Some continued fraction identities

Keith Matthews

Abstract

Abstract. We generalise some Pell equation identities of Pohst and Zassenhaus [1, pp. 143] which enable one to use only half the period of the continued fraction expansion of $\sqrt{D}$ when solving $x^2 - Dy^2 = N$ for $|N| < \sqrt{D}$.

The simple continued fraction expansion for $\sqrt{D}$ is periodic with period k:

$$\sqrt{D} = \begin{cases} [a_0, \overline{a_1, \ldots, a_{h-1}, a_{h-1}, \ldots, a_1, 2a_0}] & \text{if } k = 2h-1, \\ [a_0, \overline{a_1, \ldots, a_{h-1}, a_h, a_{h-1}, \ldots, a_1, 2a_0}] & \text{if } k = 2h. \end{cases}$$

The smallest solution of $x^2 - Dy^2 = \pm 1$ is given by

$$\eta_0 = \begin{cases} A_{2h-2} + B_{2h-2}\sqrt{D} & \text{if } k = 2h-1, \\ A_{2h-1} + B_{2h-1}\sqrt{D} & \text{if } k = 2h. \end{cases}$$

Post and Zassenhaus point out that

$$\left.\begin{array}{l} A_{2h-2} = A_{h-1}B_{h-1} + A_{h-2}B_{h-2} \\ B_{2h-2} = (B_{h-1}^2 + B_{h-2}^2) \end{array}\right. \quad \text{if } k = 2h-1,$$

$$\left.\begin{array}{l} A_{2h-1} = B_{h-1}(A_h + A_{h-2}) + (-1)^h \\ B_{2h-1} = B_{h-1}(B_h + B_{h-2}) \end{array}\right. \quad \text{if } k = 2h.$$

Also if $(P_n + \sqrt{D})/Q_n$ denotes the n-th complete quotient of the continued fraction expansion of $\sqrt{D}$, then the equations

$$\begin{array}{ll} Q_h = Q_{h-1} & \text{if } k = 2h-1, \\ P_h = P_{h+1} & \text{if } k = 2h, \end{array}$$

enable us to detect the end of the half period.

For example:

(a) $D = 21$. Here $k = 6,\ h = 3,\ P_3 = P_4$ and $\eta = 55 + 12\sqrt{21}$:

i	0	1	2	3	4	5	6
P_i	4	4	1	3	3	1	4
Q_i	1	5	4	3	4	5	1
a_i	4	1	1	2	1	1	16
A_i/B_i	4/1	5/1	9/2	23/5	32/7	55/12	912/199

(b) $D = 29$. Here $k = 5,\ h = 3,\ Q_2 = Q_3$ and $\eta = 70 + 13\sqrt{21}$:

i	0	1	2	3	4	5
P_i	5	5	3	2	3	5
Q_i	1	4	5	5	4	1
a_i	5	2	1	1	2	10
A_i/B_i	5/1	11/2	16/3	27/5	70/13	727/135

We generalise these equations to $D = b/a, a < b, \gcd(a, b) = 1$, adding two others, as follows:

(i) Let $k = 2h - 1$. Then for $0 \le t \le h - 1$, we have

$$
\begin{aligned}
A_{2h-2} &= A_{h+t-1}B_{h-t-1} + A_{h+t-2}B_{h-t-2} && (1)\\
B_{2h-2} &= B_{h+t-1}B_{h-t-1} + B_{h+t-2}B_{h-t-2} && (2)\\
DB_{2h-2} &= A_{h+t-1}A_{h-t-1} + A_{h+t-2}A_{h-t-2} && (3)\\
A_{2h-2} &= B_{h+t-1}A_{h-t-1} + B_{h+t-2}A_{h-t-2}. && (4)
\end{aligned}
$$

Equations (1) and (3) give

$$A_{h+t-2} = (-1)^{h+t+1}(-A_{2h-2}A_{h-t-1} + DB_{2h-2}B_{h-t-1}) \qquad (5)$$

and equations (2) and (4) give

$$B_{h+t-2} = (-1)^{h+t+1}(A_{2h-2}B_{h-t-1} - B_{2h-2}A_{h-t-1}). \qquad (6)$$

We can combine equations (5) and (6) to get, with $\eta = A_{2h-2} + B_{2h-2}\sqrt{D}$.

$$A_{h+t-2} + B_{h+t-2}\sqrt{D} = (-1)^{h+t+1}\eta(-A_{h-t-1} + B_{h-t-1}\sqrt{D}). \qquad (7)$$

(ii) Let $k = 2h$. Then for $0 \le t \le h - 1$, we have

$$
\begin{aligned}
A_{2h-1} &= A_{h+t-1}B_{h-t} + A_{h+t-2}B_{h-t-1} && (8)\\
B_{2h-1} &= B_{h+t-1}B_{h-t} + B_{h+t-2}B_{h-t-1} && (9)\\
DB_{2h-1} &= A_{h+t-1}A_{h-t} + A_{h+t-2}A_{h-t-1} && (10)\\
A_{2h-1} &= B_{h+t-1}A_{h-t} + B_{h+t-2}A_{h-t-1}. && (11)
\end{aligned}
$$

From equations (8) and (10) give

$$A_{h+t-1} = (-1)^{h+t}(A_{2h-1}A_{h-t-1} - DB_{2h-1}B_{h-t-1}) \tag{12}$$

and equations (9) and (11) give

$$B_{h+t-1} = (-1)^{h+t}(-A_{2h-1}B_{h-t-1} + B_{2h-1}A_{h-t-1}). \tag{13}$$

We can combine equations (12) and (13) to get, with $\eta = A_{2h-1} + B_{2h-1}\sqrt{D}$,

$$A_{h+t-1} + B_{h+t-1}\sqrt{D} = (-1)^{h+t+1}\eta(-A_{h-t-1} + B_{h-t-1}\sqrt{D}). \tag{14}$$

Lemma. Let $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}]$. Then

$$\begin{aligned} DB_{k-1} &= a_0A_{k-1} + A_{k-2} && (15)\\ A_{k-1} &= a_0B_{k-1} + B_{k-2}. && (16) \end{aligned}$$

If $D = b/a$, where $\gcd(a, b) = 1$, then a divides B_{k-1}.
Proof.

$$\begin{aligned} \sqrt{D} &= [a_0, \ldots, a_{k-1}, 2a_0 + (\sqrt{D} - a_0)] \\ &= [a_0, \ldots, a_{k-1}, a_0 + \sqrt{D}] \\ &= \frac{A_{k-1}(a_0 + \sqrt{D}) + A_{k-2}}{B_{k-1}(a_0 + \sqrt{D}) + B_{k-2}}. \end{aligned}$$

The desired result then follows by cross-multiplying and equating corresponding coefficients.
We now derive equations (1)–(4). We start from the matrix identity

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2h-2} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2h-2} & A_{2h-3} \\ B_{2h-2} & B_{2h-3} \end{bmatrix}. \tag{17}$$

Now let $0 \le t \le h-2$. Then $h + t \le 2h - 2$ and we can partition the above matrix product as

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{h+t-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{h+t} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2h-2} & 1 \\ 1 & 0 \end{bmatrix}.$$

But $a_{h+i} = a_{h-i-1}$ for $i = 0, \ldots, h-2$, so (17) becomes

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{h+t-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{h-t-1} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2h-2} & A_{2h-3} \\ B_{2h-2} & B_{2h-3} \end{bmatrix}. \tag{18}$$

Multiplying both sides of (18) on the right by $\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}$ then gives

$$\begin{aligned} \begin{bmatrix} A_{h+t-1} & A_{h+t-2} \\ B_{h+t-1} & B_{h+t-2} \end{bmatrix} \begin{bmatrix} A_{h-t-1} & A_{h-t-2} \\ B_{h-t-1} & B_{h-t-2} \end{bmatrix}^t &= \begin{bmatrix} a_0 A_{2h-2} + A_{2h-3} & A_{2h-2} \\ a_0 B_{2h-2} + B_{2h-3} & B_{2h-2} \end{bmatrix} \\ &= \begin{bmatrix} DB_{2h-2} & A_{2h-2} \\ A_{2h-2} & B_{2h-2} \end{bmatrix}, \end{aligned} \tag{19}$$

by the Lemma. Hence

$$\begin{bmatrix} A_{h+t-1} & A_{h+t-2} \\ B_{h+t-1} & B_{h+t-2} \end{bmatrix} \begin{bmatrix} A_{h+t-1} & B_{h+t-1} \\ A_{h+t-2} & B_{h+t-2} \end{bmatrix} = \begin{bmatrix} DB_{2h-2} & A_{2h-2} \\ A_{2h-2} & B_{2h-2} \end{bmatrix}. \tag{20}$$

Finally, equation (20) is equivalent to equations (1)–(4).
Similarly we derive equations (5)–(9). We start from the matrix identity

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2h-1} & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2h-1} & A_{2h-2} \\ B_{2h-1} & B_{2h-2} \end{bmatrix}. \tag{21}$$

Now let $0 \le t \le h-1$. Then $h+t \le 2h-1$ and we can partition the above matrix product as

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{h+t-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{h+t} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{2h-1} & 1 \\ 1 & 0 \end{bmatrix}.$$

But $a_{h+i} = a_{h-i}$ for $i = 0, \ldots, h-1$, so (21) becomes

$$\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_{h+t-1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_{h-t} & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} a_1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} A_{2h-1} & A_{2h-2} \\ B_{2h-1} & B_{2h-2} \end{bmatrix}. \tag{22}$$

Multiplying both sides of (22) on the right by $\begin{bmatrix} a_0 & 1 \\ 1 & 0 \end{bmatrix}$ then gives

$$\begin{aligned} \begin{bmatrix} A_{h+t-1} & A_{h+t-2} \\ B_{h+t-1} & B_{h+t-2} \end{bmatrix} \begin{bmatrix} A_{h-t} & A_{h-t-1} \\ B_{h-t} & B_{h-t-1} \end{bmatrix}^t &= \begin{bmatrix} a_0 A_{2h-1} + A_{2h-2} & A_{2h-1} \\ a_0 B_{2h-1} + B_{2h-2} & B_{2h-1} \end{bmatrix} \\ &= \begin{bmatrix} DB_{2h-1} & A_{2h-1} \\ A_{2h-1} & B_{2h-1} \end{bmatrix}, \end{aligned} \tag{23}$$

again by the Lemma. Hence

$$\left[\begin{array}{cc} A_{h+t-1} & A_{h+t-2} \\ B_{h+t-1} & B_{h+t-2} \end{array}\right]\left[\begin{array}{cc} A_{h-t} & B_{h-t} \\ A_{h-t-1} & B_{h-t-1} \end{array}\right] = \left[\begin{array}{cc} DB_{2h-1} & A_{2h-1} \\ A_{2h-1} & B_{2h-1} \end{array}\right]. \quad (24)$$

Finally, equation (24) is equivalent to equations (5)–(9).

We now prove equation (4), page 94 from Perron's *Kettenbrüche*.
Theorem. Let $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_k}]$. Then if $n \geq 1$, we have

$$\begin{aligned} A_{n+k-1} &= B_{n-1}DB_{k-1} + A_{n-1}A_{k-1} \\ B_{n+k-1} &= B_{n-1}A_{k-1} + A_{n-1}B_{k-1}. \end{aligned}$$

Equivalently

$$A_{n+k-1} + B_{n+k-1}\sqrt{D} = (A_{n-1} + B_{n-1}\sqrt{D})(A_{k-1} + B_{k-1}\sqrt{D}).$$

Proof. We start from the matrix identity

$$\left[\begin{array}{cc} a_0 & 1 \\ 1 & 0 \end{array}\right] \cdots \left[\begin{array}{cc} a_{n+k-1} & 1 \\ 1 & 0 \end{array}\right] = \left[\begin{array}{cc} A_{n+k-1} & A_{n+k-2} \\ B_{n+k-1} & A_{n+k-2} \end{array}\right].$$

We partition the matrix product:

$$\left[\begin{array}{cc} a_0 & 1 \\ 1 & 0 \end{array}\right] \cdots \left[\begin{array}{cc} a_{k-1} & 1 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} 2a_0 & 1 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} a_1 & 1 \\ 1 & 0 \end{array}\right] \cdots \left[\begin{array}{cc} a_{n-1} & 1 \\ 1 & 0 \end{array}\right].$$

Hence

$$\begin{aligned} \left[\begin{array}{cc} A_{n+k-1} & A_{n+k-2} \\ B_{n+k-1} & B_{n+k-2} \end{array}\right] &= \left[\begin{array}{cc} A_{k-1} & A_{k-2} \\ B_{k-1} & B_{k-2} \end{array}\right]\left[\begin{array}{cc} 2a_0 & 1 \\ 1 & 0 \end{array}\right]\left[\begin{array}{cc} 0 & 1 \\ 1 & -a_0 \end{array}\right]\left[\begin{array}{cc} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{array}\right] \\ &= \left[\begin{array}{cc} A_{k-1} & A_{k-2} \\ B_{k-1} & B_{k-2} \end{array}\right]\left[\begin{array}{cc} 1 & a_0 \\ 0 & 1 \end{array}\right]\left[\begin{array}{cc} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{array}\right] \\ &= \left[\begin{array}{cc} A_{k-1} & a_0A_{k-1} + A_{k-2} \\ B_{k-1} & a_0B_{k-1} + B_{k-2} \end{array}\right]\left[\begin{array}{cc} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{array}\right]. \end{aligned}$$

Now identities at the top of page 94 of Perron's book state that

$$\begin{aligned} A_{n-1} &= B_{n-1}P_n + B_{n-2}Q_n \\ DB_{n-1} &= A_{n-1}P_n + A_{n-2}Q_n. \end{aligned}$$

Then taking $n = k$ and observing that $P_k = a_0$ and $Q_k = 1$, we get

$$\begin{aligned} A_{k-1} &= B_{k-1}a_0 + B_{k-2} \\ DB_{k-1} &= A_{k-1}a_0 + A_{k-2}. \end{aligned}$$

Hence

$$\begin{bmatrix} A_{n+k-1} & A_{n+k-2} \\ B_{n+k-1} & B_{n+k-2} \end{bmatrix} = \begin{bmatrix} A_{k-1} & DB_{k-1} \\ B_{k-1} & A_{k-1} \end{bmatrix} \begin{bmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{bmatrix},$$

as required.

References

[1] M. Pohst and H. Zassenhaus, *On unit computation in real quadratic fields*, *EUROSAM '79*, Springer Lecture Notes in Computer Science, Volume 72, (1979) 140-152.

[2] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner 1954.

Keith Matthews
Department of Mathematics
University of Queensland
Brisbane
Australia 4072
e–mail: keithmatt@gmail.com