# MEMOIR ON ELLIPTIC DIVISIBILITY SEQUENCES.*

By MORGAN WARD.

## I. Introduction.

**1.** By an elliptic divisibility sequence we mean a sequence of integers,

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

which is a particular solution of

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2 \tag{1.1}$$

and such that $h_n$ divides $h_m$ whenever $n$ divides $m$. Simple instances of such sequences are:

$$h_n = n; \tag{1.2}$$

$$h_n = (n/3) \tag{1.3}$$

where $(n/p)$ is Legendre's symbol;

$$h_n = (-8/n) \tag{1.4}$$

where $(d/n)$ is Kronecker's symbol.[2]

$$h_n = Q^{(1/2)-(n/2)}U_n \tag{1.5}$$

where $P = a + b$, $Q = ab$ and

$$U_n = (a^n - b^n)/(a - b) \tag{1.6}$$

is a polynomial in $P$ and $Q$ satisfying a linear recurrence of order two. This polynomial is one of the two[3] 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 $(-8/n) = (-1)^{[n/4]}$ if $n$ is odd, where $[n/4]$ 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-linear[5] 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] $\omega_n = \sigma(nu)/\sigma(u)n^2$ 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 $\rho$, and $(h)$ is periodic modulo $p$ with period $\rho\tau$ where $\tau$ 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 $U_0, U_1, U_2, \cdots$ 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 arithmetrical 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 $a, b, \cdots$ are integers or ideals, $a \mid b$ for "$a$ divides $b$" and $(a, b, \cdots)$ for the greatest common divisor of $a, b, \cdots$. We denote the least common multiple of $a, b, \cdots$ by $[a, b, \cdots]$.

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, $\rho$ is the "restricted period" of $(h)$ modulo $p$. See Carmichael [1].

[11] Typical examples are given by the residues of the Fibonacci sequence $0, 1, 1, 2, 3, \cdots$ 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:

$$h_0 = 0,\ h_1 = 1;\ \text{not both } h_2 \text{ and } h_3 \text{ zero.} \tag{4.1}$$

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*

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqq n \geqq 1. \tag{4.11}$$

*Then* $(h)$ *is an elliptic divisibility sequence if and only if*

$$h_2, h_3 \text{ and } h_4 \text{ are integers;} \tag{4.2}$$

$$h_2 \text{ divides } h_4. \tag{4.3}$$

*Furthermore, the sequence* $(h)$ *is uniquely determined by the three initial values* $h_2$, $h_3$ *and* $h_4$.

*Proof.* Assume first that

$$h_2 \neq 0. \tag{4.31}$$

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

$$h_r \text{ divides } h_s \text{ if } r \text{ divides } s. \tag{4.4}$$

A third and final induction shows that if $n$ is greater than four, $h_n$ is uniquely determined if $h_0, h_1, \cdots, h_{n-1}$ 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]

$$h_{2n+1} = h_{n+2}h^3_n - h_{n-1}h^3_{n+1}, \qquad n \geqq 1. \tag{4.5}$$

$$h_{2n}h_2 = h_n(h_{n+2}h^2_{n-1} - h_{n-2}h^2_{n+1}), \qquad n \geqq 2. \tag{4.6}$$

We begin the first induction by assuming that

($\alpha$) $h_0, h_1, \cdots, h_{n-1}$ *are integers*;

($\beta$) $h_2$ *divides* $h_{2r}$, $2r < n$; $n \geqq 5$.

If $n$ is odd, say $n = 2k+1$, we conclude from ($\alpha$) and (4.5) with $n = k$ that $h_n$ is an integer. If $n$ is even, say $n = 2k$, then $k \geqq 3$ and (4.6) gives

$$h_n h_2 = h_k(h_{k+2}h^2_{k-1} - h_{k-2}h^2_{k+1}). \tag{4.7}$$

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

($\gamma$) $h_r \mid h_s$ provided that $r \mid s$ for $r \leqq s < n$.

We observe that ($\gamma$) is true if $n \leqq 5$. Hence we may assume that $n > 5$. Now consider $h_n$, and suppose that $n = uv$. We wish to show that $h_u \mid h_{uv}$ and it is evidently allowable to assume that $u \geqq 2$ and $v \geqq 2$.

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 ($\gamma$), $h_u \mid h_{uv/2}$. Hence $h_u \mid h_v$.

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 ($\gamma$) that the right side of this expression is divisible by $h^2_u$. Hence since $h_u \neq 0$, $h_u \mid h_{uv}$.

---

[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 $(\gamma)$. 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, $h_3 = h_4 = h_5 \cdots = h_{uv} = 0$. Hence in all cases, $h_u$ divides $h_{uv}$. (4.4) now follows by induction on $n$ in $(\gamma)$.

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]

$$h_n = \begin{cases} 0, & n \text{ even}; \\ (-1)^{[n/4]} h_3^{(n^2-1)/8}, & n \text{ odd}, \ h_3 \neq 0. \end{cases} \tag{23.4}$$

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 $r \geqq 3$, 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 $2 \leqq k \leqq r - 2$ and by the minimal property of $r$,

$$h_{k-1}h_{k+1} \neq 0. \tag{4.8}$$

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

$$h_r = 0, \quad h_{r+1} = 0, \quad h_n \neq 0, \qquad 0 < n < r. \tag{4. 9}$$

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 $\geqq 0$. 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 $n \geqq 3$. 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 $h_\rho$ but does not divide $h_r$ if $r$ divides $\rho$, then $\rho$ 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 $h_1, h_2, \cdots, h_{p+1}, h_{p+2}$ is divisible by $p$, each of the $p$ numbers

$$\frac{h_{r-1} h_{r+1}}{h_r{}^2}, \qquad (r = 2, 3, \cdots, p + 1)$$

is congruent modulo $p$ to one of the numbers $1, 2, \cdots, p - 1$. 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 $2 \leqq n < m \leqq p + 1$ 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 $\rho$ be its smallest rank of apparition. Then if*

$$h_{\rho+1} \not\equiv 0 \pmod{p}, \tag{5.1}$$

$$h_n \equiv 0 \pmod{p} \text{ if and only if } n \equiv 0 \pmod{\rho}. \tag{5.2}$$

*Proof.* By the definition of $\rho$,

$$h_\rho \equiv 0 \pmod{p}, \quad h_r \not\equiv 0 \pmod{p}, \quad 0 < r < \rho. \tag{5.3}$$

Since $(h)$ is a divisibility sequence $h_\rho$ divides $h_n$ if $\rho$ 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 $k \geqq \rho + 2$. 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 $\rho$ and let the quotient be $q$ and the remainder $r$:

$$k = q\rho + r, \quad 0 \leqq r < \rho. \tag{5.4}$$

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

$$h_{q\rho+1} h_{q\rho-1} h^2_r \equiv 0 \pmod{p}.$$

Now $q\rho - 1 < k$ and $q\rho - 1$ is not divisible by $\rho$. 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 $0 < (q-1)\rho - 1 < (q-1)\rho + 1 < q\rho + 1 \leqq k$, $h_{(q-1)\rho-1}$, 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 $\rho$ be its smallest rank of apparition. If*

$$h_{\rho+1} \equiv 0 \pmod{p} \tag{6.1}$$

*then $\rho \leqq 3$ and*

$$h_n \equiv 0 \pmod{p}, \qquad n \geqq \rho. \tag{6.2}$$

*Proof.* By definition of $\rho$,

$$h_\rho \equiv 0 \pmod{p}, \qquad h_r \not\equiv 0 \pmod{p}, \qquad 0 < r < \rho. \tag{6.3}$$

We shall show first that the assumption

$$\rho > 3 \tag{6.4}$$

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 $\geqq 0$ 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 $h_{\rho-3} h^3_{\rho-1} \equiv 0 \pmod{p}$. Since $p$ is a prime, either $h_{\rho-1}$ or $h_{\rho-3}$ is divisible by $p$ contrary to (6.3). Hence $\rho \leqq 3$. If $\rho = 2$, $h_{2n} \equiv 0 \pmod{p}$ since $h_2$ divides $h_{2n}$. Since $h_3 = 0$ by (6.1), $h_5 \equiv 0$ by (4.5) 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 $n \geqq \rho$.

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 $n \geqq 3$. 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 $\pi$ such that

$$s_{n+\pi} \equiv s_n \pmod{m} \tag{7.1}$$

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 $\pi$ 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 $\rho$ is greater than three. Let $e$ be an integral solution of the congruence*

$$e \equiv h_2/h_{\rho-2} \pmod{p}, \tag{11.1}$$

*and let $\epsilon$ and $\kappa$ be the exponents to which $e$ and $h_{\rho-1}$ respectively belong* modulo $p$. *Then $(h)$ is purely periodic* modulo $p$, *and its period $\pi$ is given by the formula $\pi = \pi\rho$ where*

$$\tau = 2^{\alpha}[\epsilon, \kappa]. \tag{7.11}$$

---

[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* $\epsilon$ *and* $\kappa$ *and the exponent* $\alpha$ *is determined as follows*:

$\alpha = +1$ *if and only if* $\epsilon$, $\kappa$ *are both odd,*

$\alpha = -1$ *if and only if* $\epsilon$, $\kappa$ *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

| | Residues of $h_i$ modulo two | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Type Number | $h_0$ | $h_1$ | $h_2$ | $h_3$ | $h_4$ | $h_5$ | Rank $\rho$ | Period $\pi$ |
| 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 $\rho$ 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 $\rho$ is greater than three, $\epsilon$ and $\kappa$ 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 $\epsilon$ | $\kappa$ | $\tau$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 $h_{\rho-n} \equiv -h_n \pmod 3$. For type 15, $h_{\rho-n} \equiv h_n \pmod 3$; $h_{\rho+n} \equiv h_{\rho-n} \pmod 3$. 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"

$$h_2 h_3 \not\equiv 0 \pmod{p}, \tag{7.2}$$

two special cases:

$$h_2 \equiv 0 \pmod{p}, \qquad h_3 \not\equiv 0 \pmod{p}; \tag{7.3}$$

$$h_3 \equiv 0 \pmod{p}, \qquad h_2 \not\equiv 0 \pmod{p}. \tag{7.4}$$

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*

$$h_{2n} \equiv 0 \pmod{p}, \qquad h_{2n+1} \equiv (-1)^{[n/4]} h_3^{(n^2-1)/8} \pmod{p}.$$

*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 three*[19] *which divides neither $h_2$ nor $h_3$. Then if $\rho$ is its rank of apparition their exist two integers $a$ and $b$ such that*

$$h_{\rho-n} \equiv a^n b h_n \pmod{p}, \qquad (n = 0, 1, 2, \cdots, \rho). \tag{8.1}$$

If we calculate successively the least positive residues modulo $p$ of the first $\rho$ 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 $\rho$ 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*

$$ac \equiv 1 \pmod{p} \tag{8.2}$$

*then the following congruences hold* modulo $p$:

$$a \equiv h_{\rho-2}/h_2 h_{\rho-1}; \quad b \equiv h_2 h^2_{\rho-1}/h_{\rho-2}; \quad b \equiv h_{\rho-1} c. \tag{8.3}$$

$$a^\rho b^2 \equiv 1; \quad c^\rho \equiv b^2. \tag{8.4}$$

$$a^2 \equiv -h_{\rho-1}/h_{\rho+1}; \quad b^2 \equiv -h_{\rho+1} h_{\rho-1}. \tag{8.5}$$

*Proof.* Let $n$ successively equal 1 and $\rho - 1$, in (8.1). We obtain:

$$h_{\rho-1} \equiv ab \pmod{p} \tag{8.6}$$

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

$$h_{\rho-2} \equiv a^2 b h_2 \equiv a h_{\rho-1} h_2 \pmod{p},$$

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 $\rho$ is odd:

$$\rho = 2\sigma + 1 \geqq 5. \tag{8.7}$$

Then on putting $n$ equal to $\sigma + 1$ and $\sigma$ in (4.6), we obtain

$$h_{\rho+1} = h_{\sigma+1} h_{\sigma+3} h^2_\sigma - h_{\sigma+1} h_{\sigma-1} h^2_{\sigma+2}, \tag{8.8}$$

$$h_{\rho-1} = h_\sigma h_{\sigma+2} h^2_{\sigma-1} - h_\sigma h_{\sigma-2} h^2_{\sigma+1}. \tag{8.9}$$

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

$$h_{\rho+1} \equiv -a^{2\rho-2}b^4 h_{\rho-1} \pmod{p}. \tag{8.10}$$

When $\rho$ 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* $n$:

$$h_{\rho+n} \equiv -bc^n h_n \pmod{p}. \tag{9.1}$$

*Proof.* Assume first that $0 \leqq n \leqq \rho$. 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 $h_\rho$, we obtain from (8.5) the congruence $h_{\rho+n}h_{\rho-n} \equiv -b^2h_n^2 \pmod{p}$ or by (8.1), $h_{\rho+n}a^nbh_n \equiv -b^2h_n^2 \pmod{p}$. 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* $0 \leqq n \leqq k\rho$ *if* $k$ *equals one.*

We now proceed by induction on $k$. Suppose that (9.1) is true for $0 \leqq n \leqq k\rho$ and assume that $k\rho \leqq n \leqq (k+1)\rho$. 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 $h_\rho$, we obtain from (8.5) the congruence

$$h_{n+\rho}h_{n-\rho} \equiv b^2h_n^2 \pmod{p}. \tag{9.2}$$

Now $0 \leqq n - \rho \leqq k\rho$. Hence by the hypothesis of the induction,

$$h_{n-\rho} \equiv -(a^{n-\rho}/b)h_n \pmod{p}. \tag{9.3}$$

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 $a^nc^n \equiv 1$ 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 $0 \leqq n \leqq \rho$, the induction is completed.

THEOREM 9.2. *Under the hypothesis of Lemma* (9.1),

$$h_{k\rho+n} \equiv (-1)^k c^{kn} b^{k^2} h_n \pmod{p}, \qquad (k, n = 0, 1, 2, \cdots). \tag{9.5}$$

*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 $\rho$ be the rank of apparition of $p$ in $(h)$, and let $\tau$ be the least positive integer such that*

$$(-b)^{\tau^2} \equiv 1, \qquad c^\tau \equiv 1 \pmod{p} \tag{10.1}$$

*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 $\tau$ is defined as in Theorem* 10.1 *and if $k$ is an integer such that*

$$(-b)^{k^2} \equiv 1, \qquad c^k \equiv 1 \pmod{p} \tag{10.2}$$

*then $\tau$ 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 $\pi$ of $(h)$ modulo $p$ is a multiple of $\rho$; 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

$$(-c)^k b^{k^2} \equiv 1, \qquad (-c)^k c^k b^{k^2} \equiv 1 \pmod{p}.$$

Since $k$ and $k^2$ have the same parity, (10.2) follows. Hence, $\tau$ divides $k$, so that $\tau\rho$ divides $\pi$. 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 $\tau$ 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 $\delta$* modulo $p$. *Then if $\delta$ is odd, there exists no integer $x$ such that the congruence*

$$d^x \equiv -1 \pmod{p} \tag{11.2}$$

*is satisfied. But if $\delta$ is even,* (11.2) *is satisfied if and only if $x$ is an odd multiple of $\delta$.*

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

$$b^\tau \equiv +1 \pmod{p}. \tag{11.3}$$

Then by (10.1), $(-b)^{\tau^2} \equiv (-1)^\tau \equiv 1 \pmod{p}$. Hence $\tau$ *must be even.* Now by (8.3), $b^\tau \equiv h^\tau_{\rho-1} c^\tau$. Since $c^\tau \equiv 1$ by (10.1), (11.3) gives

$$h^\tau_{\rho-1} \equiv 1 \pmod{p}. \tag{11.4}$$

Then by (11.1), (10.1),

$$e^\tau \equiv 1 \pmod{p}. \tag{11.5}$$

Let $\sigma = [\epsilon, \kappa]$ be the least common multiple of the exponents to which $e$ and $h_{\rho-1}$ belong modulo $p$. Then (11.4) and (11.5) imply that $\kappa \mid \tau$, $\epsilon \mid \tau$. Hence

$$\sigma \mid \tau. \tag{11.6}$$

On the other hand, $h^\sigma_{\rho-1} \equiv 1$ and $e^\sigma \equiv 1 \pmod{p}$. Hence by (11.1) and (8.3),

$$c^\sigma \equiv 1, \qquad b^\sigma \equiv 1 \pmod{p}. \tag{11.7}$$

Now if $\sigma$ 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), $\tau = \sigma$.

$\sigma$ is odd if and only if both $\epsilon$ and $\kappa$ are odd. In this case (11.7) implies that $c^{2\sigma} \equiv 1$, $(-b)^{4\sigma^2} \equiv 1 \pmod{p}$. Hence by Lemma 10.1, $\tau \mid 2\sigma$. But $\tau$ is even and by (11.6), $\sigma$ divides $\tau$. Hence $\tau = 2\sigma$. This disposes of the first case of the theorem.

Assume now that

$$b^\tau \equiv -1 \pmod{p}. \tag{11.8}$$

Then by (8.3),

[22] The lemma is false if $p = 2$.

$$h^{\tau}{}_{\rho-1} \equiv -1 \pmod{p}, \tag{11.9}$$

and by (8.3) and (11.1)

$$e^{\tau} \equiv -1 \pmod{p}. \tag{11.10}$$

Now by Lemma 11.1, (11.9) and (11.10) imply that both $\kappa$ and $\epsilon$ are even, and that $\tau$ is both an odd multiple of $\kappa/2$ and an odd multiple of $\epsilon/2$. But if $\sigma$ now denotes $[\epsilon/2, \kappa/2]$,

$$\sigma \mid \tau. \tag{11.11}$$

Hence $\sigma$ must be an odd multiple of both $\epsilon/2$ and $\kappa/2$. It follows that if (11.8) holds, both $\epsilon$ and $\kappa$ must be even and both divisible by precisely the same power of two.

Assume, conversely, that the last mentioned conditions are satisfied. Then $\sigma$ is an odd multiple of both $\epsilon/2$ and $\kappa/2$, so that by Lemma 11.1

$$h^{\sigma}{}_{\rho-1} \equiv -1, \qquad e^{\sigma} \equiv -1 \pmod{p}.$$

But then by (11.1), (8.3) and (8.8)

$$c^{\sigma} \equiv 1, \qquad b^{\sigma} \equiv -1 \pmod{p}.$$

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 divisibilty 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

$$h_0 = 0, \qquad h_1 = 1, \qquad h_2 h_3 \neq 0; \qquad h_2 \mid h_4. \tag{12.0}$$

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 $\wp(w; g_2, g_3)$ is the Weierstrass function with invariants $g_2$ and $g_3$, then*

$$h_n = \psi_n(u) = \sigma(nu)/\sigma(u)^{n^2}. \tag{12.1}$$

*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) $\quad (\alpha): \psi_2(u) = h_2;\ (\beta): \psi_3(u) = h_3;\ (\gamma): \psi_4(u) = h_4.$

We quote for reference eight familiar formulas of elliptic function theory:

(12.3) $\quad \psi_2(w) = -\wp'(w).$

(12.4) $\quad \psi_3(w)\ 3\wp^4(w) - \tfrac{3}{2}g_2\wp^2(w) - 3g_3\wp(w) - \tfrac{1}{16}g_2^2.$

(12.5) $\quad \wp(2w) - \wp(w) = \tfrac{1}{4}\left(\dfrac{\wp''(w)}{\wp'(w)}\right)^2 - 3\wp(w)$

(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) $\quad \wp(2w) - \wp(w) = -\dfrac{\psi_1(w)\psi_3(w)}{\psi_2^2(w)}.$

(12.8) $\quad \wp(3w) - \wp(w) = -\dfrac{\psi_2(w)\psi_4(w)}{\psi_3^2(w)}.$

(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) $(\alpha)$, $(\beta)$, $(\gamma)$ 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 $\wp''(u)$:

$$(13.4)\quad \wp''(u) = (h_2^5 + h_4)/h_2h_3.$$

Next, using (13.2), (12.5) and (13.1), (13.4):

$$-h_3/h_2^2 = \tfrac{1}{4}\{(h_2^5 + h_4)/-h_2^2h_3\}^2 - 3\wp(u).$$

Hence solving for $\wp(u)$:

$$(13.5)\quad \wp(u) = (h_4^2 + 2h_2^5h_4 + 4h_2^2h_3^3 + h_2^{10}) \div 12h_2^4h_3^2.$$

Next, using (12.11), (13.5) and (13.4):

$$\begin{aligned}(13.6)\quad g_2 = {} & (h_2^{20} + 4h_2^{15}h_4 - 16h_2^{12}h_3^3 + 6h_2^{10}h_4^2 - 8h_2^7h_3^3h_4 \\ & + 4h_2^5h_4^3 + 16h_2^4h_3^6 + 8h_2^2h_3^3h_4^2 + h_4^4) \div 12h_2^8h_3^4.\end{aligned}$$

Finally, using (12.12), (13.5), (13.4) and (13.6):

$$\begin{aligned}(13.7)\quad g_3 = {} & -(h_2^{30} + 6h_2^{25}h_4 - 24h_2^{22}h_3^3 + 15h_2^{20}h_4^2 - 60h_2^{17}h_3^3h_4 \\ & + 20h_2^{15}h_4^3 + 120h_2^{14}h_3^6 - 36h_2^{12}h_3^3h_4^2 + 15h_2^{10}h_4^4 \\ & - 48h_2^9h_3^6h_4 + 12h_2^7h_3^3h_4^3 + 64h_2^6h_3^9 + 6h_2^5h_4^5 \\ & + 48h_2^4h_3^6h_4^2 + 12h_2^2h_3^3h_4^4 + h_4^6) \div 216h_2^{12}h_3^6.\end{aligned}$$

(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 $\wp(w)$.

On combining (13.5) and (13.6), we find that

$$g_2 - 12\wp^2(u) = -2(h_2^5 + h_4)/h_2h_3.$$

Hence (13.4) follows from formula (12.11).

Now combining (13.7) with (13.5), (13.4) and (13.6), we obtain the formula

$$g_3 - 2\wp(u)[\wp''(u) - 4\wp^2(u)] = -h_2^2.$$

Hence by formula (12.12), $\wp'^2(u) = h_2^2$. We now choose the sign of $u$ so that (13.1) is satisfied. $u$ is now fixed up to a period of the $\wp$ function. But then (12.2)$\alpha$ follows immediately from formula (12.3).

Next, using (12.5) and substituting in it for $\wp'(u)$, $\wp''(u)$ and $\wp(u)$ from (13.1), (13.4) and (13.5), we find that $\wp(2u) - \wp(u) = -h_3/h_2^2$.

Hence (12.2)$\beta$ 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 $\wp(3u) - \wp(u) = -h_2h_4/h_3^2$.

Hence (12.2)$\gamma$ follows from (12.8 and (12.2)$\alpha$ and $\beta$.

## 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 $\rho$ as heretofore.

It follows from the results of Part IV that

$$h_n = \psi_n(u). \tag{14.1}$$

Furthermore $g_2$, $g_3$ and $\wp(u)$ 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 signma function as follows:

$$\psi_n(w) = \sigma(nw)/\sigma(w)^{n^2}. \tag{14.2}$$

If $2\omega$ is a period of the $\wp$ function, then with the usual notations of the theory of elliptic functions,

$$\sigma(w + 2\omega) = -e^{2\eta(w+\omega)}\sigma(w). \tag{14.3}$$

On the other hand, if $z = \wp(w)$, $\psi_n(w)$ may be expressed as a polynomial in $z$, say $F_n(z)$, of the form

$$\psi_n(w) = F_n(z) = e_q \sum_{r=0}^{q} A_{q-r} z^r \tag{14.4}$$

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:

$$A_k = A_k(g_2/4, g_3), \qquad k = 0, 1, \cdots, q. \tag{14.5}$$

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.

$$(14.6) \qquad A_0 = n,$$

$$(14.7) \qquad A_1 = 0, \qquad A_2 = bg_2/4, \qquad A_3 = cg_3, \qquad A_4 = dg_2^2/16$$

where $b$, $c$, $d$ are integers depending of course on $n$.

It is also well known that if we consider the roots $\zeta$ of $F_r(z) = 0$ (where it will be recalled that $r$ is the rank of apparition of $p$ in $(h)$) then each $\zeta$ may be expressed in the form

$$(14.8) \qquad \zeta = \wp(2\omega/r)$$

where $2\omega$ is some period of the $p$ 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 $\zeta$ of $F_r(z) = 0$ are algebraic integers modulo $p$ and that we have the congruence

$$h_r \equiv c_r \prod_{(\zeta)} (\wp(u) - \zeta) \pmod{p}$$

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 $\mathfrak{R}$: $\Pi(\wp(u) - \zeta) \equiv 0 \pmod{\mathfrak{p}}$. Since $\mathfrak{p}$ is a prime ideal, there must exist by (14.8) a period $2\omega$ of the $\wp$ function such that

$$(15.1) \qquad \wp(u) \equiv \wp(2\omega/r) \pmod{\mathfrak{p}}.$$

We deduce from (14.4) and (14.1) that

$$(15.2) \qquad h_n \equiv \psi_n(2\omega/r) \pmod{\mathfrak{p}}$$

for $n = 0, 1, 2, \cdots$

Consider now $\psi_{r-n}(2\omega/r)$ where $0 \leqq n \leqq r$. 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 $\alpha = e^{4\eta\omega/r}\sigma(2\omega/r)^{2r}$, and $\beta = e^{2\eta\omega} \div \sigma(2\omega/r)^{r^2}$, and we have used the fact that $\sigma(-w) = -\sigma(w)$. (15.2) now gives the congruences

$$(15.3) \qquad h_{r-n} \equiv \alpha^n\beta h_n \pmod{\mathfrak{p}}.$$

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 $\alpha$ and $\beta$ 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 $\rho$, 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 appartition $r$ 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

$$A_k \equiv 0 \pmod{p}, \qquad k = 0, 1, \cdots, q = (p^2-1)/2.$$

Let $\mathfrak{F}$ 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, $e_i = \wp(\omega_i)$, $(i = 1, 2, 3)$ 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 $\mathfrak{F}$. Then by (14.2), (14.4) and our hypothesis on the $A_h$,

$$(16.1) \qquad \sigma(p\omega_i)/\sigma(\omega_i)^{p^2} = \psi_p(\omega_i) = e_q \sum_{r=0}^{q} A_{q-r} e_i^r \equiv 0 \pmod{p}.$$

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

$$e^{\frac{1}{2}\eta\omega_i} = (e_i - e_j)^{1/4}(e_i - e_k)^{1/4}\sigma(\omega_i).$$

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),

$$(e_i - e_j)^{(p^2-1)/4}(e_i - e_k)^{(p^2-1)/4} \equiv 0 \pmod{\mathfrak{p}}, \quad i,j,k = 1,2,3, i \neq j, i \neq k.$$

Since $\mathfrak{p}$ is a prime ideal, we deduce that $e_1 \equiv e_2 \equiv e_3 \pmod{\mathfrak{p}}$. But then for every integer $\xi$ of $\mathfrak{G}$, $4\xi^3 - g_2\xi - g_3 \equiv 4(\xi - e_1)^3 \pmod{\mathfrak{p}}$. Hence

$$e_1 \equiv e_2 \equiv e_3 \pmod{\mathfrak{p}} \text{ so that } g_2 \equiv g_3 \equiv 0 \pmod{\mathfrak{p}}.$$

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) $$h_r \equiv 0 \pmod{p}, \qquad r = p \text{ or } r = 2p;$$

(17.2) $g_2$ and $g_3$ not both divisible by $p$.

We first develop some simple arithmetical concepts which are needed in the proofs that follow. Let $\mathfrak{p}$ be a prime ideal of an algebraic number field, and $\alpha$ any field element. Then the principal ideal $[\alpha]$ has a unique representation of the form $[\alpha] = \mathfrak{p}^a\mathfrak{b}\mathfrak{c}^{-1}$ where $\mathfrak{b}$ and $\mathfrak{c}$ are integral ideals which are co-prime and also prime to $\mathfrak{p}$, and the exponent $a$ is a rational integer. We call $a$ "the index of $\alpha$ (modulo $p$)." $\alpha$ 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 $\alpha$ is a fraction modulo $p$ and $\beta$ is an integer modulo $\mathfrak{p}$, $\alpha \pm \beta$ is a fraction with the same index as $\alpha$, and the index of $\alpha\beta$ is not greater than that of $\alpha$.*

LEMMA 17.2. *If $\alpha_1, \alpha_2, \cdots, \alpha_k$ are fractions modulo $\mathfrak{p}$, the index of their product is the sum of the indices of the separate factors.*

LEMMA 17.3. *If $\alpha_1, \alpha_2, \cdots, \alpha_k$ are fractions modulo $\mathfrak{p}$, the index of $(\phi - \alpha_1)(\phi - \alpha_2)\cdots(\phi - \alpha_k)$ is the same for all $\phi$ which are integers modulo $\mathfrak{p}$, and equals the sum of the indices of $\alpha_1, \alpha_2, \cdots, \alpha_k$.*

**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 $\zeta_1, \zeta_2, \cdots, \zeta_q$. 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 $\mathfrak{R}$, not all the roots $\zeta$ are integers modulo $\mathfrak{p}$. We shall now prove

LEMMA 18.1. *Not all the roots $\zeta$ of $F_r(z) = 0$ are fractions modulo $\mathfrak{p}$.*

*Proof.* Let $\phi$ denote a variable whose range is the set of all field elements of $\mathfrak{R}$ which are integers modulo $\mathfrak{p}$. Then if all the $\zeta$ 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 $\phi$. But by formula (13.5), $z = \wp(u)$ is an admissible value of $\phi$, since $\mathfrak{p}$ is prime to $6h_2h_3$. But by formulas (14.1) and (14.4),

$$h_r = F_r(z) = pl(z - \zeta_1)(z - \zeta_2) \cdots (z - \zeta_q) \tag{18.1}$$

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 $\zeta_1, \zeta_2, \cdots, \zeta_s$ be the roots of $F_r(z) = 0$ which are integers modulo $\mathfrak{p}$, and $\zeta_{s+1}, \zeta_{s+2}, \cdots, \zeta_q$ 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 $z - \zeta_1, \cdots z - \zeta_s$ is an integer modulo $\mathfrak{p}$, there exists a $\zeta$ such that $\wp(u) = z \equiv \zeta \pmod{\mathfrak{p}}$. Hence we obtain again from (14.8) the congruence (15.1) for a suitably chosen period $2\omega$ of the $\wp$-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

$$u_n = c^{n^2-1} v_n, \qquad (n = 0, 1, 2, \cdots).$$

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 $\wp(w) = \wp(w; g_2, g_3)$ 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 $w$,

$$h_n = \sigma(nu)/\sigma(u)^{n^2}. \tag{19.1}$$

By the "discriminant" of the sequence $(h)$ we mean the discriminant of the corresponding $\wp$-function:

$$\Delta = g_2^3 - 27 g_3^2. \tag{19.2}$$

We write $\Delta = \Delta(h)$, or $\Delta = \Delta(h_2, h_3, h_4)$ if we wish to emphasize the dependence of $\Delta$ 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

$$\begin{aligned}\Delta(h_2, h_3, h_4) = 1/h_2^8 h_3^3 \{ & h_4^4 + 3h_2^5 h_4^3 + (3h_2^8 + 8h_3^3) h_4^2 \\ & + h_2^7 (h_2^8 - 20 h_3^3) h_4 + h_2^4 h_3^3 (16 h_3^3 - h_2^8) \}.\end{aligned} \tag{19.3}$$

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*

$$h_2 = r, \qquad h_3 = s(r^2 - s^3), \qquad h_4 = rs^3(r^2 - 2s^3). \tag{19.4}$$

**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

$$u = h_2^4, \qquad v = h_3^3, \qquad w = h_4/h_2, \tag{20.1}$$

then $\Delta$ vanishes if and only if the diophantine equation

$$16v^2 - (u^2 + 20uw - 8w^2)v + w(u + w)^3 = 0 \tag{20.2}$$

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

$$32v = u^2 + 20uw - 8w^2 \pm \sqrt{u(u - 8w)^3}. \tag{20.3}$$

Hence it is necessary that $u(u - 8w)$ be a square. But $u$ is a square by (20.1). Hence we may write

$$u = l^2 = h_2^4, \tag{20.4}$$

$$u - 8w = m^2 = h_2^4 - 8h_4/h_2, \tag{20.5}$$

where $l$ and $m$ are integers. Then

$$w = (l^2 - m^2)/8. \tag{20.6}$$

We find from (20.4) and (20.6) that

$$u^2 + 2uw - 8w^2 = \tfrac{1}{8}(27l^4 - 18l^2m^2 - m^4),$$
$$\sqrt{u(u - 8w)^3} = lm^3.$$

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

$$(8h_3)^3 = (2l \pm 2m)(3l \mp m)^3. \tag{20.7}$$

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 $q$

$$l \pm m = 4s^3, \qquad 3l \mp m = 4q, \tag{20.8}$$

and (20.7) becomes $(8h_3)^3 = (8sq)^3$. Hence

$$h_3 = sq \tag{20.9}$$

and on solving (20.8) for $l$ and $m$, we find that

$$l = s^3 + q, \qquad m = \pm (3s^3 - q). \tag{20.10}$$

On substituting these expressions for $l$ and $m$ into (20.6), we find that

$$h_4/h_2 = w = s^3(q - s^3). \tag{20.11}$$

Finally, (20.4) and (26.10) give

$$h_2^2 = s^3 + q. \tag{20.12}$$

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,

$$g_2 = 3\{(r^2 - 4s^3)/6s^2\}^2, \qquad g_3 = -\{(r^2 - 4s^3)/6s^2\}^3. \tag{20.13}$$

Now if $e$, $e_2$ and $e_3$ denote as usual the roots of

$$4z^3 - g_2 z - g_3 = 0, \tag{20.14}$$

then $\Delta = 0$ if and only if two or more of the roots $e_i$ are equal. Suppose that

$$\Delta = 0, \qquad e_1 = e_2. \tag{20.15}$$

Then

$$e_3 = -2e_1 \tag{20.16}$$

and

$$g_2 = 3e_3^2, \qquad g_3 = e_3^3. \tag{20.17}$$

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*

$$-(r^2 - 4s^3)/6s^2, \qquad (r^3 - 4s^3)/12s^2, \qquad (r^2 - 4s^3)/12s^2.$$

*Furthermore*

$$g_2 = g_3 = 0 \quad \text{if and only if } r^2 = 4s^3. \tag{20.18}$$

*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 $(\alpha)$ 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 $\beta$ 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 $\wp(w) = \wp(w; g_2, g_3)$ and $(k) = c(h)$ is any equivalent sequence, then $(k)$ admits an elliptic function representation by means of $\wp(w') = \wp(w'; g'_2, g'_3)$ where $w' = w/c$, $g'_2 = c^4 g_2$, $g'_3 = c^6 g_3$.*

Equivalence is thus the analogue of the $\wp$-function homogeneity relation: $\wp(w/c; c^4 g_2, c^6 g_3) = c^2 \wp(w; g_2, g_3)$.

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 $b_n = (c_2 a)^{n^2-1} a_n$.

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 $\wp(w)$ are rational numbers and if $u$ is such that $\wp(u)$ 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*

$$0, 1, 2, \cdots, n, \cdots \tag{22.1}$$

*of the positive integers or to a Lucas sequence*

$$U_0, U_1, U_2, \cdots, U_n, \cdots \tag{22.2}$$

*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 $\theta$, 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

$$r^2 = 4s^3 \tag{22.3}$$

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), $h_2 = c^3 2$, $h_3 = c^8 3$, $h_4 = c^{15} 4$.

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 $\alpha$ and $\beta$ 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*

$$q^{(1-n)/2}u_n \tag{22.4}$$

*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 $\alpha$ nor $\beta$ 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*

$$U_n = (a^n - b^n)/(a - b) \tag{22.5}$$

*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,

$$h_2 = r, \qquad h_3 = s(r^2 - s^3), \qquad h_4 = rs^3(r^2 - 2s^3) \tag{19.4}$$

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

$$P = r\sqrt{s}/s^2. \tag{22.6}$$

Then (19.4) becomes

$$h_2 = c^3P, \qquad h_3 = c^8(P^2-1), \qquad h_4 = c^{15}(P^2-2).$$

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

$$h_0 = 0, \qquad h_1 = 1, \qquad h_2 \neq 0, \qquad h_3 \neq 0 \tag{23.1}$$

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

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqq n \geqq 1. \tag{4.11}$$

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

$$h_0h_2 = 0, \qquad (h_1^2-1)h_{n+1}h_{n-1} = 0, \qquad n \geqq 1; \tag{23.2}$$

$$h_0h_{2n} = 0. \tag{23.3}$$

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 $m \geqq n \geqq 1$. 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 $\geqq 0$, 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* $n > 0$,

$$h_n = \begin{cases} 0 & n \text{ even} \\ (-1)^{[n/4]} h_3^{(n^2-1)/8} & n \text{ odd.} \end{cases} \tag{23.4}$$

*Proof.* It is easily verified that $[(2n+1)/4] \equiv n + 1 + n(n+1)/2 \pmod 2$. Hence an equivalent way of stating (23.4) is:

$$h_{2n} = 0, \quad h_{2n+1} = (-1)^{n+1}(-h_3)^{n(n+1)/2}, \quad (n = 1, 2, 3, \cdots). \tag{23.5}$$

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

$$h_{2n+2}h_{2n-2} = -h_1 h_3 h_{2n}, \qquad n \geqq 1. \tag{23.6}$$

$$h_{2n+1}h_{2n-5} = h_{2n-1}h_{2n-3}h_3^2, \qquad n \geqq 3. \tag{23.7}$$

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 $n \leqq 3$. 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

$$h_n = 0, \qquad n > 1 \tag{24.1}$$

is evidently a solution of (1.1) regardless of the values of $h_0$ and $h_1$. We shall therefore assume henceforth that

$$h_0 = 0, \qquad h_1 = 1, \qquad h_3 = 0. \tag{24.2}$$

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:

$$\lambda_n = \begin{cases} 0 & \text{if } n \not\equiv \pm 1 \pmod{l}; \\ 1 & \text{if } n \equiv +1 \pmod{l}; \\ -1 & \text{if } n \equiv -1 \pmod{l}. \end{cases} \tag{24.3}$$

THEOREM 24.1. *If $c$ is a constant and not zero then*

$$l_n = \lambda_n c^{1-n\lambda_n} \tag{24.4}$$

*is a solution of* (1.1) *whose initial values satisfy the conditions of* (24.2).

In particular, on taking $c = 1$, we see that $\lambda_n$ itself satisfies (1.1).[26] If $l = 3$, $\lambda_n$ 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; namely[27] (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 $\lambda_m, \cdots$ 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 | $\lambda_m$ | $\lambda_n$ | $\lambda_{m+1}$ | $\lambda_{m-1}$ | $\lambda_{n+1}$ | $\lambda_{n-1}$ | $\lambda_{m+n}$ | $\lambda_{m-n}$ | $l_{m+n}l_{m-n}$ | $l_{m+1}l_{m-1}l_n^2$ | $-l_{n-1}l_{n+1}l_m^2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (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] $\lambda_n$ 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:

$$h_{2k+1} = h_{k+2}h_k^3 - h_{k-1}h_{k+1}^3, \qquad k \geqq 1. \tag{4.5}$$

If all terms of $(h)$ with even suffices 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

$$h_0 = h_2 = \cdots = h_{l-3} = 0; \tag{25.1}$$

$$h_{l-1} \neq 0. \tag{25.2}$$

I say that

$$h_l = 0 \tag{25.3}$$

and

$$h_n = 0 \quad \text{for} \quad 1 < n < l-1 \quad \text{if} \quad l > 3. \tag{25.4}$$

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 $1 \leqq k-1 < k+2 < 2k+1$. 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

$$h_{l+1} \neq 0. \tag{25.5}$$

[28] For odd $n$, we use (4.5) as a basis for the induction. For even $n$, we use the formula $h_{2k}h_{l-1} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$ obtained by letting $m = k + (l-1)/2$ and $n = k - (l-1)/2$ in (4.11).

I say that

$$h_n = 0 \quad \text{for} \quad l+1 < n < 2l-1 \quad \text{if} \quad l > 3; \tag{25.6}$$

$$h_{2l-1} = h_{l-1}h^3_{l+1}; \quad h_{2l} = 0; \quad h_{l+1} = -h_{l-1}h^3_{l+1}. \tag{25.7}$$

For if $n$ is even, then by (4.11)

$$h_n h_{l-1} = h_{(n+l+1)/2}h_{(n+l-3)/2}h^2_{(n-l+1)/2} - h_{(n-l+3)/2}h_{(n-l-1)/2}h^2_{(n+l-1)/2}. \tag{25.8}$$

Now if $n = l+3$, $h_{(n-l+3)/3} = h_3 = 0$ 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 $h_{(n-l\pm1)/2} = 0$ 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

$$h_n = a^{n^2-1}\lambda_n c^{1-n\lambda_n} \tag{25.9}$$

where

$$a = (-h_{l-1}h_{l+1})^{1/2l^2}, \quad c = (-h_{l-1})^{(2+l)/2l^2}h_{l+1}{}^{(2-l)/2l^2}. \tag{25.10}$$

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 $\pm 1$ 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 $h_{l\pm1}$ and $h_{2l\pm1}$ already found.

We now proceed by induction. Suppose that we have proved that the formula (25.9) gives the solution $(h)$ for $0 \leqq n < m$, where we are entitled by what proceeds to assume that $m \geqq 2l+2$. Since $(h)$ satisfies (4.11), we obtain on taking $n$ equal to $l$ the relation

$$h_{m+l}h_{m-l} = -h_{l+1}h_{l-1}h^2_m. \tag{25.11}$$

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 $\lambda_n$, (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

$$h_m = -h_{l-1}h_{l+1}h^2_{m-l}/h_{m-2l}. \tag{25.12}$$

For since $m \geqq 2l+2$, 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 $0 \leqq n < m$, then it holds for $0 \leqq n < m+1$. 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*

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2 \tag{1.1}$$

*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,

$$h_2 = \psi_2(u) = -\wp'(u); \quad h_3 = \psi_3(u);$$
$$h_4 = \psi_4(u) = \wp'(u)\,(\wp'^4(u) - \psi_3(u)\,\wp''(u)).$$

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 $(-h)^{(n^2-1)/3}(n/3)$, 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 $\lambda_n$ 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 $(\lambda)$ already discussed in Section **24** of the preceeding 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 $0, 1, h_2, 0, 0, 0, \cdots$ 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* $(h): 0, 1, h_2, h_3, \cdots$ *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

$$h_{n+\kappa} = h_n, \qquad n \geqq a \geqq 1, \qquad \kappa \geqq 2; \tag{27.1}$$

$$h_{a-1+\kappa} \neq h_{a-1}; \tag{27.2}$$

$$h_2 \neq 0; \tag{27.3}$$

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

$$h_\kappa = 0. \tag{27.4}$$

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 $h_\kappa$, 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

$$\text{Either } h_a = 0 \text{ or } h_{a+1} = 0. \tag{27.5}$$

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

$$h_{2a+1} \neq 0. \tag{27.6}$$

We can now show that

$$h_{a+1} = 1, \qquad h_{\kappa-1} = -1. \tag{27.7}$$

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,

$$h_{a-1+\kappa} = 0. \tag{27.8}$$

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,

$$h_{a+1} = 0; \quad h_a \neq 0; \quad h_{a+2} \neq 0; \quad h_{a-1} \neq 0. \tag{27.9}$$

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 of more briefly, by using the elliptic function representation theorem of Chapter IV.

THEOREM 28.1. *Let* $(h): 0, 1, h_2, h_3, \cdots$ *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* $\kappa$:

$$\begin{aligned} &\text{(i)} && h_{n+\kappa} = h_n && (n = 0, 1, \cdots, \kappa) \\ &\text{(ii)} && h_{\kappa-n} = -h_n && (n = 0, 1, \cdots, \kappa) \\ &\text{(iii)} && h_{\kappa/2+n} = -h_n && (\kappa \text{ even}; \ n = 0, 1, \cdots, \kappa/2). \end{aligned} \tag{28.1}$$

THEOREM 28.2. *Let $h_0, h_1, \cdots, h_\kappa$ 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 $m+n \leqq \kappa$. Then if $\kappa_n$ denotes the least positive residue of $n$ modulo $\kappa$, and if $h_n$ is defined to be $h_{\kappa_n}$ for $n \geqq 0$, then $(h)$ is a periodic solution of* (1.1) *with period $\kappa$.*

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

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqq n \geqq 1; \tag{29.1}$$

$$h_0 = 0,\ h_1 = 1;\ h_2, h_3, h_4 \text{ and } h_4/h_2 \text{ integers}; \tag{29.2}$$

$$(h_3\, h_4) = 1. \tag{29.3}$$

By Theorem 6.1 of Chapter III, if $(h)$ is normal

$$(h_n, h_{n+1}) = 1, \qquad (n = 1, 2, 3, \cdots) \tag{29.4}$$

and by Theorem 6.4,

$$(h_n, h_m) = h_{(n,m)}. \tag{29.5}$$

Every purely periodic elliptic divisibility sequence is normal, for if $(h)$

is purely periodic with period $\kappa \geqq 2$, 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

$$h_\rho = 0 \quad \text{but} \quad h_n \neq 0, \qquad 0 < n < \rho, \tag{29.5}$$

then $(h)$ is said to be of rank $\rho$.

THEOREM 29.1. *If $(h)$ is a normal solution of (1.1) of rank $\rho$, then $(h)$ is purely periodic and its period is either $\rho$ or $2\rho$.*

*Proof.* Let $0 \leqq n \leqq \rho$, 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 $h_{n+\rho} = \pm h_n$, $(0 \leqq n \leqq \rho)$, 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 $\rho$ or $2\rho$.

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 $m \geqq n \geqq p > 0$, then*

$$h_{m+n}h_{m-n}h_p^2 = h_{m+p}h_{m-p}h_n^2 - h_{n+p}h_{n-p}h_m^2. \tag{30.1}$$

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 $k_n = h_{nr}/h_r$, $(n = 0, 1, 2, \cdots)$ $(k)$ 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 $\rho \leqq 7$. 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 $h_5 = h_4 h_2^3 - h_3^3 \neq 0$, $h_5 = \pm 2$. But then $h_7 = h_5 h_3^3 - h_2 h_4^3 = \pm 2 \pm 1 \neq 0$. This contradiction completes the proof of the lemma.

LEMMA 30.4. *If $\rho$ is the rank of $(h)$, then $\rho$ can contain no prime factor other than two, three or five.*

For if $p$ is any prime factor of $\rho$, 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 $\rho$. Then $\rho$ is not equal to any one of the following numbers:*

$$6, 8, 9, 10, 15, 25. \tag{30.2}$$

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 $h_6 h_2 = h_3(h_5 h_2^2 - h_4^2) = 0$. Hence $h_5 = \pm 1$, $h_4 = \pm h_2$. But $h_5 = h_4 h_2^3 - h_3^3$. 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 $h_q = \pm 1$, so $h_3 = \pm 1$, and since $h_{50} = 0$, $h_{49} = \pm 1$ so $h_7 = \pm 1$. Now $0 = h_{10} h_2 = h_5(h_7 h_4^2 - h_3 h_6^2)$. Hence $h_4^2 = h_6^2$, $h_3 = \pm 1$, $h_6 = \pm h_4$. Next, $h_6 h_2 = h_3(h_5 h_2^2 - h_4^2)$. Hence $h_4 \mid h_2$, $h_4 = \pm h_2$. But then $h_6 h_2 = \pm h_2^2 = h_3 h_2^2(h_5 - 1)$. Hence $h_5 - 1 = \pm 1$, and since $h_5 \neq 0$, $h_5 = 2$. But $h_9 = h_6 h_4^3 - h_3 h_5^3$. 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 $\rho$. Then $\rho$ 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 $\rho = lm$,

$l \geqq 1$. 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 $\rho$. By Lemma 30. 4, the only prime factors of $\rho$ are two, three and five and by Lemma 30. 6, $\rho$ is not divisible by $2^2$, $3^2$, $5^2$ or $2 \times 3$, $2 \times 5$, $3 \times 5$. Hence $\rho$ 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 $(W): W_0, W_1, W_2, \cdots$ 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 $U_{p\pm1}$ 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.