DIVISIBILITY SEQUENCES OF THIRD ORDER.

By Marshall Hall.

1. *Introduction.* By a divisibility sequence of k-th order will be meant a sequence of rational integers $u_0, u_1, u_2, \cdots u_n, \cdots$ satisfying the linear recurrence

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n \tag{1}$$

where the a's are rational integers, and such that $u_n \mid u_{mn}$ (read u_n divides u_{mn}) for any m and n not zero.

It will be shown (a) that there are two types of divisibility sequences which may be distinguished according as $u_0 \neq 0$ or $u_0 = 0$. If $u_0 \neq 0$, the totality of primes dividing terms of the sequence is finite and the sequence is said to be degenerate. If $u_0 = 0$, all but a finite number of primes will appear as divisors of the terms, and we call the sequence regular. Furthermore this paper shows (b) that the factorization properties of divisibility sequences are similar to the factorization properties of the Lucas [1] sequences, and (c) that there is no regular divisibility sequence of third order whose associated cubic is irreducible. Here a_2 and a_3 are assumed to be co-prime.

Divisibility sequences are of particular interest because of their remarkable factorization properties. Lucas was the first to discover the striking relations in second order sequences and give a coherent theory, though some of his results were implied by earlier work on the theory of quadratic forms. Among other results, he developed the tests for primality applicable to the Mersenne numbers. Other special types of divisibility sequences have been investigated by Lehmer,[2] Pierce,[3] and Poulet.[4]

2. *Properties of General Linear Recurrences.* There will be occasion to use the following properties of recurring sequences, whether divisibility sequences or not. Let the sequence (u_n) be determined by the recurrence

[1] E. Lucas, "Théorie des Fonctions Numériques Simplement Périodiques," *American Journal of Mathematics*, vol. 1 (1875), pp. 184-240, 289-321.

[2] D. H. Lehmer, "An extended theory of Lucas' functions," *Annals of Mathematics* (2), vol. 31 (1930), pp. 419-448.

[3] T. A. Pierce, "The numerical factors of the arithmetic forms $\prod_{i=1}^{n} (1 \pm a_i^m)$," *Annals of Mathematics* (2), vol. 18 (1916-17), pp. 53-64.

[4] Poulet, *L'Intermédiare des Mathématiciens*, vol. 27, pp. 86-87; (2), vol. 1, p. 47; vol. 3, p. 61.

(1) and by an initial set of values $u_0, u_1, u_2, \cdots u_{k-1}$. With the recurrence (1) is associated its characteristic polynomial,

$$f(x) = x^k - a_1x^{k-1} \cdots - a_k = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k).$$

If the roots of $f(x)$ are distinct, then

$$u_n = c_1\alpha_1{}^n + c_2\alpha_2{}^n \cdots + c_k\alpha_k{}^n \tag{2}$$

where $c_1, c_2, \cdots c_k$ are constants which may be determined from the initial values $u_0, u_1, \cdots u_{k-1}$.

The sequence (u_n) is periodic [5] for an arbitrary modulus m. That is to say there exists a period τ of (u_n) modulo m, depending on m and $a_1, a_2, \cdots a_k$ such that

$$u_{n+\tau} \equiv u_n \pmod{m} \tag{3}$$

for all $n \geq n_0[m, a_1, a_2, \cdots a_k]$. In particular $n_0 = 0$ if $(a_k, m) = 1$. The period τ is taken to be the least number satisfying such a relation. All other numbers with this property are multiples of the period. If p be a prime not dividing the discriminant of $f(x)$, and if $f(x) \equiv f_1(x)f_2(x) \cdots f_s(x) \pmod{p}$ be the decomposition of $f(x)$ into irreducible factors modulo p, whose degrees are $k_1, k_2, \cdots k_s$ respectively, then τ divides the least common multiple of $p^{k_i} - 1$, $i = 1, 2, \cdots s$. Moreover (u_n) has a restricted period [6] $\mu \pmod{m}$. μ is defined to be the least integer for which there is a b such that

$$u_{n+\mu} \equiv bu_n \pmod{m} \tag{4}$$

for all $n \geq n_0$. If e is the exponent to which b belongs $\pmod{m}$, then $\mu e = \tau$. If $f(x)$ is irreducible modulo p, p a prime, then $\mu \mid \dfrac{p^k - 1}{p - 1}$.

3. *Properties of General Divisibility Sequences.* References have been given above to investigations of certain types of divisibility sequences. This paper, however, is the first to treat them in general. It is the first attempt to find what the general characteristics of a divisibility sequence are, and what types exist. In this section the fundamental difference between regular and degenerate divisibility sequences is given by Theorem II. Theorem III is the key to the factorization properties of all divisibility sequences. In § 4 these theorems are applied to third order divisibility sequences.

---

[5] H. T. Engstrom, "On sequences defined by linear recurrence relations," *Transactions of the American Mathematical Society*, vol. 33 (1931), pp. 210-218.

[6] R. Carmichael, "On sequences of integers defined by recurrence relations," *Quarterly Journal of Mathematics*, vol. 48 (1920), pp. 343-372. See page 354 for reference to the restricted period. In particular $(b, m) = 1$ if $(a_k, m) = 1$.

THEOREM I. *If* (u_n) *is a divisibility sequence and some* u_r *has a factor* m *relatively prime to* a_k, *then* $u_0 \equiv 0 \pmod{m}$.

As (u_n) is a divisibility sequence $u_r \mid u_{\tau r}$, and hence $u_{\tau r} \equiv 0 \pmod{m}$. Since $(a_k, m) = 1$, relation (3) holds with $n = 0$. This yields $u_{\tau r} \equiv u_0 \pmod{m}$ and hence $u_0 \equiv 0 \pmod{m}$ as was to be proved.

It is on the basis of this theorem that divisibility sequences have been separated into two categories, viz., degenerate if $u_0 \neq 0$, regular if $u_0 = 0$.

If u_n be any term of a degenerate divisibility sequence (u_n), it may be written as the product of two factors, $u_n = A_n B_n$, where $A_n \mid u_0$, and B_n is divisible only by primes dividing a_k. The totality of primes dividing the terms of (u_n) will be finite. Degenerate divisibility sequences will be excluded from consideration in this paper, but will be treated further elsewhere.

If (u_n) is a regular divisibility sequence satisfying (1) and p is any prime not dividing a_k, $u_{s\tau} \equiv u_0 \equiv 0 \pmod{p}$ where τ is the period of (u_n) modulo p. Hence every prime not dividing a_k will divide the terms of a subsequence of (u_n) if (u_n) is a regular divisibility sequence. Furthermore, we may take $u_1 = 1$ without loss of generality since $(u_n) = (v_n/v_1)$ is a divisibility sequence satisfying (1) if (v_n) is a divisibility sequence satisfying (1). (u_n) will, of course, be a sequence of integers as $v_1 \mid v_n$ for all n, including $n = 0$, as $v_0 = 0$.

It is convenient to state these results as a theorem.

THEOREM II. *The totality of primes dividing the terms of a degenerate sequence* (u_n) *is contained in the set of primes dividing* u_0 *and* a_k. *The totality of primes dividing the terms of a regular sequence* (u_n) *includes every prime not dividing* a_k.

Consider the factorization of u_n, a particular term of a regular divisibility sequence. By the divisibility property, any prime dividing u_r where $r \mid n$ is a divisor of u_n. The remaining primes belong essentially to the term u_n itself.

Definition. A prime p is said to be a primitive divisor of u_n if $p \mid u_n$, $p \nmid u_r$ for $r \mid n$, $r \neq n$, and if $p \nmid a_k$.

The following theorem on the factorization of terms of a divisibility sequence is fundamental.

THEOREM III. *If* p *is a primitive divisor of* u_n, *and if* μ *is the restricted period of* (u_n) *modulo* p, *then* $n \mid \mu$.

Proof. Let $(n, \mu) = r$. Then there exist positive integers x and y such that $nx - \mu y = r$.

Since $u_n \equiv 0 \pmod p$, we have $u_{nx} \equiv 0 \pmod p$ (divisibility) $u_{nx} \equiv b^y u_{nx-\mu y} \pmod p$ (restricted period) or $u_{nx} \equiv b^y u_r \equiv 0 \pmod p$, whence $u_r \equiv 0 \pmod p$ as $b \not\equiv 0 \pmod p$ if $(a_k, p) = 1$. But as p is a primitive divisor of u_n, $u_r \equiv 0 \pmod p$ for $r \mid n$ implies $r = n$. Hence $(n, \mu) = r = n$, and $n \mid \mu$ as was to be shown.

Combining this with the information on μ given in § 2, it is seen that p is restricted to certain arithmetic progressions $tn + r_i$. For example, if the sequence is of second order $\mu \mid p - 1$ or $p + 1$, whence $p = tn \pm 1$.

4. *Divisibility Sequences of Third Order.* The condition $u_0 = 0$ makes it easy to find the regular divisibility sequences of first and second order. There is no regular sequence of first order unless the trivial sequence of zeros be considered a divisibility sequence. For second order we have $u_n = t(\alpha_1{}^n - \alpha_2{}^n)/(\alpha_1 - \alpha_2)$ or tna^{n-1} according as the roots of the associated polynomial are distinct or equal. The first of these is the well known Lucas sequence.

The consideration of third order sequences is by no means so simple. We may construct formally $u_n = \left(\dfrac{\alpha_1{}^n - \alpha_2{}^n}{\alpha_1 - \alpha_2}\right)^2 = \dfrac{\alpha_1{}^{2n} + \alpha_2{}^{2n} - 2\alpha_1{}^n\alpha_2{}^n}{\alpha_1{}^2 + \alpha_2{}^2 - 2\alpha_1\alpha_2}$ which satisfies a third order sequence whose characteristic polynomial has roots $\alpha_1{}^2$, $\alpha_2{}^2$, and $\alpha_1\alpha_2$. This will be a sequence of integers if $v_n = (\alpha_1{}^n - \alpha_2{}^n)/(\alpha_1 - \alpha_2)$ is of either the Lucas or Lehmer type. Such a sequence is essentially of quadratic type and there is nothing to be gained by considering it as a third order sequence. It is probable that there are no regular third order sequences of any other type.[7]

It is easily seen that we cannot obtain a divisibility sequence of third order satisfying an arbitrary recurrence merely by an appropriate choice of initial values. Consider $u_{n+3} = u_{n+1} + u_n$. From § 3 we must take $u_0 = 0$, and may take $u_1 = 1$. The condition $u_2 \mid u_4$ implies $u_2 = \pm 1$, but in neither case does $u_4 \mid u_8$.

If a sequence is of type $v_n{}^2$ as given above, its characteristic cubic $f(x)$ has a rational root $a = \alpha_1\alpha_2$. Hence if there is a third order divisibility sequence whose $f(x)$ is irreducible, it is certainly not of type $v_n{}^2$. This possibility is considered in the following theorem.

THEOREM IV. *There is no regular divisibility sequence (u_n), whose*

[7] Since completing this paper I have learned from Dr. Morgan Ward that he has been able to show that this is the only type if $f(x)$, the characteristic polynomial, has a linear and an irreducible quadratic factor. As this paper covers the case $f(x)$ irreducible, the only doubtful possibility is that $f(x)$ is the product of three linear factors.

characteristic polynomial is an irreducible cubic whose last two coefficients are relatively prime.

As the proof of this theorem is quite long, it will be subdivided into Lemmas. Lemma 4 gives the first of the equations which lead to the contradiction of the assumption that there is a divisibility sequence satisfying the requirements of the theorem.

Assume that there is a regular divisibility sequence (u_n), whose characteristic is $f(x) = x^3 - a_1x^2 - a_2x - a_3 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $(a_2, a_3) = 1$ and let $f(x)$ be irreducible. (u_n) satisfies the recurrence

$$u_{n+3} = a_1u_{n+2} + a_2u_{n+1} + a_3u_n. \tag{5}$$

As $f(x)$ is irreducible α_1, α_2, and α_3 are distinct and

$$u_n = c_1\alpha_1{}^n + c_2\alpha_2{}^n + c_3\alpha_3{}^n. \tag{6}$$

We note that as (u_n) is a regular divisibility sequence $u_0 = 0$ or

$$c_1 + c_2 + c_3 = 0. \tag{7}$$

Moreover we take $u_1 = 1$, as is permissable.

LEMMA 1. *If $p \mid a_3$, and $p \mid u_n$, then n has a factor r, $1 < r < \bar{n}$, $\bar{n}$ a fixed number.*

For if p divides any terms of (u_n), let u_m be the first. It evidently suffices to show $(m, n) \neq 1$. Then take $\bar{n}$ greater than m. As there are only a finite number of primes dividing a_3, there is one value for $\bar{n}$ which will do for all divisors of a_3. In fact, it can be shown that $a_3{}^3$ will suffice. Now if $(m, n) = 1$, there are positive integers x and y such that $mx = ny + 1$. By the divisibility property $u_{mx} \equiv 0 \pmod{p}$ and $u_{ny} \equiv 0 \pmod{p}$. From (5)

$$u_{mx} = a_1u_{mx-1} + a_2u_{mx-2} + a_3u_{mx-3}.$$

Now $p \mid u_{mx}$, $p \mid u_{mx-1} = u_{ny}$, $p \mid a_3$, but $p \nmid a_2$ as $(a_2, a_3) = 1$. Hence $p \mid u_{mx-2}$. Similarly as

$$u_{mx-1} = a_1u_{mx-2} + a_2u_{mx-3} + a_3u_{mx-4},$$

we have $p \mid u_{mx-3}$. Proceeding thus we finally obtain $p \mid u_1 = 1$, which is a contradiction. Hence $(m, n) \neq 1$.

LEMMA 2. *If $p \mid u_n$ and p is a divisor of the discriminant of $f(x)$, n has a factor less than a finite limit $\bar{n}$.*

If p also divides a_3 then Lemma 1 proves this. If $p \nmid a_3$, then p is either a primitive divisor of u_n or of u_r where $r|n$. In this case $r|\mu$ the restricted period of (u_n) modulo p, by reason of Theorem III, and $r \neq 1$ as $u_1 = 1$. As $f(x)$ is irreducible, its discriminant is not zero and has only a finite number of divisors. The restricted periods of these primes will lie below a finite limit $\bar{n}$. Hence $r < \bar{n}$ and so n has a factor less than $\bar{n}$.

LEMMA 3. *If q is a prime greater than $\bar{n}$, then* $u_q{}^6 \equiv u_1{}^6 \pmod{q}$, $u_{q^2}{}^6 \equiv u_1{}^6 \pmod{q}$.

By Lemma 1, u_q has no prime factor dividing a_3. As $u_1 = 1$, every prime dividing u_q is a primitive divisor of u_q. Hence if $p|u_q$ and μ is the restricted period of (u_n) modulo p, then $q|\mu$ by Theorem III. As p does not divide the discriminant of $f(x)$ by Lemma 2, we have $\mu|p-1$, p^2-1, or p^3-1, and hence $q|p^6-1$. Since $p^6 \equiv 1 \pmod{q}$ for every prime p dividing u_q, it follows by multiplication that $u_q{}^6 \equiv 1 \pmod{q}$ or $u_q{}^6 \equiv u_1{}^6 \pmod{q}$ as $u_1 = 1$. Now $p^6 \equiv 1 \pmod{q^2}$ for the primitive divisors of u_{q^2}, and hence à fortiori $p^6 \equiv 1 \pmod{q}$. Since all the divisors of u_{q^2} are primitive divisors of either u_q or u_{q^2}, we have $u_{q^2}{}^6 \equiv 1 \pmod{q}$ or $u_{q^2}{}^6 \equiv u_1{}^6 \pmod{q}$ as before.

LEMMA 4.

$$c_1\alpha_2 + c_2\alpha_3 + c_3\alpha_1 = \epsilon_1(c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)$$

and

$$c_1\alpha_3 + c_2\alpha_1 + c_3\alpha_2 = \epsilon_2(c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)$$

where $\epsilon_1{}^6 = \epsilon_2{}^6 = 1$.

For if q is a prime greater than $\bar{n}$, by Lemma 3 we have

$$(8) \qquad (c_1\alpha_1{}^q + c_2\alpha_2{}^q + c_3\alpha_3{}^q)^6 \equiv (c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)^6 \pmod{q}.$$

Now if $f(x)$ is irreducible $\pmod{q}$ then

$$(9) \qquad \alpha_1{}^q \equiv \alpha_2,\ \alpha_2{}^q \equiv \alpha_3,\ \alpha_3{}^q \equiv \alpha_1 \pmod{Q}$$

where Q is a prime ideal dividing q in $K(\alpha_1, \alpha_2, \alpha_3)$. Hence from (8)

$$(10) \qquad (c_1\alpha_2 + c_2\alpha_3 + c_3\alpha_1)^6 \equiv (c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)^6 \pmod{Q}.$$

Now if $f(x)$ is irreducible there are infinitely many primes q for which $f(x)$ is irreducible $\pmod{q}$.[8] Hence the difference of the two sides of (10) is an

[8] Hasse, "Bericht über Neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper," Part II, p. 127, *Jahresbericht Ergänzungsbände*, vol. 6 (1930). Here K $(\alpha_1, \alpha_2, \alpha_3)$ is a cyclic extension of either the rational field or a quadratic field.

algebraic number divisible by infinitely many prime ideals, and consequently must be zero. Hence

$$(11) \qquad c_1\alpha_2 + c_2\alpha_3 + c_3\alpha_1 = \epsilon_1(c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)$$

where $\epsilon_1{}^6 = 1$. Similarly since $\alpha_1{}^{q^2} \equiv \alpha_3$, $\alpha_2{}^{q^2} \equiv \alpha_1$, $\alpha_3{}^{q^2} \equiv \alpha_2 \pmod{Q}$ and reasoning on u_{q^2} we have

$$(12) \qquad c_1\alpha_3 + c_2\alpha_1 + c_3\alpha_2 = \epsilon_2(c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3)$$

where $\epsilon_2{}^6 = 1$.

Combining (7), (11) and (12) we have the system of equations:

$$(13) \qquad \begin{aligned} c_1 \quad &+ c_2 &&+ c_3 &&= 0 \\ c_1(\alpha_2 - \epsilon_1\alpha_1) &+ c_2(\alpha_3 - \epsilon_1\alpha_2) &&+ c_3(\alpha_1 - \epsilon_1\alpha_3) &&= 0 \\ c_1(\alpha_3 - \epsilon_2\alpha_1) &+ c_2(\alpha_1 - \epsilon_2\alpha_1) &&+ c_3(\alpha_2 - \epsilon_2\alpha_3) &&= 0 \end{aligned}$$

If the c's all vanish, then the sequence (u_n) will consist merely of 0's. If not, the determinant of the c's

$$-(1 + \epsilon_1 + \epsilon_2)(\alpha_1{}^2 + \alpha_2{}^2 + \alpha_3{}^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3)$$

must vanish.

If $\alpha_1{}^2 + \alpha_2{}^2 + \alpha_3{}^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 = 0$, then $a_1{}^2 = 3a_2$ and the roots of $f(x)$ are

$$(14) \qquad \begin{aligned} \alpha_1 &= -a_1/3 + (a_1{}^3/27 - a_3)^{1/3} \\ \alpha_2 &= -a_1/3 + \rho(a_1{}^3/27 - a_3)^{1/3} \\ \alpha_3 &= -a_1/3 + \rho^2(a_1{}^3/27 - a_3)^{1/3} \end{aligned}$$

where ρ is a primitive cube root of unity. Here for primes $q = 3k + 2$, $\alpha_1{}^q \equiv \alpha_1$, $\alpha_2{}^q \equiv \alpha_3$, $\alpha_3{}^q \equiv \alpha_2 \pmod{q}$ and reasoning as before

$$c_1 + c_2\rho^2 + c_3\rho = \epsilon_3(c_1 + c_2\rho + c_3\rho^2).$$

Trying the six possible values of ϵ_3, we find that two of the c's must be equal, or one must vanish. In no one of these cases can the sequence (u_n) be a sequence of rational integers.

If $1 + \epsilon_1 + \epsilon_2 = 0$, we have $\epsilon_1 = \rho, \epsilon_2 = \rho^2$. Solving (13) with

$$c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 = u_1 = 1,$$

we obtain

$$(15) \quad c_1 = \frac{1}{\alpha_1 + \rho\alpha_2 + \rho^2\alpha_3}, \; c_2 = \frac{\rho}{\alpha_1 + \rho\alpha_2 + \rho^2\alpha_3}, \; c_3 = \frac{\rho^2}{\alpha_1 + \rho\alpha_2 + \rho^2\alpha_3}.$$

Here the vanishing of the denominators implies the vanishing of the second factor of the determinant, a possibility which has just been excluded. Here again the field is of the type $K(\sqrt[3]{d})$; for from the fact that u_2 is rational it is easily shown that $(\alpha_1 + \rho^2\alpha_2 + \rho\alpha_3)^3$ is rational. Hence for

$$q = 3k + 2,\ \alpha_1{}^q \equiv \alpha_1,\ \alpha_2{}^q \equiv \alpha_3,\ \alpha_3{}^q \equiv \alpha_2 \pmod{q}$$

and reasoning as before

$$c_1\alpha_1 + c_2\alpha_3 + c_3\alpha_2 = \epsilon_4(c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3).$$

Combining these six possibilities with (15) we have one of

$$\begin{array}{ll} \alpha_1 = \alpha_2 & 2\alpha_1 - \alpha_2 - \alpha_3 = 0 \\ \alpha_1 = \alpha_3 & 2\alpha_2 - \alpha_1 - \alpha_3 = 0 \\ \alpha_2 = \alpha_3 & 2\alpha_3 - \alpha_1 - \alpha_2 = 0 \end{array}$$

Each one of these contradicts the irreducibility of $f(x)$. For an irreducible polynomial has no equal roots, and if (say) $2\alpha_1 - \alpha_2 - \alpha_3 = 0$ then $3\alpha_1 = \alpha_1 + \alpha_2 + \alpha_3 = -a_1$, and the root α_1 is rational. This completes the proof of Theorem IV.

YALE UNIVERSITY.