arXiv:2304.04804v1 [math.NT] 10 Apr 2023

$GL_2(\mathbb{Z})$ 中一个矩阵的显式分解公式

D. FOSSE，物理学硕士
dominique.fosse@a3.epfl.ch

引言 设 $\mathcal{M}_2(\mathbb{Z})$ 为系数取自环 $\mathbb{Z}$ 的所有 2 阶方阵构成的环。回顾一下，$GL_2(\mathbb{Z})$ 表示 $\mathcal{M}_2(\mathbb{Z})$ 的单位群，其特征如下：

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

我们将用到 $C := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$。现在考虑

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

它是 $GL_2(\mathbb{Z})$ 的一个子群；我们定义 $A := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ 和 $B := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ 为 $SL_2(\mathbb{Z})$ 中的两个元素。众所周知（例如参见 [1]），A 和 B 生成 $SL_2(\mathbb{Z})$；从现在起，我们将使用以下记号：

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

也可以考虑其他生成元对；文献中常见的有：

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

设 $M := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z})$，并假设 $d \neq 0$（情形 $d = 0$ 是初等的，将另行处理）。本文旨在通过一种有趣的归纳法证明以下公式：

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

这里，$[n_1;\ n_2, \ldots, n_j]$ 表示与有理数 $\frac{b}{d}$ 相关联的简单有限连分数；其中 $n_1 \in \mathbb{Z}$ 且 $n_i \in \mathbb{N}^*$, $\forall i \in [\![2, j]\!]$。由于 $[n_1;\ 1] = [n_1 + 1]$ 且 $[n_1;\ n_2, \ldots, n_j, 1] = [n_1;\ n_2, \ldots, n_j + 1]$，每个有理数都可以用两种不同的方式表示，我们将证明公式（1）与所选表示方式无关。项 p_{j-1} 和 q_{j-1} 来自既约分数 $\frac{p_{j-1}}{q_{j-1}} := [n_1;\ n_2, \ldots, n_{j-1}]$，其初始条件为 $(p_0, q_0) := (1, 0)$。根据 $[n_1;\ n_2, \ldots, n_j]$ 的定义，有：

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

此外，$\left\lfloor \frac{j}{2} \right\rfloor$ 表示 $\frac{j}{2}$ 的整数部分，因此 $(-1)^{\left\lfloor \frac{j}{2} \right\rfloor} = \pm 1$，具体取决于 j 模 4 的余数。若记 $I := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$，则通过直接计算可验证 $\left(AB^{-1}A\right)^2 = -I$；因此：

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

由于 $\left(AB^{-1}A\right)^{1-(-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\operatorname{sgn}(d)} = \pm I$，该矩阵与 $GL_2(\mathbb{Z})$ 的任意元素都可交换，因此我们选择将其写成公式（1）右端的一项因子。连分数的基本理论还保证了 $q_k > 0, \forall k \in [\![1, j]\!]$，所以当比值 $\frac{p_{j-1}}{q_{j-1}}$ 为负时，p_{j-1} 的符号并无歧义。注意，$\det(M) = +1 \iff M \in SL_2(\mathbb{Z})$，于是 $\left(CA^2\right)^{\det(M)^2} = \left(CA^2\right)^0 = I$，这意味着，如预期的那样，$C$（它不属于 $SL_2(\mathbb{Z})$）在公式（1）中消失，我们便得到一个将 M 表示为由 $\langle A, B \rangle$ 构成的字的表达式。

一个明确的例子

1) 设 $M:=\left(\begin{smallmatrix}-65 & 17\\ 42 & -11\end{smallmatrix}\right)$; 我们验证 $\det(M)=1$，从而 $M\in SL_2(\mathbb{Z})$。这里我们推导出我们称为 $\frac{b}{d}=-\frac{17}{11}$ 的第一个表示，即 $[-2;\ 2,5]$。具体来说,

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

于是，$(-1)^{\lfloor\frac{j}{2}\rfloor}\operatorname{sgn}(d)=(-1)^{\lfloor\frac{3}{2}\rfloor}\operatorname{sgn}(-11)=(-1)^1(-1)=+1$。因此，$\frac{p_{j-1}}{q_{j-1}}=\frac{p_2}{q_2}$是既约分数 $[-2;\ 2]=-2+\frac{1}{2}=-\frac{3}{2}$。如引言所述，$q_2$必定是一个正整数；因此，$(p_2,q_2)=(-3,2)$。于是$b_j=b_3=(-1)^3\operatorname{sgn}(-11)(-3\cdot 42-2\cdot(-65))=4$。另外，$\det(M)=1\implies {}^{1-}\det\left(\begin{smallmatrix}&M\\2&\end{smallmatrix}\right)=0\implies \left(CA^2\right)^{\frac{1-}{}\det(M)^2}=\left(CA^2\right)^0=I$。就是这样；我们已经具备应用公式（1）所需的一切:

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

2）考虑同一个矩阵 $M:=\left(\begin{smallmatrix}-65 & 17\\ 42 & -11\end{smallmatrix}\right)$，但这次使用 $\frac{b}{d}=-\frac{17}{11}$的第二种表示，即 $[-2;\ 2、\ 4、\ 1]\implies(n_1,n_2,n_3,n_4)=(-2,2,4,1)$。这次，$j:=4$，因此 $(-1)^{\lfloor\frac{j}{2}\rfloor}\operatorname{sgn}(d)=(-1)^{\lfloor\frac{4}{2}\rfloor}\operatorname{sgn}(-11)=(-1)^2(-1)=-1$。于是，既约分数 $\frac{p_{j-1}}{q_{j-1}}=\frac{p_3}{q_3}$ 为 $[-2;\ 2、\ 4]=-2+\frac{1}{2+\frac{1}{4}}=-\frac{14}{9}\implies(p_{j-1},q_{j-1})=(p_3,q_3)=(-14,9)$。然后，$b_j=b_4=(-1)^4\operatorname{sgn}(-11)((-14)42-9(-65))=3$。然后,

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

比较（4）和（5），我们得到 M 在 $\langle A、\ B\rangle$ 中的两种不同表达式，而公式（1）在这两种表示中都成立。

一些基　　本引理 这里列出证明公式（1所需的全部结果).

引理 0.1（ A 和 B的幂）。对于所有 $n\in\mathbb{Z}$,

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

证明。假设 $n\geq 0$。对于 $n=0$ 或 $n=1$，（7）都成立。假设（7）对 $n>1$成立；则有 $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)A^n=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&n+1\\0&1\end{smallmatrix}\right)=A^n\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\implies A\cdot A^n=A^n\cdot A=A^{n+1}$。关于 B，我们有 $B\cdot B^n=\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\n&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&0\\n+1&1\end{smallmatrix}\right)=B^{n+1}=B^n\cdot B$。现在来计算 A^n 的逆：$(A^n)^{-1}=\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)^{-1}=\left(\begin{smallmatrix}1&-n\\0&1\end{smallmatrix}\right)=A^{-n}$，对于 B 也可得到类似结果：$B^{-n}=\left(\begin{smallmatrix}1&0\\-n&1\end{smallmatrix}\right)$，这就证明了（7），$\forall n\in\mathbb{Z}$。■

现在我们单独讨论 $d:=0$ 的情形。

引理 0.2（情形 $d:=0$）。设 $M_0:=\left(\begin{smallmatrix}a&b\\c&0\end{smallmatrix}\right)\in GL_2(\mathbb{Z})$，则 $M_0\in\langle A,B,C\rangle$

证明。 $M_0=\left(\begin{smallmatrix}a&b\\c&0\end{smallmatrix}\right)\implies$ 的行列式为 $(M_0)=-bc=\pm 1$。因此，有四种可能:

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

(i) $(b,c):=(1,\ \ 1)\implies M_0=\left(\begin{smallmatrix}a&1\\1&0\end{smallmatrix}\right)\implies M_0\in GL_2(\mathbb{Z})\setminus SL_2(\mathbb{Z})$，因为 $\det(M_0)=-1$。我们来验证，$\forall a\in\mathbb{Z}$:

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

(ii) $(b,c):=(-1,-1)\implies M_0=\left(\begin{smallmatrix}a&-1\\-1&0\end{smallmatrix}\right)\implies M_0\in GL_2(\mathbb{Z})\setminus SL_2(\mathbb{Z})$，因为 $\det(M_0)=-1$。注意，$M_0=-\left(\begin{smallmatrix}-a&1\\1&0\end{smallmatrix}\right)$。利用引言中提到的 $-I=(AB^{-1}A)^2$ 以及要点 (i)，可得:

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

$(iii)\ (b,c) = (1,-1) \implies M_0 = \left(\begin{smallmatrix} a & 1 \\ -1 & 0 \end{smallmatrix}\right) \implies \det(M_0) = +1 \implies M_0 \in SL_2(\mathbb{Z})$。我们验证： $\forall a \in \mathbb{Z}$:

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

$(iv)\ (b,c) = (-1,1) \implies M_0 = \left(\begin{smallmatrix} a & -1 \\ 1 & 0 \end{smallmatrix}\right) \implies \det(M_0) = +1 \implies M_0 \in SL_2(\mathbb{Z})$。我们检查可知， $\forall a \in \mathbb{Z}$:

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

结论：根据方程（8）、（9）、（10）和（11）， $M_0 \in \langle A, B, C\rangle$。此外，方程（10）和（11）表明 $M_0 \in SL_2(\mathbb{Z})$ $\implies M_0 \in \langle A, B\rangle$，正如预期的那样。■

引理 0.3 （关于简单连分数的一些基本结果）。 设 $[n_1; n_2, \ldots, n_j]$ 是一个简单有限连分数：

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

渐近分数是由以下定义的有理数 $\frac{p_i}{q_i}$: $= [n_1;\ n_2,\ \ldots\ldots,\ n_i]$, $\forall i \in [\![1,\ j]\!]$ 约定$(p_0,\ q_0)$: $=(1,\ 0)$。我们来证明以下几点：

(i) $\forall i \in [\![2,\ j]\!]$, 我们有 $p_i = n_i p_{i-1} + p_{i-2}$ 和 $q_i = n_i q_{i-1} + q_{i-2}$

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

(iii) T这些渐近分数 $\frac{p_i}{q_i} := [n_1;\ n_2, \ldots, n_i]$ 满足： p_i 和 q_i 是互质数， $\forall i \in [\![1,\ j\ ]\!]$.

(iv) 对于 $q_0 := 0$, 有 $q_1 := 1 \le q_2$ 以及 $q_2 < q_3 < \ldots q_j$。特别地， $q_i \ge 0$、 $\forall i \in [\![0,\ j\ ]\!]$.

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

证明。 (i) 由于 $p_0 = 1$, $q_1 = 1$ 和 $\frac{p_1}{q_1} = [n_1] = \frac{n_1}{1} = n_1$, 我们有 $p_1 := n_1$。于是， $n_2 p_1 + p_0 = n_2 n_1 + 1$。另一方面， $\frac{p_2}{q_2} = [n_1;\ n_2] = n_1 + \frac{1}{n_2} = \frac{n_1 n_2 + 1}{n_2} \implies (p_2, q_2) = (n_1 n_2 + 1, n_2)$, 这表明 (i) 对 $i := 2$ 成立。假设 (i) 对 $i > 2$ 成立；我们有：

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

并且我们可以直接看到 $\left[n_1;\ n_2, \ldots, n_{i-1} + \frac{1}{n_i}\right] = [n_1;\ n_2, \ldots, n_{i-1}, n_i]$。接着，

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

（*ii*）对于 $i := 1$，可验证（*ii*），因为 $p_1q_0 - p_0q_1 = n_1 \cdot 0 - 1 \cdot 1 = -1 = (-1)^1$。假设（*ii*）对 $i > 1$ 成立，则有：

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

(*iii*) 点 (*i*) 的两个递推关系都表明 $n_i \in \mathbb{Z} \implies (p_i, q_i) \in \mathbb{Z}^2, \forall i \in [\![1, j]\!]$。将点 (*ii*) 写作 $p_i\left((-1)^i q_{i-1}\right) + q_i\left((-1)^{i-1}p_{i-1}\right) = 1, \forall i \in [\![1, j]\!]$，这是一个贝祖关系。因此，$p_i$ 和 q_i 是互素数，$\forall i \in [\![1, j]\!]$。

(*iv*) 利用点 (*i*) 中的递推关系 $q_i = n_1q_{i-1} + q_{i-2}, \forall i \in [\![2, j]\!]$，以及 $(q_0, q_1) = (0, 1)$，我们通过归纳法证明 $q_i \geq 1, \forall i \in [\![1, j]\!]$。回忆一下，$n_1 \in \mathbb{Z}$ 和 $n_i \in \mathbb{N}^*, \forall i \in [\![2, j]\!]$。对于 $i := 2$，我们得到$q_2 = n_2q_1 + q_0 = n_2 \cdot 1 + 0 = n_2 \geq 1$。假设 $q_i \geq 1$ 对 $i > 2$成立，因此 $q_{i+1} = n_{i+1}q_i + q_{i-1}$；根据归纳假设，$q_{i-1} \geq 1, q_i \geq 1$ 和 $n_{i+1} \in \mathbb{N}^*$。因此，$n_{i+1}q_i + q_{i-1} \geq 1$；也就是说，$q_{i+1} \geq 1$，这表明$q_i \geq 1, \forall i \in [\![1, j]\!]$。此外，当 $i \geq 2$ 时，$n_iq_{i-1} + q_{i-2} \geq q_{i-1} + q_{i-2}$。利用点 (*i*)，我们得到 $q_i \geq q_{i-1} + q_{i-2}, \forall i \in [\![2, j]\!]$。由于只要 $i \geq 3$，就有 $q_{i-2} \geq 1$，最终得到 $q_i \geq q_{i-1} + q_{i-2} > q_{i-1}, \forall i \in [\![3, j]\!]$。

（*v*）点（*iv*）特别指出，$q_i \neq 0, \forall i \in [\![1, j]\!]$。因此，$q_iq_{i-1} \neq 0, \forall i \in [\![2, j]\!]$。于是可以将点（*ii*）中的关系除以 q_iq_{i-1}。

■

我们还将使用以下初等结果：

引理 0.4。

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

证明。回想一下，$\forall x \in \mathbb{R}$ 和 $\forall n \in \mathbb{Z}$，有 $\lfloor x + n \rfloor = \lfloor x \rfloor + n$。令$(k, k') \in \mathbb{N}^2$ 使得 $k = 4k'$，则$\left\lfloor \frac{k}{2} \right\rfloor = \frac{4k'}{2} = 2k' \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'} = +1$。现在假设$(k, k') \in \mathbb{N}^2$使得 $k = 4k' + 1$；则 $\left\lfloor \frac{k}{2} \right\rfloor = \frac{4k'+1}{2} = \left\lfloor 2k' + \frac{1}{2} \right\rfloor = 2k' + \left\lfloor \frac{1}{2} \right\rfloor = 2k' \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'} = +1$。现在假设$(k, k') \in \mathbb{N}^2$使得 $k = 4k' + 2$；则 $\left\lfloor \frac{k}{2} \right\rfloor = \frac{4k'+2}{2} = \lfloor 2k' + 1 \rfloor = 2k' + 1 \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'+1} = -1$。最后，假设$(k, k') \in \mathbb{N}^2$使得$k = 4k' + 3$；则 $\left\lfloor \frac{k}{2} \right\rfloor = \frac{4k'+3}{2} = (4k'+2)_{+1}^{2} = \underline{\lfloor 2k' + 1 + \frac{1}{2} \rfloor} = 2k' + 1 + \left\lfloor \frac{1}{2} \right\rfloor = 2k' + 1 \implies (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} = (-1)^{2k'+1} = -1$。因此我们证明了，$\forall k \in \mathbb{N}$：

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

当然，$\forall k \in \mathbb{N}$，我们有：

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

这意味着，当 $\left((-1)^{\left\lfloor \frac{k}{2} \right\rfloor}, (-1)^k\right) = (1, 1)$ 或 $(-1, -1)$ 时，$(-1)^k(-1)^{\left\lfloor \frac{k}{2} \right\rfloor}$ 等于 $+1$；而这成立当且仅当 $k \equiv 0$ 或 $3 \mod 4$，这正是等式（12）所表明的。■

主要结果设 $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$，其中 $d \neq 0$。定义 $\forall k \in [\![1, j]\!]$，

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

其中，$\frac{p_k}{q_k} := [n_1; n_2, \ldots, n_k]$，$\forall k \in [\![1, j]\!]$是连分数$\frac{b}{d} = [n_1; n_2, \ldots, n_j]$的渐近分数。我们还定义：

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

然后，

(*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 $b_j := (-1)^j \operatorname{sgn}(d) \left(p_{j-1}c - q_{j-1}a\right)$

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

证明。(i) 对于 $k := 0$，根据定义（$GL_2(\mathbb{Z})$ 是一个群），显然 $P_0 \in GL_2(\mathbb{Z})$。假设 $k > 0$；由它们的定义（13），可知 P_k 的系数都是整数。因此，我们只需检验 $\det(P_k) = \pm 1, \forall k \in [\![1, j]\!]$。下面来验证：

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

(ii) 直接利用（2），得到 $\gamma_j(b,d) = 0$，这使得 P_j 成为上三角矩阵。我们有 ：

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

由第（i）点可知 $P_j \in GL_2(\mathbb{Z})$。因此，$\alpha_j(b,d) \in \mathbb{Z}$，其中 $d \in \mathbb{Z}^*$，这意味着 q_j 整除 d（记为 $q_j \mid d$）。此外，

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

使用与（15）相同的论证，我们得到 $d \mid q_j$。因此，由于 $q_j > 0$（即引理（0.3）的第（iv）点），我们有 $\left(q_j \mid d \text{以及 } d \mid q_j\right) \implies d = \text{sgn}(d)q_j$。我们已经得到：

$$\alpha_j(b,d) = (-1)^{\left\lfloor \frac{j}{2} \right\rfloor}\text{sgn}(d) \qquad (17)$$

And,

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

最后，

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

将方程（17）、（18）和（19）合在一起，我们得到：

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

写作 $b_j:=(-1)^j\mathrm{sgn}(d)\,(p_{j-1}c-q_{j-1}a)$，可得：

(1) $M\in SL_2(\mathbb{Z}) \implies \det(M)=1$；然后，利用引理（0.1），方程（20）变为：

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

(2) $M\in GL_2(\mathbb{Z})\backslash SL_2(\mathbb{Z}) \implies \det(M)=-1$；注意，$\forall n\in\mathbb{Z}, CA^n=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&n\\0&-1\end{smallmatrix}\right)$。因此，方程（20）变为：

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

若要将方程（21）和（22）合在一起，我们注意到，当 $M\in SL_2(\mathbb{Z})$ 时，$1-\det(M)_2=0$；而当 $M\in GL_2(\mathbb{Z})$ 时，$1-\det(M)_2=1$ $\backslash SL_2(\mathbb{Z})$。因此，

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

(iii)回顾公式 (14)；根据定义，$P_0=A^{-1}MA^{-1}B$。通过直接计算，我们得到：

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

通过对 $k\geq 1$ 进行归纳，我们将证明 $P_k=B^{-1}A^{2+(-1)^kn_k}P_{k-1}$、$\forall k\in[\![1、\ j]\!]$。

- 令 $k:=1$；一方面，我们有：

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

另一方面，

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

归纳法的初始化是有效的，因为方程（25）和（26）相同。

• 假设对于 $k>1$， $P_k = B^{-1}A^{2+_{(-1)^k n_k}}P_{k-1}$ 成立；我们将证明它对于 $k+1$ 仍然成立：

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

我们将证明 $\left(\begin{smallmatrix}s & t\\ u & v\end{smallmatrix}\right) = \ddot{A}_{\alpha_{k+1}(b,d)\ \ \alpha_{k+1}(b-a,d-c)\ \gamma_{k+1}(b,d)\ \ \gamma_{k+1}(b-a,d-c)}\ddot{a}$:

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

由此，我们直接得到：

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

然后，

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

最后，利用上述对 u 的计算：

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

我们刚刚证明了：

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

使用公式（23）和 P_0 的定义，我们得到：

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

对 M 求解，我们得到公式（1）。请注意，在上述推导中，我们没有对连分数的长度 j 作任何假设；这表明，公式（1）与有理数 $\frac{b}{d}$ 所对应的连分数表示方式无关。■

作为另一个例子，我们只需将公式（1）应用于矩阵 $\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$，即可从引理（0.1）中重新得到 $A^n = \left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right)$，$\forall n \in \mathbb{Z}$ 这一事实。这里，$j := 1$，因为 $\frac{n}{1} = [n]$，并且 $b_1 = (-1)^1 \operatorname{sgn}(1)(p_0 \cdot 0 - q_0 \cdot 1) = 0$（回忆一下，$q_0 := 0$）。因此，

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

参考文献

[1] Kassel C., Dodane O., Turaev V. 辫群。数学研究生教材，247。Springer New York（2008）。