ALF'S PREPRINTS
Paper 146, Typeset December 21, 1999, Pages 69–77
Centre for Number Theory Research, Macquarie University, Sydney

ON PERIODS OF ELEMENTS FROM REAL QUADRATIC NUMBER FIELDS

ceNTRe
Macquarie University
Sydney, Australia 2109

EDWARD B. BURGER AND ALFRED J. VAN DER POORTEN

To Jonathan Borwein, on the occasion of his award of a Dhc

Preliminaries

Anyone meeting a continued fraction expansion

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{a_5 + \ddots}}}}}$$

will see that a less wasteful notation, say $[\,a_0\,,\,a_1\,,\,a_2\,,\ldots]$, is needed to represent it. Anyone attempting to compute the truncations $[\,a_0\,,\,a_1\,,\ldots,\,a_h\,] = p_h/q_h$ will be delighted to notice that the definition $[\,a_0\,,\,a_1\,,\ldots,\,a_h\,] = a_0 + 1/[\,a_1\,,\ldots,\,a_h\,]$ immediately implies by induction on h that there is a correspondence

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_h & p_{h-1} \\ q_h & q_{h-1} \end{pmatrix} \longleftrightarrow [\,a_0\,,\,a_1\,,\ldots,\,a_h\,] = p_h/q_h$$

between products of certain two by two matrices and continued fractions.

1. Introduction

Different explanations of a phenomenon often provide new insights and greater understanding. Thus our purpose here is to re-explore the phenomena reported and proved in [1].

Consider the two purely periodic continued fraction expansions

$$\alpha = [\,\overline{1\,,\,14\,,\,1\,,\,4\,,\,1\,,\,3\,,\,12\,,\,3\,,\,1\,,\,4}\,] \text{ and } \beta = [\,\overline{1\,,\,1\,,\,4\,,\,2\,,\,55\,,\,2\,,\,4\,,\,1\,,\,1\,,\,2\,,\,2}\,].$$

There's nothing immediately hitting the eye that suggests that the two expansions represent quadratic irrationals in the same quadratic number field. So if such a thing is claimed, there's then nothing for it but to do some computation, at least

Typeset December 21, 1999 [12:27].
1991 *Mathematics Subject Classification.* Primary 11J70, 11A65, 11J68.
Key words and phrases. unit, periodic continued fractions.
The first author was a Visiting Fellow at Macquarie University during the writing of this paper and wishes to thank the members of the ceNTRe for their warm hospitality. The second author was supported in part by a grant from the Australian Research Council.

to the extent of evaluating the two expansions for an entire period. The respective tableaux

h		0	1	2	3	4	5	6	7	8	9
$a_{\alpha,h}$		1	14	1	4	1	3	12	3	1	4
$p_{\alpha,h}$	0	1	1	15	16	79	95	364	4463	13753	18216	86617
$q_{\alpha,h}$	1	0	1	14	15	74	89	341	4181	12884	17065	81144

and

h		0	1	2	3	4	5	6	7	8	9	10
$b_{\beta,h}$		1	1	4	2	55	2	4	1	1	2	2
$p_{\beta,h}$	0	1	1	2	9	20	1109	2238	10061	12299	22360	57019	136398
$q_{\beta,h}$	1	0	1	1	5	11	610	1231	5534	6765	12299	31363	75025

then invite us to study the matrices

$$M_\alpha = \begin{pmatrix} 86617 & 18216 \\ 81144 & 17065 \end{pmatrix} \quad \text{and} \quad M_\beta = \begin{pmatrix} 136398 & 57019 \\ 75025 & 31363 \end{pmatrix}.$$

The rule of the game now is that each matrix

$$M = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$$

is of a special shape; namely

$$M_\gamma = \begin{pmatrix} x & -Ny \\ y & x - Ty \end{pmatrix},$$

where $T = T_\gamma$ is the trace $\gamma + \overline{\gamma}$, and where $N = N_\gamma$ is the norm $\gamma\overline{\gamma}$, of the element γ whose period has produced M.

Specifically, $86617 - 17065 = (\alpha + \overline{\alpha}) \cdot 81144$ and $18216 = -\alpha\overline{\alpha} \cdot 81144$. Plainly, we can now compute the trace T_α, and norm N_α, of α. If we recall that a real quadratic irrational has a purely periodic continued fraction expansion if and only if it is greater than 1 and its conjugate lies between -1 and 0, then we know we need the positive zero of the defining polynomial. Pressing buttons on our calculator yields $\alpha = 1.067447993571368484\ldots$; and we're little the wiser. Moreover, since our real object is to decide whether α and β belong to the same quadratic number field it might have demonstrated greater wisdom had we computed the discriminant Δ_α of α. It is $T_\alpha^2 - 4N_\alpha = 1.63265306122448979591836734 6\ldots$. Perhaps, we're still in trouble!

How about we also compute Δ_β. When we do that, we find that $T_\beta = 7/5$, $N_\beta = -19/25$, and $\Delta_\beta = 5$.

Recovering our senses, we now notice that

$$1.63265306122448979591836734 6\ldots = [\,1\,,\,1\,,\,1\,,\,1\,,\,2\,,\,1\,,\,1\,,\,2\,] = 80/49\,,$$

so that $\Delta_\alpha = (4^2/7^2) \cdot 5$, and plainly the quadratic number field containing both α and β is $\mathbb{Q}(\sqrt{5})$. In fact, backtracking a little, it's now clear that $\alpha = (3 + 2\sqrt{5})/7$ and $\beta = (7 + 5\sqrt{5})/10$. Checking the continued fractions of those numbers confirms that conclusion.

However, all this is not quite to the point. In [1] it is remarked, in effect, that the two matrices

$$M_\alpha^{25} = \begin{pmatrix} p_{\alpha,249} & -N_\alpha q_{\alpha,249} \\ q_{\alpha,249} & p_{\alpha,249} - T_\alpha q_{\alpha,249} \end{pmatrix} \quad \text{and} \quad M_\beta^{24} = \begin{pmatrix} p_{\beta,263} & -N_\beta q_{\beta,263} \\ q_{\beta,263} & p_{\beta,263} - T_\beta q_{\beta,263} \end{pmatrix}$$

have the same trace

$$246935852765152862276389138857893126556641451077000483026984 7 \backslash$$
$$8395289566538179507389432113883234418865101546019834683808080000 2\,.$$

Given, moreover, that the integers $250 = 25 \cdot 10$ and $264 = 24 \cdot 11$ have the same parity, it is then suggested that this pair of coincidences of itself entails that α and β belong to the same quadratic number field. Worse, it is then *proved* in [1] that such coincidence of trace and parity is necessary and sufficient for two given pure periodic elements to belong to the same quadratic number field.

All this is rather surprising, sufficiently so as to make one confident that the result must be entirely natural. Indeed, we will show it to be a manifestation of readily recalled properties of the group of units of the real quadratic number field.

2. What is going on

2.1. The core fact is

Theorem 1. *Suppose that* $[\,a_0\,,a_1\,,\ldots,a_{r-1}\,,a_r\,] = x/y$ *and that the previous convergent* $[\,a_0\,,a_1\,,\ldots,a_{r-1}\,]$ *is denoted by* x'/y'*. Then the claim*

$$[\,\overline{a_0\,,a_1\,,\ldots,a_r}\,] = \gamma\,, \quad \textit{where} \quad \gamma^2 - T\gamma + N = 0\,,$$

is equivalent to the allegation

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} = \begin{pmatrix} x & -Ny \\ y & x - Ty \end{pmatrix}.$$

Proof. Suppose $[\,\overline{a_0\,,a_1\,,\ldots,a_r}\,] = \alpha$, that is, $\alpha = [\,a_0\,,a_1\,,\ldots,a_r\,,\alpha\,]$. By the correspondence between continued fractions and two by two matrices we must have

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix}\begin{pmatrix} \alpha & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x\alpha + x' & x \\ y\alpha + y' & y \end{pmatrix} \longleftrightarrow \alpha.$$

That is, $(x\alpha + x')/(y\alpha + y') = \alpha$, or $y\alpha^2 - (x - y')\alpha - y' = 0$.

Thus if $x' = -Ny$ and $y' = x - Ty$ we have $y(\alpha^2 - T\alpha + N) = 0$, so $\alpha = \gamma$. Conversely, if $\alpha = \gamma$ *a priori*, then $(x - y')/y = T$ and $y'/y = -N$. ∎

Moreover, the kernel of this core is that the matrix $M = \left(\begin{smallmatrix} x & -Ny \\ y & x-Ty \end{smallmatrix}\right)$ must be unimodular , because

$$\begin{pmatrix} x & -Ny \\ y & x - Ty \end{pmatrix} = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix}$$

plainly has determinant $(-1)^{r+1}$.

Corollary. The element $x - \gamma y$ is a unit in the ring $\mathbb{Z}[\gamma]$.

Proof. The integer $x - \gamma y$ is an eigenvalue of the unimodular matrix M. ∎

2.2. Of course $\gamma = (A + B\sqrt{D})/C$ for some squarefree positive integer $D > 1$ and integers A, B and C, where $B \neq 0$ and, without loss of generality, $C > 0$. Thus γ is an element of the quadratic number field $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. It is usual then to abuse language by referring to $x - \gamma y$ as 'a unit of $\mathbb{K}$'.

Next, we should recall that if $D \equiv 1 \pmod 4$ then $\delta = \frac{1}{2}(1 + \sqrt{D})$ is an integer; if $D \not\equiv 1 \pmod 4$ we set $\delta = \sqrt{D}$. We will also write $n = \operatorname{Norm} D = \delta\overline{\delta}$ and

$t = \operatorname{Trace}\delta = \delta + \overline{\delta}$. Thus if $D \equiv 1 \pmod 4$ then $n = -\frac{1}{4}(D-1)$, $t = 1$, while if $D \not\equiv 1 \pmod 4$ we have $n = -D$, $t = 0$.

We come now to an important rule: One *must* write γ as $(P + f\delta)/Q$, where Q divides $\operatorname{Norm}(P + f\delta) = P^2 + ftP + f^2n$; here P, $f \neq 0$ and $Q > 0$ are integers, which we may suppose not to have any redundant common factor. It is a simple matter to transform $(A+B\sqrt{D})/C$ appropriately. Other than for a possible redundant common factor, $\gamma = (CA+CB\sqrt{D})/C^2$ will certainly do; the additional adjustment to change $\sqrt{D}$ to δ is straightforward.

Our insistence that Q divide $\operatorname{Norm}(P + f\delta)$ is more than just a convenient convention. One needs it to validate a correspondence between $\mathbb{Z}$-modules and ideals.

Remark 2. The $\mathbb{Z}$-module $\mathcal{I} = \langle Q, P + f\delta\rangle$ is an ideal of $\mathbb{Z}[f\delta]$.

Proof. It suffices to check that $f\delta(P + f\delta)$ is in $\mathcal{I}$. But

$$f\delta(P + f\delta) = -(P^2 + ftP + f^2n) + (P + ft)(P + f\delta),$$

and then $Q\big|(P^2 + ftP + f^2n)$ is essential to complete the verification. ∎

2.3. Plainly, we are obliged to think of the example elements $\alpha = (3+2\sqrt{5})/7$ and $\beta = (7+5\sqrt{5})/10$ as $\alpha = (7+28\varphi)/49$ and $\beta = (10+50\varphi)/50$, with $\varphi = (1+\sqrt{5})/2$. The corresponding eigenvalues of the respective matrices M_α and M_β are, as noted, $\eta_\alpha = x_\alpha - y_\alpha\alpha$ and $\eta_\beta = x_\beta - y_\beta\beta$. That is

$$\eta_\alpha = 86617 - 81144\alpha \quad \text{and} \quad \eta_\beta = 136398 - 75025\beta.$$

In better terms,

$$\eta_\alpha = 86617 - (11592 + 46368\varphi) \quad \text{and} \quad \eta_\beta = 136398 - (15005 + 75025\varphi).$$

We will find it useful to note that $46368 = 2^5 \cdot 3^2 \cdot 7 \cdot 23$, and $75025 = 5^2 \cdot 3001$.

2.4. Finally, we confirm that the quantities

$$\eta_\alpha = 75025 - 46368\varphi \quad \text{and} \quad \eta_\beta = 121393 - 75025\varphi$$

both *are* units, lest we have blundered and are about to waste our effort pointlessly. Indeed, they are; with respective norms $\operatorname{Norm}\eta_\alpha = 1$ and $\operatorname{Norm}\eta_\beta = -1$. We should recognise, however that the example is degenerate — not quite general — in that $D = 5$ is the unique D so that δ is a unit. Moreover, we also notice that $\eta_\beta = 46368 + 75025\overline{\varphi}$, so $-\varphi\eta_\beta = \eta_\alpha$.

3. Units in Quadratic Number Fields

3.1. For nonsquare positive D there always are units $x - \delta y$, that is, positive integers x, y satisfying "Pell's equation" $x^2 - txy + ny^2 = \pm 1$. That follows readily from several applications of the box principle. One first proves Dirichlet's result that there are infinitely many integers q so that the distance to the nearest integer $\|q\delta\|$ of $q\delta$ satisfies $\|q\delta\| < 1/q$. It follows that for each such q there is an integer p so that $|p^2 - tpq + nq^2| < (p - q\overline{\delta})/q < (\delta - \overline{\delta})$. Again by the box principle, there is then an integer k, with $|k| < (\delta - \overline{\delta})$, so that the equation $p^2 - tpq + nq^2 = k$ has infinitely many pairs of solutions (p, q) and, once again by the box principle, two distinct pairs of solutions (p, q) and (p', q') so that $p \equiv p'$ and $q \equiv q' \pmod k$. Then $x = |pp' - Dqq'|/k^2$, $y = |pq' - p'q|/k^2$ displays positive integers x and y satisfying $x^2 - txy + ny^2 = 1$. We add that there may be a

smaller solution (in that x or y is smaller than the minimal x, y just shown to be a solution to $x^2 - txy + ny^2 = 1$) for the equation $x^2 - txy + ny^2 = -1$.

3.2. The following is peculiarly poorly known.

Remark. One may say that a two by two matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is *column dominant* if $a > b$ implies $c \geq d$, or if $a < b$ implies $c \leq d$. A matrix that is not column dominant will be said to be *column balanced*. Dually, by transposition, we similarly have the notions of *row dominant* and *row balanced*. A matrix that is both column and row dominant may be said to be *dominant*. Similarly if it is both column and row balanced it may be said to be *balanced*. Happily, it is plain that

Proposition. A two by two positive integer unimodular matrix is dominant.

Even if one were to allow zero entries as well, the only exceptions that occur are

$$J := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \text{ notice that } J^2 = I\,.$$

Theorem. A positive integer unimodular matrix $\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ has a unique decomposition

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix},$$

in positive integers a_i, other than perhaps for a_0 or a_m which may be zero.

Proof. Apply the Euclidean algorithm to the rows of the matrix. Thus step 0 of the decomposition is

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q & s \\ p - a_0 q & r - a_0 s \end{pmatrix},$$

with a_0 selected maximally so that the remainders $p - a_0 q$ and $r - a_0 s$ both are nonnegative. Plainly one is left with a matrix whose first row dominates its second row. Thus on repeating the process the succeeding a_i are positive, at any rate until one is left with a balanced matrix.

Dually, one may apply the Euclidean algorithm to the columns of the matrix, with step 0 then being

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} r & p - a_m r \\ s & q - a_m s \end{pmatrix} \begin{pmatrix} a_m & 1 \\ 1 & 0 \end{pmatrix}.$$

∎

It follows that $a_0 = 0$ is possible only if $p \leq q$, and $a_m = 0$ only if $p \leq r$. Moreover, $p/q = [\,a_0\,,a_1\,,\ldots,a_s\,]$ and $r/s = [\,a_0\,,a_1\,,\ldots,a_{s-1}\,]$. Furthermore, the preliminary description of the notion 'continued fraction', as well as the matrix correspondence, entails that $[\,a_0\,,a_1\,,\ldots,a_{s-1}\,,0\,] = [\,a_0\,,a_1\,,\ldots,a_{s-2}\,]$.

3.3. Recall, see §§2.2, that we have set $\delta = \sqrt{D}$ or $\frac{1}{2}(1+\sqrt{D})$ according as $D \not\equiv 1$ or $D \equiv 1 \pmod 4$; with $n = \delta\overline{\delta}$ and $t = \delta + \overline{\delta}$.

Applying the peculiarly poorly known remark to the case of units $x - \delta y$, with x and y positive integers, one checks readily that

$$M = \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

for positive integers $a_0, a_1, \ldots, a_{r-1}$. Moreover, the near identity of the elements x and $x-ty$ in the main diagonal (recall that $t=0$ or $t=1$, and in particular that t is an integer) entails $a_r = a_0 - t$ and that the word $a_1 a_2 \ldots a_{r-1}$ is a palindrome[1].

In the immediate sequel x, y is the minimal pair of positive integers satisfying $x^2 - txy + ny^2 = \pm 1$, and M_δ is the matrix

$$M_\delta = \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix}$$

corresponding to the *fundamental* unit $\eta = x - \delta y$ of $\mathbb{K} = \mathbb{Q}(\sqrt{D})$.

It is fairly easy to see naïvely that $\pm\eta^h$, $h \in \mathbb{Z}$ yields all the units of $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. For if there were another unit ε, say, one could readily construct a unit $\pm\eta^k\varepsilon$, some $k \in \mathbb{Z}$, 'smaller than' the fundamental unit.

Remark. In the case $D = 5$ the *fundamental* unit is $1 - \varphi$ (recall that above we set $\varphi = \frac{1}{2}(1+\sqrt{5})$). Then $x = 1$, $y = 1$ and $n = -1$, $t = 1$, so $a_r = a_0 - 1 = 0$ and

$$M_\varphi = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

as claimed.

3.4. It is a manifestation of the Cayley-Hamilton Theorem that

$$M_\delta^{h+2} = (2x - ty)M_\delta^{h+1} - (x^2 - txy + ny^2)M_\delta^h, \quad h \in \mathbb{Z}. \tag{3.1}$$

If we now set $M_\delta^h = M_h$ then (3.1) becomes the recurrence relation

$$M_{h+2} = (2x - ty)M_{h+1} - (x^2 - txy + ny^2)M_h \quad h = 0, 1 \ \ldots,$$

reporting that the units $\eta^h = x_h - \delta y_h$ are given by the recurrence relations

$$x_{h+2} = (2x - ty)x_{h+1} \mp x_h \quad \text{and} \quad y_{h+2} = (2x - ty)y_{h+1} \mp y_h \quad h = 0, 1, \ldots.$$

Here $\eta^0 = 1 - \delta \cdot 0$ and $\eta^1 = x - \delta y$. The sign $\mp$ is chosen according as $\eta\overline{\eta} = \pm 1$.

In the example case $D = 5$ the recurrence relation is

$$\eta^{h+2} = \eta^{h+1} + \eta^h \quad \text{with } \eta^0 = 1 \text{ and } \eta = 1 - \varphi,$$

so the sequence $(y_h)_{h\geq 0}$ is $0, 1, 1, 2, 3, 5, \ldots, y_{24} = 46368, y_{25} = 75025, \ldots$.

By the way, this calculation is computationally easy. One does *not* have to wade stepwise all the way up to $h = 24$. Nor is this ease just a consequence of our happening to be looking at the Fibonacci numbers.

In general, it is a familiar fact from the theory of recurrence sequences, and is in any case easy to verify directly, that

$$y_h = y(\eta^h - \overline{\eta}^h)/(\eta - \overline{\eta}). \tag{3.2}$$

Since, moreover, always $-1 < \overline{\delta} < 0$, it is plain that $y_h \approx y\eta^h/(\eta - \overline{\eta})$, and it *is* easy to compute h given y_h.

[1]Recall that a palindrome is never even, indeed, it's never odd or even. It's a toyota.

3.5. Now it is all very well to talk blithely about the fundamental unit η of $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ but, rather more precisely, η is the fundamental unit of the domain $\mathbb{Z}[\delta]$ (recall that if D is squarefree then $\mathbb{Z}[\delta]$ is the domain of all integers of $\mathbb{K}$). This 'precision' is of importance. While $1 - \varphi = \overline{\varphi}$ is the fundamental unit of $\mathbb{Z}[\frac{1}{2}(1+\sqrt{5})]$, the fundamental unit of the domain $\mathbb{Z}[\sqrt{5}]$ cannot be $1-\varphi$ because φ does not even belong to $\mathbb{Z}[\sqrt{5}]$. Indeed, from the expansion $\sqrt{5} = [\,2\,,\,\overline{4}\,]$ we learn immediately that the fundamental unit of $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[2\varphi]$ has trace 4 and norm -1, and thus is $2 - \sqrt{5} = \overline{\varphi}^3$. Just so, $\alpha = \overline{\varphi}^{24}$ is the fundamental unit of $\mathbb{Z}[92736\varphi]$, while $\beta = \overline{\varphi}^{25}$ is the fundamental unit of the domain $\mathbb{Z}[15050\varphi]$.

Remark. We should confess that any one of the four units $\pm\eta$, $\pm\overline{\eta}$ has the right to step forward and to insist *it* generates all the units of $\mathbb{Z}[\delta]$. Our selecting $x - \delta y$ for the qualification 'fundamental' if both x and y are positive integers, is just a convention convenient for the present context.

3.6. One might well wonder how, given the fundamental unit, η_g say, of the domain $\mathbb{Z}[g\delta]$ one finds the fundamental unit, η_f say, of $\mathbb{Z}[f\delta]$, where $g \big| f$. Recall, however, that to compute η_f our remarks at §§3.3 point out that it suffices to find the period of $f\delta$. So the point of the following remarks is to explain the relationship between η_g and η_f. Indeed, if we have not insisted that D be squarefree it suffices to ask what power of the fundamental unit $\eta = x - \delta y$ has y divisible by f.

The first fact we recall is that if p is a rational prime and F is a polynomial with integer coefficients then $F(X)^p \equiv F(X^p) \pmod{p}$. Hence if γ is a zero of F it follows that $\gamma^p \equiv \gamma' \pmod{p}$, where γ' is some zero of F. Thus if F is the defining polynomial of $\eta = x - \delta y$ then $\eta^p \equiv \eta$ or $\eta^p \equiv \overline{\eta} \pmod{p}$.

Let $p \neq 2$. Suppose first that $p \big| D$. It is then immediate by the binomial expansion that η^p is equivalent to a rational integer modulo p; so η^p is in $\mathbb{Z}[p\delta]$. If $p \not| D$ then similarly $\eta^{p-1} \equiv 1 \pmod{p}$, respectively $\eta^{p+1} \equiv \overline{\eta}\eta = \pm 1 \pmod{p}$, entail that η^{p-1}, respectively η^{p+1}, is in $\mathbb{Z}[p\delta]$. The last two cases are p splits, respectively p is inert, in $\mathbb{K} = \mathbb{Q}(\delta)$. So if $\epsilon = \left(\frac{p}{D}\right)$ denotes the Kronecker symbol then all three cases speak of $\eta^{p-\epsilon}$.

Suppose now that $p = 2$. Plainly $(x - y\sqrt{D})^2$ is then always in $\mathbb{Z}[2\sqrt{D}]$. A trifle less obviously, if $D \equiv 1 \pmod{4}$ then also $(x - y\delta)^3$ is in $\mathbb{Z}[2\delta]$.

3.7. Returning to the example, it happens that $46368 = 2^5 \cdot 3^3 \cdot 7 \cdot 23$ and $75025 = 5^2 \cdot 3001$. By our previous computations we already know that $\alpha^{25} = \beta^{24}$, but it also seems worthwhile to check this in the light of the immediately preceding remarks. By those remarks, the smallest power of α that can have a 5 in its 'y' is α^5 and one notes that α^5 is not in $\mathbb{Z}[5^2\varphi]$. Thus we need α^{25} and it, indeed, is in $\mathbb{Z}[5^2 \cdot 3001\varphi]$. Had we endeavoured to get that 3001 as such, we should have considered α^m for m dividing 3000, discovering once again that $m = 25$ will do.

3.8. In particular it must be that the two matrices M_α^{25} and M_β^{24} determine the same unit. In other words, they have the same eigenvalues. In particular, they have the same 'norm' — that is, determinant — and the same trace. Since the only two possibilities for the determinant are ± 1, the coincidence of parities chatted about above is simply there to ensure the coincidence of norms.

3.9. We have said enough to make plain that (Theorem 1 of [1])

Theorem 3. *Given a pure periodic element* $\alpha = [\,\overline{a_0\,,\,a_1\,,\,\ldots\,,\,a_r}\,]$ *set*

$$[\,a_0\,,\,a_1\,,\,\ldots\,,\,a_r\,] = p_{\alpha,r}/q_{\alpha,r} \quad \textit{and} \quad [\,a_0\,,\,a_1\,,\,\ldots\,,\,a_{r-1}\,] = p_{\alpha,r-1}/q_{\alpha,r-1}\,;$$

equivalently

$$M_\alpha = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{\alpha,r} & p_{\alpha,r-1} \\ q_{\alpha,r} & q_{\alpha,r-1} \end{pmatrix}.$$

Let $\beta = [\,\overline{b_0\,,\,b_1\,,\,\ldots\,,\,b_s}\,]$. *Then* α *and* β *belong to the same quadratic number field if and only if there are positive integers* u *and* v *so that the matrices* M_α^u *and* M_β^v *are similar, that is, have the same determinant and trace; equivalently,*

$$p_{\alpha,u(r+1)-1} + q_{\alpha,u(r+1)-2} = p_{\beta,v(s+1)-1} + q_{\beta,v(s+1)-2}\ ,,$$

and $u(r+1)$, $v(s+1)$ *have the same parity.*

Remark. One can readily compute traces of powers of the matrices M^h featuring above by noticing that those traces satisfy a second order recurrence relation; to wit that satisfied by the M^h.

4. Pure periodicity and reduction

It is difficult to avoid feeling that our story is incomplete because we deal only with purely periodic continued fraction expansions.

4.1. Strictly speaking, there is nothing to add. The argument sketched at §§3.1 is readily adjusted to show that, given an arbitrary generator γ of a quadratic number field, there are integers a and b so that $\mathrm{Norm}(a - \gamma b) = 1$. A review of Theorem 1 shows that its core story only tacitly supposes that the partial quotients a_0, a_1, ... all are positive integers. So we may consider finite decompositions

$$M_\gamma = \begin{pmatrix} a & -N_\gamma b \\ b & a - T_\gamma b \end{pmatrix} = \begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} c_t & 1 \\ 1 & 0 \end{pmatrix}$$

in not necessarily positive integers c_i and deduce from Theorem 1 that γ has a purely periodic expansion $[\,\overline{c_0\,,\,c_1\,,\,\ldots\,,\,c_t}\,]$. One then works with that period, albeit that it is not unique. Then every generator of a quadratic number field has a purely periodic expansion.

There's little harm in working *en passant* with nonpositive partial quotients. Indeed, at §§3.3 we admit 0 as a partial quotient, presuming that the reader will recognise that $[\,\ldots\,,\,a\,,\,0\,,\,b\,,\,\ldots\,] = [\,\ldots\,,\,a+b\,,\,\ldots\,]$. In similar spirit, it is also not difficult to get rid of negative partial quotients; for example see the remarks at p363 of [3].

4.2. If, on the other hand, one *insists* that continued fraction expansions have all their partial quotients (other perhaps than the 0-th) positive — in other words that the expansions be 'admissible', then there's nothing for it but to deal only with *reduced* elements ρ. From here on our expansions *are* admissible.

Suppose one is given a sequence $(a_h)_{h\geq 1}$ of positive integers, and $a_0 \in \mathbb{Z}$. Then there is a real number α with continued fraction expansion $[a_0, a_1, a_2, \ldots\ldots]$. Given an arbitrary irrational complex number $\beta = \beta_0$ one may define the sequence $(\beta_h)_{h\geq 1}$ by $\beta_{h+1} = (\beta_h - a_h)^{-1}$. Vincent's Theorem (1836) points out that unless $\beta = \alpha$ there is some $k = k(\beta, \alpha)$ so that for $h \geq k$ necessarily β_h is in the left hand half of the unit circle.

Accordingly, consider the sequence of polynomials $(f_h)_{h\geq 0}$ obtained from $f(Y) = f_0(Y) = A_{0,0}Y^r + A_{0,1}Y^{r-1} + \cdots + A_{0,r}$ by the rule

$$f_{h+1}(Y) = \pm Y^r f_h(a_h + Y^{-1}). \tag{4.1}$$

The choice of sign in (4.1) is not particularly important, but morally should be made so that the f_h have positive leading coefficient; after a while the $-$ sign will always do. One sees readily that any zero β of f is transformed into a zero β_h of f_h. In particular, if α is itself a non-multiple zero of a polynomial f without rational zeros then there is an $k = k(f)$ so that for $h \geq k$ all the zeros β_h of f lie in the left hand half of the unit circle, other than for the zero α_h which is real and greater than 1. In [2] the polynomials f_h $(h \geq k)$ are said to be 'reduced', in analogy with the case $r = 2$ — where that terminology is standard.

Thus the continued fraction process eventually reduces all algebraic elements. Plainly $\alpha_k = -(q_{\alpha,k-1}\alpha - p_{\alpha,k-1})/(q_{\alpha,k}\alpha - p_{\alpha,k})$ generates the same number field over $\mathbb{Q}$ as does α, so it suffices to work just with reduced elements $\rho = \alpha_k$.

4.3. Specifically, a quadratic irrational ρ is reduced if $\rho > 1$ but its conjugate $\overline{\rho}$ satisfies $-1 < \overline{\rho} < 0$. It is a theorem attributed to Galois that ρ has a purely periodic continued fraction expansion if and only if ρ is reduced.

To see that clearly, suppose r denotes the integer part of ρ. Then the tableau yielding the continued fraction expansion of ρ begins with the line

$$\rho = r - (r - T_\rho + \overline{\rho}).$$

We know that the said tableau is eventually periodic. Now consider the conjugate of the tableau, and in particular the conjugate

$$r - T_\rho + \rho = r - \overline{\rho}$$

of the given line. Because ρ is reduced, this too is a line in some continued fraction tableau.

The preceding lines of this conjugate tableau are, albeit in reverse order, the conjugates of the succeeding lines of the original tableau. So they are periodic because the original tableau is periodic. But a period with its order reversed is a period. We invite the reader to see it now manifest that the conjugate tableau, and therefore also the original tableau, must be *purely* periodic.

References

[1] Edward B. Burger, 'On real quadratic number fields and simultaneous diophantine approximation', Monatshefte Math., **128** (1999), 201–209.

[2] Enrico Bombieri and Alfred J van der Poorten, 'Continued fractions of algebraic numbers', (*Computational Algebra and Number Theory, Sydney* 1992, Wieb Bosma and Alf van der Poorten eds., Kluwer 1995, 138–154.

[3] Alf van der Poorten, 'Formal power series and their continued fraction expansion', in Joe Buhler ed., *Algorithmic Number Theory* (Proc. Third International Symposium, ANTS-III, Portland, Oregon, June 1998), Springer Lecture Notes in Computer Science **1423** (1998), 358–371.

Department of Mathematics, Williams College, Williamstown, Massachusetts 01267
E-mail address: eburger@williams.edu (Edward B. Burger)

ceNTRe for Number Theory Research, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: alf@mpce.mq.edu.au (Alf van der Poorten)