the complete elliptic integral. The Jacobi theta functions are then

$$\Theta(u) = \theta_0(v) = \sum_{-a}^{+a} (-1)^m q^{m^2} e^{2m\pi i v},$$

$$\mathrm{H}(u) = \theta_1(v) = -i \sum_{-a}^{+a} (-1)^m q^{(m+\frac{1}{2})^2} e^{(2m+1)\pi i v}$$

$$\mathrm{H}_1(u) = \theta_2(v) = \sum_{-a}^{+a} q^{(m+\frac{1}{2})^2} e^{(2m+1)\pi i v},$$

$$\Theta_1(u) = \theta_3(v) = \sum_{-a}^{+a} q^{m^2} e^{2m\pi i v}.$$

[3] The functions were named by Weierstrass in honor of Abel who was the first to consider them.

If we write θ_α for $\theta_\alpha(0)$ and θ_0 for $\theta_0(0)$, then Weierstrass Al functions may be defined by

$$(4.1)\qquad \begin{aligned} Al_1(u) &= \theta_3/\theta_0\theta_2 \exp(-\tfrac{1}{2}v^2\theta''_0/\theta_0)\theta_1(v), \\ Al_\alpha(u) &= 1/\theta_\alpha \exp(-\tfrac{1}{2}v^2\theta''_0/\theta_0)\theta_\alpha(v), \qquad (\alpha = 0, 2, 3). \end{aligned}$$

Note that $Al_1(u)$ is odd and $Al_2(u)$, $Al_3(u)$ and $Al_0(u)$ even. Also

$$(4.11)\qquad Al_1(0) = 0, \qquad Al_\alpha(0) = 1, \qquad (\alpha = 0, 2, 3).$$

sn, *cn* and *dn* have particularly simple expressions in terms of the Als; namely

$$(4.2)\qquad snu = Al_1(u)/Al_0(u),\ cnu = Al_2(u)/Al_0(u),\ dnu = Al_3(u)/Al_0(u).$$

The relationship to the Weierstrass σ functions is also very simple; namely if $w = \omega u/K$, then

$$(4.3)\qquad \begin{aligned} Al_1(u) &= (e_1 - e_3)^{\frac{1}{2}} e^{e_3 w^2/2}\sigma(w); & Al_3(u) &= e^{e_3 w^2/2}\sigma_2(w); \\ Al_2(u) &= e^{e_3 w^2/2}\sigma_1(w); & Al_0(u) &= e^{e_3 w^2/2}\sigma_3(w). \end{aligned}$$

For the lemniscate case, $e_3 = 0$ and the Al functions are essentially the σ functions.

The fundamental three-terms sigma identity becomes

$$\begin{aligned} (4.4)\qquad & Al_1(u+u_1)Al_1(u-u_1)Al_1(u_2+u_3)Al_1(u_2-u_3) \\ & + Al_1(u+u_2)Al_1(u-u_2)Al_1(u_3+u_1)Al_1(u_3-u_1) \\ & + Al_1(u+u_3)Al_1(u-u_3)Al_1(u_1+u_2)Al_1(u_1-u_2) = 0. \end{aligned}$$

5. We next introduce four new functions $K_{\alpha n}(u)$ of u and n by the definition

$$(5.1)\qquad K_{\alpha n} = Al_\alpha(nu)/Al_0(u)^{n^2}, \qquad (n = 0, 1, 2, \cdots;\ \alpha = 0, 1, 2, 3).$$

Evidently

$$(5.2)\qquad snnu = K_{1n}/K_{0n}, \qquad cnnu = K_{2n}/K_{0n}, \qquad dnnu = K_{3n}/K_{0n}.$$

The first three initial values of the four sequences (K_α) are as follows:

TABLE I. Initial values of $K_{\alpha n}$.

α/n	0	1	2
0	1	1	$1 - k^2sn^4u.$
1	0	*snu*	$2snu\ cnu\ dnu.$
2	1	*cnu*	$1 - 2sn^2u + k^2sn^4u.$
3	1	*dnu*	$1 - 2k^2sn^2n + k^2sn^4u.$

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 $K_{\alpha n}$.

(i) $$K_{0n+m}K_{0n-m} = K^2_{0n}K^2_{0m} - k^2K^4_{1n}K^2_{1m}.$$

. . . . . .

(v) $$K_{1n+m}K_{1n-m} = K^2_{1n}K^2_{0m} - K^2_{0n}K^2_{1m}.$$

. . . . . .

(xix) $$K_{0n+m}K_{1n-m} = K_{0n}K_{1n}K_{2m}K_{3m} - K_{2n}K_{3n}K_{0m}K_{1m}.$$

. . . . . .

(xxiv) $$K_{2n+m}K_{3n-m} = K_{2n}K_{3n}K_{2m}K_{3m} - k'^2K_{0n}K_{1n}K_{0m}K_{1m}.$$

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:

$$K_{12n+1}K_{11} = K^2_{1n+1}K^2_{0n} - K^2_{0n+1}K^2_{1n}, \tag{5.3}$$

$$K_{12n} = 2K_{0n}K_{1n}K_{2n}K_{3n}. \tag{5.4}$$

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

$$K_{0n}(u) = A_n(sn^2u; k^2) \qquad n \text{ odd or even;}$$

$$K_{1n}(u) = \begin{cases} snuB_n(sn^2u; k^2) & n \text{ odd;} \\ snu\ cnu\ dnuB_n(sn^2u; k^2) & n \text{ even;} \\ cnuC_n(sn^2u; k^2) & n \text{ odd;} \end{cases} \tag{6.1}$$

$$K_{2n}(u) = \begin{cases} C_n(sn^2u;k^2) & n \text{ even}; \\ dnuD_n(sn^2u;k^2) & n \text{ odd}; \end{cases}$$

$$K_{3n}(u) = \begin{cases} D_n(sn^2u;k^2) & n \text{ even}; \end{cases}$$

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

$$x = sn^2u, \qquad a = k^2. \tag{6.2}$$

Then

$$K_{1n}(u) = \begin{cases} (x)^{\frac{1}{2}}B_n(x;a), & n \text{ odd}; \\ (x(1-x)(1-ax))^{\frac{1}{2}}B_n(x;a), & n \text{ even}; \end{cases} \tag{6.3}$$

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

$$\alpha_n = \begin{cases} (n^2-1)/2, & n \text{ odd}, \\ n^2/2, & n \text{ even}, \end{cases} \qquad \beta_n = \begin{cases} (n^2-1)/2 & n \text{ odd}, \\ (n^2-4)/2 & n \text{ even}, \end{cases} \tag{6.4}$$

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 $\tau \to \tau+1$, $\tau \to -1/\tau$ 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

$$Al_0(u+K) = 1/k'^{\frac{1}{2}}e^{\lambda(u^2-(u+K)^2)}Al_3(u),$$

$$Al_3(u+2K) = e^{\lambda(u^2-(u+K)^2)}Al_3(u),$$

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

$$K_{0n}(u+K) = Al_0(nu+nK)/Al_0(u+K)^{n^2} = k'^{(n^2-1)/2}(Al_3(nu)/Al_3(u)^{n^2}.$$

On multiplying both sides of this expression by $dnu^{n^2} = (Al_3(u)/Al_0(u))^{n^2}$, we find that

$$dnu^{n^2}K_{0n}(u+K) = k'^{(n^2-1)/2}K_{3n}(u). \tag{7.1}$$

Now $sn(u+K) = cnu/dnu$. Hence the substitution of $u+K$ for u induces the substitution of $(1-x)/(1-ax)$ for $x = sn^2u$. Therefore we obtain from (7.2) on substituting for K_{an} their expressions in terms of A_n and D_n the transformation formula

$$(1-ax)^{a_n}A_n((1-x)/(1-ax)) = (1-a)^{a_n/2}D_n(x) \qquad n \text{ odd}.$$

The following sets of transformation formulas are obtained by proceeding systematically in this manner.

8. The modular transformation $\tau \to -1/\tau$ is simply Jacobi's imaginary transformation $u \to iu$, $k \to k'$. Now Weierstrass [4] showed that

$$Al_3(iu;k') = e^{u^2/2}Al_3(u;k)$$
$$Al_0(iu;k') = e^{u^2/2}Al_2(u;k)$$

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

$$K_{3n}(iu;k') = cnu^{-n^2}K_{3n}(u;k). \tag{8.1}$$

But since $sn(iu,k') = isn(u,k)/cn(u,k)$, Jacobi's imaginary transformation induces the transformation

$$x \to -x/(1-x), \qquad a \to 1-a \tag{8.2}$$

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

$$(1-x)^{a_n}D_n(x/(x-1);1-a) = D_n(x;a).$$

The formulas listed below were obtained by systematically combining

[4] Weierstrass [1], page 20.

TABLE III. Transformation formulas.

	n odd	*n even*
$(1-ax)^{\alpha_n}A_n((1-x)/(1-ax))$	$=(1-a)^{\alpha_n/2}D_n(x)$;	$=(1-a)^{\alpha_n/2}A_n(x)$
$(1-ax)^{\beta_n}B_n((1-x)/(1-ax))$	$=(-1)^{(n-1)/2}(1-a)^{\beta_n/2}C_n(x)$;	$=(-1)^{(n-2)/2}(1-a)^{\beta_n/2}(x)$
$(1-ax)^{\alpha_n}C_n((1-x)/(1-ax))$	$=(-1)^{(n-1)/2}(1-a)^{\alpha_n/2}B_n(x)$;	$=(-1)^{n/2}(1-a)^{\alpha_n/2}C_n(x)$
$(1-ax)^{\alpha_n}D_n(1-x)/(1-ax))$	$=(1-a)^{\alpha_n/2}A_n(x)$;	$=(1-a)^{\alpha_n/2}D_n(x)$
$(\sqrt{ax})^{\alpha_n}A_n(1/ax)$	$=(-1)^{(n-1)/2}B_n(x)$;	$=(-1)^{n/2}A_n(x)$
$(\sqrt{ax})^{\beta_n}B_n(1/ax)$	$=(-1)^{(n-1)/2}A_n(x)$;	$=(-1)^{(n-2)/2}B_n(x)$
$(\sqrt{ax})^{\alpha_n}C_n(1/ax)$	$=D_n(x)$;	$=C_n(x)$
$(\sqrt{ax})^{\alpha_n}D_n(1/ax)$	$=C_n(x)$;	$=D_n(x)$
$(1-x)^{\alpha_n}A_n((1-ax)/(a-ax))$	$=((1-a)/a)^{\alpha_n/2}C_n(x)$;	$=(-1)^{n/2}((1-a)/a)^{\alpha_n/2}A_n(x)$
$(1-x)^{\beta_n}B_n((1-ax)/(a-ax))$	$=(-1)^{(n-1)/2}((1-a)/a)^{\beta_n/2}D_n(x)$;	$=((1-a)/a)^{\beta_n/2}B_n(x)$
$(1-x)^{\alpha_n}C_n((1-ax)/(a-ax))$	$=((1-a)/a)^{\alpha_n/2}A_n(x)$;	$=(-1)^{n/2}((1-a)/a)^{\alpha_n/2}C_n(x)$
$(1-x)^{\alpha_n}D_n((1-ax)/(a-ax))$	$=(-1)^{(n-1)/2}((1-a)/a)^{\alpha_n/2}B_n(x)$;	$=((1-a)/a)^{\alpha_n/2}D_n(x)$.

the two transformations $\tau \to -1/\tau$ and $\tau \to 1+\tau$; the latter transformation induces the transformation

$$x \to (x-ax)/(1-ax), \qquad a \to a/(a-1) \tag{8.3}$$

on x and a.

TABLE IV. Transformation formulas.

$$\begin{aligned}
A_n(x;a) &= (1-ax)^{a_n} D_n((x-ax)/(1-ax);\, a/(a-1)) \\
&= (1-x)^{a_n} C_n(x/(x-1);\, 1-a), \\
&= (1-ax)^{a_n} C_n(ax/(ax-1);\, (a-1)/a) = A_n(ax;\, 1/a) \\
&= (1-x)^{a_n} D_n((ax-x)/(1-x);\, 1/(1-a)). \\
B_n(x;a) &= (1-ax)^{\beta_n} B_n((x-ax)/(1-ax);\, a/(a-1)) \\
&= (1-x)^{\beta_n} B_n(x/(x-1);\, 1-a), \\
&= (1-ax)^{a_n} B_n(ax/(ax-1);\, (a-1)/a) = B_n(ax;\, 1/a) \\
&= (1-x)^{\beta_n} B_n((ax-x)/(1-x);\, 1/(1-a)). \\
C_n(x;a) &= (1-ax)^{a_n} C_n((x-ax)/(1-ax);\, a/(a-1)) \\
&= (1-x)^{a_n} A_n(x/(x-1);\, 1-a), \\
&= (1-ax)^{a_n} D_n(ax/(ax-1);\, (a-1)/a) = D_n(ax;\, 1/a) \\
&= (1-x)^{a_n} A_n((ax-x)/(1-x);\, 1/(1-a)). \\
D_n(x;a) &= (1-ax)^{a_n} A_n((x-ax)/(1-ax);\, a/(a-1)) \\
&= (1-x)^{a_n} D_n(x/(x-1);\, 1-a), \\
&= (1-ax)^{a_n} A_n(ax/(ax-1);\, (a-1)/a) = C_n(ax;\, 1/a) \\
&= (1-x)^{a_n} C_n((ax-x)/(1-x);\, 1/(1-a)).
\end{aligned} \tag{8.4}$$

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 M, the functional equation

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega^2_n - \omega_{n+1}\omega_{n-1}\omega^2_m \tag{9.1}$$

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 M to solutions of (9.1) over more general rings.

Let $\mathfrak{R}$ denote a domain of integrity; (commutative ring with a unit and no divisors of zero). $\mathfrak{R}$ may be a field; in any event we denote its quotient field by $\mathfrak{F}$, and for brevity refer to $\mathfrak{R}$ as a ring. We are interested in solutions of (9.1) over $\mathfrak{R}$ and over $\mathfrak{F}$. We lay down the following definitions:

A particular solution

$$(h): \quad h_0, h_1, h_2, \cdots, h_n, \cdots$$

of (9.1) will be said to belong to $\mathfrak{R}$ (to $\mathfrak{F}$) if all its terms belong to $\mathfrak{R}$ (to $\mathfrak{F}$). If a and b belong to $\mathfrak{R}$, we say that a divides b in $\mathfrak{R}$ if there exists an element c of $\mathfrak{R}$ such that $ac = b$. We write: $a \mid b\ (\mathfrak{R})$.

In particular, if $\mathfrak{R}$ is a field, and $b \neq 0$, $a \mid b\ (\mathfrak{R})$ for every $a \neq 0$.

If $\mathfrak{m}$ is an ideal of $\mathfrak{R}$, $a \equiv b\ (\mathfrak{m})$ means as usual $a - b$ is contained in $\mathfrak{m}$.

If $\mathfrak{p}$ is a maximal ideal of $\mathfrak{R}$, the quotient ring $\mathfrak{R}/\mathfrak{p}$ is a field. If this field is finite its order is a power of a certain rational prime p. We denote the order by $N\mathfrak{p} = p^f$ and call p the (rational) prime belonging to $\mathfrak{p}$.

Definition 9.1. *A solution of* (9.1) *is said to be "regular over* $\mathfrak{F}$*" if it belongs to* $\mathfrak{F}$ *and if*

$$h_0 = 0, \qquad h_1 = 1, \qquad h_2, h_3 \text{ not both zero.} \tag{9.2}$$

Definition 9.2. *A solution* (h) *of* (9.1) *is said to be "a divisibility sequence over* $\mathfrak{R}$*" if it belongs to* $\mathfrak{R}$ *and if*

$$h_r \mid h_s\ (\mathfrak{R}) \qquad \text{whenever } r \mid s. \tag{9.3}$$

Let (h) belong to $\mathfrak{R}$, and let $\mathfrak{m}$ be an ideal of $\mathfrak{R}$. $\mathfrak{m}$ 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 $\mathfrak{m}$ in (h). If in addition $h_r \not\equiv 0 \pmod{\mathfrak{m}}$ for every proper divisor r of n_0, then n_0 is called a rank of apparition of $\mathfrak{m}$ 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 $\mathfrak{R}$ 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) (h) *is a regular solution of* (9.1) *over* $\mathfrak{F}$,

(10.2) h_2, h_3 *and* h_4 *belong to* $\mathfrak{R}$,

(10.3) $h_2 \mid h_4\ (\mathfrak{R})$.

Then (h) *is a divisibility sequence over* $\mathfrak{R}$ *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) $$h_n = P_n(h_2, h_3, h_4),$$

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) $$P_n(a^3h_2, a^8h_3, a^{15}h_4) = a^{n^2-1}P_n(h_2, h_3, h_4).$$

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*

$$l_n = a^{n^2-1}k_n, \qquad (n = 0, 1, 2, \cdots).$$

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* $\mathfrak{R}$ *satisfying conditions* (10.1), (10.2) *and* (10.3) *such that*

$$k_n = a^{n^2-1}h_n, \qquad (n = 0, 1, 2, \cdots).$$

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* $\mathfrak{R}$ *with* $h_0 = 0$ *and* $h_1 = 1$ *(but not necessarily a regular solution). Then if* (h) *is a divisibility sequence over* $\mathfrak{R}$ *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* $\mathfrak{R}$, *and let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{R}$ *whose quotient ring* $\mathfrak{R}/\mathfrak{p}$ *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*

$$h_n = K_{1n}(u_0)/K_{11}(u_0) = K_{1n}/K_{11} \qquad (n = 0, 1, 2, \cdots) \tag{11.1}$$

then the sequence (h) *is a solution of the functional equation*

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega^2_n - \omega_{n+1}\omega_{n-1}\omega^2_m \tag{9.1}$$

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

$$K^2_{1l}K_{1m+n}K_{1m-n} + K^2_{1m}K_{1n+l}K_{1n-l} + K^2_{1n}K_{1l+m}K_{1l-m} = 0.$$

Now $K_{11} = snu_0 \neq 0$. Hence on letting $l = 1$ and dividing by K^4_{11}, we obtain from (11.1) the formula

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h^2_n - h_{n+1}h_{n-1}h^2_m;$$

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 $\mathfrak{R}_1$ be the ring of integers of $\mathfrak{F}_1$. Let $\mathfrak{F}$ be the field $F[x_0^{\frac{1}{2}}, 1-x_0^{\frac{1}{2}}, 1-a_0x_0^{\frac{1}{2}}]$, and $\mathfrak{R}$ the ring of integers of $\mathfrak{F}$. Clearly $\mathfrak{R} \supseteq \mathfrak{R}_1$, $\mathfrak{F} \supseteq \mathfrak{F}_1$, and every ideal of either ring has a finite norm. We shall use German letters to denote either ideals of $\mathfrak{R}$ or of $\mathfrak{R}_1$, 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 $\mathfrak{R}_1$ while the four sequences (K_α), $(\alpha = 0, 1, 2, 3)$ belong to $\mathfrak{R}$.

Let u_0 be chosen in a period parallelogram so that [5]

$$snu_0 = (x_0)^{\frac{1}{2}}.$$

Then

$$h_n = \begin{cases} B_n(x_0, a_0), & n \text{ odd}, \\ ((1-x_0)(1-a_0x_0))^{\frac{1}{2}} B_n(x_0, a_0), & n \text{ even}. \end{cases} \tag{11.2}$$

Hence the initial values of (h) are

$$h_0 = 0, \quad h_1 = 1, \quad h_2 = 2((1-x_0)(1-a_0x_0))^{\frac{1}{2}},$$
$$h_3 = B_3(x_0, a_0), \quad h_4 = ((1-x_0)(1-a_0x_0))^{\frac{1}{2}} B_4(x_0, a_0).$$

Now by direct calculation or from Table III,

$$B_3(1; a_0) = -(1-a_0)^2, \quad B_3(1/a_0; a_0) = -(1-a_0/a_0^2)^2. \tag{11.3}$$

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 $h_2 \mid h_4\ (\mathfrak{R})$.

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*

$$h_n = B_n(x_0; a_0), \ n \text{ odd}; \qquad = ((1-x_0)(1-a_0x_0))^{\frac{1}{2}} B_n(x_0; a_0), \ n \text{ even} \tag{11.2}$$

is an elliptic divisibility sequence over the ring $\mathfrak{R}$. Every prime ideal $\mathfrak{p}$ of $\mathfrak{R}$ 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

$$h_n \equiv 0 \pmod{\mathfrak{p}} \quad \text{if and only if } n \equiv 0 \pmod{\rho}. \tag{11.4}$$

[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

$$B_3(x_0; a_0) \equiv 0 \pmod{\mathfrak{p}}, \tag{12.1}$$

$$((1-x_0)(1-a_0x_0))^{\frac{1}{2}} B_4(x_0; a_0) \equiv 0 \pmod{\mathfrak{p}}.$$

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 $\mathfrak{R}_1/\mathfrak{p}$. 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 $3 - 4x_0 \equiv 4 - 8x_0 \equiv 0 \bmod \mathfrak{p})$ are impossible.

If $a_0 \equiv 1 \pmod{\mathfrak{p}}$, *then* $x_0 \equiv 1 \pmod{\mathfrak{p}}$. For by Tables IV and V,

$$\left.\begin{aligned} B_3(x_0, a_0) &\equiv (1-x_0)^3(3-x_0) \\ B_4(x_0, a_0) &\equiv 4(1-x_0)^5(1+x_0) \end{aligned}\right\} \pmod{\mathfrak{p}}$$

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*

$$a_0 \equiv 1 \text{ and } x_0 \equiv 1 \pmod{\mathfrak{p}} \text{ or}$$
$$2 \equiv 0 \text{ and } a_0x_0^2 \equiv 1 \pmod{\mathfrak{p}} \text{ but}$$
$$a_0 \not\equiv 1 \text{ and } x_0 \not\equiv 1 \pmod{\mathfrak{p}}.$$

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 $\mathfrak{R}$ and $\mathfrak{R}_1$ 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; $\cdots$, C_n, D_n are always null divisors of the sequence (B).*

Proof. Suppose, for example, that for a certain fixed value of n

$$A_n \equiv 0 \pmod{\mathfrak{p}} \text{ and } B_n \equiv 0 \pmod{\mathfrak{p}}, \qquad \mathfrak{p} \text{ regular.}$$

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),

$$K_{12n} \equiv K_{11}K_{12n+1} \equiv 0 \pmod{\mathfrak{p}}$$

so that $K_{11}h_{2n} \equiv K^2{}_{11}h_{2n+1} \equiv 0 \pmod{\mathfrak{p}}$ by formula (11.1). But $K^2{}_{11} = sn^2u_0 = x_0 \not\equiv 0 \pmod{\mathfrak{p}}$. 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,

$$(14.1) \qquad B_n \equiv 0 \pmod{\mathfrak{p}} \qquad \text{if and only if } n \equiv 0 \pmod{\rho},$$

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 $A_k \equiv 0 \pmod{\mathfrak{p}}$. Now by the duplication formula (5.4),

$$K_{2k} \equiv 2K_{0k}K_{1k}K_{2k}K_{3k}. \tag{14.2}$$

Hence by the preceding remarks, $B_{2k} \equiv 0 \pmod{\mathfrak{p}}$ so that $\rho \mid 2k$ by (14.1). Therefore $\rho \mid k$ so that $A_k \equiv B_k \equiv 0 \pmod{\mathfrak{p}}$ contrary to Theorem 13.1. In like manner, $\mathfrak{p}$ cannot be a divisor of (C) or (D).

THEOREM 14.2. *Let $\mathfrak{p}$ be a regular prime ideal of even rank of apparition in (B). Then $\mathfrak{p}$ is a divisor of precisely one of the three sequences (A), (C) and (D). If $\mathfrak{p}$ is a divisor of (C), then $C_n \equiv 0 \pmod{\mathfrak{p}}$ if and only if n is an odd multiple of $\rho/2$, with similar results if $\mathfrak{p}$ is a divisor of (A) or (D).*

Proof. Let $\mathfrak{p}$ and ρ satisfy the hypothesis of the theorem. Then by the duplication formula (5.4)

$$K_{1\rho} \equiv 2K_{0(\rho/2)}K_{1(\rho/2)}K_{2(\rho/)}K_{3(\rho/2)} \pmod{\mathfrak{p}}.$$

Hence since $B_\rho \equiv 0 \pmod{\mathfrak{p}}$ and $\mathfrak{p}$ is regular, precisely one of $A_{\rho/2}$, $B_{\rho/2}$, $C_{\rho/2}$, $D_{\rho/2}$ is divisible by $\mathfrak{p}$. Evidently, $B_{\rho/2} \not\equiv 0 \pmod{\mathfrak{p}}$. Assume that $C_{\rho/2} \equiv 0 \pmod{\mathfrak{p}}$ so that $\mathfrak{p}$ is a divisor of (C). Then $\mathfrak{p}$ is not a divisor of (A) or (D). For if for example $D_k \equiv 0 \pmod{\mathfrak{p}}$, then by the duplication formula (14.2), $B_{2k} \equiv 0 \pmod{\mathfrak{p}}$. Hence $\rho \mid 2k$, $\rho/2 \mid k$ and $B_k \equiv 0 \pmod{\mathfrak{p}}$ contrary to Theorem 13.1. In precisely the same way we can show that $A_k \not\equiv 0 \pmod{\mathfrak{p}}$, and that if $C_k \equiv 0 \pmod{\mathfrak{p}}$, then k must be an odd multiple of $\rho/2$. 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 $\rho/2$. Then $2k$ is a multiple of ρ. Hence by (14.1) and (14.2)

$$0 \equiv 2A_kB_kC_kD_k \pmod{\mathfrak{p}}.$$

Now either B_k or C_k must be divisible by $\mathfrak{p}$ but not both, by what we have already proved. If k is an even multiple of $\rho/2$, it is a multiple of ρ, so that $B_k \equiv 0$ and $C_k \not\equiv 0 \pmod{\mathfrak{p}}$. But if k is an odd multiple of $\rho/2$, it is not a multiple of ρ. Consequently, $B_k \not\equiv 0 \pmod{\mathfrak{p}}$, so that $C_k \equiv 0 \pmod{\mathfrak{p}}$, 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 $\mathfrak{p}$ is a prime ideal dividing a_0 say, we have $A_n(x; a_0) \equiv A_n(x; 0) \pmod{\mathfrak{p}}$. Consequently the arithmetical behavior of the sequences modulo $\mathfrak{p}$ is given immediately by the algebraic behavior of the elliptic polynomials in the following five singular cases:

(15.1) (i) $a=0$; (ii) $a=1$; (iii) $x=0$; (iv) $x=1$; (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

$$U_n=U_n(x)=(\alpha^n-\beta^n)/(\alpha-\beta) \qquad V_n=V_n(x)=\alpha^n+\beta^n$$

are the Lucas functions of the quadratic equation $t^2-2t\sqrt{1-x}+1$ where

(15.2) $$x=\sin^2 u,$$

then we readily find that

$$\begin{aligned}
&A_n(x;0)=D_n(x;0)=1;\\
&B_n(x;0)=\sin nu/\sin u=U_n(x), && n \text{ odd},\\
&\quad =sin\ nu/(\sin u\cos u)=2U_n(x)/V_1(x), && n \text{ even};\\
&C_n(x;0)=\cos nu/\cos u=V_n(x)/V_1(x), && n \text{ odd}\\
&\quad \cos nu=V_n(x)/2, && n \text{ even}.
\end{aligned}$$

We thus obtain the following theorem:

THEOREM 15.1. *If* $\mathfrak{p}$ *is a prime ideal of the first category dividing* a_0, *then*

$$\begin{aligned}
&A_n\equiv D_n\equiv 1 \pmod{\mathfrak{p}}\\
&B_n\equiv U_n, \quad n \text{ odd}; \quad \equiv 2U_n/V_1, \quad n \text{ even};\\
&C_n\equiv V_n/V_1, \quad n \text{ odd}; \quad \equiv \tfrac{1}{2}V_n, \quad n \text{ even}.
\end{aligned}$$

Here $U_n=U_n(x_0)$ *and* $V_n\equiv V_n(x_0)$ *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),

$$\begin{aligned} A_n(x;1) &= \sec r^{n^2} \cos nr = (2/V_1)^{n^2} V_n/2 \,^{6} \\ &= \sec r^{n^2-3}(\sin nr/\sin r) = (2/V_1)^{n^2-3} U_n, && n \text{ even} \\ B_n(x;1) &= \sec r^{n^2-1}(\sin nr/\sin r) = (2/V_1)^{n^2-1} U_n, && n \text{ odd} \\ C_n(x;1) &= D_n(x;1) = \sec r^{2an} = (2/V_1)^{2an}. \end{aligned}$$

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*

$$A_n \equiv (2/V_1)^{n^2} V_n/2);$$

$$B_n \equiv \begin{cases} (2/V_1)^{n^2-1} U_n, & n \text{ odd}, \\ (2/V_1)^{n^2-3} U_n, & n \text{ even}; \end{cases}$$

$$C_n \equiv D_n \equiv \begin{cases} (2/V_1)^{n^2-1}, & n \text{ odd}, \\ (2/V_1)^{n^2}, & n \text{ even}. \end{cases}$$

Here $U_n = U_n(x_0/(x-1))$, $V_n = V_n(x_0/(x_0-1))$ 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 $x = -\tan^2 r$.

	n odd	n 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* $1 - a_0 x_0 \equiv 0 \pmod{\mathfrak{p}}$. *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 preceeding 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 $\mathfrak{F}_1$ are precisely the same as for the field $\mathfrak{F}$. 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 $l \leqq k$, the rank of apparition of p^l in (B) is 2ρ, and if $l \geqq k$, 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 $l \leqq k$ or $l \geqq k$. Furthermore $D_n \equiv 0 \bmod p^l$ 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.