An explicit decomposition formula of a matrix in $GL_2(\mathbb{Z})$

D. FOSSE, MSc. Physics
dominique.fosse@a3.epfl.ch

Introduction Let $\mathcal{M}_2(\mathbb{Z})$ the ring of all square matrices of order 2 with coefficients in the ring $\mathbb{Z}$. Recall that $GL_2(\mathbb{Z})$ denotes the unit group of $\mathcal{M}_2(\mathbb{Z})$ and has the following caracterization:

$$GL_2(\mathbb{Z}) = \left\{ M \in \mathcal{M}_2(\mathbb{Z}) \,\middle|\, \det(M) = \pm 1 \right\}$$

We will make use of $C := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$. Let's consider now

$$SL_2(\mathbb{Z}) = \left\{ M \in \mathcal{M}_2(\mathbb{Z}) \,\middle|\, \det(M) = +1 \right\}$$

which is a subgroup of $GL_2(\mathbb{Z})$; we define $A := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ two elements of $SL_2(\mathbb{Z})$. It is well known (for instance, see [1]) that A and B generates $SL_2(\mathbb{Z})$; and from now on, we will use the following notation:

$$\langle A, B \rangle = SL_2(\mathbb{Z})$$

Other pairs of generators can be considered; one can often find in the literature:

$$S := B^{-1}AB^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \qquad \text{and} \qquad T := B$$

Let $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ and suppose $d \neq 0$ (the case $d = 0$ is elementary and will be treated separately). The aim of this article is to demonstrate, using a funny induction, the following formula:

$$\boxed{M = \left(AB^{-1}A\right)^{1-(-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d)} A\Big(\prod_{k=1}^{j} A^{-\left(2+(-1)^k n_k\right)} B\Big) \left(CA^2\right)^{\frac{1-\det(M)}{2}} A^{(-1)^j \operatorname{sgn}(d)(p_{j-1}c - q_{j-1}a)} B^{-1} A} \tag{1}$$

Here, $[n_1; n_2, \ldots, n_j]$ represents the simple finite continued fraction associated to the rational $\frac{b}{d}$; where $n_1 \in \mathbb{Z}$ and $n_i \in \mathbb{N}^*$, $\forall i \in [\![2, j]\!]$. Since $[n_1; 1] = [n_1 + 1]$ and $[n_1; n_2, \ldots, n_j, 1] = [n_1; n_2, \ldots, n_j + 1]$, every rational number can be represented in two different ways and we will show that formula (1) is independant of this choice of representation. The terms p_{j-1} and q_{j-1} come from the reduced fraction $\frac{p_{j-1}}{q_{j-1}} := [n_1; n_2, \ldots, n_{j-1}]$ with the initial condition $(p_0, q_0) := (1, 0)$. By definition of $[n_1; n_2, \ldots, n_j]$, one has:

$$\frac{p_j}{q_j} = \frac{b}{d} \iff p_j d - q_j b = 0 \tag{2}$$

Also, $\left\lfloor \frac{j}{2} \right\rfloor$ denotes the integer part of $\frac{j}{2}$ so that $(-1)^{\left\lfloor \frac{j}{2} \right\rfloor} = \pm 1$, depending on the residue of j modulo 4. If we note $I := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then we verify by direct calculation that $\left(AB^{-1}A\right)^2 = -I$; therefore:

$$\left(AB^{-1}A\right)^{1-(-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d)} = \begin{cases} \left(AB^{-1}A\right)^0 = I & \text{if } (-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d) = +1 \\ \left(AB^{-1}A\right)^2 = -I & \text{if } (-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d) = -1 \end{cases} \tag{3}$$

As $\left(AB^{-1}A\right)^{1-(-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d)} = \pm I$, this matrix commutes with any element of $GL_2(\mathbb{Z})$ and we chose to write it as a factor of the right member of formula (1). The basic theory of continued fractions also ensures that $q_k > 0$, $\forall k \in [\![1, j]\!]$ and so there is no ambiguity regarding the sign of p_{j-1} in case the ratio $\frac{p_{j-1}}{q_{j-1}}$ is negative. Note that $\det(M) = +1 \iff M \in SL_2(\mathbb{Z})$, then $\left(CA^2\right)^{\frac{1-\det(M)}{2}} = \left(CA^2\right)^0 = I$ which means, as expected, that C (which doesn't belong to $SL_2(\mathbb{Z})$) vanishes from formula (1) and we retrieve an expression of M as a word in $\langle A, B \rangle$.

An explicit example

1) Let $M := \left(\begin{smallmatrix} -65 & 17 \\ 42 & -11 \end{smallmatrix}\right)$; we verify that $\det(M) = 1$ so that $M \in SL_2(\mathbb{Z})$. We develop here what we call the *first represention* of $\frac{b}{d} = -\frac{17}{11}$ which is $[-2; 2, 5]$. Explicitely,

$$-\frac{17}{11} = -2 + \cfrac{1}{2 + \cfrac{1}{5}} \implies j := 3 \text{ and } (n_1, n_2, n_3) = (-2, 2, 5)$$

Then, $(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d) = (-1)^{\lfloor \frac{3}{2} \rfloor}\mathrm{sgn}(-11) = (-1)^1(-1) = +1$. The reduced fraction $\frac{p_{j-1}}{q_{j-1}} = \frac{p_2}{q_2}$ is then $[-2; 2] = -2 + \frac{1}{2} = -\frac{3}{2}$. As stated in the introduction, q_2 is necessarily a positive integer; thus $(p_2, q_2) = (-3, 2)$. Then $b_j = b_3 = (-1)^3\mathrm{sgn}(-11)\,(-3 \cdot 42 - 2 \cdot (-65)) = 4$. Also, $\det(M) = 1 \implies \frac{1-\det(M)}{2} = 0 \implies \left(CA^2\right)^{\frac{1-\det(M)}{2}} = \left(CA^2\right)^0 = I$. That's it; we have everything to apply formula (1):

$$\begin{aligned} M &= I \cdot A\left(A^{-(2-n_1)}B\right)\left(A^{-(2+n_2)}B\right)\left(A^{-(2-n_3)}B\right)I \cdot A^{b_3}B^{-1}A \\ &= A\left(A^{-(2-(-2))}B\right)\left(A^{-(2+2)}B\right)\left(A^{-(2-5)}B\right)A^4B^{-1}A \\ &= A^{-3}BA^{-4}BA^3BA^4B^{-1}A \end{aligned} \tag{4}$$

2) Let's consider the same matrix $M := \left(\begin{smallmatrix} -65 & 17 \\ 42 & -11 \end{smallmatrix}\right)$ but this time, let's use the *second representation* of $\frac{b}{d} = -\frac{17}{11}$ which is $[-2; 2, 4, 1] \implies (n_1, n_2, n_3, n_4) = (-2, 2, 4, 1)$. This time, $j := 4$ and thus $(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d) = (-1)^{\lfloor \frac{4}{2} \rfloor}\mathrm{sgn}(-11) = (-1)^2(-1) = -1$. The reduced fraction $\frac{p_{j-1}}{q_{j-1}} = \frac{p_3}{q_3}$ is then $[-2; 2, 4] = -2 + \frac{1}{2+\frac{1}{4}} = -\frac{14}{9} \implies (p_{j-1}, q_{j-1}) = (p_3, q_3) = (-14, 9)$. Then, $b_j = b_4 = (-1)^4\mathrm{sgn}\,(-11)\,((-14)42 - 9(-65)) = 3$. Then,

$$\begin{aligned} M &= \left(AB^{-1}A\right)^2 A\left(A^{-(2-n_1)}B\right)\left(A^{-(2+n_2)}B\right)\left(A^{-(2-n_3)}B\right)\left(A^{-(2+n_4)}B\right)A^{b_4}B^{-1}A \\ &= \left(AB^{-1}A\right)^2 A\left(A^{-(2-(-2))}B\right)\left(A^{-(2+2)}B\right)\left(A^{-(2-4)}B\right)\left(A^{-(2+1)}B\right)A^3B^{-1}A && (5) \\ &= AB^{-1}A^2B^{-1}A^2A^{-4}BA^{-4}BA^2BA^{-3}BA^3B^{-1}A \\ &= AB^{-1}A^2B^{-1}A^{-2}BA^{-4}BA^2BA^{-3}BA^3B^{-1}A && (6) \end{aligned}$$

Comparing (4) and (5), we get two different expressions of M in $\langle A, B \rangle$ and formula (1) works well in both representations.

Some basic lemmas We list here all the requiered results used in the demonstration of formula (1).

Lemma 0.1 (Powers of A and B)**.** *For all $n \in \mathbb{Z}$,*

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad B^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \tag{7}$$

Proof. Suppose $n \geq 0$. For $n = 0$ or $n = 1$, (7) are both verified. Suppose (7) true for $n > 1$; one gets $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) A^n = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & n+1 \\ 0 & 1 \end{smallmatrix}\right) = A^n \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \implies A \cdot A^n = A^n \cdot A = A^{n+1}$. Regarding B, we have $B \cdot B^n = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ n+1 & 1 \end{smallmatrix}\right) = B^{n+1} = B^n \cdot B$. Now let's compute the inverse of A^n: $(A^n)^{-1} = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) = A^{-n}$ and we get something similar for B: $B^{-n} = \left(\begin{smallmatrix} 1 & 0 \\ -n & 1 \end{smallmatrix}\right)$ which proves (7), $\forall n \in \mathbb{Z}$. ■

Let's now treat the case $d := 0$ separately.

Lemma 0.2 (The case $d := 0$)**.** *Let $M_0 := \left(\begin{smallmatrix} a & b \\ c & 0 \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$, then $M_0 \in \langle A, B, C \rangle$*

Proof. $M_0 = \left(\begin{smallmatrix} a & b \\ c & 0 \end{smallmatrix}\right) \implies \det(M_0) = -bc = \pm 1$. Thus, there are four possibilities:

$$(b, c) \in \{(1, 1), (-1, -1), (1, -1), (-1, 1)\}$$

(*i*) $(b, c) := (1, 1) \implies M_0 = \left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right) \implies M_0 \in GL_2(\mathbb{Z}) \setminus SL_2(\mathbb{Z})$ as $\det(M_0) = -1$. We check that, $\forall a \in \mathbb{Z}$:

$$CB^{-1}AB^{a-1} = \left(\begin{smallmatrix} a & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \langle A, B, C \rangle \tag{8}$$

(*ii*) $(b, c) := (-1, -1) \implies M_0 = \left(\begin{smallmatrix} a & -1 \\ -1 & 0 \end{smallmatrix}\right) \implies M_0 \in GL_2(\mathbb{Z}) \setminus SL_2(\mathbb{Z})$ as $\det(M_0) = -1$. Note that $M_0 = -\left(\begin{smallmatrix} -a & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Using $-I = (AB^{-1}A)^2$ as mentioned in the introduction and point (*i*), we get:

$$M_0 = AB^{-1}A^2B^{-1}ACB^{-1}AB^{-a-1} \in \langle A, B, C \rangle \tag{9}$$

(*iii*) $(b,c)=(1,-1) \implies M_0 = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix} \implies \det(M_0)=+1 \implies M_0 \in SL_2(\mathbb{Z})$. We check that, $\forall a \in \mathbb{Z}$:

$$M_0 = A^{1-a}B^{-1}A \in \langle A,B\rangle \subseteq \langle A,B,C\rangle \tag{10}$$

(*iv*) $(b,c)=(-1,1) \implies M_0 = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \implies \det(M_0)=+1 \implies M_0 \in SL_2(\mathbb{Z})$. We check that, $\forall a \in \mathbb{Z}$:

$$M_0 = BA^{-1}B^{1-a} \in \langle A,B\rangle \subseteq \langle A,B,C\rangle \tag{11}$$

Conclusion: as per equations (8), (9), (10) and (11), $M_0 \in \langle A,B,C\rangle$. On top of that, equations (10) and (11) show that $M_0 \in SL_2(\mathbb{Z}) \implies M_0 \in \langle A,B\rangle$, as expected. ∎

Lemma 0.3 (Some basic results on simple continued fractions). *Let* $[n_1;n_2,\ldots,n_j]$ *a simple and finite continued fraction:*

$$\frac{p_j}{q_j} = [n_1;n_2,\ldots,n_j] = n_1 + \cfrac{1}{n_2 + \cfrac{1}{n_3 + \cfrac{1}{n_4 + \ddots + \cfrac{1}{n_{j-1} + \frac{1}{n_j}}}}}$$

The convergents *are the rational numbers defined by* $\frac{p_i}{q_i} := [n_1;n_2,\ldots,n_i]$, $\forall i \in [\![1,\, j]\!]$ *with the convention* $(p_0,q_0) := (1,0)$. *Let's prove the following points:*

(*i*) $\forall i \in [\![2,\, j]\!]$, *we have* $p_i = n_i p_{i-1} + p_{i-2}$ *and* $q_i = n_i q_{i-1} + q_{i-2}$

(*ii*) $p_i q_{i-1} - p_{i-1} q_i = (-1)^i$, $\forall i \in [\![1,\, j]\!]$

(*iii*) *The convergents* $\frac{p_i}{q_i} := [n_1;n_2,\ldots,n_i]$ *are such that* p_i *and* q_i *are coprime numbers,* $\forall i \in [\![1,\, j]\!]$.

(*iv*) *With* $q_0 := 0$, *one has* $q_1 := 1 \leq q_2$ *and* $q_2 < q_3 < \ldots q_j$. *In particular,* $q_i \geq 0$, $\forall i \in [\![0,\, j]\!]$.

(*v*) $\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^i}{q_i q_{i-1}}$, $\forall i \in [\![2,\, j]\!]$

Proof. (*i*) As $p_0 = 1$, $q_1 = 1$ and $\frac{p_1}{q_1} = [n_1] = \frac{n_1}{1} = n_1$, we have $p_1 := n_1$. Then, $n_2 p_1 + p_0 = n_2 n_1 + 1$. On the other side, $\frac{p_2}{q_2} = [n_1;n_2] = n_1 + \frac{1}{n_2} = \frac{n_1 n_2 + 1}{n_2} \implies (p_2,q_2) = (n_1 n_2 + 1, n_2)$ and this shows that (*i*) is valid for $i := 2$. Suppose that (*i*) is valid for $i > 2$; we have:

$$\frac{p_i}{q_i} = [n_1,n_2,\ldots,n_{i-1},n_i] = n_1 + \cfrac{1}{n_2 + \cfrac{1}{n_3 + \cfrac{1}{n_4 + \ddots + \cfrac{1}{n_{i-1} + \frac{1}{n_i}}}}}$$

And we see directly that $\left[n_1;n_2,\ldots,n_{i-1}+\frac{1}{n_i}\right] = [n_1;n_2,\ldots,n_{i-1},n_i]$. Then,

$$\begin{aligned}
\frac{p_i}{q_i} = [n_1;n_2,\ldots,n_{i-1},n_i] &= \left[n_1;n_2,\ldots,n_{i-1}+\tfrac{1}{n_i}\right] \\
&= \frac{p_{i-1}\left(n_1,n_2,\ldots,n_{i-1}+\frac{1}{n_i}\right)}{q_{i-1}\left(n_1,n_2,\ldots,n_{i-1}+\frac{1}{n_i}\right)} \\
&= \frac{\left(n_{i-1}+\frac{1}{n_i}\right)p_{i-2} + p_{i-3}}{\left(n_{i-1}+\frac{1}{n_i}\right)q_{i-2} + q_{i-3}} \qquad \text{(by inductive hypothesis)} \\
&= \frac{(n_{i-1}p_{i-2} + p_{i-3}) + \frac{1}{n_i}p_{i-2}}{(n_{i-1}q_{i-2} + q_{i-3}) + \frac{1}{n_i}q_{i-2}} \\
&= \frac{p_{i-1} + \frac{1}{n_i}p_{i-2}}{q_{i-1} + \frac{1}{n_i}q_{i-2}} \qquad \text{(by inductive hypothesis)} \\
&= \frac{n_i p_{i-1} + p_{i-2}}{n_i q_{i-1} + q_{i-2}}
\end{aligned}$$

(ii) For $i := 1$, (ii) is verified, as $p_1q_0 - p_0q_1 = n_1 \cdot 0 - 1 \cdot 1 = -1 = (-1)^1$. Suppose (ii) is true for $i > 1$; one gets:

$$\begin{aligned} p_{i+1}q_i - p_iq_{i+1} &= (n_{i+1}p_i + p_{i-1})\, q_i - p_i\,(n_{i+1}q_i + q_{i-1}) \qquad \text{(using } (i)\text{)} \\ &= n_{i+1}p_iq_i + p_{i-1}q_i - n_{i+1}q_ip_i - p_iq_{i-1} = -\left(p_iq_{i-1} - p_{i-1}q_i\right) \\ &= -(-1)^i \qquad \text{(by inductive hypothesis)} \\ &= (-1)^{i+1} \end{aligned}$$

(iii) Both recurrence relations of point (i) show that $n_i \in \mathbb{Z} \implies (p_i, q_i) \in \mathbb{Z}^2$, $\forall i \in [\![1, j]\!]$. Let's write point (ii) as $p_i\left((-1)^i q_{i-1}\right) + q_i\left((-1)^{i-1}p_{i-1}\right) = 1$, $\forall i \in [\![1, j]\!]$ which is a Bézout relation. Therefore, p_i and q_i are coprime numbers, $\forall i \in [\![1, j]\!]$.

(iv) Using the recurrence relation $q_i = n_1q_{i-1} + q_{i-2}$, $\forall i \in [\![2, j]\!]$ from point (i) with $(q_0, q_1) = (0, 1)$, we show, by induction, that $q_i \geq 1$, $\forall i \in [\![1, j]\!]$. Recall that $n_1 \in \mathbb{Z}$ and $n_i \in \mathbb{N}^*$, $\forall i \in [\![2, j]\!]$. For $i := 2$, we get $q_2 = n_2q_1 + q_0 = n_2 \cdot 1 + 0 = n_2 \geq 1$. Suppose that $q_i \geq 1$ for $i > 2$, hence $q_{i+1} = n_{i+1}q_i + q_{i-1}$; by induction hypothesis, $q_{i-1} \geq 1$, $q_i \geq 1$ and $n_{i+1} \in \mathbb{N}^*$. Therefore, $n_{i+1}q_i + q_{i-1} \geq 1$; i.e, $q_{i+1} \geq 1$ and this shows that $q_i \geq 1$, $\forall i \in [\![1, j]\!]$. Moreover, $n_iq_{i-1} + q_{i-2} \geq q_{i-1} + q_{i-2}$ when $i \geq 2$. Using point (i), we get $q_i \geq q_{i-1} + q_{i-2}$, $\forall i \in [\![2, j]\!]$. As $q_{i-2} \geq 1$ whenever $i \geq 3$, we get finally $q_i \geq q_{i-1} + q_{i-2} > q_{i-1}$, $\forall i \in [\![3, j]\!]$.

(v) Point (iv) showed, in particular, that $q_i \neq 0$, $\forall i \in [\![1, j]\!]$. Hence, $q_iq_{i-1} \neq 0$, $\forall i \in [\![2, j]\!]$. It's then possible to divide point (ii) relation by q_iq_{i-1}.

■

We will also make use of the following elementary result:

Lemma 0.4.

$$(-1)^{\left\lfloor \frac{k+1}{2} \right\rfloor} = (-1)^k(-1)^{\left\lfloor \frac{k}{2} \right\rfloor} \qquad \forall k \in \mathbb{N}$$

Proof. Recall that $\forall x \in \mathbb{R}$ and $\forall n \in \mathbb{Z}$, one has $\lfloor x + n \rfloor = \lfloor x \rfloor + n$. Let $(k, k') \in \mathbb{N}^2$ such $k = 4k'$, then $\left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{4k'}{2} \right\rfloor = 2k' \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'} = +1$. Suppose now $(k, k') \in \mathbb{N}^2$ such $k = 4k' + 1$; then $\left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{4k'+1}{2} \right\rfloor = \left\lfloor 2k' + \frac{1}{2} \right\rfloor = 2k' + \left\lfloor \frac{1}{2} \right\rfloor = 2k' \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'} = +1$. Suppose now $(k, k') \in \mathbb{N}^2$ such $k = 4k' + 2$; then $\left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{4k'+2}{2} \right\rfloor = \lfloor 2k' + 1 \rfloor = 2k' + 1 \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'+1} = -1$. Finally, suppose $(k, k') \in \mathbb{N}^2$ such $k = 4k' + 3$; then $\left\lfloor \frac{k}{2} \right\rfloor = \left\lfloor \frac{4k'+3}{2} \right\rfloor = \left\lfloor \frac{(4k'+2)+1}{2} \right\rfloor = \left\lfloor 2k' + 1 + \frac{1}{2} \right\rfloor = 2k' + 1 + \left\lfloor \frac{1}{2} \right\rfloor = 2k' + 1 \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'+1} = -1$. Hence we showed that, $\forall k \in \mathbb{N}$:

$$(-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = \begin{cases} 1 & \text{if } k \equiv 0 \text{ or } 1 \mod 4 \\ -1 & \text{if } k \equiv 2 \text{ or } 3 \mod 4 \end{cases} \implies (-1)^{\left\lfloor \frac{k+1}{2} \right\rfloor} = \begin{cases} 1 & \text{if } k \equiv 0 \text{ or } 3 \mod 4 \\ -1 & \text{if } k \equiv 1 \text{ or } 2 \mod 4 \end{cases} \tag{12}$$

Of course, $\forall k \in \mathbb{N}$, we have:

$$(-1)^k = \begin{cases} 1 & \text{if } k \equiv 0 \text{ or } 2 \mod 4 \\ -1 & \text{if } k \equiv 2 \text{ or } 3 \mod 4 \end{cases}$$

That means $(-1)^k(-1)^{\left\lfloor \frac{k}{2} \right\rfloor}$ equals $+1$ when $\left((-1)^{\left\lfloor \frac{k}{2} \right\rfloor}, (-1)^k\right) = (1, 1)$ or $(-1, -1)$ and this is the case if and only if $k \equiv 0$ or $3 \mod 4$ and this is exactly what shows equation (12). ■

The main result Let $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$ with $d \neq 0$. Let's define, $\forall k \in [\![1, j]\!]$,

$$\begin{cases} \alpha_k(b, d) := (-1)^{\left\lfloor \frac{k}{2} \right\rfloor}\left(q_kb - p_kd + (-1)^k\,(q_{k-1}b - p_{k-1}d)\right) \\ \gamma_k(b, d) := (-1)^{\left\lfloor \frac{k}{2} \right\rfloor}\,(p_kd - q_kb) \end{cases} \tag{13}$$

where, $\frac{p_k}{q_k} := [n_1; n_2, \ldots, n_k]$, $\forall k \in [\![1, j]\!]$ are the convergents of the continued fraction $\frac{b}{d} = [n_1; n_2, \ldots, n_j]$. Let's also define:

$$P_0 := A^{-1}MA^{-1}B \qquad \text{and} \qquad P_k := \begin{pmatrix} \alpha_k(b, d) & \alpha_k(b - a, d - c) \\ \gamma_k(b, d) & \gamma_k(b - a, d - c) \end{pmatrix} \quad \forall k \geq 1 \tag{14}$$

Then,

(i) $P_k \in GL_2(\mathbb{Z})$, $\forall k \in [\![0, j]\!]$

(ii) $P_j = (-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d)\left(CA^2\right)^{\frac{1-\det(M)}{2}} A^{b_j}$; where $b_j := (-1)^j\operatorname{sgn}(d)\,(p_{j-1}c - q_{j-1}a)$

(iii) $P_k = B^{-1}A^{2+(-1)^k n_k}P_{k-1}$, $\forall k \in [\![1,\, j]\!]$

Proof. *(i)* For $k := 0$, it is clear, from its definition ($GL_2(\mathbb{Z})$ is a group), that $P_0 \in GL_2(\mathbb{Z})$. Suppose $k > 0$; from their definitions (13), we see that the coefficients of P_k are integers. Therefore, the only thing we have to check is $\det(P_k) = \pm 1$, $\forall k \in [\![1,\, j]\!]$. Let's do it:

$$\begin{aligned}
\det(P_k) =& \alpha_k(b,d)\gamma_k(b-a,d-c) - \gamma_k(b,d)\alpha_k(b-a,d-c)\\
=& (-1)^{2\lfloor \frac{k}{2} \rfloor}\left(q_k b - p_k d + (-1)^k\left(q_{k-1}b - p_{k-1}d\right)\right)\left(p_k(d-c) - q_k(b-a)\right)\\
&- (-1)^{2\lfloor \frac{k}{2} \rfloor}\left(p_k d - q_k b\right)\left(q_k(b-a) - p_k(d-c) + (-1)^k\left(q_{k-1}(b-a) - p_{k-1}(d-c)\right)\right)\\
=& q_k p_k b(d-c) - q_k^2 b(b-a) - p_k^2 d(d-c) + p_k q_k d(b-a) + (-1)^k p_k q_{k-1} b(d-c)\\
&- (-1)^k q_k q_{k-1} b(b-a) - (-1)^k p_k p_{k-1} d(d-c) + (-1)^k p_{k-1} q_k d(b-a) - p_k q_k d(b-a) + p_k^2 d(d-c)\\
&- (-1)^k p_k q_{k-1} d(b-a) + (-1)^k p_k p_{k-1} d(d-c) + q_k^2 b(b-a) - q_k p_k b(d-c) + (-1)^k q_k q_{k-1} b(b-a)\\
&- (-1)^k q_k p_{k-1} b(d-c)\\
=& (-1)^k b(d-c)\left(p_k q_{k-1} - q_k p_{k-1}\right) - (-1)^k d(b-a)\left(p_k q_{k-1} - p_{k-1} q_k\right)\\
=& (-1)^k\left(p_k q_{k-1} - q_k p_{k-1}\right)(ad - bc)\\
=& (-1)^k(-1)^k \det(M) \qquad \text{(using lemma (0.3), point } (ii))\\
=& \det(M)\\
=& \pm 1 \qquad (\text{as } M \in GL_2(\mathbb{Z}))
\end{aligned}$$

(ii) Using (2), we get directly $\gamma_j(b,d) = 0$ and this makes P_j upper triangular. We have:

$$\begin{aligned}
\alpha_j(b,d) &= (-1)^{\lfloor \frac{j}{2} \rfloor}\left(q_j b - p_j d + (-1)^j\left(q_{j-1}b - p_{j-1}d\right)\right)\\
&= (-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(q_{j-1}b - p_{j-1}d\right) \qquad \text{(using equation (2))}\\
&= (-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(q_{j-1}\left(d\frac{p_j}{q_j}\right) - p_{j-1}d\right) \qquad \text{(using equation (2) again)}\\
&= (-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(p_j q_{j-1} - p_{j-1}q_j\right)\frac{d}{q_j}\\
&= (-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j(-1)^j\frac{d}{q_j} \qquad \text{(using lemma (0.3), point } (ii))\\
&= (-1)^{\lfloor \frac{j}{2} \rfloor}\frac{d}{q_j}
\end{aligned} \tag{15}$$

From point *(i)*, we know that $P_j \in GL_2(\mathbb{Z})$. Therefore, $\alpha_j(b,d) \in \mathbb{Z}$ with $d \in \mathbb{Z}^*$ and this means that q_j divides d (let's note this $q_j \mid d$). Also,

$$\begin{aligned}
\gamma_j(b-a,d-c) =& (-1)^{\lfloor \frac{j}{2} \rfloor}\left(p_j(d-c) - q_j(b-a)\right) = (-1)^{\lfloor \frac{j}{2} \rfloor}\left(p_j d - p_j c - q_j b + q_j a\right)\\
=& (-1)^{\lfloor \frac{j}{2} \rfloor}\left(q_j a - p_j c\right) \qquad \text{(using equation (2))}\\
=& (-1)^{\lfloor \frac{j}{2} \rfloor}\left(q_j a - \left(\frac{q_j}{d}b\right)c\right) \qquad \text{(using equation (2) again)}\\
=& (-1)^{\lfloor \frac{j}{2} \rfloor}\frac{q_j}{d}(ad - bc)\\
=& (-1)^{\lfloor \frac{j}{2} \rfloor}\frac{q_j}{d}\det(M)
\end{aligned} \tag{16}$$

Using the same argument as for (15), we get $d \mid q_j$. So, as $q_j > 0$ (that is lemma (0.3), point *(iv)*), we have $\left(q_j \mid d \text{ and } d \mid q_j\right) \implies d = \mathrm{sgn}(d)q_j$. We have found:

$$\alpha_j(b,d) = (-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d) \tag{17}$$

And,

$$\gamma_j(b-a,d-c) = (-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\det(M) \tag{18}$$

Finally,

$$\begin{aligned}
\alpha_j\,(b-a,d-c) =& (-1)^{\lfloor \frac{j}{2} \rfloor}\left(q_j(b-a)-p_j(d-c)+(-1)^j\,(q_{j-1}(b-a)-p_{j-1}(d-c))\right)\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\,(q_{j-1}(b-a)-p_{j-1}(d-c))\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(q_{j-1}\left(d\frac{p_j}{q_j}\right)-q_{j-1}a-p_{j-1}d+p_{j-1}c\right) \qquad \text{(using eq. (2))}\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(\frac{d}{q_j}\,(p_jq_{j-1}-q_jp_{j-1})+p_{j-1}c-q_{j-1}a\right)\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\left(\frac{d}{q_j}(-1)^j+p_{j-1}c-q_{j-1}a\right) \qquad \text{(using lemma (0.3), point } (ii))\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}\frac{d}{q_j}+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\,(p_{j-1}c-q_{j-1}a)\\
=& -\gamma_j(b-a,d-c)+(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\,(p_{j-1}c-q_{j-1}a) \qquad \text{(using eq. (15) and (17))}\\
=& -(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\det(M)+(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)+(-1)^{\lfloor \frac{j}{2} \rfloor}(-1)^j\,(p_{j-1}c-q_{j-1}a) \qquad \text{(using eq. (18))}\\
=&(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\left(1-\det(M)+(-1)^j\mathrm{sgn}(d)\,(p_{j-1}c-q_{j-1}a)\right) \qquad \left(\text{as } (\mathrm{sgn}(d))^2=\mathrm{sgn}(d)\right) \qquad (19)
\end{aligned}$$

Putting equations (17), (18) and (19) together, we found:

$$P_j=(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\begin{pmatrix}1 & 1-\det(M)+(-1)^j\mathrm{sgn}(d)\,(p_{j-1}c-q_{j-1}a)\\ 0 & \det(M)\end{pmatrix} \qquad (20)$$

Let's write $b_j:=(-1)^j\mathrm{sgn}(d)\,(p_{j-1}c-q_{j-1}a)$, we get:

(1) $M\in SL_2(\mathbb{Z}) \implies \det(M)=1$; then, using lemma (0.1), equation (20) becomes:

$$P_j^+=(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\begin{pmatrix}1 & b_j\\ 0 & 1\end{pmatrix}=(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)A^{b_j} \qquad (21)$$

(2) $M\in GL_2(\mathbb{Z})\backslash SL_2(\mathbb{Z}) \implies \det(M)=-1$; note that, $\forall n\in\mathbb{Z}$, $CA^n=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&n\\0&-1\end{smallmatrix}\right)$. Therefore, equation (20) becomes:

$$P_j^-=(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\begin{pmatrix}1 & 2+b_j\\ 0 & -1\end{pmatrix}=(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)CA^{2+b_j} \qquad (22)$$

If we want to put equations (21) and (22) together, we note that $\frac{1-\det(M)}{2}=0$ when $M\in SL_2(\mathbb{Z})$ and $\frac{1-\det(M)}{2}=1$ when $M\in GL_2(\mathbb{Z})\setminus SL_2(\mathbb{Z})$. Therefore,

$$\begin{aligned}
P_j =&(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)\left(CA^2\right)^{\frac{1-\det(M)}{2}}A^{b_j}\\
=&\left(AB^{-1}A\right)^{1-(-1)^{\lfloor \frac{j}{2} \rfloor}\mathrm{sgn}(d)}\left(CA^2\right)^{\frac{1-\det(M)}{2}}A^{b_j} \qquad \text{(using equation (3))} \qquad (23)
\end{aligned}$$

(iii) Recall equation (14); we have, by definition, $P_0=A^{-1}MA^{-1}B$. By direct calculation, we get:

$$P_0:=\begin{pmatrix}b-d & b+c-(a+d)\\ d & d-c\end{pmatrix} \qquad (24)$$

By induction on $k\geq 1$, we will show that $P_k=B^{-1}A^{2+(-1)^k n_k}P_{k-1}$, $\forall k\in [\![1,\,j]\!]$.

- Let $k:=1$; on one side, we have:

$$\begin{aligned}
B^{-1}A^{2+(-1)^1 n_1}P_0 =& \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & 2-n_1\\ 0 & 1\end{pmatrix}\begin{pmatrix}b-d & c+b-a-d\\ d & d-c\end{pmatrix}=\begin{pmatrix}1 & 2-n_1\\ -1 & n_1-1\end{pmatrix}\begin{pmatrix}b-d & c+b-a-d\\ d & d-c\end{pmatrix}\\
=&\begin{pmatrix}b+d-dn_1 & -c+d+b-a+(c-d)n_1\\ -b+dn_1 & -b+a+(d-c)n_1\end{pmatrix} \qquad (25)
\end{aligned}$$

On the other side,

$$\begin{aligned}
P_1 =& \begin{pmatrix}\alpha_1 & \beta_1\\ \gamma_1 & \delta_1\end{pmatrix}\\
=& (-1)^{\lfloor \frac{1}{2} \rfloor}\begin{pmatrix}(q_1b-p_1d+(-1)^1\,(q_0b-p_0d)) & (q_1(b-a)-p_1(d-c)+(-1)^1\,(q_0(b-a)-p_0(d-c)))\\ (p_1d-q_1b) & (p_1(d-c)-q_1(b-a))\end{pmatrix}\\
=& \begin{pmatrix}b-n_1d+d & b-a-n_1(d-c)+(d-c)\\ n_1d-b & n_1(d-c)-(b-a)\end{pmatrix} \qquad \left(\text{using } \left(\begin{smallmatrix}p_0&p_1\\q_0&q_1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&n_1\\0&1\end{smallmatrix}\right)\right) \qquad (26)
\end{aligned}$$

The initialisation of the induction is valid as equations (25) and (26) are the same.

- Suppose that $P_k = B^{-1}A^{2+(-1)^k n_k}P_{k-1}$ is true for $k > 1$; we will show that it remains true for $k+1$:

$$\begin{aligned}
B^{-1}A^{2+(-1)^{k+1}n_{k+1}}P_k &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2+(-1)^{k+1}n_{k+1} \\ 0 & 1 \end{pmatrix} P_k \\
&= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2+(-1)^{k+1}n_{k+1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha_k(b,d) & \alpha_k(b-a,d-c) \\ \gamma_k(b,d) & \gamma_k(b-a,d-c) \end{pmatrix} \qquad \text{(by inductive hyp.)} \\
&= \begin{pmatrix} 1 & 2+(-1)^{k+1}n_{k+1} \\ -1 & -1+(-1)^{k+2}n_{k+1} \end{pmatrix}\begin{pmatrix} \alpha_k(b,d) & \alpha_k(b-a,d-c) \\ \gamma_k(b,d) & \gamma_k(b-a,d-c) \end{pmatrix} := \begin{pmatrix} s & t \\ u & v \end{pmatrix}
\end{aligned}$$

We will show that $\left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha_{k+1}(b,d) & \alpha_{k+1}(b-a,d-c) \\ \gamma_{k+1}(b,d) & \gamma_{k+1}(b-a,d-c) \end{smallmatrix}\right)$:

$$\begin{aligned}
s &= 1\cdot\alpha_k(b,d) + \left(2+(-1)^{k+1}n_{k+1}\right)\gamma_k(b,d) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(q_k b - p_k d + (-1)^k\left(q_{k-1}b - p_{k-1}d\right) + \left(2+(-1)^{k+1}n_{k+1}\right)(p_k d - q_k b)\right) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(q_k b - p_k d + (-1)^k q_{k-1}b - (-1)^k p_{k-1}d + 2p_k d - 2q_k b + (-1)^{k+1}n_{k+1}p_k d - (-1)^{k+1}n_{k+1}q_k b\right) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(p_k d - q_k b + (-1)^{k+1}d\left(n_{k+1}p_k + p_{k-1}\right) - (-1)^{k+1}b\left(n_{k+1}q_k + q_{k-1}\right)\right) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(p_k d - q_k b + (-1)^{k+1}\left(dp_{k+1} - bq_{k+1}\right)\right) \qquad \text{(using lemma (0.3), point } (i)) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}(-1)^k\left((-1)^k(p_k d - q_k b) + (bq_{k+1} - dp_{k+1})\right) \\
&= (-1)^{\lfloor \frac{k+1}{2} \rfloor}\left(q_{k+1}b - p_{k+1}d - (-1)^k(q_k b - p_k d)\right) \qquad \text{(using lemma (0.4))} \\
&= (-1)^{\lfloor \frac{k+1}{2} \rfloor}\left(q_{k+1}b - p_{k+1}d + (-1)^{k+1}(q_k b - p_k d)\right) \\
&= \alpha_{k+1}(b,d)
\end{aligned}$$

From this, we get directly:

$$\begin{aligned}
t &= 1\cdot\alpha_k(b-a,d-c) + \left(2+(-1)^{k+1}n_{k+1}\right)\gamma_k(b-a,d-c) \\
&= \alpha_{k+1}(b-a,d-c)
\end{aligned}$$

Then,

$$\begin{aligned}
u &= (-1)\cdot\alpha_k(b,d) + \left(-1+(-1)^{k+2}n_{k+1}\right)\gamma_k(b,d) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(-q_k b + p_k d + (-1)^{k+1}\left(q_{k-1}b - p_{k-1}d\right) + \left(-1+(-1)^{k+2}n_{k+1}\right)(p_k d - q_k b)\right) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}\left(p_k d - q_k b + (-1)^{k+1}\left(q_{k-1}b - p_{k-1}d\right) - p_k d + q_k b - (-1)^{k+1}n_{k+1}p_k d + (-1)^{k+1}q_k b n_{n+1}\right) \\
&= (-1)^{\lfloor \frac{k}{2} \rfloor}(-1)^{k+1}\left(b\left(n_{k+1}q_k + q_{k-1}\right) - d\left(n_{k+1}p_k + p_{k-1}\right)\right) \\
&= (-1)^{\lfloor \frac{k+1}{2} \rfloor}\left(dp_{k+1} - bq_{k+1}\right) \qquad \text{(using lemma (0.3), point } (i) \text{ and lemma (0.4))} \\
&= \gamma_{k+1}(b,d)
\end{aligned}$$

Finally, using above calculation for u:

$$\begin{aligned}
v &= (-1)\alpha_k(b-a,d-c) + \left(-1+(-1)^{k+2}n_{k+1}\right)\gamma_k(b-a,d-c) \\
&= \gamma_{k+1}(b-a,d-c)
\end{aligned}$$

We just showed:

$$\begin{aligned}
P_j &= \left(B^{-1}A^{2+(-1)^j n_j}\right)\left(B^{-1}A^{2+(-1)^{j-1}n_{j-1}}\right)\cdots\left(B^{-1}A^{2+(-1)^1 n_1}\right)P_0 \\
&= \left(\prod_{k=1}^{j} B^{-1}A^{2+(-1)^{j+1-k}n_{j+1-k}}\right)P_0
\end{aligned}$$

Using equation (23) and the definition of P_0, we get:

$$\left(AB^{-1}A\right)^{1-(-1)^{\lfloor \frac{j}{2} \rfloor}\operatorname{sgn}(d)}\left(CA^2\right)^{\frac{1-\det(M)}{2}}A^{b_j} = \left(\prod_{k=1}^{j} B^{-1}A^{2+(-1)^{j+1-k}n_{j+1-k}}\right)A^{-1}MA^{-1}B \tag{27}$$

Solving this for M, we obtain formula (1). Note that we made, in above development, no assumptions on the continued fraction's length j; this shows that formula (1) is independant of the chosen representation of the continued fraction associated to the rational $\frac{b}{d}$. ■

As another example, we can retrieve the fact that $A^n = \left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$, $\forall n \in \mathbb{Z}$ from lemma (0.1) simply by applying formula (1) to the matrix $\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$. Here, $j := 1$ as $\frac{n}{1} = [n]$ and $b_1 = (-1)^1\mathrm{sgn}(1)\,(p_0 \cdot 0 - q_0 \cdot 1) = 0$ (recall that $q_0 := 0$). Thus,

$$\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} = \underbrace{\left(AB^{-1}A\right)^{1-(-1)^{\left\lfloor \frac{1}{2} \right\rfloor}\mathrm{sgn}(1)}}_{=I} AA^{-(2-n)} \underbrace{BA^0B^{-1}}_{=I} A = AA^{n-2}A = A^n \tag{28}$$

References

[1] Kassel C., Dodane O., Turaev V. *Braid Groups.* Graduate Texts in Mathematics, 247. Springer New York (2008).