Journal of Integer Sequences, Vol. 8 (2005),
Article 05.3.4

Curves of Genus 2, Continued Fractions, and Somos Sequences

Alfred J. van der Poorten[1]
Centre for Number Theory Research
1 Bimbil Place
Killara, Sydney
NSW 2071
Australia
alf@math.mq.edu.au

Abstract

We detail the continued fraction expansion of the square root of monic sextic polynomials. We note in passing that each line of the expansion corresponds to addition of the divisor at infinity, and interpret the data yielded by the general expansion. In particular we obtain an associated Somos sequence defined by a three-term recurrence relation of width 6.

1 Introduction

In the present note I study the continued fraction expansion of the square root of a sextic polynomial, inter alia allowing the identification of sequences generated by recursions

$$A_{h-3}A_{h+3} = a\,A_{h-2}A_{h+2} + bA_h^2\,.$$

Specifically, see §6 at page 6 for the case $(T_h) = (\ldots, 2, 1, 1, 1, 1, 1, 1, 2, 3, 4, 8, 17, 50, 107, 239, 1103, \ldots)$, where I illustrate how the continued fraction expansion data readily allows one to identify the genus 2 curve $\mathcal{C} : Y^2 = (X^3 - 4X + 1)^2 + 4(X - 2)$ as giving rise to the sequence.

[1] The author's only support was a grant from the Australian Research Council.

2 Some Brief Reminders

A reminder exposition on continued fractions in quadratic function fields appears as §4 of [8]. However, the naïve reader needs little more than that a continued fraction expansion of a quadratic irrational integer function Z is a two-sided sequence of lines, h in $\mathbb{Z}$,

$$\frac{Z+P_h}{Q_h} = a_h - \frac{\overline{Z}+P_{h+1}}{Q_h}\,; \quad \text{in brief } Z_h = a_h - \overline{R}_h\,,$$

with $(Z+P_{h+1})(\overline{Z}+P_{h+1}) = -Q_hQ_{h+1}$ defining the sequences (P_h) and (Q_h) of polynomials. Necessarily, one must have Q_0 divides $(Z+P_0)(\overline{Z}+P_0)$ in which case the sequence (a_h) consisting of polynomials guarantees that always Q_h divides $(Z+P_h)(\overline{Z}+P_h)$. If each *partial quotient* a_h is always chosen as the polynomial part of Z_h then Z_0 *reduced* (that is, $\deg Z > 0$ and $\deg \overline{Z} < 0$) implies that all the Z_h and R_h are reduced; and always a_h also is the polynomial part of R_h. Then conjugation — in brief: studying the lines $R_h = a_h - \overline{Z}_h$ — retrieves the left hand half of the expansion of Z_0 from the right hand half of the expansion of R_0.

3 Curves of Genus

Set $A(X) = X^3 + fX + g$ and $R(X) = u(X^2 - vX + w)$. Then

$$\mathcal{C} : Z^2 - AZ - R = 0 \tag{1}$$

defines a quadratic irrational integer function Z as a Laurent series $\sum_{h=-3}^{\infty} z_h X^{-h}$ in X^{-1}. Here $\deg Z = 3$ refers to the degree in X of Z. Note that because the other zero $\overline{Z}$ of equation (1) satisfies $Z\overline{Z} = -R$, and $\deg R \le 2$, we must have $\deg \overline{Z} < 0$, so Z is reduced. We also note that the discriminant $D(X)$ of (1) is given by $D = A^2 + 4R$ and is thus a general sextic polynomial. Evidently, if $Y^2 = D$ we may think of Z as $Z = \frac{1}{2}(Y + A)$.

However, in defining Z by (1) we allow the base field $\mathbb{F}$ to be of arbitrary characteristic, whereas any talk of Y of course requires that $\operatorname{char}\mathbb{F} \ne 2$.

Now set $Z_0 = (Z + P_0)/Q_0$ with $P_0 = d_0(X + e_0)$. Suppose that $Q_0(X) = X^2 - v_0X + w_0$ divides the norm

$$Z_0\overline{Z}_0 = -R + d_0(X+e_0)\bigl(A + d_0(X+e_0)\bigr)\,,$$

and that Z_0 has been so chosen that its partial quotients are of degree 1. Such a choice is 'generic' if the base field is infinite. It follows from recursion formulæ immediately below that our requirement on Z_0 is the same as insisting that the d_h alll† be nonzero.

For $h = 0, 1, 2, \ldots$ we denote the complete quotients of Z_0 by

$$Z_h = \bigl(Z + d_h(X + e_h)\bigr)/u_h(X^2 - v_hX + w_h)\,, \tag{2}$$

noting that the Z_h all are reduced, namely $\deg Z_h > 0$ but $\deg \overline{Z}_h < 0$. The upshot is that the h-th line of the continued fraction expansion of Z_0 is

$$Z_h = \frac{Z + d_h(X+e_h)}{u_h(X^2 - v_hX + w_h)} = \frac{X + v_h}{u_h} - \frac{\overline{Z} + d_{h+1}(X + e_{h+1})}{u_h(X^2 - v_hX + w_h)}\,. \tag{3}$$

†Of course it suffices that just those d_h actually participating in our discussion not vanish.

Theorem 3.1. *In the special case $u = 0$, that is: $R = -v(X - w)$, the sequence of parameters (d_h) given by the continued fraction expansion of Z_0 satisfies*

$$d_{h-2}d_{h-1}^2d_h^3d_{h+1}^2d_{h+2} = v^2d_{h-1}d_h^2d_{h+1} - v^3(g + wf + w^3)\,. \tag{4}$$

Note here that $g + wf + w^3 = A(w)$ and, I add this *en passant*, the result, with $g + wf + w^3$ replaced by $A(w)$, does not in fact depend on the convenient assumption throughout that $A(X)$ has no term in X^2. However, the main feature is that the recursion (4) depends only on the given curve $\mathcal{C}$ and not on the 'initial' complete quotient Z_0.

Now define a sequence (T_h) of elements of $\mathbb{F}$ by the recursive relation

$$T_{h-1}T_{h+1} = d_hT_h^2\,, \quad h \in \mathbb{Z}\,. \tag{5}$$

One then sees fairly readily that

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

and thus that multiplying (4) by T_h^2 provides the principal result of this note.

Theorem 3.2. *A curve*

$$\mathcal{C} : Z^2 - (X^3 + fX + g)Z + v(X - w) = 0$$

gives rise to sequences (T_h) of Somos type defined by suitable initial values and the recursive relation

$$T_{h-3}T_{h+3} = v^2T_{h-2}T_{h+2} - v^3(g + wf + w^3)T_h^2\,. \tag{6}$$

Remarks. All that is well and good of course but the real point here is this. The d_h are generically, so to speak, random rationals growing in height with h so as to have logarithmic height $O(h^2)$; thus they become complicated indeed. Very differently, however, recursions such as (6) of 'Somos type' and width, or 'gap' (the maximum difference of the indices), at most seven — 6 in the present case — are now well known to 'want to' consist of integers. Specifically, results of Fomin and Zelevinsky summarised in [6] guarantee that the T_h are Laurent polynomials in the 'initial values' $T_{-3}, \ldots, T_2$, say, with coefficients in the ring $\mathbb{Z}[a, b]$ — where in the present case $a = v^2$ and $b = -v^3(g + wf + w^3)$. This explains why the example sequence (at page 6) with $a = b = 1$ and the six initial values all 1 takes only integer values — mind you, integers whose logarithm grows at rate $O(h^2)$.

For a different emphasis, notice that the pair of zeros of each $Q_h(X)$ produced by the continued fraction expansion defines a *divisor* on $\mathcal{C}$; I talk loosely immediately below of the 'divisor class Q_h', meaning the class of the divisor given by the pair of points on $\mathcal{C}$ defined over some quadratic extension of the base field $\mathbb{F}$ with X co-ordinates the two zeros of the polynomial $Q_h(X)$. Viewed as points on the additive group Jac$\mathcal{C}$ it is well understood that the sequence of divisor classes (Q_h) is an arithmetic progression with common difference S the class of the divisor at infinity. In brief, exactly as in the elliptic case [8]. each step of the continued fraction expansion adds the divisor at imfinity to the divisor belonging to the complete quotient. Concerned readers might contemplate the introduction to Cantor's paper [5] and the instructive discussion by Kristin Lauter in [7]. A central theme of the paper [1] is a generalisation of the phenomenon to Padé approximation in arbitrary algebraic function fields.

More of course, Theorem 3.2 is in tight analogy with the corresponding result for quartic polynomials detailed in [8]. In that case, however, *singular* cases are incorporated. Here, cases when one or more of the d_h vanish and therefore one or more of the T_h vanish are more problematic and will have to be the subject of further analysis elsewhere. I do not yet know whether my assumption that the continued fraction expansion is generic, thus that none of the d_h vanish, is or is not essential to the validity of the present results.

4 Continued Fraction Expansion of the Square Root of a Sextic

Given that the h-th line of the continued fraction expansion of Z_0 is given by

$$Z_h = \frac{Z + d_h(X + e_h)}{u_h(X^2 - v_hX + w_h)} = \frac{X + v_h}{u_h} - \frac{\overline{Z} + d_{h+1}(X + e_{h+1})}{u_h(X^2 - v_hX + w_h)}\,, \tag{3}$$

evident recursion formulas yield

$$f + d_h + d_{h+1} = -v_h^2 + w_h \tag{7}$$

$$g + d_he_h + d_{h+1}e_{h+1} = v_hw_h \tag{8}$$

and

$$\begin{aligned} &-u_hu_{h+1}(X^2 - v_hX + w_h)(X^2 - v_{h+1}X + w_{h+1}) \\ &\qquad\qquad = \big(Z + d_{h+1}(X + e_{h+1})\big)\big(\overline{Z} + d_{h+1}(X + e_{h+1})\big). \end{aligned} \tag{9}$$

Hence, noting that $Z\overline{Z} = -u(X^2 - vX + w)$ and $Z + \overline{Z} = A = X^3 + fX + g$, we may equate coefficients in (9) to see that

$$d_{h+1} = -u_hu_{h+1}\,. \tag{9 : X^4}$$

Given that, we obtain, after in each case dividing by $-u_hu_{h+1}$,

$$e_{h+1} = -v_h - v_{h+1}\,; \tag{9 : X^3}$$

$$(f + d_{h+1}) = v_hv_{h+1} + (w_h + w_{h+1}) + u/d_{h+1}\,; \tag{9 : X^2}$$

$$(f + d_{h+1})e_{h+1} + (g + d_{h+1}e_{h+1}) = -v_hw_{h+1} - v_{h+1}w_h - uv/d_{h+1}\,; \tag{9 : X^1}$$

$$(g + d_{h+1}e_{h+1})e_{h+1} = w_hw_{h+1} + uw/d_{h+1}\,. \tag{9 : X^0}$$

The $:X^2$ equation readily becomes

$$-d_h = f - w_h + v_h^2 + d_{h+1} = v_h(v_h + v_{h+1}) + w_{h+1} + u/d_{h+1}\,,$$

so $d_{h+1}(v_h e_{h+1} - w_{h+1}) = d_h d_{h+1} + u$. With similar manipulation of the next two equations we felicitously obtain

$$d_{h+1}(v_h e_{h+1} - w_{h+1}) = d_h d_{h+1} + u\,; \tag{10a}$$
$$-v_h d_{h+1}(v_h e_{h+1} - w_{h+1}) = d_h d_{h+1}(e_h + e_{h+1}) - uv\,; \tag{10b}$$
$$w_h d_{h+1}(v_h e_{h+1} - w_{h+1}) = d_h d_{h+1} e_h e_{h+1} + uw\,. \tag{10c}$$

That immediately yields

$$d_h d_{h+1}(e_h + e_{h+1} + v_h) = u(v - v_h)\,; \tag{11a}$$
$$d_h d_{h+1}(e_h e_{h+1} - w_h) = -u(w - w_h)\,. \tag{11b}$$

Incidentally, by

$$-d_{h+1} = f - w_h + v_h^2 + d_h = v_h(v_{h-1} + v_h) + w_{h-1} + u/d_h\,,$$

we also discover that, mildly surprisingly,

$$d_h d_{h+1} + u = d_{h+1}(v_h e_{h+1} - w_{h+1}) = d_h(v_h e_h - w_{h-1}). \tag{12}$$

5 A Ridiculous Computation

It is straightforward to notice that the three final equations (9) yield

$$e_h^2(v_{h-1}v_h + w_{h-1} + w_h) + e_h(v_{h-1}w_h + v_h w_{h-1}) + w_{h-1}w_h = -u(e_h^2 + ve_h + w)/d_h\,.$$

Remarkably, by (12)

$$\begin{aligned}(d_{h-1}d_h + u)(d_h d_{h+1} + u) &= d_h^2(v_{h-1}e_h - w_h)(v_h e_h - w_{h-1})\\ &= e_h^2 v_{h-1}v_h - e_h(v_{h-1}w_{h-1} + v_h w_h) + w_{h-1}w_h\end{aligned}$$

and so, because

$$\begin{aligned}-(v_{h-1}w_{h-1} + v_h w_h) &= v_{h-1}w_h + v_h w_{h-1} - (w_{h-1} + w_h)(v_{h-1} + v_h)\\ &= v_{h-1}w_h + v_h w_{h-1} + e_h(w_{h-1} + w_h)\,,\end{aligned}$$

we obtain the surely useful identity

$$(d_{h-1}d_h + u)(d_h d_{h+1} + u) = -ud_h(e_h^2 + ve_h + w)\,. \tag{13}$$

This is just one of the nine such identities provided by the equations (10), and (12).

5.1 The special case $u = 0$

Consider now the case in which R, the remainder term $u(X^2 - vX + w)$, is replaced by $-v(X - w)$. In effect $u \leftarrow 0$ except that $uv \leftarrow v$, $uw \leftarrow vw$. For instance, (13) becomes

$$d_{h-1}d_hd_{h+1} = -v(e_h + w)\,, \tag{13$'$}$$

and, we'll need this, we now have

$$e_h + e_{h+1} + v_h = v/d_hd_{h+1}\,; \tag{11$'$a}$$
$$e_he_{h+1} - w_h = -vw/d_hd_{h+1}\,. \tag{11$'$b}$$

Indeed, we find that

$$d_{h-1}d_h^2d_{h+1}^2d_{h+2} = v^2(e_he_{h+1} + w(e_h + e_{h+1}) + w^2) = v^2(w_h - wv_h + w^2) \tag{14}$$

and therefore that

$$\begin{aligned} &d_{h-2}d_{h-1}^3d_h^4d_{h+1}^3d_{h+2} = \\ &v^4\big(w_{h-1}w_h + w^2\big(v_{h-1}v_h + (w_{h-1} + w_h)\big) - w(v_{h-1}w_h + w_{h-1}v_h) - w^3(v_{h-1} + v_h) + w^4\big)\,. \end{aligned} \tag{15}$$

This last expression is transformed by the equations (9) to become

$$\begin{aligned} v^4\big((g + d_he_h)e_h - vw/d_h + w^2(f + d_h) + \\ + w\big((f + d_h)e_h + (g + d_he_h) + v/d_h\big) + w^3e_h + w^4\big) \\ = v^4(e_h + w)\big((g + d_he_h) + w(f + d_h) + w^3\big)\,. \end{aligned} \tag{16}$$

Thus

$$d_{h-2}d_{h-1}^2d_h^3d_{h+1}^2d_{h+2} = -v^3\big((g + d_he_h) + w(f + d_h) + w^3\big)\,. \tag{17}$$

But wait, there's more! By (13$'$) we know that $-ve_h = d_{h-1}d_hd_{h+1} + vw$, so

$$d_{h-2}d_{h-1}^2d_h^3d_{h+1}^2d_{h+2} = v^2d_{h-1}d_h^2d_{h+1} - v^3(g + wf + w^3)\,,\ tag6 \tag{18}$$

already announced as Theoren 3.1.

6 A Cute Example

The example

$$T_{h-3}T_{h+3} = T_{h-2}T_{h+2} + T_h^2\,, \tag{19}$$

with $T_0 = T_1 = T_2 = T_3 = T_4 = T_5 = 1$ is readily found to derive from the genus 2 curve

$$\mathcal{C} : Z^2 - (X^3 - 4X + 1)Z + (X - 2) = 0\,. \tag{20}$$

To indeed see this, we first note that of course we need $d_1 = d_2 = d_3 = d_4 = 1$ to produce the initial values from $T_0 = T_1 = 1$. Since, plainly, $T_{-1} = T_6 = 2$, clearly $d_0 = 2$. By the

Theorem, we expect to require $v^2 = 1$ and $-v^3(g+wf+w^3) = 1$. Without loss of generality, we may take $v = -1$. From (13′) we then read off that

$$e_1 = 2 - w \quad \text{and} \quad e_2 = 1 - w\,.$$

Thus, by (7) and (8) we have

$$f + 2 = -v_1^2 + w_1 \quad \text{and} \quad g + 3 - 2w = v_1 w_1\,.$$

But from (11′a) and (11′b) we evaluate v_1 and w_1 in terms of w as

$$3 - 2w + v_1 = -1 \quad \text{and} \quad (2-w)(1-w) - w_1 = w\,.$$

Substituting appropriately we find that $1 = g + fw + w^3 = 6w - 11$ so, as already announced, $v = -1$, $w = 2$, $g = 1$, and $f = -4$.

Furthermore, we have $v_1 = 0$ and $v_0 + v_1 + e_1 = 0$, so $v_0 = 0$; then $f + 3 = -v_0^2 + w_0$ yields $w_0 = -1$. Noting that $g + 2e_0 + e_1 = 0$, we find that $e_0 = -1/2$. Thus the relevant continued fraction expansion commences

$$\begin{aligned}
Z_0 := \frac{Z + 2X - 1}{X^2 - 1} &= X - \frac{\overline{Z} + X}{X^2 - 1} \\
\frac{Z + X}{-(X^2 - 2)} &= -X - \frac{\overline{Z} + X - 1}{-(X^2 - 2)} \\
\frac{Z + X - 1}{X^2 - X - 1} &= X + 1 - \frac{\overline{Z} + X - 1}{X^2 - X - 1} \\
\frac{Z + X - 1}{-(X^2 - 2)} &= -X - \frac{\overline{Z} + X}{-(X^2 - 2)} \\
\frac{Z + X}{X^2 - 1} &= X - \frac{\overline{Z} + 2X - 1}{X^2 - 1} \\
&\cdots
\end{aligned}$$

providing a useful check on our allegations and displaying an expected symmetry (both the defining recursion and the set of initial values are symmetric). Denote by M the divisor class defined by the pair of points $(\varphi, 0)$ and $(\overline{\varphi}, 0)$ — here, φ is the golden ratio, a happenstance that will please adherents to the cult of Fibonacci — and by S the divisor class at infinity. Then the sequence $(T_h) = (\ldots, 2, 1, 1, 1, 1, 1, 1, 2, 3, 4, 8, 17, 50, 107, 239, 1103, \ldots)$ may be thought of as arising from the points $\ldots, M - S, M, M + S, M + 2S, \ldots$ on the Jacobian of the curve $\mathcal{C}$ displayed at (20). Evidently, $M - S = -M$ so $2M = S$ on $\mathrm{Jac}(\mathcal{C})$.

Allegation. Of course I do not do it here, but I suggest that my remarks suffice to show that one may readily prove that given a sequence (A_h) satisfying a recusive relation $A_{h-3}A_{h+3} = aA_{h-2}A_{h+2} + bA_h^2$ and with given values A_{h-3}, A_{h-2}, $\ldots$, A_{h+2} one may identify both a genus 2 curve $\mathcal{C} : Z^2 - AZ - R = 0$, $\deg A = 3$, $\deg R = 1$ and a divisor M on $\mathcal{C}$ giving rise to the sequence.

7 Comments

I consider the argument given in §5 above to be quite absurd and am ashamed to have spent a great deal of time in extracting it. Such are the costs of truly low lowbrow arguments; see [3] for heights of 'brow'. The only saving grace is my mildly ingenious use of symmetry in the argument's later stages. I do not know whether there is an appealing result of the present genre if $u \neq 0$; but see my remarks below. I should admit that I realised, but only after having successfully selected $u = 0$, that Noam Elkies had suggested to me at ANTS, Sydney 2002, that an identity of the genre (6) would exist, but had in fact specified just the special case $\deg R = 1$.

Mind you, with some uninteresting effort one can show (say by counting free parameters) that over an algebraic extension of the base field there is a birational transformation which transforms the given curve to one where $\deg R = 1$. That does not truly better the present theorem.

On the other hand, a dozen years ago‡, David Cantor [5] mentions that his results lead readily to Somos sequences both in genus 1 and 2; the latter of width 8. That his results provide Somos sequences in genus 2 is not obvious; however, recently, Cantor has told me a rather ingenious idea which clearly yields the result for all hyperelliptic curves $Y^2 = E(X)$, E a quintic, say with constant coefficient 1. In brief, Cantor's result is more general than mine but does not deal with all cases I handle here; nor does it produce the expected recursion formulæ of width 6. Moreover, after this paper was submitted I learned of the work [2] which produces Cantor's width 8 recurrences from addition formulas for the corresponding hyperelliptic functions.

The most serious disappointment is that the best argument I can produce here is just a much more complex version of that of [8] for genus 1. Seemingly a new view on the issues is needed if my methods are to yield results in higher genus.

References

[1] Enrico Bombieri and Paula B. Cohen, Siegel's lemma, Padé approximations and Jacobians (with an appendix by Umberto Zannier, and dedicated to Enzio De Giorgi), *Ann. Scuola Norm. Sup. Pisa* Cl. Sci. (4) **25** (1997), 155–178.

[2] Harry W. Braden, Victor Z. Enolskii, and Andrew N. W. Hone, Bilinear recurrences and addition formulae for hyperelliptic sigma functions, (2005), 15pp: at `http://arxiv.org/abs/math.NT/0501162`.

[3] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996. xiv+219 pp.

[4] David G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48**.177 (1987), 95–101.

‡I have a revision of his manuscript dated November, 1992.

[5] David G. Cantor, On the analogue of the division polynomials for hyperelliptic curves, *J. Reine Angew. Math.* **447** (1994), 91–145.

[6] Sergey Fomin and Andrei Zelevinsky, The Laurent phenomenon, *Adv. in Appl. Math.*, **28**, (2000), 119–144. Also 21pp: at `http://www.arxiv.org/math.CO/0104241`.

[7] 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, 2003.

[8] Alfred J. van der Poorten, Elliptic curves and continued fractions. *J. Integer Sequences* **8**, (2005), article 05.2.5.