

Quadratic irrational integers with partly prescribed continued fraction expansion

By ALFRED J. VAN DER POORTEN (Sydney)

To the memory of Professor Dr. Béla Brindza

Abstract. We generalise remarks of Euler and of Perron by explaining how to detail all quadratic integers for which the symmetric part of their continued fraction expansion commences with prescribed partial quotients.

I last saw Béla Brindza, my once postdoctoral student, in April, 2002. I was working on the paper below and attempted to enthuse him with its results, particularly those concerning periodic expansions in function fields of characteristic zero.

1. Periodic continued fractions

Suppose ω satisfies $\omega^2 - t\omega + n = 0$ and is an integer. That is, its trace $t = \omega + \bar{\omega}$ and norm $n = \omega\bar{\omega}$ both are rational integers. Then it is well known that the continued fraction expansion of ω is periodic and is of the

Mathematics Subject Classification: 11J70, 11A65, 11J68.

Key words and phrases: periodic continued fraction, function field.

This paper was commenced while the author enjoyed the hospitality and support of the Erwin Schrödinger Institute, Vienna and substantially augmented during an immediately subsequent visit to the Kossuth Lajos University, Debrecen.

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

shape

$$\omega = [a_0, \overline{a_1, \dots, a_{r-1}, 2a_0 - (\omega + \overline{\omega})}], \tag{1}$$

where the word a_1, \dots, a_{r-1} is a palindrome.

Example 1. We have $\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}]$. Just so, $(1 + \sqrt{61})/2$, an integer of trace 1, has expansion $[4, \overline{2, 2, 7}]$.

Although the question was already asked and is partially answered by Euler, see the very interesting translation [3], and is discussed by PERRON [9], it is noticeably less well known that given an arbitrary palindrome a_1, \dots, a_{r-1} in positive integers there are infinitely many positive integers $A = a_0$ so that (1) displays the expansion of a quadratic integer.

We explain that argument and rather more. Indeed, noting that for every h we have the expansion $\omega = [A, a_1, \dots, a_h, (\omega + P_{h+1})/Q_{h+1}]$ with integers $P = P_{h+1}$, and $Q = Q_{h+1}$ (that is, the complete quotients ω_{h+1} of ω all are of the indicated shape), we find all quadratic integers ω for which the symmetric part of its continued fraction expansion commences with the integers a_1, \dots, a_h . Specifically, we find the constraints on A , P , and Q so that ω is indeed integral with trace t and norm n .

Our remarks are of particular interest in the function field case, where such translations as ‘positive integer’ = ‘polynomial of degree at least one’, ‘integer part’ = ‘polynomial part’, and ‘integer’ = ‘polynomial’ are to be applied. There, however, the results in the the characteristic two case demand a distinct summary.

2. Continued fractions

Anyone attempting to compute the truncations $[a_0, a_1, \dots, a_h] = x_h/y_h$ of a continued fraction will be delighted to notice that the definition

$$[a_0, a_1, \dots, a_h] = a_0 + 1/[a_1, \dots, a_h]$$

immediately implies by induction on h that there is a correspondence

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \iff [a_0, a_1, \dots, a_h] = x_h/y_h$$

between products of certain two by two matrices and the convergents of fractions.

If $\alpha = [a_0, a_1, a_2, \dots]$ then the sequence (α_h) of complete quotients of α is defined by $\alpha = [a_0, a_1, \dots, a_h, \alpha_{h+1}]$. It follows from the correspondence that

$$\begin{aligned} \alpha &\longleftrightarrow \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{h+1} & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \begin{pmatrix} \alpha_{h+1} & 1 \\ 1 & 0 \end{pmatrix} \longleftrightarrow \frac{x_h \alpha_{h+1} + x_{h-1}}{y_h \alpha_{h+1} + y_{h-1}}. \end{aligned}$$

That is, we have

$$\alpha = \frac{x_h \alpha_{h+1} + x_{h-1}}{y_h \alpha_{h+1} + y_{h-1}}, \quad \text{and so} \quad \alpha_{h+1} = -\frac{y_{h-1} \alpha - x_{h-1}}{y_h \alpha - x_h}.$$

Recalling that $x_{-1} = 1$, $y_{-1} = 0$ because an empty matrix product is the identity matrix, we obtain

$$(-1)^{h+1} \alpha_1 \alpha_2 \cdots \alpha_{h+1} = (y_h \alpha - x_h)^{-1}. \quad (2)$$

Example 2. Indeed, set $\delta = \sqrt{61}$ and let $\bar{\delta}$ denote its conjugate, $-\sqrt{61}$. The continued fraction expansion of δ commences

$$\begin{aligned} \delta &= 7 - (\bar{\delta} + 7)/1 \\ \delta_1 &= (\delta + 7)/12 = 1 - (\bar{\delta} + 5)/12 \\ \delta_2 &= (\delta + 5)/3 = 4 - (\bar{\delta} + 7)/3 \\ \delta_3 &= (\delta + 7)/4 = 3 - (\bar{\delta} + 5)/4. \end{aligned}$$

Note, in part to set notation, that a typical line in this tableau is

$$\delta_h = (\delta + P_h)/Q_h = a_h - (\bar{\delta} + P_{h+1})/Q_h, \quad (3)$$

where

$$\begin{aligned} P_h + P_{h+1} + (\delta + \bar{\delta}) &= a_h Q_h && \text{and} \\ -Q_h Q_{h+1} &= \delta \bar{\delta} + (\delta + \bar{\delta}) P_h + P_h^2. \end{aligned} \quad (4)$$

Thus, by (2) and (4),

$$\begin{aligned} x_h^2 - 61y_h^2 &= \text{Norm}(x_h - \delta y_h) \\ &= \text{Norm}(\delta_1 \delta_2 \cdots \delta_{h+1}) = (-1)^{h+1} Q_{h+1}. \end{aligned} \tag{5}$$

One can, by (3) and (4), readily confirm that the continued fraction expansion of δ is eventually periodic. Indeed, by induction one notices that both

$$0 < 2P_{h+1} + (\delta + \bar{\delta}) < \delta - \bar{\delta} \quad \text{and} \quad 0 < Q_h < \delta - \bar{\delta}. \tag{6}$$

Thus the box principle guarantees periodicity.

Moreover, conjugation is an involution on the tableau (this is why I denote the remainders in the manner I do), turning the tableau upside down. At the cost of replacing δ_0 by $\delta + 7$ at line $h = 0$ and continuing the expansion to see the additional symmetry at lines $h = 5$ and 6 (see Example 3) we could both again have proved periodicity and have confirmed that the preperiod is just the line $h = 0$.

Suppose, more generally, that $\omega^2 - t\omega + n = 0$ and that ω is the larger real zero. Then our remarks apply without essential change to ω in place of $\sqrt{61}$. In the function field case, with ω replaced by $Y(X)$ and $\deg_X Y = g + 1$, the cited inequalities (6) become $\deg Q_h \leq g$ and $\deg P_{h+1} = g + 1$. Now, however, the box principle does not apply (unless the base field is finite) and periodicity is at best happenstance. Nonetheless, if periodicity happens to happen then the period will indeed commence no later than at line 1.

The issue of periodicity is encapsulated by the following remark which emphasises that periodicity coincides with the existence of units.

Proposition 1. *Suppose that x and y are positive integers satisfying $x^2 - txy + ny^2 = \pm 1$. Then the decomposition*

$$N = \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_r & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in positive integers b_0, b_1, \dots, b_r entails that

$$\omega = [\overline{b_0, b_1, \dots, b_{r-1}, b_r, 0}] = [\overline{b_0, \bar{b}_1, \dots, b_{r-1}, b_r + b_0}]$$

for some ω satisfying $\omega^2 - t\omega + n = 0$.

PROOF. Consider the periodic continued fraction

$$[\overline{b_0, b_1, \dots, b_r, 0}] = \gamma, \quad \text{say.}$$

Thus $\gamma = [b_0, b_1, \dots, b_r, 0, \gamma]$. By the matrix correspondence we have

$$\gamma \longleftrightarrow N \begin{pmatrix} \gamma & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x\gamma - ny & x \\ y\gamma + x - ty & y \end{pmatrix} \quad \text{so} \quad \gamma = \frac{x\gamma - ny}{y\gamma + x - ty}.$$

But this is $y(\gamma^2 - t\gamma + n) = 0$. Hence $y \neq 0$ confirms our claim. \square

Note here that $x/y = [b_0, b_1, \dots, b_{r-1}]$ provides the unit $x - \omega y$. Moreover, the symmetry of the matrix

$$N \begin{pmatrix} t & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -ny + tx & x \\ x & y \end{pmatrix}$$

confirms that the word $[b_0, b_1, \dots, b_{r-1}, b_r + t]$ is a palindrome, again explaining the symmetry under conjugation to which we alluded above.

Example 3. The expansion of $\delta = \sqrt{61}$ continues with the lines

$$\delta_4 = (\delta + 5)/9 = 1 - (\bar{\delta} + 4)/9$$

$$\delta_5 = (\delta + 4)/5 = 2 - (\bar{\delta} + 6)/5$$

$$\delta_6 = (\delta + 6)/5 = 2 - (\bar{\delta} + 4)/5$$

with $Q_5 = Q_6$ signalling the symmetry. Notice that in this case the period length $r = 11$ is odd (equivalently, the fundamental unit of $\mathbb{Z}[\sqrt{61}]$ has norm -1).

For a case $r = 2s$, even, the symmetry is given by the line

$$\omega_s = (\omega + P_s)/Q_s = a_s - (\bar{\omega} + P_s)/Q_s,$$

that is, by $P_{s+1} = P_s$. We have $Q_s \mid (2P_s + t)$. In this ‘ambiguous’ case, that is equivalent to Q_s also dividing the discriminant $t^2 - 4n$ of the quadratic order $\mathbb{Z}[\omega]$.

**3. Quadratic integers
with partly prescribed expansion**

Theorem 2. *Suppose that $\omega^2 - t\omega + n = 0$ and its continued fraction expansion is*

$$\omega = [A, a_1, a_2, \dots, a_h, (\omega + P_{h+1})/Q_{h+1}].$$

Set $P = P_{h+1}$, $Q = Q_{h+1}$, and

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p & p' \\ q & q' \end{pmatrix}.$$

Then both

$$p(P^2 + tP + n) + p'Q(A + P) = -q'Q,$$

$$p(A^2 - tA + n) + q(A + P) = -q'Q.$$

PROOF. The data is equivalent to

$$\begin{aligned} \begin{pmatrix} A & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} p & p' \\ q & q' \end{pmatrix} \begin{pmatrix} 1 & P \\ 0 & Q \end{pmatrix} &= \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix} \\ &= \begin{pmatrix} Ap + q & Ap' + q' \\ p & p' \end{pmatrix} \begin{pmatrix} 1 & P \\ 0 & Q \end{pmatrix} \\ &= \begin{pmatrix} Ap + q & P(Ap + q) + Q(Ap' + q') \\ p & Pp + Qp' \end{pmatrix}. \end{aligned}$$

Thus $x = Ap + q$ and $y = p$ and $Pp + Qp' = Ap + q - pt$. Hence

$$\begin{aligned} p(A - t - P) - p'Q &= -q \\ p(PA + n) + p'QA &= -qP - q'Q. \end{aligned} \tag{7}$$

Strategic additions of multiples of the first equation to the second provides the allegation. □

3.1. The classical result. Specifically, if $h = r - 1$ so that we are given the complete symmetric part of the period of ω , then $P = A - t$, $Q = 1$ and the identities become

$$Np - Tq = -q' \text{ with } N = \text{Norm}(\omega - A) \text{ and } T = \text{Trace}(\omega - A).$$

Because $pq' - p'q = (-1)^{r-1}$, we know immediately that the general solution for the integers N and T is

$$N = (-1)^r(q'^2 - Lq) \quad \text{and} \quad T = (-1)^r(p'q' - Lp), \quad (8)$$

where L is an arbitrary integer. The latter equation congenially reports that

$$2A = t - (-1)^r(p'q' - Lp).$$

Thus if p' and q' both are odd while Lp is even then t must be taken odd; say $t = 1$ as in $\omega = \frac{1}{2}(1 + \sqrt{D})$; here $D = T^2 - 4N$. In all other cases one may take $t = 0$ and obtain ω the square root \sqrt{D} of an integer, not a square; then $4D = T^2 - 4N$. In either case, of course, $D = D(L)$ is a polynomial quadratic in the integer parameter L . Distinguishing the cases brings difficulties, see for example [5].

In the function field case this parity matter is no issue, unless the characteristic is 2 where we see that then $t = p'q' + Lp$, with L an arbitrary polynomial, gives us all possible discriminants $t^2 - 4n = t^2$.

3.2. The general result. We recall that $pq' - p'q = (-1)^h$ and that $(P^2 + tP + n) = -Q_hQ := -Q'Q$. Thus we have the two general solutions

$$P^2 + tP + n = (-1)^{h+1}Q(q'^2 - K_1p') \quad - (A + P) = (-1)^{h+1}(qq' - K_1p),$$

$$A^2 - tA + n = (-1)^{h+1}(q'^2Q - K_2q) \quad - (A + P) = (-1)^{h+1}(p'q'Q - K_2p),$$

where K_1 and K_2 denote arbitrary integers. Set $kq' = K := K_2 - K_1$.

The dexter pair of equations is $Kp = q'(p'Q - q)$. Indeed q' does divide K and also $q + kp \equiv 0 \pmod{p'}$, showing that K is fixed modulo $p'q'$. In fact, because $pq' = (-1)^h + p'q$, we have $k \equiv (-1)^{h+1}qq' \pmod{p'}$. Thus, for integers L ,

$$(-1)^{h+1}k = qq' - Lp' \quad \text{and then} \quad (-1)^{h+1}Q = q^2 - Lp; \quad (9)$$

and $L = q'Q - kq$. Note that (9) in any case is immediate from (7) at page 486 above. Hence, at very first glance surprisingly, knowing Q_{h+1} as well as a_1, \dots, a_h restricts us to just one parameter families of solutions.

The sinister equations and those for $A + P$, very helpfully yield $k = A - t - P$, and therefore, with $T = \text{Trace}(\omega - A)$, $N = \text{Norm}(\omega - A)$,

$$T = (-1)^h(K_1p - Lp'), \quad N = (-1)^h(K_1q - Lq'). \quad (10)$$

Thus the discriminant $t^2 - 4n = T^2 - 4N$ is a quadratic expression in K_1 and L .

Note, however, that many choices of K_1 and L lead to inadmissible cases. For instance, we must have $t^2 - 4n$ a positive non-square; and Q positive obviously constrains L .

Additional data, such as a relationship on the quantities P , Q , and Q' , leads to just a family of polynomials quadratic in one variable as in the classical case; in that context see HALTER-KOCH and PACHER [4], which expands considerably on [10] and [6].

The special case $Q = Q'$ entails $(-1)^{h+1}Q = K_1p' - q'^2$. The special case $P = P' := P_h$ is $Q \mid (2P + t)$; note that $2P + t = (-1)^h(2qq' - Lp' - K_1p)$. Again in these cases, the families of discriminants are quadratic polynomials in the surviving parameter. Conversely, of course, the quadratic polynomials $D(L)$, say, have the property that the period length of $\sqrt{D(l)}$, l an integer for which $D(l)$ is positive and not a square, is constant for all but possibly several exceptional l . This case is discussed by SCHINZEL [14]; see also [13] and note the ‘sleepers’ of [8].

Example 4. Suppose we are given just $a_1 = 1$, $a_2 = 4$; that is: $p = 5$, $q = 4$, $p' = 1$, $q' = 1$. Thus

$$\begin{aligned} P^2 + tP + n &= Q(K_1 - 1) & A + P &= 4 - 5K_1, \\ A^2 - tA + n &= 4K_2 - Q & A + P &= Q - 5K_2. \end{aligned}$$

The equations on the right yield $Q - 4 = 5(K_2 - K_1)$. Subtracting the first equation on the left from the second gives $(A + P)(A - t - P) = 4K_2 - QK_1$. Substituting for Q this is $(K_2 - K_1)(4 - 5K_1)$, so indeed $A - t - P = K_2 - K_1$. Thus if $Q = 4$ then $A - t = P$ and $2A - t = 4 - 5K_1$. The smallest example then has $A - t = 7$ with $K_2 = -2$ and so $t^2 - 4n = 4 \cdot 61$.

Example 5. Given $a_1 = 1$, $a_2 = 4$, $a_3 = 3$, $a_4 = 1$, $a_5 = 2$, together with $Q_5 = Q_6$ – so that we are half way in a period of odd length, we have $p = 58$, $q = 47$, $p' = 21$, $q' = 17$. Thus

$$\begin{aligned} -Q' &= 289 - 21K_1 & A + P &= 58K_1 - 799, \\ A^2 - tA + n &= 289Q - 47K_2 & A + P &= 58K_2 - 357Q. \end{aligned}$$

On the right we see that $357Q - 799 \equiv 9Q - 45 \equiv 0 \pmod{58}$ and only the smallest example, that with $Q = 5$, is going to be at all small. Moreover, if $Q = 5$ then $K_2 - K_1 = q'K = 17$, so $k = 1$. Recalling that $Q' = Q$, the equation for $-Q'$ gives $K_1 = 14$, and so $K_2 = 31$. All that amounts to $A + P = 13$. As above, we also have $(A + P)(A - t - P)$, so $2P + t = 12$ and $2A - t = 14$. We see that $t^2 - 4n = 4 \cdot 61$.

This example is just of the right size reliably to check our formulas just above at the start of §3.2; we need only that the choice $Q = 5$ is $L = 38$, and then $Q = Q'$ is $K_1 = 14$.

Example 6. Given $a_1 = 2$ and $P = P_2 = P_3$, signalling halfway in a period of even length, we have $p = 2$, $q = 1$, $p' = 1$, $q' = 0$. Hence $K_2 = K_1$, and $(A + P)(A - t - P) = K_1(Q - 1)$. Since $A + P = 2K_1$ we see that $A - t - P = (Q - 1)/2$ and Q is odd. Thus the condition $Q \mid (2P + t)$ is $4K_1 \equiv -1 \pmod{Q}$. We obtain a family of possible discriminants controlled by one near arbitrary integer parameter and by $(2P + t)/Q$.

4. Function fields

We will apply Theorem 2 in function fields (with base field not of characteristic two) to determine polynomials of even degree whose square root has a periodic continued fraction expansion defined over the base field. We first look at quartic polynomials $D(X) = A^2 + 4v(X + w)$ and, as example, first consider the case

$$\sqrt{D} = [A, \overline{B, C, E, C, B, 2A}]$$

with B, C , and E of degree 1, and A of course of degree 2. Note here that the *regulator*, namely the degree of the unit, or, equivalently, the sum of the degrees of the partial quotients comprising the period, is $m = 7$.

In order to apply the classical result we must first compute

$$\begin{aligned} & \begin{pmatrix} B & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} C & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} E & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} C & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} B & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} BCECB + ECB + 2BCB + BCE + 2B + E & BCEC + EC + 2BC + 1 \\ CECEB + 2CB + CE + 1 & CEC + 2C \end{pmatrix}. \end{aligned}$$

Next we write say $B = b(X + \beta)$, $C = c(X + \gamma)$, and $E = e(X + \varepsilon)$, allowing us explicitly to detail the polynomials p , $q = p'$, and q' appearing in the proof of Theorem 2. In particular, we notice that $\deg p = 5$, $\deg q = 4$, and $\deg q' = 3$. We then endeavour to find A .

Indeed, by Theorem 2 we know that $2A = Kp - qq'$ (noting that here $t = 0$ and $h = 5$); in principle K denotes an arbitrary polynomial.

However, we require $\deg D = 4$ and, therefore, $\deg A = 2$. Because $\deg qq' = 7$ and $\deg p = 5$ it follows that K must be of degree 2. Thus we detail $Kp - qq'$, say with $K = kX^2 + k'X + k''$, and set the leading coefficients of $2A$, those of X^7 , X^6 , \dots , and X^3 , equal to zero.

Note that there are a total of 9 unknowns $k, \dots, b, \beta, \dots$, thus far controlled by the 5 conditions ensuring that A is of degree just 2.

But we can tame $D(X)$, and hence $A(X)$, considerably further. First, it loses no generality to divide by the leading coefficient of D (this must be a square because A is defined over the base field) and, thus, to suppose D is monic. Second, we may translate X by a constant, thus fixing the coefficient of X^3 of D (and hence the coefficient of X of A), say to 0. That leaves two degrees of freedom. Third, we may dilate X , replacing it by a nonzero multiple, and then divide by the new leading coefficient; one finds that for quartics such a dilation reduces the number of free variables by one in all but the cases $m = 2$ and $m = 3$. From related work [12] it happens I know that a congenial dilation is that yielding $c = 2$.

All that reduces the degrees of freedom to just one. We therefore should find at most a one parameter family of possibilities for $A(X) = X^2 + u$, say, thus for D , and hence for each of the already mentioned ‘unknowns’.

4.1. The classical result in action. It would be neat to apply the classical result to the example but, frankly, the hard yakka¹ involved seems inappropriate here, so we’ll retreat to the case $m = 5$ and leave it to the reader to check that there $p = BCB + 2B$, $q = p' = CB + 1$, and $q' = B$, and that *mutatis mutandis* we will there too find a one parameter family of continued fractions; in the case $m = 5$ we will need $\deg K = 0$ and will set $K = k$.

¹yakka: work [Australian Aboriginal].

For $m = 5$, when we review the coefficients of $2A(X) = 2(X^2 + u) = Kp - qq'$ we find that

$$X^3 : kb^2c - bc^2 \text{ which vanishes, so } kb = c;$$

$$X^2 : kb^2c(2\beta + \gamma) - b^2c(\beta + 2\gamma) = bc^2(\beta - \gamma);$$

$$X : kb^2c(2\beta\gamma + \beta^2) + 2kb - bc^2(2\beta\gamma + \gamma^2) - c = bc^2(\beta - \gamma)(\beta + \gamma) + c;$$

$$1 : kb^2c\beta^2\gamma + 2kbb\beta - bc^2\beta\gamma^2 - c\gamma = bc^2(\beta - \gamma)\beta\gamma + c(2\beta - \gamma).$$

Just so, it will be convenient to check the consistency of our solution by noting that the coefficients of $Kq - q'^2 = D - A^2 = R$, say, are given by

$$X^2 : kbc - c^2 \text{ which must vanish, so } kb = c;$$

$$X : kbc(\beta + \gamma) - 2c^2\gamma = c^2(\beta - \gamma);$$

$$1 : kbc\beta\gamma + k - c^2\gamma^2 = c^2(\beta - \gamma)\gamma + k.$$

Our normalisation $A = X^2 + u$ gives $bc^2(\beta - \gamma) = 2$, and then $2(\beta + \gamma) + c = 0$. Dilating X by the ratio $-(\beta + \gamma)$ is equivalent to taking $\beta + \gamma = -1$. If, further, we choose to write $\beta - \gamma = s$, then $\beta = (s - 1)/2$, $\gamma = -(s + 1)/2$, and we obtain $2u = (1 - s^2)/2 + (3s - 1)$, or $u = -(s^2 - 6s + 1)/4$. Because $bc^2(\beta - \gamma) = 4bs = 2$ we have $b = 1/2s$, $c = 2$, and $k = 4s$.

Further, we find that $R(X) = 4sX - 2s(s + 1) + 4s = 4sX - 2s(s - 1)$. Thus

$$Y^2 = D(X) = \left(X^2 - \frac{1}{4}(s^2 - 6s + 1) \right)^2 + 4s \left(X - \frac{1}{2}(s - 1) \right) \quad (11)$$

is the family of monic quartic polynomials defined over $\mathbb{K} = \mathbb{Q}(s)$ and with zero trace so that the function field $\mathbb{K}(X, Y)$ has a unit of regulator 5.

One should promptly check such an allegation. Indeed, we find that

$$Y = \left[X^2 - \frac{1}{4}(s^2 - 6s + 1), \overline{\left(X + \frac{1}{2}(s - 1) \right)} / 2s \right. \\ \left. \overline{2 \left(X - \frac{1}{2}(s + 1) \right), \left(X + \frac{1}{2}(s - 1) \right) / 2s, 2 \left(X^2 - \frac{1}{4}(s^2 - 6s + 1) \right)} \right].$$

This computation provides the reminder that, of course, $s = 0$ is not admissible because, if $s = 0$, then D is a square.

4.2. The generalised result in action. Notwithstanding this success of the classical result, the case $m = 7$ already seems too painful for any other than a willing and energetic student. Our generalisation should however at least halve the pain and, it is to be hoped, more than double the willingness.

Recall we suppose $Y^2 = D(X) = (X^2 + u)^2 + 4v(X + w) = A^2 + R$. In applying the new result we first compute just

$$\begin{pmatrix} B & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} C & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} BC+1 & B \\ C & 1 \end{pmatrix} = \begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$$

so $p = BC + 1$, $p' = B$, $q = C$, $q' = 1$ and note that $Q \mid (2P + t)$. Checking degrees in the equations at §3.2 we see the K_i are constants k_i , and as remarked, we obtain $A - t - P = k_2 - k_1 = k$, say, $(BC + 1)k = (BQ - C)$, $A + P = C - k_1(BC + 1)$.

Comparing coefficients in that last equation yields

$$X^2 : 2 = -k_1bc$$

$$X : 0 = c - k_1bc(\beta + \gamma) = c + 2(\beta + \gamma),$$

the latter by normalisation whereby A , and so also P , has zero trace. By dilation we may choose $c = 2$ obtaining $k_1b = -1$ and $\beta + \gamma = -1$.

We note that E is the integer part of $(Y + P)/Q$. Hence, because $D(X)$ is monic and has zero trace, necessarily $Q = 2(X - \varepsilon)/e$. Thus $(BC + 1)k = (BQ - C)$ alleges that

$$X^2 : kbc = 2b/e, \quad \text{so } 2 = kce;$$

$$X : kbc(\beta + \gamma) = 2b(\beta - \varepsilon)/e - c \quad \text{or } kb(\gamma + \varepsilon) = -1;$$

$$1 : kbc\beta\gamma + k = -2b\beta\varepsilon/e - c\gamma \quad \text{or } kbc\beta(\gamma + \varepsilon) = -k - c\gamma = -c\beta,$$

$$\text{and so } c(\beta - \gamma) = k.$$

The equation $-Q' = (-1)^{h+1}(q'^2 - K_1p')$ contains no new information other than for the reminder that in fact $C = c(X + \gamma)$ entails $Q' = 2(X - \gamma)/c$. Just so the equation for $A^2 - tA + n$ simply gives $-R$.

However, $Q = 2(X - \varepsilon)/e$ divides $2P + t = -k + C - k_1BC - k_1$ says that $-k + c(X + \gamma) - k_1bc(X^2 + (\beta + \gamma)X + \beta\gamma) - k_1$ has ε as a zero. That is

$$-k_1bc\varepsilon^2 = k - c\gamma + k_1bc\beta\gamma + k_1 \quad \text{so} \quad 2\varepsilon^2 = k - (2\gamma + 2\beta\gamma - k_1).$$

Subtracting $2\gamma^2$ from each side of this equation we get

$$2(\varepsilon^2 - \gamma^2) = 2(\varepsilon - \gamma)(\varepsilon + \gamma) = k - 2\gamma - 2\gamma(\beta + \gamma) + k_1 = k + k_1.$$

Set $\varepsilon + \gamma = -s$. Notice that $kbs = 1$ and $k_1b = -1$ gives $k_1 = -ks$. We have

$$\begin{array}{ll} \beta + \gamma = -1 & \text{or} \quad 2(\beta + \gamma)s = -2s \\ \varepsilon + \gamma = -s & 2(\varepsilon + \gamma)s = -2s^2 \\ 2(\beta - \gamma) = k & 2(\beta - \gamma)s = ks \\ 2(\varepsilon - \gamma)s = k(s - 1) & 2(\varepsilon - \gamma)s = k(s - 1). \end{array}$$

It is now straightforward to solve the various equations and to obtain

$$\begin{aligned} B &= \left(X + \frac{1}{2}(s^2 - s - 1) \right) / 2s^2(s - 1) & C &= 2 \left(X - \frac{1}{2}(s^2 - s + 1) \right) \\ E &= \left(X + \frac{1}{2}(s^2 - 3s + 1) \right) / 2s(s - 1), \end{aligned}$$

as well as $k = 2s(s - 1)$. As remarked, we obtain A from $2A - t = k + C - k_1BC - k_1$ and $v(X + w)$ as $Q - (k + k_1)C$. Thus $Y^2 = (X^2 + u)^2 + 4v(X + w) = A^2 + R$ with

$$\begin{aligned} A &= X^2 - \frac{1}{4}(s^4 - 6s^3 + 3s^2 + 2s + 1) & \text{and} \\ R &= 4s^2(s - 1) \left(X - \frac{1}{2}(s^2 - s - 1) \right). \end{aligned}$$

On our checking, a direct computation of the continued fraction expansion of Y so given indeed yields the partial quotients predicted at (12) above.

5. Comments

5.1. Schinzel's theorem. ANDRZEJ SCHINZEL [14] shows that if a polynomial $D(X)$ taking integer values at integers l has the property that the length of the period of the continued fraction expansion of $\sqrt{D(l)}$ is bounded as $l \rightarrow \infty$ then (a) the function field $\mathbb{Q}(X, Y)$ – where $Y = \sqrt{D(X)}$ – contains non-trivial units; equivalently, the function field continued fraction expansion of Y is periodic, and (b) some nontrivial units $a(X) + b(X)Y$ in $\mathbb{Q}(X, Y)$ have both a and b in $\mathbb{Z}[X]$. If $\deg D = 2$, say $D(X) = A^2X^2 + BX + C$, then the function field condition (a) is trivial, but the arithmetic condition (b) entails that the discriminant $(B^2 - 4A^2C)$ divides $4(2A^2, B)^2$.

Section 4 provides examples of classes of polynomials of degree 4 satisfying the function field condition (a). ROGER PATTERSON, see [7], has carried through the interesting exercise of finding which values of the parameters lead to (b) also being satisfied; see also comments in [8].

5.2. Explicit continued fraction expansion. I have learned how to expand explicitly the general quartic (and sextic) polynomial, that is, I found nontrivial recursion relations on the complete quotients; see [11]. In principle, at any rate, those techniques generalise to higher genus cases. Thus, fortunately perhaps, the ideas of §4 are mostly an amusing diversion rather than a necessary method.

5.3. Short periods and long periods. In principle one is interested in relatively long periods, in the hope of obtaining insight into Gauss's conjecture to the effect that the majority of real quadratic number fields with prime discriminant have class number one. In that context, short periods, as discussed here only give one a view of the enemy. Nonetheless, as wonderfully exemplified by recent work of ANDRÁS BIRÓ, [1], [2], the short case raises fascinating issues. The polynomials $X^2 + 4$ and $4X^2 + 1$ satisfy Schinzel's conditions so we can write the corresponding numerical periods explicitly. That gives, as Biró ingeniously shows, sufficient handle on the matter after all to determine all cases $X = l$ that yield class number one. But, for example, the corresponding class number two problems appear yet less accessible because as l varies one seems not to have a bound on

the period length of expansions of reduced elements not from the principal class.

It is not so much the length of the period as the size of the regulator (the logarithm of the absolute value of the fundamental unit) that matters. Discriminants D belonging to families alluded to in this paper have regulator $O(\log D)$ only. In fact, see [7, 8], it seems that if one has a formula for the units of a parametrised family then the regulators are never more than $O((\log D)^2)$.

References

- [1] ANDRÁS BIRÓ, Yokoi's conjecture, *Acta Arith.* **106.1** (2003), 85–104.
- [2] ANDRÁS BIRÓ, Chowla's conjecture, *Acta Arith.* **107.2** (2003), 179–194.
- [3] LEONHARD EULER, An essay on continued fractions, (translated by Myra F. Wyman and Botswick F. Wyman), *Math. Systems Theory* **18** (1985), 295–328; see also: Christopher Byrnes, 'Editor's introduction', *ibid.* 293–294.
- [4] FRANZ HALTER-KOCH and MAXIMILIAN PACHER, The diophantine equation $x^2 - Dy^2 = N$ and continued fractions, *JP J. Algebra Number Theory Appl.* **3.1** (2003), 85–120.
- [5] JAMES MC LAUGHLIN, Multivariable polynomial solutions to Pell's equation in real quadratic number fields, *Pacific J. Math.* **210.2** (2003), 335–349.
- [6] R. A. MOLLIN, A. J. VAN DER POORTEN and H. C. WILLIAMS, Halfway to a solution of $X^2 - DY^2 = -3$, *J. Théorie de Nombres de Bordeaux* **6** (1994), 421–459.
- [7] ROGER PATTERSON, Creepers: Real quadratic fields with large class number, PhD thesis, *Macquarie University, Sydney*, 2004.
- [8] ROGER D. PATTERSON and ALFRED J. VAN DER POORTEN, Jeepers, Creepers, . . . , in *High Primes and Misdemeanours: Lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Institute Communications **42**, (Alf van der Poorten and Andreas Stein, eds.), *American Mathematical Society*, 2004, 305–316.
- [9] OSKAR PERRON, Die Lehre von den Kettenbrüchen, 2nd edn, *Chelsea Publishing Company, New York, NY*, 1929.
- [10] ALFRED J. VAN DER POORTEN, Explicit quadratic reciprocity, in: *Number Theoretic and Algebraic Methods in Computer Science, Moscow 1993*, (Alf van der Poorten, Igor Shparlinski and Horst G. Zimmer, eds.), *World Scientific*, 1995, 175–180.
- [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*, Fields Institute Communications **42**, (Alf van der Poorten and Andreas Stein, eds.), *American Mathematical Society*, 2004, 353–365; see also 'Elliptic curves and continued fractions', <http://www.arxiv.org/math.NT/0403225>, 11 pages.

- [12] ALFRED J. VAN DER POORTEN and XUAN CHUONG TRAN, Periodic continued fractions in elliptic function fields, Algorithmic Number Theory (Proc. Fifth International Symposium, ANTS-V, Sydney, NSW, Australia July 2002), (Claus Fieker and David R. Kohel, eds.), *Springer Lecture Notes in Computer Science 2369*, 2002, 390–404.
- [13] A. J. VAN DER POORTEN and H. C. WILLIAMS, On certain continued fraction expansions of fixed period length, *Acta Arith.* **89.1** (1999), 23–35.
- [14] A. SCHINZEL, On some problems of the arithmetical theory of continued fractions, *Acta Arith.* **6** (1961), 393–413, *ibid.* **7** (1962), 287–298.

ALFRED J. VAN DER POORTEN
CENTRE FOR NUMBER THEORY RESEARCH
1 BIBIL PLACE, SYDNEY, NSW 2071
AUSTRALIA

E-mail: alf@math.mq.edu.au

(Received May 30, 2004)