ALF'S PREPRINTS
Paper 169, Draft of March 11, 2004, Pages 69–80
Centre for Number Theory Research, 1 Bimbil Place, Killara, Australia 2071

ELLIPTIC CURVES AND CONTINUED FRACTIONS

ceNTRe
Sydney, Australia 2071

ALFRED J. VAN DER POORTEN

ABSTRACT. Given $Y^2 = (X^2+f)^2 + 4v(X-w)$ we explicitly expand Y as the continued fraction of an element of $\mathbb{Q}((X^{-1}))$ and interpret the data so obtained.

A delightful 'essay' [16] by Don Zagier explains why the sequence $(B_h)_{h\in\mathbb{Z}}$, defined by $B_{-2}=1$, $B_{-1}=1$, $B_0=1$, $B_1=1$, $B_2=1$ and the recursion

$$B_{h-2}B_{h+3} = B_{h+2}B_{h-1} + B_{h+1}B_h\,, \tag{1}$$

consists only of integers. Zagier comments that "the proof comes from the theory of elliptic curves, and can be expressed either in terms of the denominators of the co-ordinates of the multiples of a particular point on a particular elliptic curve, or in terms of special values of certain Jacobi theta functions."

In the present note I study the continued fraction expansion of the square root of a quartic polynomial, inter alia obtaining sequences generated by recursions such as (1). Here, however, it is clear that I have also constructed the co-ordinates of the shifted multiples of a point on an elliptic curve and it is it fairly plain how to relate the surprising integer sequences and the elliptic curves from which they arise.

A brief reminder exposition on continued fractions in quadratic function fields appears as §4, starting at page 76 below.

1. Continued Fraction Expansion of the Square Root of a Quartic

We suppose the base field $\mathbb{F}$ is not of characteristic 2 because that case requires nontrivial changes throughout the exposition and not of characteristic 3 because that requires some trivial changes to parts of the exposition. We study the continued fraction expansion of a quartic polynomial $D\in\mathbb{F}[X]$. Set

$$\mathcal{C} : Y^2 = D(X) := (X^2+f)^2 + 4v(X-w), \tag{2}$$

and for brevity write $A = X^2+f$ and $R = v(X-w)$. For $h = 0, 1, 2, \ldots$ we denote the complete quotients of Y_0 by

$$Y_h = (Y + A + 2e_h)/v_h(X-w_h)\,, \tag{3}$$

Typeset March 11, 2004 [15:42].

2000 *Mathematics Subject Classification.* Primary 11J70, 11A65, 11J68.

Key words and phrases. continued fraction expansion, function field of characteristic zero, Somos sequence.

The author was supported in part by a grant from the Australian Research Council.

noting that the Y_h all are reduced, namely $\deg Y_h > 0$ but $\deg \overline{Y}_h < 0$. The upshot is that the continued fraction expansion of Y_0 has typical line, line h:

$$\frac{Y + A + 2e_h}{v_h(X - w_h)} = \frac{2(X + w_h)}{v_h} - \frac{\overline{Y} + A + 2e_{h+1}}{v_h(X - w_h)}.$$

Thus evident recursion formulas, see (25) at page 77, yield

$$f + e_h + e_{h+1} = -w_h^2 \tag{4}$$

and $-v_h v_{h+1}(X - w_h)(X - w_{h+1}) = (Y + A + 2e_{h+1})(\overline{Y} + A + 2e_{h+1})$. Hence

$$v_h v_{h+1}(X - w_h)(X - w_{h+1}) = -4(X^2 + f + e_{h+1})e_{h+1} + 4v(X - w). \tag{5}$$

Equating coefficients in (5), and then dividing by $-4e_{h+1}$, we get

X^2: $\qquad -4e_{h+1} = v_h v_{h+1}$;

X^1: $\qquad v/e_{h+1} = w_h + w_{h+1}$;

X^0: $\qquad f + e_{h+1} + vw/e_{h+1} = w_h w_{h+1}$.

The five displayed equations immediately above readily lead by several routes to

$$e_h e_{h+1} = v(w - w_h). \tag{6}$$

For example, apply the remainder theorem to the right hand side of (5) after noting it is divisible by $X - w_h$, and recall (4).

Proposition 1 (Adams and Razar [1]). *Denote the two points at infinity on the elliptic curve* (2) *by* S *and* O*, with* O *the zero of its group law. The points* $M_{h+1} := (w_h, e_h - e_{h+1})$ *all lie on* $\mathcal{C}$*. Set* $M_1 = M$*, and* $M_{h+1} =: M + S_h$*. Then* $S_h = hS$*.*

Proof. The points M_{h+1} lie on the curve $\mathcal{C} : Y^2 = D(X)$ because

$$\begin{aligned}(e_h - e_{h+1})^2 - (w_h^2 + f)^2 &= \big(e_h - (e_{h+1} + w_h^2 + f)\big)\big((e_h + w_h^2 + f) - e_{h+1}\big) \\ &= -4e_h e_{h+1} = 4v(w_h - w).\end{aligned}$$

The birational transformations

$$X = \big(V - v\big)/U, \qquad Y = 2U - (X^2 + f); \tag{7}$$

conversely,

$$2U = Y + X^2 + f, \qquad 2V = XY + X^3 + fX + 2v, \tag{8}$$

move the point S to $(0,0)$, leave O at infinity, and change the quartic model to a Weierstrass model

$$\mathcal{W} : V^2 - vV = U^3 - fU^2 + vwU. \tag{9}$$

Specifically, one sees that $U(M_{h+1}) = -e_{h+1}$, and $V(M_{h+1}) = v - w_h e_{h+1}$. We also note that $U(-M_{h+1}) = -e_{h+1}$, $V(-M_{h+1}) = w_h e_{h+1}$.

To check $S + (M + S_{h-1}) = M + S_h$ on $\mathcal{W}$ it suffices for us to show that the three points $(0,0)$, $(-e_h, v - w_{h-1}e_h)$, and $(-e_{h+1}, w_h e_{h+1})$ lie on a straight line. But that is $(v - w_{h-1}e_h)/e_h = w_h$. So $w_{h-1} + w_h = v/e_h$ proves the claim. ∎

1.1. The sequence (A_h).

Proposition 2. *Let* (A_h) *be the sequence defined by the 'initial' values* A_0, A_1 *and the recursive definition*

$$A_{h-1}A_{h+1} = e_h A_h^2 \,. \tag{10}$$

Then, given A_0, A_1, A_2, A_3, A_4 *satisfying* (10), *the recursive definition*

$$A_{h-2}A_{h+2} = v^2 A_{h-1}A_{h+1} + v^2(f+w^2)A_h^2 \tag{11}$$

defines the same sequence as does (10). *Just so, also*

$$A_{h-2}A_{h+3} = -v^2(f+w^2)A_{h-1}A_{h+2} + v^3\big(v + 2w(f+w^2)\big)A_hA_{h+1} \tag{12}$$

defines that sequence.

Proof. By (6) we obtain

$$e_{h-1}e_h^2e_{h+1} = v^2(w-w_{h-1})(w-w_h)$$
$$= v^2(w_{h-1}w_h - w(w_{h-1}+w_h)+w^2) = v^2\left(\big(f+e_h+vw/e_h\big) - w\cdot(v/e_h) + w^2\right).$$

Thus

$$e_{h-1}e_h^2e_{h+1} = v^2\left(e_h + (f+w^2)\right). \tag{13}$$

However, $A_{h-1}A_{h+1} = e_hA_h^2$ entails

$$A_{h-2}A_hA_{h-1}A_{h+1}A_hA_{h+2} = e_{h-1}e_he_{h+1}A_{h-1}^2A_h^2A_{h+1}^2\,,$$

and so $A_{h-2}A_{h+2} = e_{h-1}e_he_{h+1}A_{h-1}A_{h+1}$, which is

$$A_{h-2}A_{h+2} = e_{h-1}e_h^2e_{h+1}A_h^2\,. \tag{14}$$

On multiplying (13) by A_h^2 we obtain (11).

Similarly (10) yields $A_{h-1}A_{h+1}A_hA_{h+2} = e_he_{h+1}A_h^2A_{h+1}^2$, and so

$$A_{h-1}A_{h+2} = e_he_{h+1}A_hA_{h+1}\,. \tag{15}$$

It follows readily that

$$A_{h-2}A_{h+3} = e_{h-1}e_h^2e_{h+1}^2e_{h+2}A_hA_{h+1}\,. \tag{16}$$

Moreover, (13) implies that

$$e_{h-1}e_h^3e_{h+1}^3e_{h+2} = v^4\left(e_he_{h+1} + (f+w^2)(e_h+e_{h+1}) + (f+w^2)^2\right).$$

However, by (4) we know that $v^2\left(e_h+e_{h+1}+f+w^2\right) = -v^2(w_h^2-w^2)$. But $v(w-w_h) = e_he_{h+1}$ and $v(w+w_h) = -v(w-w_h)+2vw = -e_he_{h+1}+2vw$. So

$$e_{h-1}e_h^2e_{h+1}^2e_{h+2} = v^2\left(-(f+w^2)e_he_{h+1} + v^2 + 2vw(f+w^2)\right), \tag{17}$$

which immediately allows us to see that also (12) yields the sequence (A_h). ∎

1.2. Two-sided infinite sequences. It is plain that the various definitions of the sequence (A_h) encourage one to think of it as bidirectional infinite. Indeed, albeit that one does feel a need to start a continued fraction expansion — so one conventionally begins it at Y_0, one is not stopped from thinking of the tableau listing the lines of the expansion as being two-sided infinite; note the remark at the end of § 4.1, page 77. In summary: we may and should view the various sequences (e_h), ..., defined above, as two-sided infinite sequences.

1.3. **Vanishing.** If say $v_k = 0$, then line k of the continued fraction expansion of Y_0 makes no sense both because the denominator $Q_k(X) := v_k(X - w_k)$ of the complete quotient Y_k seems to vanish identically and because the alleged partial quotient $a_k := 2(X + w_k)/v_k$ blows up.

The second difficulty is real. The vanishing of v_k entails a partial quotient blowing up to higher degree. We deal with vanishing by refusing to look at it. We move the point of impact of the issue by dismissing most of the data we have obtained, including the continued fraction tableau, and keep only a part of the sequence (e_h). That makes the first difficulty moot.*

Remark. There is no loss of generality in taking $k = 0$. Then, up to an irrelevant normalisation, $Y_0 = Y + A$. If more than one of the v_h vanish then it is a simple exercise to confirm that the continued fraction expansion of Y_0 necessarily is purely periodic, see the discussion at page 79. If Y_0 does not have a periodic continued fraction expansion then there is some h_0, namely $h_0 = 0$, so that, for all $h > h_0$, line h of the expansion of Y_0 does make sense.

Except of course when dealing explicitly with periodicity, we suppose in the sequel that if $v_k = 0$ then $k = 0$; we refer to this case as the *singular* case.

2. Elliptic sequences

We remark that in the singular case the sequence $(e_h)_{h\geq 1}$ defines antisymmetric double-sided sequences (W_h), that is with $W_{-h} = -W_h$, by $W_{h-1}W_{h+1} = e_hW_h^2$ and so that, for all integers h, m, and n,

$$W_{h-m}W_{h+m}W_n^2 + W_{n-h}W_{n+h}W_m^2 + W_{m-n}W_{m+n}W_h^2 = 0\,. \tag{18'}$$

Actually, one may find it preferable to forego an insistence on antisymmetry in favour of rewriting (18′) less elegantly as

$$W_{h-m}W_{h+m}W_n^2 = W_{h-n}W_{h+n}W_m^2 - W_{m-n}W_{m+n}W_h^2\,, \tag{18}$$

just for $h \geq m \geq n$. In any case, (18) seems more dramatic than it is. An easy exercise confirms that, if $W_1 = 1$, (18) is equivalent to just

$$W_{h-m}W_{h+m} = W_m^2W_{h-1}W_{h+1} - W_{m-1}W_{m+1}W_h^2 \tag{19}$$

for all integers $h \geq m$. Indeed, (19) is just a special case of (18). However, given (19), obvious substitutions in (18) quickly show one may return from (19) to the apparently more general (18).

But there is a drama here. As already remarked in a near identical situation, the recurrence relation $W_{h-2}W_{h+2} = W_2^2W_{h-1}W_{h+1} - W_1W_3W_h^2$, and five or so initial values, already suffices to produce (W_h). Thus (19) for all m is apparently entailed by its special case $m = 2$.

I can show this directly†, by way of new relations on the e_h, for $m = 3$. But the case $m = 4$ already did not seem worth the effort. Whatever, my approach

---

*In any case, the first apparent difficulty is just an artifact of our notation. If, from the start, we had written $Q_h = v_hX + y_h$, as we might well have done at the cost of nasty fractions in our formulas, we would not have entertained the thought that $v_k = 0$ entails $y_k = 0$. Plainly, we must allow $v_k = 0$ yet $v_kw_k \neq 0$.

†Plainly $e_{h-2}e_{h-1}^2e_h^3e_{h+1}^2e_{h+2}\cdot e_h = v^4\big(e_{h-1} + (f + w^2)\big)\big(e_{h-1} + (f + w^2)\big)e_h^2$. Now notice that $(e_{h-1}e_h + e_he_{h+1})e_h = v(w - w_{h-1} + w - w_h)e_h = v^2 - 2vwe_h$ and recall that $e_{h-1}e_h^2e_{h+1} = v^2\big(e_h + (f + w^2)\big)$. The upshot is a miraculous cancellation yielding

$$e_{h-2}e_{h-1}^2e_h^3e_{h+1}^2e_{h+2}\cdot e_h = v^4\big((f + w^2)^2e_h^2 + v(v + 2w(f + w^2))e_h\big)$$

gave me no hint as to how to concoct an inductive argument leading to general m. Plan B, to look it up, fared little better. In her thesis [11], Rachel Shipsey shyly refers the reader back to Morgan Ward's opus [15]; but Ward does not comment on the matter at all, having *defined* his sequences by (19). Well, perhaps Ward does comment. The issue is whether (19) is coherent: do different m yield the one sequence? Ward notes that if σ is the Weierstraß σ-function then a sequence $\big(\sigma(hu)/\sigma(u)^{h^2}\big)$ satisfies (19) for all m. Whatever, a much more direct argument would be much more satisfying.

Proposition 2 shows that certainly $W_{h-2}W_{h+2} = W_2^2W_{h-1}W_{h+1} - W_1W_3W_h^2$ for $h = 1, 2, \ldots$, in which case (19) apparently follows by arguments in [15] and anti-symmetry; (18) is then just an easy exercise.

The singular case is initiated by $v_1 = 4v$, $w_1 = w$, $e_1 = 0$, $e_2 = -(f + w^2)$. For temporary convenience set $x = v/(f + w^2)$. From the original continued fraction expansion of $Y + A$ or, better, the recursion formulas of page 70, we fairly readily obtain $v_2 = 1/x$, $w_2 = w-x$, $e_3 = -x(x+2w)$, $e_4 = v(x^2(x+2w)-v)/x^2(x+2w)^2$.

We are now free to choose, say $W_1 = 1$, $W_2 = v$, leading to $W_3 = -v^2(f + w^2)$, $W_4 = -v^4\big(v + 2w(f + w^2)\big)$, $W_5 = -v^6\big(v(v + 2w(f + w^2)) - (f + w^2)^3\big)$, ...

That allows us to notice that (12) apparently is

$$vA_{h-2}A_{h+3} = W_2W_3A_{h-1}A_{h+2} - W_1W_4A_hA_{h+1}$$

and that (11) of course is

$$A_{h-2}A_{h+2} = W_2^2A_{h-1}A_{h+1} - W_1W_3A_h^2\,.$$

2.1. **Elliptic divisibility sequences.** Recall that for $h = 1, 2, \ldots$ the $-e_h$ are in fact the U co-ordinates of the multiples hS of the point $S = (0, 0)$ on the curve $V^2 - vV = U^3 - fU^2 + vwU$.

Suppose we are working in the ring $Z = \mathbb{Z}[f, v, vw]$ of 'integers' (or just suppose that f, v and vw are integers). If $\gcd(v, vw) = 1$ — so the exact denominator of the 'rational' w is v — then our choices $W_1 = 1$, $W_2 = v$ lead the definition $W_{h-1}W_{h+1} = e_hW_h^2$ to be such that W_h^2 is always the exact denominator of the 'rational' e_h. It is this that is shown in detail by Rachel Shipsey [11]. In particular it follows that (W_h) is an elliptic divisibility sequence as described by Ward [15]. A convenient recent introductory reference is Chapter 10 of the book [3].

Set $hS = (U_h/W_h^2, V_h/W_h^3)$, thus defining sequences (U_h), (V_h), and (W_h) of integers, with W_h chosen minimally. Shipsey notices, provided that indeed $\gcd(v, vw) = 1$, that $\gcd(U_h, V_h) = W_{h-1}$ and $W_{h-1}W_{h+1} = -U_h$. Here, I have used this last fact to define the sequence (W_h).

Starting, in effect, from the definition (18), Morgan Ward [15] shows that with $W_0 = 0$, $W_1 = 1$, and $W_2\big|W_4$, the sequence (W_h) is a divisibility sequence; that is, if $a\big|b$ then $W_a\big|W_b$. A little more is true. If also $\gcd(W_3, W_4) = 1$ then in fact $\gcd(W_a, W_b) = W_{\gcd(a,b)}$. On the other hand, a prime dividing both W_3 and W_4 divides W_h for all $h \geq 3$.

---

and allowing us to divide by the auxiliary e_h. Thus the bottom line is

$$A_{h-3}A_{h+3} = v^4\big((f + w^2)^2A_{h-1}A_{h+1} + v(v + 2w(f + w^2))A_h^2\big),$$

which is $A_{h-3}A_{h+3} = W_3^2A_{h-1}A_{h+1} - W_2W_4A_h^2$.

2.2. **Periodicity.** Suppose now that the sequence (W_h) is periodic. On my reading, this is the issue most exercising Ward in [15]. From the continued fraction expansion and, say, [8], we find that $v = 0$ (but $w' = vw \neq 0$ if our curve is to be elliptic) is the case of the continued fraction having quasi-period $r = 1$ and the divisor at infinity on the curve having torsion $m = 2$. Just so, $f + w^2 = 0$, thus $W_3 = 0$, signals $r = 2$ and $m = 3$, and $x + 2w = 0$, or $W_4 = 0$, is $r = 3$ and $m = 4$. And so on; for more see [8].

However, Morgan Ward's careful study [15] includes him proving that precisely the periods 1, 2, 3, 4, 5, 6, 8, or 10 are possible for an integral elliptic sequence defined by (19). This result does not cohere comfortably with what we now know to be true, see for example [7], of torsion on elliptic curves defined over $\mathbb{Q}$. However, closer examination of the matter reveals that the adjective 'integral' is indeed of material importance and that explicit use of anti-symmetry appears to simplify Ward's arguments.

Aside: It has been suggested in my hearing that "Mathematics is the study of degeneracy", so the following warrants careful consideration. In the singular case we have $e_1 = 0$ and then the recursion $e_{h-1}e_h^2e_{h+1} = v^2\big(e_h + (f + w^2)\big)$ and $e_2 = -(f + w^2)$ forces $e_0 \cdot 0^2 = -v^2$ in the case $h = 1$. In a context in which $v = 0$ and $w' = vw \neq 0$ passes without comment this is no great matter. However, we must also cope with $W_{-1}W_1 = e_0W_0^2$, so $W_{-1} = e_0 \cdot 0^2$, and with both $W_{-2}W_0 = e_{-1}W_{-1}^2$ and $W_{-3}W_{-1} = e_{-2}W_{-2}^2$. In like spirit one might notice that if $v = 0$, the case of quasi-period 1, then $W_{h-2}W_{h+2} = w'^2W_h^2$.

3. Examples

3.1. Consider the curve $\mathcal{C} : Y^2 = (X^2 - 29)^2 - 4 \cdot 48(X + 5)$; here a corresponding cubic model is $\mathcal{E} : V^2 + 48V = U^3 + 29U^2 + 240U$. Set $A = X^2 - 29$. The first several preceding and succeeding steps in the continued fraction expansion of $Y_0 = (Y + A + 16)/8(X + 3)$ are[‡]

line $\overline{3}$: $$\frac{Y + A + 18}{16(X + 2)/3} = \frac{X - 2}{8/3} - \frac{\overline{Y} + A + 32}{16(X + 2)/3}$$

line $\overline{2}$: $$\frac{Y + A + 32}{12(X + 1)} = \frac{X - 1}{6} - \frac{\overline{Y} + A + 24}{12(X + 1)}$$

line $\overline{1}$: $$\frac{Y + A + 24}{4(X + 3)} = \frac{X - 3}{2} - \frac{\overline{Y} + A + 16}{4(X + 3)}$$

line 0 : $$\frac{Y + A + 16}{8(X + 3)} = \frac{X - 3}{4} - \frac{\overline{Y} + A + 24}{8(X + 3)}$$

line 1 : $$\frac{Y + A + 24}{6(X + 1)} = \frac{X - 1}{3} - \frac{\overline{Y} + A + 32}{6(X + 1)}$$

line 2 : $$\frac{Y + A + 32}{32(X + 2)/3} = \frac{X - 2}{16/3} - \frac{\overline{Y} + A + 18}{32(X + 2)/3}$$

$$\frac{Y + A + 18}{9(3X + 10)/8} = \cdots$$

where elegance has suggested we write 'line $\overline{h}$' as short for 'line $-h$'.

[‡] Here my choice of $v_0 = 8$ is arbitrary but not at random.

The feature motivating this example is the six integral points $(-2,\pm7)$, $(-1,\pm4)$, and $(-3,\pm4)$ on $\mathcal{C}$. With $M_{\mathcal{C}}=(-3,4)$ and $S_{\mathcal{C}}$ the 'other' point at infinity these are in fact the six points $M_{\mathcal{C}}+hS_{\mathcal{C}}$ for $h=-3$, -2, -1, 0, 1, and 2.

Correspondingly, on $\mathcal{E}$ we have the integral points $M+2S=(-16,-32)$ and $M-2S=(-16,-16)$, $M-S=(-12,-36)$ and $M+S=(-12,-12)$; here $M=M_{\mathcal{E}}=(-8,-24)$; $S=S_{\mathcal{E}}=(0,0)$. Of course $\mathcal{E}$ is not minimal; nor, for that matter was $\mathcal{C}$. In fact the replacements $X\leftarrow 2X+1$, $Y\leftarrow 4Y$ yield

$$Y^2=(X^2+X-7)^2-4\cdot 6(X+3)\,, \tag{20}$$

correctly suggesting we need a more general treatment than that presented in the discussion above. It turns out to be enough for present purposes to replace $e_h\leftarrow 4e_h$ obtaining

$$\ldots,\ e_{-3}=\tfrac{9}{4},\ e_{-2}=4,\ e_{-1}=3,\ e_0=2,\ e_1=3,\ e_2=4,\ e_3=\tfrac{9}{4},\ \ldots\,.$$

Then $A_0=1$, $A_1=1$ and

$$A_{h-1}A_{h+1}=e_hA_h^2$$

yields the sequence $\ldots$, $A_{-4}=2^53^5$, $A_{-3}=2^53^2$, $A_{-2}=2^33$, $A_{-1}=2$, $A_0=1$, $A_1=1$, $A_2=3$, $A_3=2^23^2$, $A_4=2^23^5$, $\ldots$. Notice that we're hit for six[§] by increasingly high powers of primes dividing 6 appearing as factors of the A_h. However, we know that (12) derives from (17). With the original e_hs divided by 4 that yields

$$A_{h-2}A_{h+3}=6^2A_{h-1}A_{h+2}+6^3A_hA_{h+1}\,. \tag{21}$$

Remarkably, one may remove the effect of the 6 by renormalising to a sequence (B_h) of integers satisfying

$$B_{h-2}B_{h+3}=B_{h-1}B_{h+2}+B_hB_{h+1}\,.$$

Specifically, $\ldots$, $B_{-4}=3$, $B_{-3}=2$, $B_{-2}=1$, $B_{-1}=1$, $B_0=1$, $B_1=1$, $B_2=1$, $B_3=2$, $B_4=3$, $B_5=5$, $B_6=11$, $B_7=37$, $B_8=83$, $\ldots$, and the sequence is symmetric about $B=0$. Interestingly, the choice of each B_h as a divisor of A_h is forced, in the present case by the data $A_0=A_1=1$ and the decision that the coefficient of B_hB_{h+1} be 1. I am hoping[¶] that Christine Swart's thesis [14] may assist me in further explaining the phenomena here exposed. Of course it is straightforward to verify that $A_{h-2}A_{h+3}$ is always divisible by 6^3 and $A_{h-1}A_{h+2}$ always by 6.

3.2. Take $v=\pm1$ and $f+w^2=1$. Thus $e_{h-1}e_h^2e_{h+1}=e_h+1$ and so $e_0=1$, $e_1=1$ yields the sequence $\ldots$, 2, 1, 1, 2, $3/4$, $14/9$, $\ldots$, of values of e_h. As explained above, with $A_0=1$ and $A_1=1$, the definition $A_{h-1}A_{h+1}=e_hA_h^2$ yields the symmetric sequence $\ldots$, 2, 1, 1, 1, 1, 2, 3, 7, 23, 59, $\ldots$, of values of A_h satisfying the recursion

$$A_{h-2}A_{h+2}=A_{h-1}A_{h+1}+A_h^2\,.$$

Plainly, one can get four consecutive values 1 in a sequence (A_h) as just defined only by having two consecutive values 1 in the corresponding sequence (e_h).

[§] My remark is guided by knowing that $V^2+UV+6V=U^3+7U^2+12U$ is a minimal model for $\mathcal{E}$, and noticing that $\gcd(6,12)=6$.

[¶] But notwithstanding her enthusiastic response to my request she has not yet sent me the damned thing.

Set $Y^2 = A^2 + 4v(X - w)$, where $A = X^2 + f$. With $Z = \frac{1}{2}(Y + A)$, we have $Z\overline{Z} = -v(X - w)$ and $Z + \overline{Z} = A$. Thus the consecutive lines

$$\frac{Z+1}{X-b} = \quad (X+b) - \frac{\overline{Z}+1}{X-b}$$
$$\frac{Z+1}{-(X-c)} = -(X+c) - \frac{\overline{Z}+2}{-(X-c)}$$

entail

$$f + 2 = -b^2\,, \quad f + 3 = -c^2\,, \quad \text{and} \quad b + c = v\,, \quad bc = f + vw + 1\,,$$

which is $v = \pm 1$, $b = \pm 1$, $c = 0$, $f = -3$, and $w = \pm 2$. Up to $X \leftarrow -X$, the sequence (A_h) is given by the curve $\mathcal{C} : Y^2 = (X^2 - 3)^2 + 4(X - 2)$ and its points $M_{\mathcal{C}} + hS_{\mathcal{C}}$, $M_{\mathcal{C}} = (1, 0)$, $S_{\mathcal{C}}$ the 'other point' at infinity; equivalently by

$$\mathcal{E} : V^2 - V = U^3 + 3U^2 + 2U \quad \text{with } M = (-1, 1)\,,\ S = (0, 0)\,.$$

Indeed, $M + S = (-1, 0)$, $M + 2S = (-2, 1)$, $M + 2S = (-3/4, 3/8)$, $\ldots$. Note that it is impossible to have three consecutive values 1 in the sequence (e_h) if also $v = \pm 1$, except for trivial periodic cases, so the hoo-ha of the example at §3.1 above is in a sense unavoidable.

3.3. **Remarks.** The two examples get a rather woolly treatment at [13] and its preceding discussion, see [5] for context. The observation that a twist $V^2 - vV = dU^3 - fU^2 + vwU$ becomes $V^2 - dvV = U^3 - fU^2 + dvw$ by $U \leftarrow dU$, $V \leftarrow dV$ allows one to presume $v = \pm 1$. A suitable choice of e_0, e_1 and A_0, A_1 should now allow one to duplicate the result$^{\|}$ claimed in [13] in somewhat less brutal form.

4. Rappels

4.1. **Continued fraction expansion of a quadratic irrational.** Let $Y = Y(X)$ be a quadratic irrational integral element of the field $\mathbb{F}((X^{-1}))$ of Laurent series

$$\sum_{h=-d}^{\infty} f_{-h} X^{-h}, \quad \text{some } d \in \mathbb{Z} \tag{22}$$

defined over some given base field $\mathbb{F}$; that is, there are polynomials T and D defined over $\mathbb{F}$ so that

$$Y^2 = T(X)Y + D(X)\,. \tag{23}$$

Plainly, by translating Y by a polynomial if necessary, we may suppose that $\deg D \geq 2 \deg T + 2$, with $\deg D = 2g + 2$, say, and $\deg T \leq g$; then $\deg Y = g + 1$. Recall here that a Laurent series (22) with $f_d \neq 0$ has degree d.

Set $Y_0 = (Y + P_0)/Q_0$ where P_0 and Q_0 are polynomials so that Q_0 divides the norm $(Y + P_0)(\overline{Y} + P_0)$; notice here that an $\mathbb{F}[X]$-module $\langle Q, Y + P\rangle$ is an ideal in $\mathbb{F}[X, Y]$ if and only if $Q \big| (Y + P)(\overline{Y} + P)$.

Further, suppose that $\deg Y_0 > 0$ and $\deg \overline{Y}_0 < 0$; that is, Y_0 is *reduced*. Then the continued fraction expansion of Y_0 is given by a sequence of lines, of which the h-th is

$$Y_h := (Y + P_h)/Q_h = a_h - (\overline{Y} + P_{h+1})/Q_h\,; \quad \text{in brief} \quad Y_h = a_h - \overline{B}_h\,. \tag{24}$$

$^{\|}$Namely, to obtain elliptic curves yielding a sequence (A_h) with nominated A_{-1}, A_0, A_1, A_2 and such that $A_{h-2}A_{h+2} = \kappa A_{h-2}A_{h-2} + \lambda A_{h-2}A_{h-2}$.

Here the polynomial a_h is a *partial quotient*, and the next *complete quotient* Y_{h+1} is the reciprocal of the preceding *remainder* $-(\overline{Y}+P_{h+1})/Q_h$. Plainly the sequences of polynomials (P_h) and (Q_h) are given by the recursion formulas

(25) $P_h+P_{h+1}+(Y+\overline{Y}\,)=a_hQ_h$ and $Y\overline{Y}+(Y+\overline{Y})P_{h+1}+P_{h+1}^2=-Q_hQ_{h+1}$.

It is easy to see by induction on h that Q_h divides the norm $(Y+P_h)(\overline{Y}+P_h)$.

We observe also that we have a conjugate expansion with h-th line

(26) $$B_h:=(Y+P_{h+1})/Q_h=a_h-(\overline{Y}+P_h)/Q_h\,,\quad \text{that is,}\quad B_h=a_h-\overline{Y}_h\,.$$

Note that the next line of this expansion is the conjugate of the previous line of its conjugate expansion: conjugation reverses a continued fraction tableau. Because the conjugate of line 0 is the last line of its tableaux we can extend the expansion forming the conjugate tableaux, leading to lines $h=1,\,2,\,\dots$

$$(Y+P_{-h+1})/Q_{-h}=a_{-h}-(Y+P_{-h})/Q_{-h}\,;\quad \text{that is,}\quad B_{-h}=a_{-h}-\overline{Y}_{-h}\,.$$

Plainly the original continued fraction tableau also is two-sided infinite and our thinking of it as ‘starting’ at Y_0 is just convention.

4.2. **Continued fractions.** One writes $Y_0=[\,a_0\,,\,a_1\,,\,a_2\,,\,\dots]$, where formally

(27) $$[\,a_0\,,\,a_1\,,\,a_2\,,\,\dots\,,\,a_h\,]=a_0+1/[\,a_1\,,\,a_2\,,\,\dots\,,\,a_{h-1}\,]\quad\text{and}\quad[\quad]=\infty\,.$$

It follows, again by induction on h, that the definition

$$\begin{pmatrix}a_0&1\\0&1\end{pmatrix}\begin{pmatrix}a_1&1\\0&1\end{pmatrix}\cdots\begin{pmatrix}a_h&1\\0&1\end{pmatrix}=:\begin{pmatrix}x_h&x_{h-1}\\y_h&y_{h-1}\end{pmatrix}$$

entails $[\,a_0\,,\,a_1\,,\,a_2\,,\,\dots\,,\,a_h\,]=x_h/y_h$. This provides a correspondence between the *convergents* x_h/y_h and certain products of 2×2 matrices (more precisely, between the sequences (x_h), (y_h) of *continuants* and those matrices). It is a useful exercise to notice that $Y_0=[\,a_0\,,\,a_1\,,\,\dots\,,\,a_h\,,\,Y_{h+1}\,]$ implies that

$$Y_{h+1}=-(y_{h-1}Y-x_{h-1})/(y_hY-x_h)$$

and that this immediately gives

(28) $$Y_1Y_2\cdots Y_{h+1}=(-1)^h(x_h-y_hY)^{-1}.$$

The quantity $-\deg(x_h-y_hY)=\deg y_{h+1}$ is a weighted sum giving a measure of the “distance” traversed by the continued fraction expansion to its $(h+1)$-st complete quotient. Taking norms yields

(29) $$(x_h-y_hY)(x_h-y_h\overline{Y})=(-1)^{h+1}Q_{h+1}\,.$$

4.3. **Conjugation, symmetry, and periodicity.** Each partial quotient a_h is the polynomial part of its corresponding complete quotient Y_h. Note, however, that the assertions above are independent of that conventional selection rule.

One readily shows that Y_0 *reduced*, to wit $\deg Y_0>0$ and $\deg\overline{Y}_0<0$, implies that each complete quotient Y_h is reduced. Indeed, it also follows that $\deg B_h>0$, while plainly $\deg\overline{B}_h<0$ since $-\overline{B}_h$ is a remainder; so the B_h too are reduced. In particular a_h, the polynomial part of Y_h, is also the polynomial part of B_h.

Plainly, at least the first two leading terms of each polynomial P_h must coincide with the leading terms of $Y-T$. It also follows that the polynomials P_h and Q_h satisfy the bounds

(30) $$\deg P_h=g+1\quad\text{and}\quad\deg Q_h\le g\,.$$

Thus, if the base field $\mathbb{F}$ is finite the box principle entails the continued fraction expansion of Y_0 is periodic. If $\mathbb{F}$ is infinite, periodicity is just happenstance.

Suppose, however, that the function field $\mathbb{F}(X,Y)$ is exceptional in that Y_0, say, has a periodic continued fraction expansion. If the continued fraction expansion of Y_0 is periodic then, by conjugation, also the expansion of B_0 is periodic. But conjugation reverses the order of the lines comprising a continued fraction tableau. Hence the conjugate of any preperiod is a 'postperiod', an absurd notion. It follows that, if periodic, the two conjugate expansions are purely periodic.

Denote by A the polynomial part of Y, and recall that $Y+\overline{Y}=T$. It happens that line 0 of the continued fraction expansion of $Y+A-T$ is

$$Y+A-T=2A-T-(\overline{Y}+A-T) \tag{31}$$

and is symmetric. In general, if the expansion of Y_0 has a symmetry, and if the continued fraction expansion is periodic, its period must have a second symmetry**. So if Y is exceptional in having a periodic continued fraction expansion then its period is of lenght $2s$ and has an additional symmetry of the first kind $P_s=P_{s+1}$, or its period is of length $2s+1$ and also has a symmetry of the second kind, $Q_s=Q_{s+1}$. Conversely, this is the point, if the expansion of Y has a second symmetry then it must be periodic as just described.

4.4. **Units.** It is easy to apply the Dirichlet box principle to prove that an order $\mathbb{Q}[\omega]$ of a quadratic number field $\mathbb{Q}(\omega)$ contains nontrivial units. Indeed, by that principle there are infinitely many pairs of integers (p,q) so that $|q\omega-p|<1/q$, whence $|p^2-(\omega+\overline{\omega})pq+\omega\overline{\omega}q^2|<(\omega-\overline{\omega})+1$. It follows, again by the box principle, that there is an integer l with $0<|l|<(\omega-\overline{\omega})+1$ so that the equation $p^2-(\omega+\overline{\omega})pq+\omega\overline{\omega}q^2=l$ has infinitely many pairs (p,q) and (p',q') of solutions with $p\equiv p'$ and $q\equiv q' \pmod{l}$. For each such distinct pair, $xl=pp'-\omega\overline{\omega}qq'$, $yl=pq'-p'q+(\omega+\overline{\omega})qq'$, yields $(x-\omega y)(x-\overline{\omega}y)=1$.

In the function field case, we cannot apply the the box principle for a second time if the base field $\mathbb{F}$ is infinite. So the existence of a nontrivial unit $x(X)-y(y)Y(X)$ is exceptional. This should not be a surprise. By the definition of the notion 'unit', such a unit $u(X)$ say, has a divisor supported only at infinity. Moreover, u is a function of the order $\mathbb{F}[X,Y]$, and is say of degree m, so the existence of u implies that the class containing the divisor at infinity is a torsion divisor on the Jacobian of the curve (23). The existence of such a torsion divisor is of course exceptional.

Suppose now that the function field $\mathbb{F}(X,Y)$ does contain a nontrivial unit u, say of norm $-\kappa$ and degree m. Then $\deg(yY-x)=-m<-\deg y$, so x/y is a convergent of Y and so some Q is $\pm\kappa$, say $Q_r=\kappa$ with r odd. That is, line r of the continued fraction expansion of $Y+A-T$ is

line r: $$Y_r:=(Y+A-T)/\kappa=2A/\kappa-(\overline{Y}+A-T)/\kappa\,;$$

here we have used the fact that $(Y+P_r)/\kappa$ is reduced to deduce that necessarily $P_r=P_{r+1}=A-T$.

By conjugation of the $(r+1)$-line tableau commencing with (31) we see that

line 2r: $$Y_{2r}:=Y+A-T=2A-T-(\overline{Y}+A-T)\,,$$

so that in any case if $Y+A-T$ has a quasi-periodic continued fraction expansion then it is periodic of period twice the quasi-period. This result of Tom Berry [2]

** The case of period length 1 is an exception, but, if $r=1$, also 2 and 3 are period lengths.

applies to arbitrary quadratic irrationals with polynomial trace. Other elements $(Y+P)/Q$ of $\mathbb{F}(X,Y)$, with Q dividing the norm $(Y+P)(\overline{Y}+P)$, may be honest-to-goodness quasi-periodic, that is, not also periodic.

Further, if $\kappa \neq -1$ then r *must* be odd. To see that, notice the identity

$$B[\,Ca_0\,,Ba_1\,,Ca_2\,,Ba_3\,,\dots] = C[\,Ba_0\,,Ca_1\,,Ba_2\,,Ca_3\,,\dots], \tag{32}$$

reminding one how to multiply a continued fraction expansion by some quantity; this cute formulation of the multiplication rule is due to Wolfgang Schmidt [10]. The 'twisted symmetry' occasioned by division by κ, equivalent to the existence of a non-trivial quasi-period, is noted by Christian Friesen [4].

In summary, if the continued fraction expansion of Y is quasi-periodic it is periodic, and the expansion has the symmetries of the more familiar number field case, as well as twisted symmetries occasioned by a nontrivial κ.

One shows readily that if $x/y = [\,A\,,a_1\,,\dots,a_{r-1}\,]$ and $x - Yy$ is a unit of the domain $\mathbb{F}[X,Y]$ then, with $a_{r-1} = \kappa a_1$, $a_{r-2} = a_2/\kappa$, $a_{r-3} = \kappa a_3$, $\dots$,

$$[\,\overline{2A-T\,,a_1\,,\dots,a_{r-1}\,,(2A-T)/\kappa\,,a_{r-1}\,,\dots,a_1}\,]$$

is the quadratic irrational Laurent series $Y + A - T$. Alternatively, given the expansion of $Y + A - T$, and noting that therefore $\deg Q_r = 0$, the fact that the said expansion of x/y yields a unit follows directly from (29).

5. Comments

5.1. According to Gauss (*Disquisitiones Arithmeticæ*, Art. 76) ... *veritates ex notionibus potius quam ex hauriri debebant*††. Nonetheless, one should not underrate the importance of notation; good notation can decrease the viscosity of the flow to truth. From the foregoing it seems clear that, given $Y^2 = A^2 + 4v(X-w)$, one should study the continued fraction expansion of $Z = \frac{1}{2}(Y+A)$, as is done in [1]. Moreover, it is a mistake to be frustrated by minimal models $V^2 + UV - vV = U^3 - fU + vwU$.

Specifically, we understand that $V^2 - 8vV = U^3 - (4f-1)U^2 + 8v(2w-1)U$ yields $Y^2 = (X^2+4f-1)^2 + 4\cdot 8v\bigl(X-(2w-1)\bigr)$ by way of $2U = X^2 + Y + (4f-1)$ and $(V-8v) = XU$. Now $X \leftarrow 2X+1$, $Y \leftarrow 4Y$ means that, instead, we obtain $Y^2 = (X^2 + +X + f)^2 + 4v\bigl(X-(w-1)\bigr)$. This derives from $V^2 + UV - vV = U^3 - fU + vwU$ by taking $2U = X^2 + X + Y + f$ and $V - v = XU$.

5.2. Although my discussion may have some interest for its own sake, its primary purpose is to test ideas for generalisation to higher genus g. An important difficulty when $g > 1$ is that partial quotients may be of degree greater than one without that entailing periodicity, whence my somewhat eccentric aside at page 74.

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, 'On periodicity of continued fractions in hyperelliptic function fields', *Arch. Math.* **55** (1990), 259–266.

[3] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs 104, American Mathematical Society 2003, 318pp.

[4] Christian Friesen, 'Continued fraction characterization and generic ideals' in [6], 465–474.

†† [mathematical] truths flow from notions rather than from notations.

[5] David Gale 'The strange and surprising saga of the Somos sequences', *Mathematical Intelligencer* **13**.1 (1991), 40–42; and 'Somos sequence update', *ibid.* **13**.4 (1991), 49–50. For more see Jim Propp, 'The Somos Sequence Site', `http://www.math.wisc.edu/~propp/somos.html`.

[6] David Goss, David R. Hayes and Michael I. Rosen eds., *The Arithmetic of Function Fields*, Proceedings of the workshop held at The Ohio State University, Columbus, Ohio, June 17–26, 1991. Ohio State University Mathematical Research Institute Publications, **2**. Walter de Gruyter & Co., Berlin, 1992. viii + 482 pp.

[7] B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186.

[8] Alfred J. van der Poorten, 'On torsion on elliptic curves and periodic continued fractions', in Alf van der Poorten and Andreas Stein eds., *High Primes and Misdemeanours; lectures in honour of the 60th birthday of Hugh Cowie Williams*, 13pp

[9] Alfred J. van der Poorten and Xuan Chuong Tran, 'Quasi-elliptic integrals and periodic continued fractions', *Monatshefte Math.*, 131 (2000), 155-169.

[10] Wolfgang M, Schmidt, 'On continued fractions and diophantine approximation in power series fields', *Acta Arith.* **95** (2000), 139–166.

[11] Rachel Shipsey, *Elliptic divisibility sequences*, Phd Thesis, Goldsmiths College, University of London, 2000 (see `http://homepages.gold.ac.uk/rachel/`).

[12] Rachel Shipsey, talk at 'The Mathematics of Public Key Cryptography', Toronto 1999; see `http://homepages.gold.ac.uk/rachel/toronto/sld006.htm`.

[13] David Speyer, E-mail concluding `http://www.math.wisc.edu/~propp/somos/elliptic`.

[14] Christine Swart, PhD Thesis, Royal Holloway, 2003.

[15] Morgan Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.* **70** (1948), 31–74.

[16] Don Zagier, 'Problems posed at the St Andrews Colloquium, 1996', Solutions, 5th day; see `http://www-groups.dcs.st-and.ac.uk/~john/Zagier/Problems.html`.

Centre for Number Theory Research, 1 Bimbil Place, Killara, Sydney, NSW 2071, Australia

E-mail address: `alf@math.mq.edu.au (Alf van der Poorten)`