A unimodular matrix connected with Pell's equation

Keith Matthews

December 29, 2009

Theorem. Suppose $u^2 - Dv^2 = \epsilon = \pm 1$, where u, v, D are positive integers, $D > 1$ and not a square. Also suppose the unimodular matrix $A = \begin{pmatrix} Dv & u \\ u & v \end{pmatrix}$ has the (unique) factorisation

$$A = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix},$$

where all $a_i > 0$. Then

(a) the sequence $a_0, \ldots, a_n$ is palindromic,

(b) $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0}]$,

(c) $u/v = [a_0, \ldots, a_{n-1}]$,

(d) $Dv/u = [a_0, \ldots, a_n]$.

Remarks

1. The period is a multiple of the least period and will be the least period if and only if $u + v\sqrt{D}$ is the fundamental solution of $u^2 - Dv^2 = \epsilon$.

2. These results are also treated in [1, pages 110-111]. Also see [3, pages 276-281]. Our treatment is partly based on that in [2, §21].

Lemma. ([2, page 193].) Let $a_1, \ldots, a_n, x, y$ be positive real numbers, a_0 a real number. Also let

$$z = [a_0, a_1, \ldots, a_n, x/y].$$

Then $z = r/s$, where

$$\begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Proof of the Theorem. (a)

$$A^t = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = A,$$

so the uniqueness of the expansions of A and A^t implies equality of the sequences $a_0, \ldots, a_n$ and $a_n, \ldots, a_0$.

(b) We have

$$A \begin{pmatrix} 1 \\ \sqrt{D} \end{pmatrix} = \begin{pmatrix} Dv + u\sqrt{D} \\ u + v\sqrt{D} \end{pmatrix} = \begin{pmatrix} \sqrt{D}(u + v\sqrt{D}) \\ u + v\sqrt{D} \end{pmatrix}.$$

With $x = 1, y = \sqrt{D}, r = \sqrt{D}(u + v\sqrt{D}), s = u + v\sqrt{D}$, the Lemma then gives

$$\begin{aligned} \sqrt{D} &= [a_0, \ldots, a_n, 1/\sqrt{D}] \\ &= [a_0, \ldots, a_{n-1}, a_n + \sqrt{D}] \\ a_0 + \sqrt{D} &= [2a_0, \ldots, a_{n-1}, a_0 + \sqrt{D}] \\ &= [\overline{2a_0, \ldots, a_{n-1}}] \\ \sqrt{D} &= [a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0}]. \end{aligned}$$

For (c) and (d), see

`http://www.numbertheory.org/courses/MP313/lectures/lecture16/page1.html`

Example. $D = 14, u = 15, v = 4$. Then $u^2 - Dv^2 = 1$ and

$$\begin{pmatrix} 56 & 15 \\ 15 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$$

Hence

$$\begin{aligned} \sqrt{14} &= [3, \overline{1, 2, 1, 6}] \\ 56/15 &= [3, 1, 2, 1, 3] \\ 15/4 &= [3, 1, 2, 1]. \end{aligned}$$

References

[1] A.J van der Poorten, *An introduction to continued fractions*, LMS Lecture Note Series **109**, 99-138, CUP 1985

[2] O. Forster, *Algorithmische Zahlentheorie*, Vieweg 1996

[3] H. Koch, *Zahlentheorie: Algebraische Zahlen und Funktionen*, Vieweg 1997