Determined Sequences, Continued Fractions, and Hyperelliptic Curves

Alfred J. van der Poorten

Centre for Number Theory Research, 1 Bimbil Place, Killara, NSW 2071, Australia
alf@math.mq.edu.au

Abstract. In this report I sanitise (in the sense of 'bring some sanity to') the arguments of earlier reports detailing the correspondence between sequences $(M+hS)_{-\infty<h<\infty}$ of divisors on elliptic and genus two hyperelliptic curves, the continued fraction expansion of quadratic irrational functions in the relevant elliptic and hyperelliptic function fields, and certain integer sequences satisfying relations of Somos type. I note that one may often readily determine the coefficients in those relations by elementary linear algebra.

I begin with some musings on here called 'determined sequences', and continue with detail on continued fraction expansion of square roots of polynomials and associated Somos type sequences particularly in the genus 1 and 2 cases.

1 Remarks on Determined Sequences

1.1 Michael Somos' Sequences

The canonical details are given in [8], but for story telling purposes[1] let me introduce the matter as follows. Some fifteen years ago, Michael Somos noticed [8] that the two-sided sequence

$$C_{h-2}C_{h+2} = C_{h-1}C_{h+1} + C_h^2,$$

[1] Referee 1 warns me that grossly simplified (in plain language: falsified) stories will not do. More precisely, David Gale [8] reports that Michael Somos discovered the apparent integrality of $1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 3,\ 5,\ 9,\ 23,\ 75,\ 421,\ 1103,\ 4057,\ 41783,\ \dots$, namely 6-Somos, leading others to investigate 4-Somos and 5-Somos; specifically, Janice Malouf was the first to prove the integrality of 4-Somos. The trouble was that the early integrality proofs (of 4, 5, and 6-Somos) seemingly relied on algebraic accident and could not properly be said to give any explanation. To me, it seemed sufficient to mention a first-hand source allowing readers to replace legend by history. However, all this did provoke me to reread [8] alerting me to a number of interesting facts I had quite forgotten. I use this aside also to report a recent note of Chris Swart and Andy Hone [19] giving an alternative proof that the T_h satisfying (1) are Laurent polynomials in the initial data, and sharper integrality conditions than immediately derivable from [7]. Referee 2 adds that "[this alternative] proof is based on (6) with $t=1$ and the analogous formula with asymmetric shifts, and there is also a (much more verbose) discussion similar in spirit to §1.2."

F. Hess, S. Pauli, and M. Pohst (Eds.): ANTS 2006, LNCS 4076, pp. 393–405, 2006.

which I refer to as 4-Somos in his honour, apparently takes only integer values if we start from C_{-1}, C_0, C_1, $C_2 = 1$.

Indeed, Somos goes on to investigate also the width 5 sequence, $B_{h-2}B_{h+3} = B_{h-1}B_{h+2} + B_hB_{h+1}$, now with five initial 1s, the width 6 sequence $D_{h-3}D_{h+3} = D_{h-2}D_{h+2} + D_{h-1}D_{h+1} + D_h^2$, and so on, testing whether each, when initiated by an appropriate number of 1s, yields only integers. Naturally, he asks: "What is going on here?"

While 4-Somos (A006720), 5-Somos (A006721), 6-Somos (A006722), and 7-Somos (A006723), do yield only integers; 8-Somos does *not*. The codes in parentheses refer to Neil Sloane's *On-line encyclopedia of integer sequences*.

Fomin and Zelevinsky [7] give an algebraic explanation. For example, their theory of *cluster algebras* entails that a sequence (T_h) satisfying

$$\alpha T_{h-2}T_{h+2} + \beta T_{h-1}T_{h+1} + \gamma T_h^2 = 0\,, \quad \text{for all } h \in \mathbb{Z}, \tag{1}$$

has the T_h Laurent polynomials in the four initial values over $\mathbb{Z}[\beta/\alpha, \gamma/\alpha]$.

1.2 Self-determining Relations

Suppose we are given a family $\mathcal{T}$ of sequences (T_h) all satisfying a relation (1) with constant coefficients α, β, γ not all zero depending only on the family $\mathcal{T}$. Further, there is no loss of generality in supposing that our family $\mathcal{T}$ contains a *singular* sequence, (W_h) say, here specified by $W_0 = 0$.

Then we readily determine the nontrivial coefficients by noting that

$$\begin{aligned}\Delta_{0,1,h} &= \begin{vmatrix} W_{-2}W_2 & W_{-1}W_1 & 0 \\ W_{-1}W_3 & 0 & W_1^2 \\ W_{h-2}W_{h+2} & W_{h-1}W_{h+1} & W_h^2 \end{vmatrix} \\ &= W_{-1}W_1^3W_{h-2}W_{h+2} - W_{-2}W_2W_1^2W_{h-1}W_{h+1} - W_{-1}^2W_1W_3W_h^2 = 0\,. \end{aligned} \tag{2}$$

In the context I have in mind, (W_h) is in fact anti-symmetric: $W_{-h} = -W_h$, and clearly $W_1 \neq 0$ must be supposed, so our determination yields

$$W_1^2T_{h-2}T_{h+2} = W_2^2T_{h-1}T_{h+1} - W_1W_3T_h^2\,. \tag{3}$$

Whatever, given that there is a relation as described, one readily identifies its coefficients in terms of several initial elements of a, or the, singular sequence in the family.

1.3 Elliptic Sequences

In the sequel I discuss curves $\mathcal{C} : Z^2 - AZ - R = 0$ with polynomial coefficients A and R satisfying $\deg A = g + 1$, $0 < \deg R \leq g$.

Disclaimer. Here and throughout below I disregard the possibility that the given curve is of genus lower than g. In particular, if $\mathcal{C}$ is of genus zero then the continued fraction expansions are different from what we assert generic below.

In the case $g = 1$, set $R = v(X - w)$. The transformation

$$U = Z \qquad V - v = XU \tag{4}$$

transforms $\mathcal{C}$ into a Weierstrass model $\mathcal{E}$ for an elliptic curve, in effect by taking one of the points, say S, at infinity on $\mathcal{C}$ to $S_{\mathcal{E}} = (0,0)$ on $\mathcal{E}$.

It is an interesting but non-trivial exercise to confirm that there are well-defined integers U_h, V_h, W_h so that the rational points $hS_{\mathcal{E}}$ for $h \in \mathbb{Z}$ have co-ordinates of the shape $(U_h/W_h^2, V_h/W_h^3)$ satisfying

$$\gcd(U_h, V_h) = W_{h-1} \quad \text{and } U_h = -W_{h-1}W_{h+1}\,; \tag{5}$$

all this up to at most finitely many primes. For details see Rachel Shipsey's thesis [16]. It follows, as long ago observed by Morgan Ward [20], that there is indeed a sequence W_h as above satisfying

$$W_{h-m}W_{h+m}W_t^2 = W_m^2 W_{h-t}W_{h+t} - W_{m-t}W_{m+t}W_h^2 \tag{6}$$

for all integers h, m, and t.

It turns out [14], given an arbitrary point $M_{\mathcal{E}}$ on $\mathcal{E}$, that just so the 'denominators' T_h of the 'translated' points $M_{\mathcal{E}} + hS_{\mathcal{E}}$ satisfy

$$W_t^2 T_{h-m}T_{h+m} = W_m^2 T_{h-t}T_{h+t} - W_{m-t}W_{m+t}T_h^2\,. \tag{7}$$

It is easy to check that (6) is self-determining as h or t varies but to prove the identity requires showing, say by induction on m as in [14], that it is implied by the particular case (3) where $m = 2$. Such an argument does not require an understanding of the genesis of the family of sequences exemplified by (T_h).

Alternatively, one might recognise (T_h) as an 'elliptic sequence', identify the corresponding elliptic curve by analytic means, and prove (7) as coming from an identity satisfied by the relevant $\wp$-function. That's done by Ward [20], and rather more directly by Andy Hone [9].

Below I explain the identification by algebraic methods of M and the curve $\mathcal{C}$, or $\mathcal{E}$. It is intriguing that the recursion (3) depends only on the curve, but that four nonzero initial values of T_h are required both to fix the curve among a class of admissible curves and to find the translation M.

1.4 Division Polynomials

One might remark that there is gain in generality in having changed the transformation, by $U \leftarrow (U - x)$, $V \leftarrow (V - y)$, whereby in effect the co-efficients of $\mathcal{E}$ become polynomials in x and y and S is sent to $S_{\mathcal{E}} = (x, y)$. The result is that the integers W_h become polynomials $W_h(x, y)$ with the evident property that $W_m(a, b) = 0$ if and only if (a, b) is a point of torsion order dividing m. In other words, $W_h(x, y)$ is the h-th division polynomial. That inter alia entails $\gcd\bigl(W_r(x,y), W_s(x,y)\bigr) = W_{\gcd(r,s)}(x,y)$, explaining the division properties of the $W_h(0,0)$ and — conversely — the rapid growth of the coefficients of the division polynomials.

1.5 Hyperelliptic Sequences

The formulas (4) so relate the cubic and quartic models that the recursion relations for division polynomials produced from studying the quartic model coincide with those produced by the more familiar cubic model. One cannot expect that to be so if $g > 1$. It should therefore be no special surprise that sequences obtained by David Cantor [5] by studying Padé approximants to square roots of polynomials of odd degree $2g+1$ and with constant coefficient say 1, viewed as power series about zero, are not the same as sequences I obtain below from the continued fraction expansion of square roots of monic polynomials of even degree viewed as Laurent series about infinity. Just so, the results obtained in [3] by studying Kleinian σ-functions in genus 2 are not immediately applicable to my discussion below.

2 Continued Fraction of the Square Root of a Polynomial

Suppose $A(X)$ denotes a polynomial of degree $g+1$ and $R(X)$ a polynomial of positive degree at most g. Then, the equation

$$Z^2 - AZ - R = 0 \tag{8}$$

defines a quadratic irrational integer function Z of degree $g+1$ and with conjugate $\overline{Z}$ of negative degree. Note that this definition makes sense over base fields of arbitrary characteristic.

2.1 Laurent Series

Explicitly, albeit not in characteristic two, set $Y^2 = D(X)$ where D, not a square, is a monic polynomial over some field K and is of degree $2g+2$ in X. Then we may write

$$D(X) = \bigl(A(X)\bigr)^2 + 4R(X)\,,$$

where A is the polynomial part of the square root Y of D; here $4R$, with $\deg R$ at most g, may be referred to as the *remainder*. We then take

$$Y = A\bigl(1 + 4R/A^2\bigr)^{1/2} = A(X) + c_1X^{-1} + c_2X^{-2} + \cdots \tag{9}$$

thereby viewing Y as an element of $K((X^{-1}))$, Laurent series in the variable $1/X$. Note that the degree of such a Laurent series is the degree in X of its leading term. Of course $Z = \frac{1}{2}(Y+A)$ and does make sense in characteristic 2.

2.2 Continued Fraction Expansions

Now, for $h \in \mathbb{Z}$ set

$$Z_h = (Z + P_h)/Q_h\,,$$

where P_h and Q_h are polynomials such that $\deg Z_h > 0$ and $\deg \overline{Z}_h < 0$ — one says that Z_h is *reduced*. It follows that both $\deg P_h \le g-1$ and $\deg Q_h \le g$.

Further we require that Q_h divides the norm $(Z+P_h)(\overline{Z}+P_h)$; this divisibility condition is equivalent to the requirement that the $K[X]$-module $\langle Q_h, Z+P_h\rangle$ be an ideal of the domain $K[X,Z]$.

Finally, denote by a_h the polynomial part of Z_h. Then the continued fraction expansion of, say, Z_0 is a sequence of lines (or steps)

$$(Z+P_h)/Q_h = a_h - (\overline{Z}+P_{h+1})/Q_h \quad \text{in brief:} \quad Z_h = a_h - \overline{R}_h\,,$$

where, $-Q_h/(\overline{Z}+P_{h+1}) = (Z+P_{h+1})/Q_{h+1}$. Necessarily

$$P_h + P_{h+1} + A = a_hQ_h \quad \text{and} \quad (Z+P_{h+1})(\overline{Z}+P_{h+1}) = -Q_hQ_{h+1}\,,$$

and one readily verifies that the conditions on the P_h and Q_h are in fact sustained for all h.

This does require a minor miracle, but happily one that is well understood. Because the *complete quotients* Z_h all are reduced it follows that also all the R_h are reduced. It follows that the *partial quotients* a_h, which begin life as the polynomial parts of the Z_h, also are the polynomial parts of the R_h.

Hence also the 'conjugate line'

$$R_h = (Z+P_{h+1})/Q_h = a_h - (\overline{Z}+P_h)/Q_h = a_h - \overline{Z}_h$$

is a line in an admissible continued fraction expansion. Thus we may view the continued fraction expansion as being *bi-directional* infinite.

2.3 Normal Expansion

In the immediate sequel I suppose that the base field K is infinite. Given that, I assert that a generic choice of P_0 and Q_0 is so that *all* the a_h are linear — equivalently, so that all the Q_h are of degree g — indeed, a teeny bit less obviously, so that all the P_h are of their maximal degree $g-1$. That's so because the probability of an element of K being 0 *is* zero. Equivalently, a *generic* divisor of the curve (8) is defined by a g-tuple of elements of an algebraic extension of K.

2.4 The Cases $g=1$ and $g=2$ are Atypical

All the conditions just mentioned are equivalent to the nonvanishing of the sequence (d_h) of coefficients of the leading term (of degree $g-1$) of the polynomials P_h. Accordingly, it is an appropriate goal to attempt to obtain relations involving only the parameter d_h.

Denote a typical zero of Q_h by ω_h and recall the recursion relations

$$\begin{aligned} &P_h + P_{h+1} + A = a_hQ_h \quad \text{and} \\ &\qquad -Q_hQ_{h+1} = (Z+P_{h+1})(\overline{Z}+P_{h+1}) = -R + P_{h+1}(A+P_{h+1})\,. \end{aligned} \tag{10}$$

Thus $P_h(\omega_h) + P_{h+1}(\omega_h) + A(\omega_h) = 0$ and so $R(\omega_h) = -P_{h+1}(\omega_h)P_h(\omega_h)$.

Hence $Q_h(X)$ divides $R(X)+P_{h+1}(X)P_h(X)$, and so

$$C_h(X)/u_h = \big(R(X)+P_{h+1}(X)P_h(X)\big)/Q_h(X) \tag{11}$$

defines a polynomial C_h; here u_h denotes the leading coefficient of Q_h.

One notices that $\deg C_h = \max\big(g, 2(g-1)\big) - g$; so C_h is a constant if and only if $g=1$ or $g=2$. In the sequel I deal primarily just with these simpler cases.

2.5 More General Formulæ

If $P_h(\varepsilon_h)=0$, then by (11) we have both

$$C_h(\varepsilon_h)Q_h(\varepsilon_h) = u_hR(\varepsilon_h) \quad \text{and} \quad C_{h+1}(\varepsilon_{h+1})Q_h(\varepsilon_{h+1}) = u_hR(\varepsilon_{h+1});$$

$$\text{and thus} \quad C_{h-1}(\varepsilon_h)C_h(\varepsilon_h)Q_{h-1}(\varepsilon_h)Q_h(\varepsilon_h) = u_{h-1}u_hR(\varepsilon_h)^2\,. \tag{12}$$

From the recursion formulæ (10),

$$u_{h-1}u_h = -d_h\,, \text{ and } Q_{h-1}(\varepsilon_h)Q_h(\varepsilon_h) = R(\varepsilon_h)\,. \tag{13}$$

Hence

$$C_{h-1}(\varepsilon_h)C_h(\varepsilon_h) = -d_hR(\varepsilon_h)\,, \tag{14}$$

a formula that seemed inexplicably miraculous when I first stumbled upon it [13] in the case $g=2$.

If ω is a zero of R we have

$$C_h(\omega)Q_h(\omega) = u_hP_h(\omega)P_{h+1}(\omega) \tag{15}$$

and therefore

$$C_{h-1}(\omega)C_h(\omega)Q_{h-1}(\omega)Q_h(\omega) = u_{h-1}u_hP_{h-1}(\omega)P_h(\omega)^2P_{h+1}(\omega)\,.$$

By (10) and $u_{h-1}u_h=-d_h$ this is

$$C_{h-1}(\omega)C_h(\omega)P_h(\omega)\big(A(\omega)+P_h(\omega)\big) = d_hP_{h-1}(\omega)P_h(\omega)^2P_{h+1}(\omega) \tag{16}$$

2.6 What the Continued Fraction Does

It also follows from $Q_h(\omega_h)=0$ that, for $h\in\mathbb{Z}$, the points $\big(\omega_h, -P_h(\omega_h)\big)$ specify a sequence (M_h) of divisor classes on the Jacobian of the curve $\mathcal{C}$: $Z^2-AZ-R=0$.

We may set $M_h = M+S_h$ (so $M=M_0$). It then turns out that $S_h=hS$ — with S the class of the divisor at infinity. In other words, *each step of the continued fraction expansion corresponds to addition of the divisor at infinity.* Comments by David Cantor [4] and Kristin Lauter [10] assist one in accepting this notion. Adams and Razar [1] give a very explicit proof in the elliptic case and Tom Berry [2] provides analogous arguments for general g.

We note that $\deg Q_h \le g$ and $\deg P_h \le g-1$, generically with equality if the base field is of characteristic zero. I note that because the complete quotients all are reduced, always $\deg P_h < \deg Q_h$.

The pairs $(Q_h, -P_h)$ of polynomials are the respective Mumford representations of divisors $M+hS$ on the hyperelliptic curve $\mathcal{C}: Z^2-AZ-R=0$.

3 Continued Fraction Relations

3.1 The Elliptic Case $g = 1$

Here $R = v(X - w)$ and the $P_h(X) = d_h$ are polynomials of degree $g - 1 = 0$. Plainly $C_h = v$. The relation (16) becomes just

$$v^2(A(w) + d_h) = d_{h-1}d_h^2 d_{h+1}\,. \tag{17}$$

This identity depends only on the given curve, *not* on the 'translation' M.

It follows from (17) that $d_{h+1}d_h + v^2/d_h + d_h d_{h-1}$ is independent of h. A little work then yields

$$d_{h-1}d_h^2 d_{h+1}^2 d_{h+2} = v^2 A(w) d_h d_{h+1} + v^3\big(v + 2wA(w)\big). \tag{18}$$

For more detail see [12] or [14]; for the complex function view note Hone [9].

3.2 The Hyperelliptic Case $g = 2$; First Steps

In general we have $R = u(X - \omega)(X - \overline{\omega}) = u(X^2 - vX + w)$, say, and the $P_h(X) = d_h(X + e_h)$ are polynomials of degree one; thus the ε_h above are given by $\varepsilon_h = -e_h$. Evidently, $C_h = d_h d_{h+1} + u$. Here the relations (16)

$$C_{h-1}C_h\big(A(\omega) + P_h(\omega)\big) = d_h P_{h-1}(\omega)P_h(\omega)P_{h+1}(\omega)$$

still require an elimination of the (e_h), to be assisted by the 'miraculous' identity

$$C_{h-1}C_h = (d_{h-1}d_h + u)(d_h d_{h+1} + u) = -d_h R(-e_h)\,. \tag{19}$$

However,

$$-d_h R(-e_h) = -u d_h(\omega + e_h)(\overline{\omega} + e_h) = -uP_h(\omega)(\overline{\omega} + e_h)\,.$$

Thus we are to deal with

$$-u(\overline{\omega} + e_h)\big(A(\omega) + P_h(\omega)\big) = d_h P_{h-1}(\omega)P_{h+1}(\omega)\,. \tag{20}$$

It now seems natural to multiply by the conjugate equation and to use

$$uP_h(\omega)P_h(\overline{\omega}) = ud_h^2(e_h + \omega)(e_h + \overline{\omega}) = -d_h(d_{h-1}d_h + u)(d_h d_{h+1} + u)\,.$$

But that leaves an e_h on the left. Specifically, one obtains

$$\begin{aligned} -\,uC_{h-1}C_h\big(A(\omega)A(\overline{\omega}) + d_h\big((\overline{\omega} + e_h)A(\omega) + (\omega + e_h)A(\overline{\omega})\big) \\ -\,d_h C_{h-1}C_h/u\big) = d_{h-1}d_h^3 d_{h+1}C_{h-2}C_{h-1}C_h C_{h+1}/u^2\,. \end{aligned} \tag{21}$$

While we do have the identity (19), it is quadratic in e_h and seems unhelpful in eliminating e_h. Of course there is no e_h in the happenstance $A(\omega) + A(\overline{\omega}) = 0$.

3.3 The Special Case $g = 2$, $\deg R = 1$

It's all much easier if $R = v(X - w)$. Then $u = 0$, $\omega = w$ and is rational, and (19) becomes

$$C_{h-1}C_h = d_{h-1}d_h^2 d_{h+1} = d_h v(e_h + w) = vP_h(w)\,. \tag{22}$$

Hence (16) is just

$$v^2 d_{h-1}d_h^2 d_{h+1}\big(vA(w) + d_{h-1}d_h^2 d_{h+1}\big) = d_{h-2}d_{h-1}^3 d_h^5 d_{h+1}^3 d_{h+2}.$$

Recasting this, we obtain Theorem 1 of [13]

$$d_{h-2}d_{h-1}^2 d_h^3 d_{h+1}^2 d_{h+2} = v^2 d_{h-1}d_h^2 d_{h+1} + v^3 A(w)\,. \tag{23}$$

4 Somos Sequences

4.1 Suitable Identities

The identities (17) and (23) are *suitable* in the following sense. It turns out that generically the d_h are rationals increasing in complexity with h at frantic pace: the logarithmic height of d_h is $O(h^2)$. One tames the d_h somewhat by introducing a sequence (T_h) given by the recursive definition

$$T_{h-1}T_{h+1} = d_h T_h^2\,. \tag{24}$$

That this yields elements integral at all but at most a few exceptional primes is not too difficult to show by elementary means in the elliptic case (see my introductory remarks) and is experientially the case for $g = 2$, no doubt *inter alia* for algebraic reasons of the kind described by Fomin and Zelevinsky [7].

Happily, (24) easily yields $T_{h-1}T_{h+2} = d_h d_{h+1} T_h T_{h+1}$ and then

$$d_{h-1}d_h^2 d_{h+1}T_h^2 = T_{h-2}T_{h+2}\,, \quad d_{h-1}d_h^2 d_{h+1}^2 d_{h+2}T_h T_{h+1} = T_{h-2}T_{h+3}\,,$$
$$\text{and} \quad d_{h-2}d_{h-1}^2 d_h^3 d_{h+1}^2 d_{h+2}T_h^2 = T_{h-3}T_{h+3}\,.$$

So the identities (17) and (18) become

$$T_{h-2}T_{h+2} = v^2 T_{h-1}T_{h+1} + v^2 A(w)T_h^2$$
$$\text{and} \quad T_{h-2}T_{h+3} = v^2 A(w)T_{h-1}T_{h+2} + v^3\big(u + 2wA(w)\big)T_h T_{h+1}\,; \tag{25}$$

and (23) yields

$$T_{h-3}T_{h+3} = v^2 T_{h-2}T_{h+2} + v^3 A(w)T_h^2\,. \tag{26}$$

4.2 Canonical Examples

4-Somos: Suppose $(C_h) = (\dots, 2, 1, 1, 1, 1, 2, 3, 7, \dots)$ with $C_{h-2}C_{h+2} = C_{h-1}C_{h+1} + C_h^2$. One sees that $v = \pm 1$, $w = \mp 2$, $A(w) = 1$, and thus that (C_h) arises from

$$Z^2 - (X^2 - 3)Z - (X - 2) = 0 \quad \text{with } M = (1, -1);$$

equivalently from $\mathcal{E}: V^2 - V = U^3 + 3U^2 + 2U$ with $M_{\mathcal{E}} = (-1, 1)$.

5-Somos: The case $(B_h) = (\dots, 2, 1, 1, 1, 1, 1, 2, 3, 5, 11, \dots)$ with $B_{h-2}B_{h+3} = B_{h-1}B_{h+2} + B_hB_{h+1}$ is trickier. One needs to define $c_hB_{h-1}B_{h+1} = d_hB_h^2$ with c_hc_{h+1} independent of h.

One finds that (B_h) arises from

$$Z^2 - (X^2 - 29)Z + \cdot 48(X+5) = 0 \quad \text{with } M = (-3, -8);$$

equivalently from $\mathcal{E}: V^2 + UV + 6V = U^3 + 7U^2 + 12U$ with $M_{\mathcal{E}} = (-2, -2)$. The fact $\gcd(a_3, a_4) = \gcd(6, 12) \neq 1$ may here be thought of as 'necessitating' the width 5 recursion.

By symmetry each respective M is a point of order 2 on its curve.

A Width 6 Example à la Somos. The sequence $(T_h) = (\dots,\ 2,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ 3,\ 4,\ 8,\ 17,\ 50,\ \dots)$, with

$$T_{h-3}T_{h+3} = T_{h-2}T_{h+2} + T_h^2\,,$$

may be thought of as arising from the points (thus, divisor classes) $\dots,\ M - S$, M, $M + S$, $M + 2S$, $\dots$ on the Jacobian of the genus 2 hyperelliptic curve

$$\mathcal{C}: Z^2 - (X^3 - 4X + 1)Z - (X - 2) = 0\,.$$

Here S is the class of the divisor at infinity and M is instanced by the divisor defined by the pair of points $(\varphi, \overline{\varphi})$ and $(\overline{\varphi}, \varphi)$: where φ is the golden ratio. The symmetry dictates that $M - S = -M$ so $2M = S$ on $\operatorname{Jac}(\mathcal{C})$.

4.3 An Identity for $g = 2$

In just the above spirit, multiplying (21) by T_h^3 yields

$$\begin{aligned} u^3A(\omega)A(\overline{\omega})T_h^3 &+ u^2(\mathcal{D}T_{h-1}T_hT_{h+1} + \mathcal{F}d_he_hT_h^3) \\ &- u^3(T_{h-2}T_{h+1}^2 + T_{h-1}^2T_{h+2}) - u^4T_{h-1}T_hT_{h+1} + T_{h-3}T_hT_{h+3} \\ &+ u(T_{h-3}T_{h+1}T_{h+2} + T_{h-2}T_{h-1}T_{h+3}) = 0\,, \end{aligned} \tag{27}$$

a *suitable* expression for $d_he_hT_h^3$. Mind you, this suitability — in other words: that here multiplication by T_h^3 tames the equation — requires a fortunate coincidence of the first term in the expansion of $u^2d_hC_{h-1}C_h$ and the last term in the expansion of $d_{h-1}d_h^3d_{h+1}C_{h-2}C_{h+1}$.

Moreover, in the happenstance $\mathcal{F} = u\big(A(\omega) + A(\overline{\omega})\big) = 0$, (27) *is* the sought for relation. Apropós of comments at §1.5 on page 396 above, I note that terms of the shapes $T_{h-3}T_{h+1}T_{h+2}$ and $T_{h-2}T_{h-1}T_{h+3}$, or $T_{h-2}T_{h+1}^2$ and $T_{h-1}^2T_{h+2}$, do *not* occur in Cantor's recurrence formulas.

4.4 Example

Set $A(X) = X^3 - 7X^2 + 8X + 7$ and $R(X) = u(X-2)(X-5)$, noting that $A(2) = 3$ and $A(5) = -3$ so $\mathcal{F} = 0$, $\mathcal{D} = 9u$, $A(2)A(5) = -9$. A computation, done for me by David Gruenewald, confirms that the singular sequence $\ldots$, $2,\ 1,\ 1,\ W_{-1}=0,\ W_0=0,\ W_1=1,\ 1,\ 2,\ 7,\ -112,\ -103,\ 1803,\ 132603,$ $-1042153,\ -31597909,\ -1759068155,\ \ldots$, indeed satisfies

$$\begin{aligned}-9u^3W_h^3+(9u^3-u^4)&W_{h-1}W_hW_{h+1}\\ &-u^3(W_{h-2}W_{h+1}^2+W_{h-1}^2W_{h+2})+W_{h-3}W_hW_{h+3}\\ &\qquad+u(W_{h-3}W_{h+1}W_{h+2}+W_{h-2}W_{h-1}W_{h+3})=0\,, \qquad (28)\end{aligned}$$

of course with $u=1$. As always set $Z^2-AZ-R=0$. Here, to avoid singular steps in the continued fraction, one expands Z/R, deeming that to provide line 1 of the expansion of Z. The recursion relation allows one to fill gaps in and generally to extend the two-sided sequence.

5 Not Enough Determination

5.1 A Determined Sequence for Every *g*

During ANTS V, Sydney, Noam Elkies was provoked by remarks of mine to notice that Fay's trisecant formula suggests that hyperelliptic curves

$$Z^2-AZ-v(X-w)=0$$

of arbitrary genus g, thus $\deg A=g+1$ but $\deg R=1$, yield a Somos relation just on the three terms $T_{h-g-1}T_{h+g+1}$, $T_{h-g}T_{h+g}$, and T_h^2 — incidentally explaining the elliptic case and my $g=2$ result [13] at (25).

In this case, the singular expansion — that of Z itself — yields a sequence (W_h) with g central zeros occasioned by the partial quotient A of degree $g+1$, followed by a 1, and then $g-1$ zeros occasioned by the next partial quotient, $\big(A(X)-A(w)\big)/v(X-w)$, of degree g. For $g=2k+1$ odd I set notation so that $W_{-h}=W_h$ and if $g=2s$ even then $W_{-h}=W_{h+1}$. By the way, after bypassing the singular part of the continued fraction expansion, one computes the singular sequence; then backtracking, using the experimentally discovered recurrence relation, one locates the zero entries.

The determined form of Elkies' remark is

$$W_s^2W_{5s}T_{h-(2s+1)}T_{h+(2s+1)}=-W_{3s}^2W_{3s+1}T_{h-2s}T_{h+2s}+W_sW_{3s+1}W_{5s}T_s^2 \qquad (29)$$

and respectively

$$\begin{aligned}&W_{k+1}^2W_{5k+3}T_{h-(2k+2)}T_{h+(2k+2)}\\ &\qquad=-W_{3k+2}^2W_{3k+3}T_{h-(2k+1)}T_{h+(2k+1)}+W_{k+1}W_{3k+3}W_{5k+3}T_k^2\,. \qquad (30)\end{aligned}$$

Incidentally, numbering the lines in singular continued fraction expansions, and thence indexing the W_h, is rather problematic. That would have been so even in the elliptic case were it not that Morgan Ward [20] had already set a notation. Determinations such as the present example assist in leading to a coherent notation.

5.2 Determined Sequences for $g = 2$

My remarks above suggest that the general relation linearly relates the terms $T_{h-3}T_hT_{h+3}$, $T_{h-2}T_hT_{h+2}$, $T_{h-1}T_hT_{h+1}$, T_h^3, $T_{h-3}T_{h+1}T_{h+2} + T_{h-2}T_{h-1}T_{h+3}$, and $T_{h-2}T_{h+1}^2 + T_{h-1}^2T_{h+2}$. That this is so is clear from experiment. Here a determination of the coefficients is not immediately successful because it yields the six coefficients as polynomials in $W_1 = 1$, W_2, ..., W_7. Recall that $W_{-h-1} = W_h$ and $W_{-1} = W_0 = 0$.

However, W_7 plainly is supernumerary since it is given — by the as yet unknown relation — in terms of $W_1 = 1$, W_2, ..., W_6. Indeed, if the last two pairs of terms above have a nonzero coefficient, the unknown relation already gives W_6 in terms of W_2, W_3, W_4, W_5.

If not, we have the simpler case of only four terms all divisible by W_h and then yet more plainly W_6 is given in terms of W_2, W_3, W_4 and W_5. In that special case the determined relation must be

$$W_1W_2W_3W_4T_h^3 - W_2^3W_4T_{h-1}T_hT_{h+1} + W_1W_2W_3^2T_{h-2}T_hT_{h+2} = W_1^2W_2W_3T_{h-3}T_hT_{h+3}\,, \quad (31)$$

a matter of interest if one hopes to detail the source of the 6-Somos sequence.

In the case $g = 1$, I had the foresight already to know the relation and, indeed, to have explicit expressions for $W_1 = 1$, W_2, W_3, W_4, W_5 in terms of the parameters defining the elliptic curve. Here, explicit computation of W_2, W_3, ... in the general case quickly seems to become too messy to be informative. Whatever, I have not as yet disentangled the determination just now sketched, probably out of laziness but principally, I claim, because I am looking for methods and ideas that may generalise to arbitrary genus; hard yakka [2] mucking about with absurd identities is unlikely to do that. I should here also admit that extensive computations of quite general examples by David Gruenewald have helped to 'verify' various guesses of mine, and of his, but have not as yet proved useful in readily identifying the coefficients of the general relation as polynomials in W_2, W_3, W_4, and W_5.

6 Comments

I find the Somos sequences interesting as an infinite base field phenomenon which continues to give meaningful information after reduction or specialisation — after all, the elliptic case will do for this remark, the sequences begin life as 'denominators' yet persist under transformation of the base field to a finite field. That all said, the sequences may well be a distraction, hence my feeling that not enough determination is quite enough.

Indeed, a principal charm of the continued fraction expansions is their encapsulating a sequence of divisors $M + hS$ allowing one ready entrance to open questions dealing with torsion possibilities in higher genus, note for easy example

[2] yakka: work [Australian Aboriginal].

the modular curves mentioned in [11]. In this context I also note that many of the phenomena touched on above will reappear in studying multi-sequences of Padé approximants to higher degree algebraic functions.

I also note, as hinted at in my opening comment just above, that studying curves over an infinite field, say $\mathbb{Q}$ — though computationally hopeless — does nonetheless give insight into the corresponding curves over finite fields, moreover all at once for almost all p. I hope to give more emphasis to that thought in future work.

Thoughtful remarks from the two referees helped me to omit some of the errors in my remarks.

References

1. William W. Adams and Michael J. Razar, 'Multiples of points on elliptic curves and continued fractions', *Proc. London Math. Soc.* **41** (1980), 481–498.
2. T. G. Berry, 'A type of hyperelliptic continued fraction', *Monatshefte Math.*, **145**.4 (2005), 269–283.
3. Harry W. Braden, Victor Z. Enolskii, and Andrew N. W. Hone, 'Bilinear recurrences and addition formulæ for hyperelliptic sigma functions', *J. Nonlin. Math. Phys.* **12**, Supplement 2 (2005), 46–62; also at `http://www.arxiv.org/math.NT/0501162`.
4. D.G. Cantor, 'Computing in the Jacobian of a hyperelliptic curve', *Math. Comp.* **48**.177 (1987), 95–101.
5. David G. Cantor, 'On the analogue of the division polynomials for hyperelliptic curves', *J. für Math.* (Crelle), **447**, (1994), 91–145.
6. Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence Sequences*. Mathematical Surveys and Monographs 104, American Mathematical Society, (2003), xiv+318pp.
7. Sergey Fomin and Andrei Zelevinsky 'The Laurent phenomenon', *Adv. in Appl. Math.*, **28**, (2002), 119–144. Also 21pp: at `http://www.arxiv.org/math.CO/0104241`.
8. David Gale, 'The strange and surprising saga of the Somos sequences', *The Mathematical Intelligencer* **13**.1 (1991), 40–42; Somos sequence update. *Ibid.* **13**.4, 49–50.
9. A. N. W. Hone, 'Elliptic curves and quadratic recurrence sequences', *Bull. London Math. Soc.* **37**, (2005), 161–171.
10. Kristin E. Lauter, 'The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves', *Topics in algebraic and noncommutative geometry* (Luminy/Annapolis, MD, 2001), 165–171, *Contemp. Math.*, **324**, Amer. Math. Soc., Providence, RI.
11. Alfred J. van der Poorten, 'Periodic continued fractions and elliptic curves', in *High Primes and Misdemeanours*: lectures in honour of the 60th birthday of Hugh Cowie Williams, Alf van der Poorten and Andreas Stein eds., Fields Institute Communications **42**, American Mathematical Society, 2004, 353–365.
12. Alfred J. van der Poorten, 'Elliptic sequences and continued fractions', *Journal of Integer Sequences*, **8** 05.2.5 (2005), 1–19.
13. Alfred J. van der Poorten, 'Curves of genus 2, continued fractions, and Somos sequences', *Journal of Integer Sequences*, **8** 05.3.4, (2005), 1–9.

14. Alfred J. van der Poorten and Christine S. Swart, 'Recurrence relations for elliptic sequences: every Somos 4 is a Somos k', to appear in *Bull. London Math. Soc.*; at `http://arxiv.org/math.NT/0412293`.
15. Jim Propp, *The Somos Sequence Site*. `http://www.math.wisc.edu/~propp/somos.html`.
16. Rachel Shipsey, *Elliptic divisibility sequences*, Phd Thesis, Goldsmiths College, University of London, 2000; at `http://homepages.gold.ac.uk/rachel/`.
17. Sloane, Neil. *On-Line Encyclopedia of Integer Sequences.* `http://www.research.att.com/~njas/sequences/`.
18. Christine Swart, *Elliptic curves and related sequences.* PhD Thesis, Royal Holloway, University of London, 2003; `http://www.isg.rhul.ac.uk/alumni/thesis/swart_c.pdf`.
19. Christine Swart and Andrew Hone, 'Integrality and the Laurent phenomenon for Somos 4 sequences', 18pp at `http://www.arxiv.org/math.NT/0508094`.
20. Ward, Morgan (1948). Memoir on elliptic divisibility sequences *Amer. J. Math.* **70**, 31–74.