ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

A NOTE ON HADAMARD ROOTS OF RATIONAL FUNCTIONS

A.J. VAN DER POORTEN

To Wolfgang Schmidt on the occasion of the celebration of his 60th birthday

ABSTRACT. Suppose F is a polynomial and $\sum_{h\geq 0} F(b_h)X^h$ represents a rational function. If the b_h all belong to a field finitely generated over $\mathbf{Q}$, then it is a generalization of a conjecture of Pisot that there is a sequence (c_h) with $F(c_h) = F(b_h)$ for $h = 0, 1, \ldots$ so that also $\sum_{h\geq 0} c_h X^h$ represents a rational function. We explain the context of this Hadamard root conjecture and make some suggestions that might lead to its proof, emphasizing the apparent difficulties that have to be overcome and the ideas that might be employed to that end.

1. Introduction. Suppose that a polynomial $f(X) \in \mathbf{Z}[X]$ is a cube for all integer values of X. In effect, by the Hilbert irreducibility theorem, but in any case directly, it is easy to show that f is the cube of a polynomial in $\mathbf{Z}[X]$.

In such a spirit, Pisot conjectured, see the remark in [**1**], that if a power sum

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

is a cube for all h then there is a power sum $b(h) = b_h$ so that $a(h) = b_h^3$ for all h. Here the *roots* α_i are distinct numbers and the coefficients A_i are polynomials, say of respective degrees $n_i - 1$. One says that the power sum has *order* $\sum_{i=1}^{m} n_i = n$. We should recall that a generalized power sum $a(h) = a_h$ provides the sequence (a_h) of Taylor coefficients of a rational function $r(X)/s(X) = \sum_{h=0}^{\infty} a_h X^h$, with

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

Received by the editors on February 5, 1995, and in revised form on May 3, 1995.
1991 AMS *Mathematics Subject Classification.* 11B37, 11B39.
Work supported in part by grants from the Australian Research Council and a research agreement with Digital Equipment Corporation.

and $\deg r < n$. It is then plain that (a_h) is a *recurrence sequence*, satisfying

$$a_{h+n} = s_1 a_{h+n-1} + s_2 a_{h+n-2} + \cdots + s_n a_h.$$

In slightly different language, if E denotes the operator $E : f(h) \mapsto f(h+1)$ one sees that the operator $\prod (E - a_i)^{n_i}$ annihilates the power sum $a(h)$.

Thus, Pisot suggests that if $\sum_{h\geq 0} b_h^3 X^h$ is a rational function and all the b_h are integers, then also its *Hadamard cube root* $\sum_{h\geq 0} b_h X^h$ is a rational function. The notion of *Hadamard operation* on a power series seems to arise from a theorem of Hadamard of 1898, see [**5**], on the singularities of the series $\sum a_h b_h z^h$ relative to those of $\sum a_h z^h$ and $\sum b_h z^h$.

This note was to have sketched a proof of Pisot's conjecture. It does not. It discusses the context of the problem and mentions some new ideas that may bring us closer to a solution.

The genesis of problems of the present genre is Pólya's theorem [**8**], that if $\sum h a_h X^h$ is a rational function and the a_h all are integers, then also $\sum a_h X^h$ is a rational function. This leads to the observation that a rational function $\sum_{h\geq 1} b_h X^h$ has no simple poles if and only if the quantities b_h/h all belong to a ring finitely generated over $\mathbf{Z}$. It is easy to see, because the Taylor coefficients are given by a power sum, that if a series $\sum a_h X^h$ is rational, then the a_h do all belong to a ring finitely generated over $\mathbf{Z}$. Of course, this evidently necessary condition for rationality is generally far from sufficient.

Here, however, we shall sketch arguments that might lead to a generalization of Pisot's conjecture, whereby if there is a series $\sum b_h X^h$ that is *possibly* rational, in the sense just alluded to, and $\sum b_h^k X^h$ is rational, then there exists a rational series $\sum c_h X^h$ with $c_h^k = b_h^k$ for all $h = 0, 1, 2, \ldots$.

There are analytic analogues of the arithmetic conjectures and results discussed here. Continued to $\mathbf{C}$, the power sum $a(h)$ becomes an *exponential polynomial*

$$a(z) = \sum A_i(z) \exp(z \log \alpha_i);$$

actually, one of infinitely many such functions, according to choice of the logarithms. Theorems of Ritt say that if a quotient of exponential

polynomials is entire then it is essentially an exponential polynomial [**16**]; and if a zero of a polynomial

$$\mathcal{F}(z, Y) = a_{(0)}(z)Y^k + a_{(1)}(z)Y^{k-1} + \cdots + a_{(k)}(z), \tag{1}$$

with exponential polynomial coefficients is entire, then that zero is essentially an exponential polynomial [**15**]. The qualification 'essentially' is required to cope with such exceptions as $(e^z - 1)/z$ which may arise from dividing by a polynomial, and can occur only if the divisor, respectively the leading coefficient $a_{(0)}(z)$, have a polynomial factor in the ring of exponential polynomials. Pisot's root conjecture is the arithmetic analogue of the case $\mathcal{F}(z, Y) = Y^3 - a(z)$.

For an extensive survey of these and many related matters, see [**10**].

2. The dominant root case. Pisot's conjecture seems peculiarly intractable. However, suppose we order the roots α_i so that

$$|\alpha_1| = |\alpha_2| = \cdots = |\alpha_t| > |\alpha_{t+1}| \geq \cdots \geq |\alpha_m|.$$

When $t = 1$, the 'dominant root' case, it is a general principle that power sums are much less recalcitrant. Indeed, in this case there is a relatively simple proof of the conjecture for kth roots [**18**]. We need only the hypothesis that there is a field finitely generated over $\mathbf{Q}$ containing a kth root of each $a(h)$. Then an argument generalizing that of Perelli and Zannier [**7**] shows one loses no generality in supposing that the leading coefficient $A_1(h)$ is a constant, so after dividing by the leading term if necessary, we lose no generality in writing $a(h) = a_h = 1 + c_h$, with c_h a power sum with roots all of absolute value less than 1. Hence we may write

$$\begin{aligned} b_h = a_h^{1/k} &= 1 + \binom{1/k}{1} c_h + \cdots + \binom{1/k}{l} c_h^l + R_l(h) \\ &= C_l(h) + R_l(h), \end{aligned} \tag{2}$$

where the number of terms of the power sums $C_l(h)$ increases linearly in l as $l \to \infty$, and the remainder $R_l(h)$ is very small.

Because the $C_l(h)$ are power sums, there are polynomials P_l independent of h so that the operator $P_l(E)$ annihilates $C_l(h)$. That yields

$$P_l(E)(b_h) = P_l(E)(R_l(h)). \tag{3}$$

The left-hand side of (3) has size $O(e^{\theta l+\kappa h})$ whereas the right-hand side is as small as $O(e^{-\delta lh})$; here θ, κ and δ are positive constants. When the data is algebraic, so the b_h all lie in some number field, this is absurd for l and h sufficiently large unless $P_l(E)(b_h) = 0$; that is, since it is annihilated by a linear operator $P_l(E)$, $b(h) = b_h$ is a power sum and $\sum b_h X^h$ is a rational function. One deals with the nonalgebraic case by a specialization argument detailed in [**18**].

For its dominant root case, a very similar argument proves a related conjecture of Pisot to the effect that if a quotient $c(h)/a(h)$ of power sums is in $\mathbf{Z}$ for all h, then it is itself a power sum. That was shown by David Cantor [**2, 3**] when $a(h)$ has a dominant root. Eventually, the general case required a rather different proof [**9**] seemingly relying on quite other principles.

Naturally, I expected that the new ideas used to prove the Hadamard quotient theorem could also be applied successfully to the present problem. However, the late Philippe Robba alerted me to a seemingly fatal obstruction. Namely, the binomial expansion (2), which relies in an essential way on there being a dominant root with respect to some absolute value $|\quad|$, does more than just explicitly display the kth roots. It actually guarantees that we are choosing those kth roots *coherently*.

In any event, the root problem presented other difficulties more complicated than those of the quotient case, so I never had to meet incoherence head-on. Then, recently, in sketching an elementary proof [**12**] of the Lech-Mahler theorem on zeros of the Taylor coefficients of rational functions to my student Sam Williams, I noticed a technique that might lead around those other difficulties.

3. Principles. There is a well-known criterion for the rationality of a power series $\sum b_h X^h$. Namely, the series is rational if and only if the Kronecker-Hankel determinants

$$K_N(b) = |b_{i+j}|_{0\le i,j\le N} = \begin{vmatrix} b_0 & b_1 & \cdots & b_N \\ b_1 & b_2 & \cdots & b_{N+1} \\ \vdots & \vdots & & \vdots \\ b_N & b_{N+1} & \cdots & b_{2N} \end{vmatrix}$$

vanish for all N greater than some n. The recurrence relation for the b_h makes necessity obvious, and sufficiency follows by remarking

that if $K_{n-1}(b) \neq 0$ whilst $K_n(b) = 0$, we may set $c_h = b_{h+n} - s_1 b_{h+n-1} - \cdots - s_n b_n$, with certain constants $s_1, \ldots, s_n$ so that $c_h = 0$ for $h = 0, 1, \ldots, n$. Then $K_{n+1}(b) = -c_{n+1}^2 K_{n-1}(b)$, and $K_{n+1}(b) = 0$ entails also $c_{n+1} = 0$. So, by induction, $K_N(b) = 0$ for all $N \geq n$ entails $c_h = 0$ for all $h = 0, 1, \ldots$.

In his proof of the Weil conjecture on the rationality of the Zeta-function of varieties, see [**6**], Dwork proves the vanishing of the $K_N(b)$ in effect by showing that closely related determinants $|b_{i+j}|_{M \leq i,j \leq N}$ are divisible by an arbitrary high power of a prime p. The chosen prime p divides some root β_i of the putative power sum $b(h)$. In contrast, following a suggestion of Pourchet [**14**], one may work with a complementary set of primes. One uses a large set $\mathcal{P}$ of primes all splitting completely in the underlying number field and eventually shows that, for large N,

$$\prod_{p \in \mathcal{P}} p^{\lfloor N(N+1)/(p-1) \rfloor} \Bigg| K_N(b),$$

or so. I add the 'or so' to acknowledge that the precise exponents for the p need minor adjustment; see [**18**] for a very detailed discussion. The $p \in \mathcal{P}$ must be so that roots of power sums appearing amongst the data all are p-adic units. The $K_N(b)$ vanish because one may choose $\mathcal{P}$ so that $\prod_{p \in \mathcal{P}} p^{1/(p-1)}$ is arbitrarily large.

However, working with more than one prime means one has to combine p-adic data for different p. The trick is to be naive. One chooses to deal just with congruences $\mod p^{M_p}$, for suitable integers M_p at least as large as $2N/(p-1)$. Then the Chinese remainder theorem allows one to combine the data as information modulo $\prod_{p \in \mathcal{P}} p^{M_p}$.

An effect of the naive approach is that power sums become polynomials. Suppose that $\alpha_i \equiv 1 \pmod p$ for all the roots of the power sum $\sum_{i=1}^m A_i(h) \alpha_i^h$. Then

$$\begin{aligned} a(h) &= \sum A_i(h)(1 + (\alpha_i - 1))^h \\ &= \sum_j \sum_i \mathfrak{A}_i(j)(\alpha_i - 1)^j \binom{h}{j}; \end{aligned} \tag{4}$$

some thought and reorganization is required to obtain the polynomials

$\mathfrak{A}_i$, each again of degree $n_i - 1$. Now the point is that

$$\mathfrak{a}_j = \sum_i \mathfrak{A}_i(j)(\alpha_i - 1)^j$$

satisfies a recurrence relation $\mathfrak{a}_{h+n} = t_1\mathfrak{a}_{h+n-1} + \cdots + t_n\mathfrak{a}_h$ with all roots divisible by p, so $\operatorname{ord}_p t_j \geq j$. Hence the minimum $\mu = \min \operatorname{ord}_p \mathfrak{a}_j$ can occur only for $j < n$. By renormalizing we may suppose that $\mu = 0$ and obtain

$$a(h) \equiv \sum_{0 \leq j < n} \sum_i \mathfrak{A}_i(j)(\alpha_i - 1)^j \binom{h}{j} \tag{5}$$

over the finite field $\mathbf{F}_p$.

It is easy to pursue the preceding argument to see that the recurrence relation entails $\operatorname{ord}_p \mathfrak{a}_j > j - n$. In particular, we may interpolate p-adically and use (4) to view $a(t)$ as a function of a p-adic variable, convergent for all t with $\operatorname{ord}_p t > -1 + 1/(p-1)$. It now follows from (5), in effect the Weierstraß preparation theorem, that $a(t)$ has fewer than n zeros if $p > n$; for more on that topic see [**13**].

For our purposes it is helpful to notice that, if $\Delta = E - 1$ is the difference operator, then $\operatorname{ord}_p \Delta^k a(h) > k - n$. Hence, by

$$K_N(a) = |a(i+j)|_{0 \leq i,j \leq N} = |\Delta^{i+j} a(\underline{0})|_{0 \leq i,j \leq N},$$

it follows that $p^{N(N+1)} | K_N(a)$. The $\underline{\ }$ marks the quantity on which Δ operates.

In general, we don't have $\alpha_i \equiv 1 \pmod{p}$. But, if p splits completely in the base field and is prime to the α's, we may restrict to subsequences. The roots α_i^{p-1} of the power sums

$$a(r + h(p-1)), \quad 0 \leq r < p - 1$$

are all congruent to 1. The remarks above now hold only for each of the $p - 1$ subsequences $a(r + h(p-1))$, that is, we have

$$\operatorname{ord}_p \Delta^k a(r + \underline{h}(p-1)) > k - n$$

for each r. Mildly more complicated manipulations within the Kronecker-Hankel determinants lead to $\operatorname{ord}_p K_N(a) \gtrsim \lfloor N(N+1)/(p-1) \rfloor$.

4. Short sketch of the proof of the Hadamard quotient theorem. It may yield conviction to the eventual suggestions I make for attacking the root theorem to provide first an analogous sketch of an established argument, the proof of the quotient theorem. Here, after specialization if necessary, we have power sums $c(h) = c_h = \sum_j C_j(h)\gamma_j^h$ and $a(h) = a_h$, and are given that the quotients $c_h/a_h = b_h = b(h)$ all belong to a ring of S-integers of some number field. As usual, S is some finite set of places including the archimedean places. As in Section 3, we suppose first that for some prime p the roots γ_j and α_i all are congruent to 1 mod p. Then the quotient $c(h)/a(h)$ may be p-adically interpolated to yield a quotient $c(t)/a(t) = b(t)$ of p-adic exponential polynomials, converging for $\operatorname{ord}_p t > -1 + 1/(p-1)$, other than for possible poles occasioned by the zeros of $b(t)$. Since there are at most $n-1$ such zeros if p is larger than n, there is a polynomial $f_p(t)$ defined over $\mathbf{Z}_p$, and of degree less than n, so that $f_p(t)b(t)$ has no such poles. Less technically, the point is, as above, that multiplication by $f_p(h)$ yields $\operatorname{ord}_p \Delta^k f_p(h)b(h) > k - n$ and hence $\operatorname{ord}_p K_N(f_p \cdot b) \geq N(N+1)$.

Of course, we cannot expect to have those useful congruence conditions on the roots of the given power sums. Accordingly, let $\mathbf{K}$ be a number field containing all the data, to wit the roots and the coefficients of the polynomial coefficients of $c(h)$ and $a(h)$, and thus also the quotients $b(h)$. We next choose rational primes p that split completely in $\mathbf{K}$ and that are large enough to avoid the finitely many primes at which any datum is nonintegral or at which a root of either power sum is a nonunit. By Tschebotarev, there are finite sets $\mathcal{P}$ of such p so that $\prod_{p\in\mathcal{P}} p^{1/(p-1)}$ is as large as we wish.

Next we restrict to subsequences to get the congruence conditions on the roots, at the cost of obtaining just

$$\operatorname{ord}_p K_N(f_p \cdot b) \gtrsim \lfloor N(N+1)/(p-1) \rfloor.$$

Now the problem is that we need such an inequality for all $p \in \mathcal{P}$, of course with an $f_{\mathcal{P}}$ common to all those p. As said above at Section 3, naivete comes to the rescue. We only ever use $f_p \bmod p^{M_p}$, so no harm whatsoever is done if we truncate the coefficients of f_p modulo p^{M_p} and allow abuse of notation to transform f_p to a polynomial over $\mathbf{Z}$, mind you, with rather hefty coefficients since they are remainders

$\bmod p^{M_p}$. Now we can use the Chinese remainder theorem to concoct a polynomial $f_{\mathcal{P}}$, with coefficients remainders modulo $\mathcal{M}_{\mathcal{P}} = \prod_{p\in\mathcal{P}} p^{M_p}$, to serve as the common multiplier.

Thus, finally we have $\operatorname{ord}_p K_N(f_{\mathcal{P}}\cdot b) \gtrsim \lfloor N(N+1)/(p-1)\rfloor$ for all $p\in\mathcal{P}$. This entails that $K_N(f_{\mathcal{P}}\cdot b)=0$ or, for all large N,

$$|K_N(f_{\mathcal{P}}\cdot b)| \gtrsim \prod_{p\in\mathcal{P}} p^{\lfloor N(N+1)/(p-1)\rfloor}.$$

One would now like to conclude, because we are free to choose $\prod_{p\in\mathcal{P}} p^{1/(p-1)}$ as large as we wish, that indeed $K_N(f_{\mathcal{P}}\cdot b)=0$.

That doesn't work because of the coefficients of $f_{\mathcal{P}}$, which may be as large as $\mathcal{M}_{\mathcal{P}}$, and thus depend on both $\mathcal{P}$ and N. Although I do not believe that a proof of the root conjecture can involve a multiplier, for completeness I explain the resolution of the difficulty just mentioned. The idea, very obscurely suggested in [**14**], is that multiplication by some polynomial f with integer coefficients, yielding $g_{\mathcal{P}} = f\cdot f_{\mathcal{P}}$ with coefficients remainders modulo $\mathcal{M}_{\mathcal{P}}$, provides just as good a multiplier as did $f_{\mathcal{P}}$. One applies the box principle to show the existence of an f yielding a multiplier $g_{\mathcal{P}}$ of rather larger degree than that of $f_{\mathcal{P}}$, but with coefficients that are remainders modulo $\mathcal{M}_{\mathcal{P}}$ fairly small in absolute value when viewed as elements of $\mathbf{Z}$. For quantitative details, see [**9**].

Now one can prove $K_N(g_{\mathcal{P}}\cdot b)=0$ for a long range of N, sufficiently long to allow the decision that $\sum g_{\mathcal{P}}(h)b_hX^h$ is a rational function. Finally, the Pólya-Cantor lemma, David Cantor's generalization of Pólya's result, permits the conclusion that also $\sum b_hX^h$ is rational, as was to have been proved.

The complete argument is detailed *in extenso* by Robert Rumely [**17**].

5. Arguments that might prove a Hadamard root theorem. Finally we are ready to consider the supposition that $a(h)=b_h^k$ with $a(h)$ a power sum, and the b_h all in some number field, after our having specialized if necessary. Let $\mathbf{K}$ be a number field containing all the data, namely the roots and coefficients of the polynomial coefficients of $a(h)$, and the sequence of given kth roots b_h. Let p be a prime much larger than n and k, and $\equiv 1 \pmod k$. Then $\mathbf{F}_p$ contains the k different kth roots of unity. Supposing that all the roots α_i of $a(h)$ are $1 \bmod p$, just

as we temporarily assumed above, we have (5) reporting that over $\mathbf{F}_p$, the power sum $a(h)$ is some polynomial $F_p(h)$ of degree less than n. That is, over $\mathbf{F}_p$ we have a curve

$$y^k = F_p(x) \tag{6}$$

with lots of rational points, that is, points (x, y) in $\mathbf{F}_p^2$, because for each x there is a $y \in \mathbf{F}_p$ by the kth root data, and, therefore, because $\mathbf{F}_p$ contains the kth roots of unity, other than corresponding to the fewer than n zeros of F_p, there are k different such y.

It is hardly necessary to invoke Weil's theorem on the number of points on curves over a finite field, and of course weaker results will do, but it suffices to remark that, with k and n much smaller than p^2, say, an irreducible curve (6) of degree $\max(k, n)$ has genus much smaller than $\sqrt{p}$ and cannot have many more than p rational points. Since we have found almost kp rational points, it follows that (6) splits into factors linear in y. That is, F_p, which is just $a(h) \bmod p$, is a kth power of a polynomial in $\mathbf{F}_p[x]$.

Accordingly, we may choose an arbitrary kth root of $a(h) \bmod p$, and endeavor to construct a kth root $b_{p,C}(h) \bmod p^{M_p}$ with $\operatorname{ord}_p \Delta^k b_{p,C}(h) > k - n$. Here the subscript C alludes to the *choice* we have made of kth root. Were our endeavor to succeed, we would obtain $\operatorname{ord}_p K_N(b_{p,C}) \geq N(N+1)$.

The realization that $a(h) \bmod p$ automatically just had to be a kth power, given the data, is the first of my new thoughts on Pisot's conjecture. I am indebted to Gerry Myerson for reminding me that Weil's theorem might be invoked to confirm that fact. I say 'just had to be' because it had long been evident to me that in the root case there is no analogue of the multiplier which is applied in the quotient case to remove possible singularities. Thus, for the present approach to work, all just has to be well. Unfortunately, all is not well.

The fact that $a(h)$ is a kth power $\bmod p$ does not automatically lift to it being a kth power $\bmod p^N$. With a little work one can show that the remarks above entail that the p-adic power series $b_{p,C}(t)$ have no singularities in $\mathbf{Z}_p$. But, showing these functions have no singularities for $\operatorname{ord}_p t > -1 + 1/(p-1)$, which is what is needed, requires an additional idea allowing one to use the data that for $h = 0, 1, 2, \ldots$, the $b_{p,C}(h)$ all lie in some number field. Nevertheless, for the next few

paragraphs, let me suppose that, somehow, we have shown that the $b_{p,C}(t)$ do converge for $\operatorname{ord}_p t > -1 + 1/(p-1)$.

Of course, generally we would not have the congruence conditions on the roots of the given power sum. Accordingly, let $\mathbf{K}$ be a number field containing all the data, to wit the roots and the coefficients of the polynomial coefficients of $a(h)$, and the given kth roots b_h. Let ζ_k denote a primitive kth root of unity. We now choose rational primes p that split completely in $\mathbf{K}(\zeta_k)$ and that are large enough to avoid the finitely many primes at which any datum is nonintegral or at which a root of either power sum is a nonunit. Moreover, to sustain the argument above, we require that the p be much larger than k and n. By Tschebotarev, there are finite sets $\mathcal{P}$ of such p so that $\prod_{p\in\mathcal{P}} p^{1/(p-1)}$ is as large as we wish.

Now we restrict to subsequences, as described above in Section 3, to get the congruence conditions on the roots. The cost is that we obtain just $\operatorname{ord}_p K_N(b_{p,C}) \gtrsim \lfloor N(N+1)/(p-1)\rfloor$. Here the subscript $C = C_p$ refers to the *set* of choices of kth root we have made for the $p-1$ remainders r.

At this point we would have constructed sequences of rational integers $b_{p,C}(h)$, strictly speaking, of remainders $\bmod p^{M_p}$. Next we apply the Chinese remainder theorem to piece together the information so obtained. That yields sequences $b_C(h)$ of rational integers defined $\bmod \mathcal{M}_\mathcal{P} = \prod_{p\in\mathcal{P}} p^{M_p}$, with the property that the determinants $K_N(b_C)$ satisfy $\operatorname{ord}_p K_N(b_C) \gtrsim \lfloor N(N+1)/(p-1)\rfloor$ for each $p \in \mathcal{P}$. By now, $C = C_\mathcal{P}$ refers to the collection of choices made for all $p \in \mathcal{P}$ and all their respective r.

Now we would meet the next difficulty. We cannot allege ourselves to have guaranteed any sort of coherence in our 'choices.' Indeed, there seems to be no *a priori* meaning at all for coherence in this context other than to beg the question and to describe a sequence (b_h) of kth roots of a power sum $a(h)$ as 'coherent' if and only if $b_h = b(h)$ does indeed provide a power sum. To make the point, even our $p-1$ choices for each p seem independent. So it does not make sense to claim that the $b_C(h)$ p-adically, let alone globally, simulate kth roots of the a_h, whatever our good local planning for the subsequences given by $b_{p,C}(r+h(p-1))$ for fixed C, p and r. Locally, of course, each such subsequence is p-adically close to a kth root of the power sum $a(r+h(p-1))$. But, not only have

we no guarantee as r varies that we are close to the 'same' kth root of $a(h)$, because it is not completely clear what that might mean, all the more for a given choice $C_{\mathcal{P}}$ yielding $r + h(p-1) = r' + h'(p'-1)$, we surely have no way of having forced the two values $b_{p,C}(r+h(p-1))$ and $b_{p',C}(r'+h'(p'-1))$ to be close p-adically, and respectively p'-adically, to the same kth root.

This fundamental incoherence seemed always to vitiate the present line of argument. Nonetheless, I believe I can show that, given earlier suppositions, there is a choice C in the collection of all choices so that $b_C(h)$ does yield a power sum.

The idea is to embrace the incoherence. All said, for each p and r there are just k choices. Denote the finite set of all choices by $\mathcal{C}$. Set $P = \prod_{p\in\mathcal{P}}(p-1)$. We may then remark that there are just $|\mathcal{C}| = k^P$ choices all up.

Thus, if there were no gap in our argument, we would have shown, for each choice $C \in \mathcal{C}$, that we obtain a determinant $K_N(b_C)$ highly divisible by the $p \in \mathcal{P}$, as explained above.

Now consider the product $\prod_{C\in\mathcal{C}} K_N(b_C)$ of those determinants over all the choices. This product is invariant under permutation of choice, so by symmetry it must be a function $D_N(\bar{a})$ of quantities $\bar{a}_h$ coinciding modulo p^{M_p} with the original data a_h for each $p \in \mathcal{P}$; that is, the $\bar{a}_h$ coincide modulo $\mathcal{M}_{\mathcal{P}}$ with the original data a_h. But

$$\operatorname{ord}_p D_N(\bar{a}) \gtrsim |\mathcal{C}|\lfloor N(N+1)/(p-1)\rfloor.$$

Thus, if the M_p satisfy $M_p \geq |\mathcal{C}|N(N+1)/(p-1)$, then

$$\operatorname{ord}_p D_N(a) \gtrsim |\mathcal{C}|\lfloor N(N+1)/(p-1)\rfloor$$

for each $p \in \mathcal{P}$. On the other hand, it is easy to see that there is a positive constant $\mathcal{A}$, depending only on the original power sum $a(h)$, which provides an evident upper bound of the shape $\mathcal{A}^{|\mathcal{C}|N(N+1)/k}$ for the height of $D_N(a)$. Comparing the p-adic bounds with that upper bound shows that taking sufficiently many primes in $\mathcal{P}$ forces $D_N(a) = 0$. That shows that $K_N(b_C) = 0$ for some choice $C \in \mathcal{C}$, and some long range of N, which is what we hoped to be able to show. Finally, it is explained in [**18**] that if there is a power sum Hadamard kth root then there is such a root with order bounded in terms of n

and k. That suffices to prove that the vanishing of the $K_N(b_C) = 0$ for a sufficiently long range of N entails that $b_C(h)$ is indeed a power sum.

My suggestion that incoherence can be tamed, by avoiding the kth roots as such and returning to the original data, is the second new idea. That realization was not immediate. Several years ago I had sketched a hopeless argument which ultimately I named, 'A divergent argument...' [**11**]. For a while I feared having to title this note, 'An incoherent argument...'.

I have pretended throughout that all the data lies in some number field. In fact, for the kth root case Rumely and the author [**18**] have proved that this loses no generality. That relies on a specialization argument allowing one to revert to the algebraic case. Ultimately one lifts back to the transcendental case.

Recall, however, that these fine ideas are relevant only if it is indeed possible to show directly that the p-adic kth roots converge in a 'large' circle.

6. Discussion, remarks and acknowledgments. I have long feared that the argument for the root case may turn out to be technically simpler than that required in the quotient case; and I think so now. There will be no relatively delicate estimates or subtle constructions such as are needed to provide the multiplier in the earlier case.

It also warrants remark that the present argument will be able to be recounted so that the word 'p-adic' never occurs (I now realize that the same holds for the quotient theorem). Thus, technically, the proof will be able to be made elementary.

The argument suggested in Section 5 would provide the proof of the following:

Hadamard Root Conjecture. *Let k denote a positive integer and suppose that $\sum_{h\geq 0} b_h^k X^h$ represents a rational function. If the b_h all belong to a field finitely generated over $\mathbf{Q}$, then there is a sequence (c_h) with $c_h^k = b_h^k$ for $h = 0, 1, \ldots$ so that also $\sum_{h\geq 0} c_h X^h$ represents a rational function.*

In fact, one could then claim a little more. With a_h replacing b_h^k above, the argument would not require that *all* the a_h be kth powers, but only that sufficiently many consecutive a_h be known to be kth powers. The sufficient number would depend on k and the given rational function and could be determined effectively, at any rate up to estimates arising from the invocation of Tschebotarev.

Consequently, it is reasonable to suggest that if $\sum_{h\geq 0} a_h X^h$ represents a rational function and if, for some dense subset $H \subseteq \mathbf{Z}_{\geq 0}$, we have $a_h = b_h^k$ with the b_h all belonging to a field finitely generated over $\mathbf{Q}$ when $h \in H$, then there is a positive integer d and some r with $0 \leq r < d$, and a sequence (c_h) with $c_h^k = a_{r+hd}$ so that also $\sum_{h\geq 0} c_h X^h$ represents a rational function. That would follow from the above by virtue of Szemeredi's result to the effect that H contains arbitrarily long arithmetic progressions, on noting that $\sum_{h\geq 0} a_{r+hd} X^h$ represents a rational function.

Incidentally, in light of terms like 'symmetric square' currently bandied about in relation to Fermat's last theorem, it may be though amusing to remark that what we are attempting to prove is *inter alia* that if a rational function has too many consecutive squares amongst its Taylor coefficients, then that rational function is the *symmetric square* of a rational function.

One presumes that Pisot asked about *cube* roots because an integer has just one real cube root and so, apparently, the Hadamard cube root of a rational function with Taylor coefficients in $\mathbf{Z}$ is therefore well defined. The p-adic nature of our proposed argument is such that this seems to bring no advantage, and in any case it can bring no advantage in the general setting in which we try to argue. Indeed, our argument clearly would allow a generalization to the case where F is a polynomial and $\sum_{h\geq 0} F(b_h) X^h$ represents a rational function. Namely, if the b_h all belong to a field finitely generated over $\mathbf{Q}$, then there is a sequence (c_h) with $F(c_h) = F(b_h)$ for $h = 0, 1, \ldots$, so that also $\sum_{h\geq 0} c_h X^h$ represents a rational function.

The argument proving such a result in the dominant root case was first sketched for me by Graham Everest half a dozen years ago.

In justification of the opening allusion to the Hilbert irreducibility theorem, I should also remark that a successful argument would entail that if an equation $F(y) = a(z)$, with F a polynomial and a an

exponential polynomial, has a solution $(z, y(z))$ for sufficiently many consecutive integer values of z, with the corresponding $y(z)$ all belonging to some field finitely generated over the rationals $\mathbf{Q}$, then there is an exponential polynomial $b(z)$ so that $a(z) = f \circ b(z)$. This is a weak generalization of a result of Davenport, Lewis and Schinzel [**4**], and is in the spirit of results proposed in [**10**].

It would be satisfying to be able to suggest a program for dealing with the more general question concerning

$$\mathcal{F}(h, Y) = a_{(0)}(h)Y^k + a_{(1)}(h)Y^{k-1} + \cdots + a_{(k)}(h), \tag{7}$$

the power sum analogue of (1), given that for each $h = 0, 1, 2, \ldots$, there is a b_h so that $\mathcal{F}(h, b_h) = 0$, with the b_h all in some ring finitely generated over $\mathbf{Z}$. The obstruction to such a generalization of the sketched argument is that, to prove the existence of a linear factor over $\mathbf{F}_p$, one seems to need to place restrictions on p that themselves depend on p, whereas in the kth root case the restriction depends only on k. At this time, I incline to the view that I am overlooking some simple fact whereby a curve over a finite field $\mathbf{F}_p$ that has a rational point for each ordinate $x \in \mathbf{F}_p$ necessarily has a linear factor. Of course, that is not true as stated. But it should be true under conditions on p that may be imposed in the present context, such as that p be sufficiently large and is $\equiv 1$ modulo some constant K depending only on (7).

Acknowledgments. I have relied upon all sorts of assistance, not least the work of David Cantor. The late Philippe Robba first warned me about incoherence. Recently, Eric Liverance, Gerry Myerson, Robert Rumely, Frits Beukers and Jaap Top have listened to parts of the present arguments and made useful remarks, or winced at appropriate moments. I am indebted to Robert Rumely for alerting me to a fatal flaw in the complete argument I had hoped to be able to present.

I am delighted to be able to dedicate this report to Wolfgang Schmidt, and dearly regret that it is flawed by a blatant gap I cannot currently leap.

REFERENCES

1. Benali Benzaghou, *Algèbres de Hadamard*, Bull. Soc. Math. France **98** (1970), 209–252.

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

3. ———, *On arithmetic properties of the Taylor series of rational functions* II, Pacific J. Math. **41** (1972), 329–334.

4. H. Davenport, D.J. Lewis and A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math. **12** (1961), 304–312.

5. P. Dienes, *The Taylor series*, OUP 1931; reprinted by Dover Books, 1957; p. 346ff.

6. Neal Koblitz, *p-adic numbers, p-adic analysis, and Zeta-functions*, Springer Verlag, New York, 1977.

7. A. Perelli and U. Zannier, *Arithmetic properties of certain recurrence sequences*, J. Austral. Math. Soc., Ser. A **37** (1984), 4–16.

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

9. Alfred J. van der Poorten, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C.R. Acad. Sci. Paris **306** (1988), 97–102.

10. ———, *Some facts that should be better known; Especially about rational functions*, in *Number theory and applications* (Richard A. Mollin, ed.), Kluwer Academic Publishers, Dordrecht, 1989.

11. ———, *A divergent argument concerning Hadamard roots of rational functions*, in *Analytic number theory* (B.C. Berndt, H.G. Diamond, H. Halberstam and A. Hildebrand, eds.), Birkhäuser, Boston, 1990.

12. ———, *The Lech-Mahler theorem ... with tears*, unpublished manuscript.

13. A.J. van der Poorten and Robert S. Rumely, *Zeros of p-adic exponential polynomials* II, J. London Math. Soc. **36** (1987), 1–15.

14. Yves Pourchet, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles*, C.R. Acad. Sci. Paris **288** (1979), 1055–1057.

15. J.F. Ritt, *Algebraic combinations of exponentials*, Trans. Amer. Math. Soc. **31** (1929), 654–679.

16. ———, *On the zeros of exponential polynomials*, Trans. Amer. Math. Soc. **31** (1929), 680–686.

17. Robert S. Rumely, *Notes on van der Poorten's proof of the Hadamard quotient theorem*, in *Sém. Théorie des Nombres de Paris* (Catherine Goldstein, ed.), Birkhäuser, 1988.

18. Robert S. Rumely and A.J. van der Poorten, *A note on the Hadamard kth root of a rational function*, J. Austral. Math. Soc., Ser. A **43** (1987), 314–327.

Centre for Number Theory Research, Macquarie University, NSW 2109, Australia
E-mail address: alf@mpce.mq.edu.au