# A FULL CHARACTERISATION OF DIVISIBILITY SEQUENCES

By JEAN-PAUL BÉZIVIN, ATTILA PETHŐ*, and ALFRED J. VAN DER POORTEN**

*Dedicated to the memory of Kurt Mahler*

---

Divisibility sequences are recurrence sequences $(a_h)$, that is sequences satisfying linear homogeneous recurrence relations with constant coefficients, with the interesting property that whenever $h|k$, then $a_h|a_k$. A well known example is the sequence of Fibonacci numbers. It has long been an open question, variously attributed to Marshall Hall and to Morgan Ward, whether all divisibility sequences are, essentially, just termwise products of second order recurrence sequences generalising the Fibonacci numbers. We characterise all divisibility sequences, employing the factorisation theory for exponential polynomials and a deep arithmetic result on the Hadamard quotient of rational functions.

We rehearse a number of well known facts, principally to set our notation and terminology, but also because this is a field in which it is peculiarly difficult to find congenial summaries that warrant citing.

The present paper arises from discussion at the First Conference of the Canadian Number Theory Society, Banff 1988, between the latter two authors (see [14], Section 6.7) and independent contemporaneous work of the first author [1].

Of course, we are aware that, in the literature, the notion "divisibility sequence" need not entail that the sequence be a recurrence sequence. Thus some qualifying adjective should have been attached to each use of the phrase "divisibility sequence." However, since our no-

---

Manuscript received 25 November 1988.

*Work partially supported by Hungarian National Foundation for Scientific Research Grant No. 273/86.

**Work partially supported by the Australian Research Council.

*American Journal of Mathematics* 112 (1990), 985–1001.

tion "divides" is more general than in the classical case, we feel we can indulge in the luxury of avoiding a repeated qualifier and may allow our notion "divisibility sequence" to be more restrictive than needs be.

## 1. Introduction.

**1.1. A divisibility sequence.** Consider the Fibonacci numbers $(f_h)$, defined by the recurrence relation $f_{h+2} = f_{h+1} + f_h$ and the initial conditions $f_0 = 0$, $f_1 = 1$:

| $h$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_h$ | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | 144 | 233 | 377 | 610 | 987 | 1597 | 2584 | 4181 | 6765 | .... |

One notices such phenomena as $13|377$ and $55|6765$—the reason is that, respectively, $7|14$ and $10|20$. Indeed, the Fibonacci sequence has the interesting property that $h|k$ implies $f_h|f_k$.

**1.2. Divisibility sequences.** Let $\Sigma\, a_h X^h$ represent a rational function defined over a field $\mathbf{F}$ of characteristic zero and vanishing at $\infty$. Then the sequence of Taylor coefficients $(a_h)$ is called a *divisibility sequence* (or a *suite récurrente arithmétique*) if the set of quotients $\{a_k/a_h : h|k\}$ is a subset of a ring $R$ finitely generated over $\mathbb{Z}$, or *of finite type* over $\mathbb{Z}$. (Should $a_h = a_k = 0$, it is useful to define the quotient, say to be 0.) In the classical, and simpler, formulation one supposes the $a_h$ to be rational integers and for the quotients to belong to $\mathbb{Z}$. However, the new setting introduces no new problems and allows our proof to deal with various generalisations of the original question (*cf* [8], [24]) that have appeared in the literature.

Ward (*cf* [22]) adds the qualifier *linear* to emphasise that his divisibility sequences satisfy a linear homogeneous recurrence relation with constant coefficients. Elsewhere, [24] he refers to such divisibility sequences as *Lucasian* sequences; this terminology has not persisted.

If, moreover, one always has $\gcd(a_h, a_k) = a_{\gcd(h,k)}$, perhaps expressed as an equality of ideals, then the sequence $(a_h)$ is called a *strong* divisibility sequence. Schinzel [20] characterises all second order such sequences in algebraic number fields.

The reader will note that the divisibility property of itself does not

guarantee an especially interesting sequence. However quite amusing sequences arise from iteration: for if both $(a_h)$ and $(b_h)$ are divisibility sequences and the $b_h$ all are nonnegative rational integers, then, plainly, $(a_{b_h})$ has the divisibility property. See also Ward [25].

**1.3. A statement of our result.** It is relatively easy to see, and is shown by Hall [5], that there are two cases according as $a_0 = 0$ or not, the second case being "degenerate." In the first, interesting, case we lose no generality in normalising so that $a_1 = 1$.

We shall show that *if* $(a_h)$ *is recurrence sequence and there is a suitable integer* $d > 1$ *so that* $a_h | a_{dh}$ *for* $h = 0, 1, 2, \ldots$ *(in the sense that the quotients all belong to a ring finitely generated over* $\mathbb{Z}$*) then there is a recurrence sequence* $(\bar{a}_h)$ *given by*

$$\bar{a}_h = h^k \prod_i \left( \frac{\alpha_i^h - \beta_i^h}{\alpha_i - \beta_i} \right),$$

*and* $a_h | \bar{a}_h$ *for* $h = 0, 1, 2, \ldots$. *It follows that* $a(h)$ *divides* $\bar{a}(h)$ *in the ring of generalised power sums. A fortiori* this is so if $(a_h)$ is a divisibility sequence. We provide detail of those divisors of $(\bar{a}_h)$ that yield a divisibility sequence. Since, for example, the polynomial $p(X) = (X + 1)(X^3 - 1)$ divides the polynomial $p(X^d)$ in the ring of polynomials for all $d = 1, 2, \ldots$ these divisors are not all of as simple a shape as one might have supposed.

## 2. Notation and terminology.

**2.1. Generalised power sums.** A *generalised power sum* $a(h), h = 0, 1, 2, \ldots$ is an expression of the shape

$$a(h) = \sum_{i=1}^{m} A_i(h)\alpha_i^h, \qquad h = 0, 1, 2, \ldots \tag{2.1.1}$$

with *roots* $\alpha_i$, $1 \le i \le m$, distinct nonzero quantities, and *coefficients* $A_i(h)$ polynomials respectively of degree $n(i) - 1$, for positive integers $n(i)$, $1 \le i \le m$. It is useful to say that the roots $\alpha_i$ have *multiplicity* $n(i)$ respectively. If each multiplicity is 1—thus if the coefficients all are

constant—we may refer to the generalised power sum as a *power sum*. The generalised power sum $a(h)$ has *order*

$$n = \sum_{i=1}^{m} n(i).$$

Set

$$(2.1.2) \quad s(X) = \prod_{i=1}^{m} (1 - \alpha_i X)^{n(i)} = 1 - s_1 X - \cdots - s_n X^n.$$

Then the sequence $(a_h)$ with $a_h = a(h)$, $h = 0, 1, 2, \ldots$ satisfies the linear homogeneous recurrence relation

$$(2.1.3) \quad a_{h+n} = s_1 a_{h+n-1} + \cdots + s_n a_h, \qquad h = 0, 1, 2, \ldots.$$

**2.2. . . . and rational functions.** To see this let $E : f(h) \mapsto f(h + 1)$ be the shift operator and $\Delta = E - 1$ the difference operator. Then

$$(E - \alpha)A(h)\alpha^h = (\Delta A(h))\alpha^{h+1}$$

and since $\Delta A(h)$ has lower degree than does $A$, by linearity and induction it is plain that

$$\prod_{i=1}^{m} (E - \alpha_i)^{n(i)}$$

annihilates the sequence $(a_h)$ as asserted. Thus generalised power sums are interesting in that they coincide with the sequences satisfying the recurrence relations (2.1.3). It follows that there is a polynomial $r(x)$, of degree less than $n$, so that the power series

$$(2.2.1) \qquad \sum_{h=0}^{\infty} a_h X^h = \frac{r(X)}{s(X)}$$

is a rational function; to see this, multiply by $s(X)$ and note the recurrence relation.

Conversely given a rational function as above, with deg $r <$ deg $s$, a partial fraction expansion yields

$$\frac{r(X)}{s(X)} = \sum_{\iota=1}^{m} \sum_{j=1}^{n(i)} \frac{r_{ij}}{(1 - \alpha_\iota X)^j} = \sum_{h=0}^{\infty} \left( \sum_{\iota=1}^{m} \sum_{j=1}^{n(i)} r_{ij} \binom{h + j - 1}{j - 1} \alpha_i^h \right) X^h$$

and the coefficients of $X^h$, $h = 0, 1, 2, \ldots$ are indeed the values of a generalised power sum as described.

**2.3. The Hadamard product.** Accordingly, results on generalised power sums are equivalent to corresponding results for the Taylor coefficients of rational functions. For example, the evident observation that the product of generalised power sums is again a generalised power sum becomes the more interesting: the Hadamard product (the "child's product")

$$\sum_{h=0}^{\infty} a_h b_h X^h$$

of rational functions $\Sigma\, a_h X^h$, $\Sigma\, b_h X^h$ is again rational. A partial converse of this remark, the Pólya-Cantor Lemma [3], and a general converse, the Hadamard Quotient Theorem [13], play critical rôles in our proof below.

**2.4. Recurrence sequences.** We call a sequence $(a_h)$ satisfying a relation (2.1.3) a *recurrence sequence* of *order* $n$; the polynomial $X^n s(X^{-1})$ reciprocal to the polynomial (2.1.2) is its *characteristic polynomial*. Our roots $\alpha_i$ are the distinct zeros of the characteristic polynomial. The recurrence sequence has simple roots if and only if its characteristic polynomial has no repeated zeros.

The archetypal example of a recurrence sequence is of course the celebrated Fibonacci sequence $(f_h)$ defined by

$$f_{h+2} = f_{h+1} + f_h, \qquad h = 0, 1, 2, \ldots \text{ with } f_0 = 0, f_1 = 1;$$

and generated by

$$\frac{X}{1 - X - X^2} = \sum_{h=0}^{\infty} f_h X^h.$$

**2.5. Exponential polynomials.** It is plain that the generalised power sum is the restriction to the nonnegative integers of an *exponential polynomial*

$$a(z) = \sum_{i=1}^{m} A_i(z)e^{z \log \alpha_i} = \sum_{i=1}^{m} A_i(z)e^{z\omega_i}, \qquad z \in \mathbb{C}.$$

Note that, however, because we are free to choose the branches of the $\log \alpha_i$, the analytic continuation of a generalised power sum to an exponential polynomial is not well defined. We will refer to the $\log \alpha_i = \omega_i$ as the *frequencies* of the exponential polynomial.

There is a factorisation theory for the ring of exponential polynomials, essentially due to Ritt [16]. It provides a second major ingredient of our proof. We rehearse the proof to show that Ritt's argument for exponential sums readily generalises to exponential polynomials as required.

## 3. A brief history.

**3.1. Resultant sequences.** Let $\phi_1, \ldots, \phi_k$ and $\theta_1, \ldots, \theta_l$ be distinct elements of the given field $\mathbf{F}$ of characteristic zero. Define the sequences of polynomials $(\Phi_h)$ and $(\Theta_h)$ by $\Phi_h(X) = \Pi(X - \phi_i^h)$ and $\Theta_h(X) = \Pi(X - \theta_i^h)$. Denote by $R_h(\Phi, \Theta)$ the resultant of $\Phi_h$ and $\Theta_h$. Then $(R_h)$ is a recurrence sequence with roots of multiplicity one and the corresponding normalised sequence $(r_h)$ is given by

$$r_h = \prod_{i=1}^{k} \prod_{j=1}^{l} \frac{\phi_i^h - \theta_j^h}{\phi_i - \theta_j}.$$

It is plain that such a *resultant sequence* is a divisibility sequence. Ward [23] remarks that "it appears probable that *all* Lucasian sequences may be exhibited as $R$-sequences [that is, resultant sequences] or divisors of $R$-sequences." Kimberling [9] observes that Ward "conjectured repeatedly that every linear divisibility sequence is the divisor of a resultant sequence.[1]"

[1]He continues (1980): "No proof of this conjecture seems to be known or imminent, even in the case that all the roots are indeterminates."

Pierce [11] follows Lucas in studying divisibility properties of resultant sequences in the context of primality testing.

**3.2. Repeated roots.** The observations above appear to neglect both degenerate cases and those with repeated roots. Notionally, however, one can cope with repeated roots by identifying quantities through taking appropriate limits. Then a generalised resultant sequence $(r_h)$ is of the shape

$$r_h = h^k \gamma^{h-1} \prod_i \left( \frac{\alpha_i^h - \beta_i^h}{\alpha_i - \beta_i} \right),$$

some nonnegative integer $k$, and we may rephrase Ward's remark[2] in terms of generalised resultant sequences. Incidentally, there is a natural tendency to overlook, or disregard, the case of repeated roots in that, for second or third order recurrence sequences, these lead to relatively uninteresting examples.

**3.3. "Degenerate" divisibility sequences.** Hall's analysis [5] of third order divisibility sequences of rational integers commences with the observation that every prime relatively prime to the product of the roots of a divisibility sequence $(a_h)$ and dividing some term of the recurrence sequence must divide $a_0$. Hence, unless there are just finitely many distinct primes dividing terms of the integer divisibility sequence, necessarily $a_0 = 0$. Rephrased for general divisibility sequences, this statement becomes either $a_0 = 0$, or the terms of the divisibility sequence $(a_h)$ all belong to a finitely generated multiplicative subgroup of the field of definition.

Indeed, a recurrence sequence is periodic with respect to every modulus $\mu$. If the recurrence relation is

$$a_{h+n} = s_1 a_{h+n-1} + \cdots + s_n a_h, \qquad h = 0, 1, 2, \ldots$$

then it is pure-periodic with respect to all moduli $\mu$ relatively prime to

[2]Nowadays, one would speak of "Ward's Conjecture." It is questionable, however, whether Ward would have considered that an impression not backed by numerical evidence warranted a conjecture as such.

$s_n$; that is, relatively prime to each of the roots of the recurrence sequence. The $p$-adic embedding argument described at Section 3.5 of [14] is one way to see these claims for general recurrence sequences.

If the period is, say, $\rho$ and if $\mu$ divides some term $a_h$ of the recurrence sequence, the divisibility condition $a_h | a_{\rho h}$ entails $\mu | a_{\rho h}$, whilst pure periodicity implies $a_{\rho h} \equiv a_0 \bmod \mu$. Hence, either $a_0 = 0$ or the terms of the divisibility sequence $(a_h)$ all belong to a finitely generated multiplicative group.

This latter, "degenerate" case is discussed at Section 3.4 of [14]. By a result of Pólya [12] one sees that these "degenerate" recurrence sequences $(b_h)$ are of the shape

$$b_h = k^{-1} \sum_{j=0}^{k-1} B_j \beta_j^h \left( \sum_{i=0}^{k-1} \zeta^{i(h-j)} \right),$$

with constants $B_j$, $k$ a positive integer, and $\zeta$ a $k$-th root of unity. This is

$$b_h = B_j \beta_j^h \text{ according as } h \equiv j \bmod k.$$

With the proviso that all the coefficients $B_j$ be nonzero, the sequences just described are units in the semigroup of divisibility sequences. Indeed, this is just the observation that the rational function $\Sigma\, b_h X^h$ is Hadamard invertible. Therefore, it is appropriate to neglect altogether the presence of these sequences and to have it implicit below that certain statements are prefaced by the qualification: "Up to multiplication by "degenerate" divisibility sequences . . . ."

It is usual to say (*cf* Section 3.6.3 of [14]) that a recurrence sequence is degenerate if it has a pair $\alpha_i \neq \alpha_j$ of roots so that $\alpha_i/\alpha_j$ is a root of unity, or if some root $\alpha_i$ is a root of unity. We could restrict our discussion to divisibility sequences that are nondegenerate in this sense; but, once $k > 1$, the notion of a "degenerate" divisibility sequence is more restrictive.[3]

[3]Hence we write ""degenerate"" rather than just "degenerate."

**3.4. Third order divisibility sequences.** Hall [5] proves that non-degenerate divisibility sequences $(a_h)$ over $\mathbb{Z}$ of order 2 are of the shape

$$a_h = h\alpha^{h-1} \quad \text{or} \quad \frac{\alpha^h - \beta^h}{\alpha - \beta},$$

and those of order 3 include those of the shape

$$a_h = h^2\alpha^{h-1}, \qquad h\left(\frac{\alpha^h - \beta^h}{\alpha - \beta}\right) \quad \text{and} \quad \left(\frac{\alpha^h - \beta^h}{\alpha - \beta}\right)^2.$$

He conjectures that these are the only possibilities, but, for order 3, he can deal only with the case of characteristic polynomial irreducible over $\mathbb{Z}$.

Our more general setting views matters over the splitting field and suggests that Hall's argument might be capable of completion by adopting that more general viewpoint. Our argument below, however, relies on principles quite different from those employed by Hall and other early investigators.

## 4. Preliminary results.

**4.1. Factorisation in the ring of exponential polynomials.** The ring of exponential polynomials has a unique factorisation theorem, essentially due to Ritt [16]. The units of the ring are of course the exponential polynomials $Ae^{\omega z}$, with constants $A \neq 0$. Irritatingly, the exponential polynomials of the shape $1 - Ae^{\theta z}$ have factors $1 - A^{1/n}e^{\theta z/n}$ for all positive integers $n$. Plainly we have to treat these exponential polynomials separately; we do that by referring to them as *simple* exponential polynomials. We note that a product of simple exponential polynomials with the same frequency $\theta$ yields a polynomial over the base field in the single variable $e^{\theta z}$.

Finally, there are honest-to-goodness *irreducible* exponential polynomials. In the light of the presence of simple exponential polynomials, however, the existence of irreducibles is not at all obvious. One argues as follows: Suppose that the free $\mathbb{Z}$-module generated by the frequencies $\omega_1, \ldots, \omega_m$ of the given exponential polynomial has a $\mathbb{Z}$-basis $\tau_1, \ldots, \tau_t$. Setting $x_i = e^{\tau_i z}$, and after multiplying by an appropriate unit, if

necessary, displays the given exponential polynomial as a polynomial in $z$ and the $x_i$. Factorisations of the given exponential polynomial correspond to factorisations of that polynomial in polynomials in the variables $z$ and fractional powers of the $x_i$. Monomial (one term) factors correspond to units or to powers of $z$; binomial (two term) factors with coefficients independent of $z$ correspond to associates of simple exponential polynomials; the remaining irreducible factors are polynomials in $z$ and either binomial expressions in $z$ and the $x_i$, or polynomials with at least three terms. For these last polynomials Ritt [16] shows that there is a finite (this is the point of difficulty) factorisation in fractional powers of the $x_i$. Ritt presumes constant coefficients, but the generalisation involves no more than including an extra variable $z$, for which, moreover, only integral powers are permitted in the factorisation.

The upshot is that: *Up to units of the ring, an exponential polynomial has a unique factorisation as a product of a polynomial in $z$, a finite number of polynomials each in a single variable $e^{\theta_j z}$, with the frequencies $\theta_j$ not rational multiples one of the other, and a finite number of irreducible exponential polynomials.*

**4.2. Factorisation of polynomials in fractional powers.** The matter of factorisation of polynomials in fractional powers is detailed by Schinzel [19], see pages 101–113. The argument refining Ritt's is that of Gourin [4]. The precise quantitative result is as follows[4]:

We say that a polynomial $f(x_1, \ldots, x_n)$ is *primary* (in each of its variables respectively) if an identity $f(x_1, \ldots, x_n) = g(x_1^{q_1}, \ldots, x_n^{q_n})$ with some polynomial $g$ and positive integers $(q_1, \ldots, q_n)$ entails $q_1 = \cdots = q_n = 1$. One sees, in the course of the proof (which we do not detail here), that to establish finiteness of factorisation in fractional powers it suffices to consider just factorisations in primary polynomials.

*Let $f(x_1, \ldots, x_n)$ be an irreducible polynomial of multi-degree $d_1, \ldots, d_n$ defined over an algebraically closed field of characteristic zero. Suppose that, for positive integers $(q_1, \ldots, q_n)$, the polynomial $f(x_1^{q_1}, \ldots, x_n^{q_n})$ has a factorisation in primary polynomials. Suppose that, viewed as a polynomial in just $x_i$ and $x_j$, with $(i, j)$ some pair $i \neq j \in \{1,$*

[4]From a manuscript: G. R. Everest and A. J. van der Poorten, 'Factorisation in the ring of exponential polynomials,' detailing a proof in modern terminology.

$2, \ldots, n\}$, *the polynomial* $F_{i,j}(x_i, x_j) \equiv f(x_1, \ldots, x_n)$ *has at least three terms. Then*

$$q_i q_j \leq \gcd(q_i, q_j) d_i d_j.$$

*It follows that if* $f(x_1, \ldots, x_n)$ *has at least three terms then it has a finite factorisation into irreducibles in the ring generated over the ground field by all fractional powers of the variables* $x_1, \ldots, x_n$. *Indeed, the number of such irreducible factors does not exceed* $\min d_i d_j$, *with the minimum taken over the pairs* $(i, j)$ *described above.*

**4.3. Polynomials dividing certain transforms of themselves.** In this section $f$ denotes a polynomial $f(x) = f(x_1, \ldots, x_t)$ defined over an algebraically closed field $\mathbf{F}$ of characteristic zero and is deemed *admissible* if it has the property that, in the ring $\mathbf{F}[x]$, $f(x)$ divides $f(x^d) = f(x_1^d, \ldots, x_t^d)$ for every positive integer $d$. We assume, as we may, that $f$ is not divisible by a nontrivial monomial in the variables $x$.

Let $t = 1$. Denote by $\mathfrak{Z}$ the set of distinct zeros of an admissible $f$. Suppose $\alpha \in \mathfrak{Z}$ and that $\beta$ belongs to the multiplicative subgroup of $\mathbf{F}^\times$ generated by $\alpha$. Then $\beta = \alpha^d$ for some $d \in \mathbb{N}$. But $f(x) \mid f(x^d)$ so $\beta$ is a zero of $f$. Thus *the multiplicative subgroup of* $\mathbf{F}^\times$ *generated by any zero of f is a subset of* $\mathfrak{Z}$. It follows, of course, that $\mathfrak{Z}$ consists of certain roots of unity. For $\alpha = \zeta_{k_\alpha}$ a primitive $k_\alpha$th root of unity in $\mathfrak{Z}$ denote by $n_\alpha$ its multiplicity. Suppose, for $\beta \in \mathfrak{Z}$, that $k_\beta \mid k_\alpha$. Then, for some $d \in \mathbb{N}$, we have $\beta = \alpha^d$ whilst $(x - \alpha)^{n_\alpha}$ divides both $f(x)$ and $f(x^d)$. Necessarily, *if* $k_\beta \mid k_\alpha$ *we have* $n_\beta \geq n_\alpha$.

Conversely, *if both the multiplicative subgroup of* $\mathbf{F}^\times$ *generated by any zero of f is a subset of* $\mathfrak{Z}$ *and if, for* $\alpha, \beta \in \mathfrak{Z}$, *whenever* $k_\beta \mid k_\alpha$ *we have* $n_\beta \geq n_\alpha$, *then* $f(x) \mid f(x^d)$, *for all* $d \in \mathbb{N}$. Indeed, for each $\alpha, \beta \in \mathfrak{Z}$ with $d = k_\alpha \mid k_\beta$, we have $(x - \alpha)^{n_\alpha} \mid (x^d - \beta)^{n_\beta}$. Thus $f(x) \mid f(x^d)$, whence the assertion.

For completeness, we also deal with the several variable case $t > 1$. As usual, $x^a$ denotes a monomial $x_1^{a_1} \cdots x_t^{a_t}$. By the factorisation theory briefly sketched at Section 4 we know that an admissible polynomial is a product of binomials $x^a - \alpha x^b$, some nonzero constant $\alpha$, and plainly each $\alpha$ is a root of unity. Moreover, the reducibility of such binomials is independent of $\alpha$ (since the ground field is algebraically

closed) and relies only on the $t$-tuple $a - b$. We shall say the binomial is of *type* $\pm(a - b)$.

Suppose that $f(x)$ is admissible and denote by $g(x) = g_{a-b}(x)$ the product of all of its irreducible binomial factors of type $\pm(a - b)$. Then the factor $g(x)$ is itself admissible because the irreducible factors of $g(x^d)$ are each of type $\pm(a - b)$ and so are prime to irreducible factors of distinct type.

Finally, it is quite obvious that $g_{a-b}(x) = \Pi(x^a - \alpha x^b)^{n_\alpha}$ is admissible if and only if the polynomial in the single variable $x$, $\Pi(x - \alpha)^{n_\alpha}$, is an admissible polynomial in $x$.

**4.4. The Pólya-Cantor lemma.** *Suppose* $\Sigma\, a_h X^h$ *is a formal series with coefficients belonging to a finitely generated ring* $R$ *and let* $f$ *be a polynomial. If* $\Sigma\, f(h)a_h X^h$ *represents a rational function then so does* $\Sigma\, a_h X^h$.

This is Cantor's generalisation [3] of a result of Pólya [12].

Because a recurrence sequence is the sequence of values of an exponential polynomial at the nonnegative integers (note Section 2.5 above), it is plain that the Pólya-Cantor Lemma asserts that if a polynomial $f$ and an exponential polynomial $b$ have the property that the quotients $b(h)/f(h)$ of their values at the nonnegative integers $h = 0, 1, 2, \ldots$ happen all to belong to a ring $R$ of finite type, then $f(z)$ divides $b(z)$ in the ring of exponential polynomials. It is easy to see, from the proof of the lemma, for example, that this entails that the polynomial $f$ divides each of the coefficients of $b$ in the ring of polynomials.

**4.5. The Hadamard quotient theorem.** *Let* $\mathbf{F}$ *be a field of characteristic zero and* $(a'_h)$ *a sequence of elements of a subring* $R$ *of* $\mathbf{F}$ *which is finitely generated over* $\mathbb{Z}$. *Let* $\Sigma\, b_h X^h$ *and* $\Sigma\, c_h X^h$ *be formal series over* $\mathbf{F}$ *representing rational functions. Denote by* $J$ *the set of integers* $h \geq 0$ *such that* $b_h \neq 0$. *Suppose that* $a'_h = c_h/b_h$ *for all* $h \in J$. *Then there is a sequence* $(a_h)$, *with* $a_h = a'_h$ *for* $h \in J$, *such that the series* $\Sigma\, a_h X^h$ *represents a rational function.*

This is a far-reaching generalisation of the result of Pólya-Cantor. It asserts that if the Hadamard quotient of two rational functions is possibly rational—in the sense that the quotient sequence belongs to a ring of finite type—then it is indeed rational. The steps of the proof are detailed in [13] and the lecture notes of Rumely [17] provide a full

account, almost from first principles. The proof fills the gaps in the claims made by Pourchet [15].

It is plain that the Hadamard Quotient Theorem asserts that if exponential polynomials $c(z)$ and $b(z)$ have the property that the quotients $c(h)/b(h)$ of their values at the nonnegative integers $h = 0, 1, 2, \ldots$ happen all to belong to a ring $R$ of finite type, then $b(z)$ divides $c(z)$ in the ring of exponential polynomials. Of course this entails that each simple and each irreducible factor of the exponential polynomial $b$, in the ring of exponential polynomials, divides some simple, respectively irreducible, factor of the exponential polynomial $c$ in the ring of exponential polynomials. One *caveat* must be entered: The Hadamard Quotient Theorem is a result dealing with generalised power sums. Its analytic continuation to exponential polynomials relies on the exponential polynomials being given *a priori*, or upon there being a coherent analytic continuation of the data.

## 5. Divisibility sequences.

**5.1. Proof of the main result.** Let $(a_h)$ be a recurrence sequence and let $d > 1$ be a positive integer. By the Hadamard Quotient Theorem (Section 4.5), if $a_h | a_{dh}$ for all $h = 0, 1, 2, \ldots$ (in the sense that the quotients all belong to a ring $R$ of finite type), then

$$\sum \frac{a_{dh}}{a_h} X^h,$$

is a rational function, which is to say, $b(h) = a(dh)/a(h)$ $h = 0, 1, 2, \ldots$ is a generalised power sum. We allege that appropriate analytic continuation $\mathbb{N} \hookrightarrow \mathbb{C}$, yields an identity in exponential polynomials $b(z) = a(dz)/a(z)$. As remarked above, we must show that this continuation can be effected coherently. Accordingly, let $\mathcal{A}$ be the multiplicative subgroup of the base field generated by the roots of the generalised power sum $a$. Suppose $l$ is the order of the torsion subgroup. By using just the data $a_{hl} | a_{dhl}$ for all $h = 0, 1, 2, \ldots$, we shall, in the immediate sequel, suppose that $\mathcal{A}$ is free. By Proposition 1 of Rumely and van der Poorten [18], the given generalised power sum identity entails that the roots of the generalised power sum $b$ belong to the group generated by $\mathcal{A}$ and $\mathcal{A}^d$, that is, to $\mathcal{A}$. Thus, given a minimal generating set for $\mathcal{A}$, a

selection of a logarithm of each of the generators effects the claimed coherent continuation.

According to the factorisation theory in the ring of exponential polynomials (see Section 4.1) an exponential polynomial in the variable $z$ is a product of irreducible exponential polynomials, simple exponential polynomials and possibly a polynomial in $z$. If $c(z)$ is an irreducible exponential polynomial then $c(dz)$ is not divisible, by virtue of its irreducibility, by $c(z)$ in the ring of exponential polynomials; nor can $c(z)$ divide any irreducible exponential polynomial other than its own associates. It follows that the exponential polynomial $a(z)$ is a product of simple exponential polynomials and, possibly, a polynomial in $z$.

But simple exponential polynomials factor into exponential polynomials of the shape $\exp(\omega z) - A$. The discussion at Section 4.3 makes it plain that if a product $g(z)$ of such exponential polynomials divides $g(dz)$ in the ring of exponential polynomials then each $A$ is a root of unity. After a congenial normalisation, products of these simple exponential polynomials yield the resultant sequences introduced at Section 3.1. Moreover, the discussion at Section 4.3 allows one to describe all products of simple exponential polynomials yielding nondegenerate divisibility sequences.

Finally, by the Pólya-Cantor Lemma (see Section 4.4), a polynomial $p(z)$ divides an exponential polynomial in the ring of exponential polynomials if and only if each coefficient of that exponential polynomial is divisible by $p(z)$ in the ring of polynomials. Thus, if $p(z)$ divides $a(z)$ then $p(dz)$ divides $a(dz)$ in the ring of exponential polynomials. So $p(z) \mid p(dz)$ in the ring of polynomials and, obviously, $p(z)$ is of the shape $Bz^k$, some nonzero constant $B$ and some nonnegative integer $k$.

We have written as if the group of roots $\mathcal{A}$ of $(a_h)$ were free. If it has torsion $l$ then we have shown only that there is a generalized resultant sequence $(R_h)$ such that $a_{lh} \mid R_h$ for all $h$. However, also $a_h \mid a_{lh}$, since $(a_h)$ is a divisibility sequence. Thus $a_h \mid R_h$ for all $h$.

This concludes our proof of the claim that if $(a_h)$ is a divisibility sequence, then there is a recurrence sequence

$$\bar{a}_h = h^k \prod_i \left( \frac{\alpha_i^h - \beta_i^h}{\alpha_i - \beta_i} \right),$$

and $a_h \mid \bar{a}_h$ for $h = 1, 2, 3, \ldots$.

**5.2. Remarks on a more general result.** At Section 1.3 we undertook to prove that if there is a suitable integer $d > 1$ so that $a_h | a_{dh}$ for all $h$ then the recurrence sequence $(a_h)$ divides a generalised resultant sequence.

The preceding argument in effect declares that $d$ is suitable if the order $l$ of the torsion subgroup of the group generated by the roots of the recurrence sequence divides $d$. We are indebted to the referee for pointing out that our argument is capable of being carried through for any $d > 1$. We confine ourselves to a sketch of that argument.

Given $d$ one chooses $l'$ maximal so that $\gcd(l', d) = 1$ and $l' | l$. Then there are positive integers $k$ and $e$ so that $l | l'd^k$ and $d^e \equiv 1 \pmod{l'}$. In place of $a(h)$, consider the $l'$ generalised power sums

$$a_r(h) = a(l'd^k h + rd^k) = \sum_{i=1}^{m} \alpha_i^{rd^k} A_i(l'd^k h + rd^k))\alpha_i^{l'd^k})^h$$

where $r = 0, 1, \ldots, l' - 1$.

Note that $\gcd(l', d) = 1$ entails that $rd^k$ runs through the distinct residue classes mod $l'$ as $r$ does.

The data $a(h) | a(dh)$ and $d^e \equiv 1 \pmod{l'}$ yields, for each $r$ and all $h$,

$$a_r(h) | a_r(d^e h + rd^k(d^e - 1)/l').$$

We have arranged that the group generated by the roots of $a_r(h)$ has no torsion so, by the Hadamard Quotient Theorem, the data lifts to an exponential polynomial dividing a corresponding exponential polynomial. A similar, though a more complicated and considerably more notation intensive argument to that of Section 5.1 eventually shows that each $a_r(h)$ is the translation, by $rd^k$, of a generalised power sum dividing a generalised power sum given by a generalised resultant sequence. Pursued *in extenso* the argument *inter alia* retrieves the remarks on degeneracy and the result of Pólya on Hadamard invertible rational functions cited at Section 3.3.

UNIVERSITÉ PARIS VI, 75230 PARIS CEDEX 05 FRANCE
KOSSUTH LAJOS UNIVERSITY, H—4010 DEBRECEN PF. 12 HUNGARY
MACQUARIE UNIVERSITY, NSW 2109 AUSTRALIA

## REFERENCES


[1] Jean-Paul Bézivin, Solution d'une conjecture de M. Ward sur les suites récurrentes arithmétiques, (manuscript).

[2] P. Bundschuh and A. Pethö, Zur Transzendenz gewisser Reihen, *Monatshefte Math.*, **104** (1987), 199–223.

[3] David G. Cantor, On arithmetic properties of the Taylor series of rational functions, *Canad. J. Math.*, **21** (1969), 378–382.

[4] Eli Gourin, On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves, *Trans. Amer. Math. Soc.*, **32** (1930), 485–501.

[5] Marshall Hall, Divisibility sequences of third order, *Amer. J. Math.*, **58** (1936), 577–584.

[6] P. Horak and L. Skula, A characterisation of the second-order strong divisibility sequences, *The Fibonacci Quarterly*, **23** (1985), 126–132.

[7] Clark Kimberling, Strong divisibility sequences with nonzero initial term, *The Fibonacci Quarterly*, **16** (1978), 541–544.

[8] ———, Strong divisibility sequences and some conjectures, *The Fibonacci Quarterly*, **17** (1979), 13–17.

[9] ———, Generating functions of linear divisibility sequences, *The Fibonacci Quarterly*, **18** (1980), 193–208.

[10] A. Pethö, Divisibility properties of linear recursive sequences, *Proc. International Conf. Number Theory, Coll. Math. Soc. János Bolyai*, Budapest, 1987.

[11] Tracy A. Pierce, The numerical factors of the arithmetic forms $\Pi_{i=1}^{n}(1 \pm \alpha_i^m)$, *Annals of Math.*, **18** (1917), 53–64.

[12] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. für Math.*, **151** (1920), 1–31.

[13] Alfred J. van der Poorten, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles, *C. R. Acad. Sc. Paris*, **306** Série 1, (1988), 97–102.

[14] ———, Some facts that should be better known, especially about rational functions, in R. A. Mollin ed., *Number Theory and Applications*, (NATO-ASI, Banff 1988), Kluwer Academic Publishers, Dordrecht, (1989), 497–528.

[15] Yves Pourchet, Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles, *C. R. Acad. Sc. Paris*, **288** (1979), A1055–1057.

[16] J. F. Ritt, A factorisation theory for functions $\Sigma_{i=1}^{n} a_i e^{\alpha_i z}$, *Trans. Amer. Math. Soc.*, **29** (1927), 584–596.

[17] Robert S. Rumely, Notes on van der Poorten's proof of the Hadamard Quotient Theorem, *Sém. Théorie des Nombres de Paris 1986–87*, Birkhäuser (1989), Part I, 349–382; Part II, 383–409.

[18] ——— and A. J. van der Poorten, Remarks on generalised power sums, *Bull. Austral. Math. Soc.*, **36** (1987), 311–329.

[19] Andrzej Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor (1982).

[20] ———, Second order strong divisibility sequences in an algebraic number field, *Archivum Mathematicum (Brno)*, **23** (1987), 181–186.

[21] Ronald Solomon, Divisibility properties of certain recurring sequences, *The Fibonacci Quarterly*, **14** (1976), 153–158.

[22] Morgan Ward, Linear divisibility sequences, *Trans. Amer. Math. Soc.*, **41** (1937), 276–286.
[23] _____, The law of apparition of primes in a Lucasian sequence, *Trans. Amer. Math. Soc.*, **44** (1938), 68–86.
[24] _____, Arithmetical properties of sequences in rings, *Annals of Math.*, **39** (1938), 210–219.
[25] _____, Memoir on elliptic divisibility sequences, *Amer. J. Math.*, **70** (1948), 31–74.