ZESZYTY NAUKOWE UNIWERSYTETU JAGIELLOŃSKIEGO
CCLII PRACE MATEMATYCZNE, ZESZYT 15 1971

Józef Drewniak

An Algorithm for the Decomposition of Modular Transformations into a Finite Product of Generators

The *modular group* is the transformation group (see e.g. [1], [2]) of all transformations

$$w = (az+b)/(cz+d) \tag{1}$$

with

$$ad-bc = 1\,, \tag{2}$$

where a, b, c, d are real integers. The subgroup of the modular group for which b and c are even is called the *even modular group*.

The purpose of this paper is to give an algorithm which permits to decompose each member of the modular group (the even subgroup) into a finite product of its generators.

1. MODULAR GROUP

For every pair of integers R_{-1} and R_0 there is a finite calculation procedure named *Euclid's Algorithm*. We denote by k the number of remainders in this procedure which are not zero. Then

$$\begin{aligned}
&R_{-1} = R_0 Q_1 + R_1 && (|R_1| < |R_0|)\,,\\
&R_0 = R_1 Q_2 + R_2 && (|R_2| < |R_1|)\,,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&R_{s-1} = R_s Q_{s+1} + R_{s+1} && (|R_{s+1}| < |R_s|)\,,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&R_{k-2} = R_{k-1} Q_k + R_k && (|R_k| < |R_{k-1}|)\,,\\
&R_{k-1} = R_k Q_{k+1}\,,
\end{aligned} \tag{3}$$

and $|R_k|$ is the greatest common divisor of R_0 and R_{-1}.

It is well known (see [3] and [4]) that the modular group is generated by the transformations $S(z) = z+1$ and $T(z) = -1/z$.

We shall prove the following

Theorem 1. *Every member* (1) *of the modular group is a finite product of the transformations S and T, namely* (i) *if* $c = 0$ *then* $w = S^p$, $p = b/d$, (ii) *if* $a = 0$ *then* $w = TS^p$, $p = d/c$, (iii) *if* $ac \neq 0$ *then* $w = S^{p_1}TS^{p_2} \dots TS^{p_{k+1}}TS^{p_{k+2}}$, *where*

$$p_i = (-1)^{i-1}Q_i \ (i = 1, \dots, k+1), \quad p_{k+2} = d/c + \sum_{s=1}^{k} (-1)^s/(R_{s-1}R_s)$$

and Q_i, R_s *are given by* (3) *with* $R_{-1} = a$, $R_0 = c$.

Proof. First observe that for every integer p,

$$S^p(z) = z+p, \quad TS^p(z) = -1/(z+p), \quad S^pT(z) = p-1/z. \tag{4}$$

Now, if (i) holds true, then $ad = 1$, so that $a/d = 1$. Hence by (4) $w = (az+b)/d = z+p = S^p(z)$, where $p = b/d$.

If (ii) holds true, then $-bc = 1$, so that $b/c = -1$. This and (4) imply that $w = b/(cz+d) = -1/(z+p) = TS^p(z)$, where $p = d/c$.

Finally, if (iii) is satisfied, we shall now decompose

$$w = (az+b)/(cz+d), \quad a \neq 0, \quad c \neq 0, \quad ad-bc = 1,$$

into a finite product of powers of S and T.

By (3) we have

$$w = \frac{R_{-1}z+B_{-1}}{R_0z+B_0} = \frac{R_0Q_1z+R_1z+B_{-1}}{R_0z+B_0} = \frac{Q_1(R_0z+B_0)+R_1z+B_{-1}-Q_1B_0}{R_0z+B_0}$$

$$= Q_1 - \frac{1}{\alpha_1} = S^{p_1}T\alpha_1,$$

where $R_{-1} = a$, $R_0 = c$, $B_{-1} = b$, $B_0 = d$, $p_1 = Q_1$ and

$$\alpha_1 = (-1)\frac{R_0z+B_0}{R_1z+B_1}, \quad B_1 = B_{-1}-Q_1B_0.$$

Again by (3),

$$\alpha_1 = (-1)\frac{R_1Q_2z+R_2z+B_0}{R_1z+B_1} = -Q_2 - \frac{1}{\alpha_2} = S^{p_2}T\alpha_2,$$

where

$$\alpha_2 = (-1)^2\frac{R_1z+B_1}{R_2z+B_2}, \quad B_2 = B_0-Q_2B_1, \quad p_2 = -Q_2.$$

By induction we get $w = S^{p_1}TS^{p_2} \dots TS^{p_s}T\alpha_s$, where

$$\alpha_s = (-1)^s\frac{R_{s-1}z+B_{s-1}}{R_sz+B_s}, \quad B_s = B_{s-2}-Q_sB_{s-1}, \tag{5}$$

$$p_s = (-1)^{s-1}Q_s \quad (s = 1, \dots, k).$$

For $s = k$ we get

$$\alpha_k = (-1)^k \frac{R_{k-1}z + B_{k-1}}{R_k z + B_k} = (-1)^k Q_{k+1} + \frac{(-1)^k B_{k+1}}{R_k z + B_k}, \qquad B_{k+1} = B_{k-1} - Q_{k+1} B_k .$$

To get the required decomposition we shall now calculate $R_k B_{k+1}$ and $R_k B_k$. By (3) and (5) we have $R_k B_{k+1} = R_k(B_{k-1} - Q_{k+1} B_k) = R_k B_{k-1} - R_{k-1} B_k = R_k B_{k-1} - R_{k-1}(B_{k-2} - Q_k B_{k-1}) = (R_k + Q_k R_{k-1}) B_{k-1} - R_{k-1} B_{k-2} = R_{k-2} B_{k-1} - R_{k-1} B_{k-2} = (-1)(R_{k-1} B_{k-2} - R_{k-2} B_{k-1})$. By induction we get

$$R_k B_{k+1} = (-1)^s (R_{k-s} B_{k-s-1} - R_{k-s-1} B_{k-s}) \qquad (s = 1, \ldots, k) .$$

Hence

$$R_k B_{k+1} = (-1)^k (R_0 B_{-1} - R_{-1} B_0) = (-1)^k (cb - ad) = (-1)^{k+1}$$

and

$$R_{k-s} B_{k-s-1} - R_{k-s-1} B_{k-s} = (-1)^{k+1-s} \qquad (s = 1, \ldots, k) .$$

Therefore

$$B_s/R_s - B_{s-1}/R_{s-1} = (-1)^s/(R_{s-1} R_s) \qquad (s = 1, \ldots, k)$$

whence

$$B_k/R_k = d/c + \sum_{s=1}^{k} (-1)^s/(R_{s-1} R_s) .$$

It follows from (2) that $|R_k| = 1$. So $B_k/R_k = R_k B_k$ and

$$\alpha_k = (-1)^k Q_{k+1} + \frac{(-1) R_k B_{k+1}}{z + R_k B_k} = (-1)^k Q_{k+1} + \frac{-1}{z + R_k B_k} .$$

Therefore $\alpha_k = S^{p_{k+1}} T S^{p_{k+2}}$, where $p_{k+1} = (-1)^k Q_{k+1}$ and $p_{k+2} = R_k B_k$.

Observe that our decomposition of w may be written equivalently in the form of the following continued fraction,

$$w = Q_1 + \cfrac{-1}{-Q_2 + \cfrac{-1}{Q_3 + \ddots + \cfrac{-1}{(-1)^k Q_{k+1} + \cfrac{-1}{z + R_k B_k}}}} .$$

2. EVEN MODULAR GROUP

To get the decomposition of an even modular transformation we introduce the following modification of the Euclid's Algorithm. Given any two integers R_{-1} and R_0 different from zero, let $R_i \neq 0$ $(i = 1, \ldots, s)$ denote the successive re-

mainders and let Q_i $(i=1,\ldots,s)$ denote the successive quotients in the algorithm to be defined, so that

$$R_{i-1}=2Q_{i+1}R_i+R_{i+1} \quad (|R_{i+1}|\leqslant|R_i|, \quad i=0,\ldots,s-1). \tag{6}$$

There exists a unique integer t such that R_{s-1} belongs to the interval $[2(t-1)R_s, 2tR_s]$ of the real axis. Define Q_{s+1} by the condition

$$|2Q_{s+1}R_s-R_{s-1}|=\min(|R_{s-1}-2(t-1)R_s|, |2tR_s-R_{s-1}|)$$

and put $R_{s+1}=R_{s-1}-2Q_{s+1}R_s$. It follows from the definition of Q_{s+1} that $2Q_{s+1}R_s$ is identical with this end of the interval $[2(t-1)R_s, 2tR_s]$ which is closer to R_{s-1}. Since the length of the interval is equal to $2|R_s|$, we have $|R_{s+1}|\leqslant|R_s|$. The described procedure may be continued further if $R_s\neq 0$.

Lemma. *If the integers $R_{-1}\neq 0$, $R_0\neq 0$ in algorithm are neither even nor odd then there is k such that $R_{k+1}=0$ and $R_i\neq 0$ for $i=1,\ldots,k$.*

Indeed, it follows from (6) that R_{i-1}, R_i are neither even nor odd together. Therefore $|R_{i-1}|>|R_i|$, whence the Lemma follows.

It is well known ([3], [4]) that given any member G of the even modular group,

$$G(z)=(az+2b)/(2cz+d), \quad ad-4bc=1, \tag{7}$$

we may write it as a finite product of the transformations

$$S(z)=z+2, \quad T(z)=z/(2z+1).$$

We shall describe a procedure which leads to an effective decomposition of G into a finite product of S and T.

Theorem 2. *Let G be an even modular transformation given by (7). Then (i) if $c=0$ then $G=S^p$, where $p=b/d$, (ii) if $c=a$ then $G=TS^p$, where $p=bc$, (iii) if $c\neq 0$, $c\neq a$ then $G=TS^{p_1}T^{\varepsilon_1}S^{p_2}\ldots T^{\varepsilon_{k+1}}S^{p_{k+1}}$, where*

$$\varepsilon_i=(-1)^{\sum_{s=1}^{i}(1+Q_s)}, \quad p_i=\frac{1}{2}\left[(-1)^iQ_i-\frac{\varepsilon_{i-1}+\varepsilon_i}{2}\right] \quad (i=1,\ldots,k+1),$$

$$p_{k+2}=\frac{1}{4}\left[\frac{d}{c}+\sum_{s=0}^{k}\frac{(-1)^{s-1}}{R_{s-1}R_s}-\varepsilon_{k+1}\right], \quad R_{-1}=c, \quad R_0=a-c$$

and R_s $(s=1,\ldots,k)$ are given by (6).

Proof. Since (i) and (ii) may be easily checked we shall prove only (iii). First observe that we have successively

$$T^\varepsilon(z)=\frac{\varepsilon}{2}+\frac{-1/4}{\frac{\varepsilon}{2}+z} \quad (\varepsilon=1,-1), \quad S^p(z)=z+2p \quad (p=0,\pm1,\pm2,\ldots)$$

and

$$TS^{p_1}(z) = \frac{1}{2} + \frac{-1/4}{2p_1 + \frac{1}{2} + z},$$

$$TS^{p_1}T^{\varepsilon_1}(z) = \frac{1}{2} + \frac{-1/4}{2p_1 + \frac{1+\varepsilon_1}{2} + \frac{-1/4}{\frac{\varepsilon_1}{2} + z}},$$

(8) .....

$$TS^{p_1}T^{\varepsilon_1}\dots T^{\varepsilon_i}S^{p_{i+1}}(z)$$

$$= \frac{1}{2} + \cfrac{-1/4}{2p_1 + \cfrac{1+\varepsilon_1}{2} + \cfrac{-1/4}{2p_1 + \cfrac{\varepsilon_1+\varepsilon_2}{2} + \ddots + \cfrac{-1/4}{2p_i + \cfrac{\varepsilon_{i-1}+\varepsilon_i}{2} + \cfrac{-1/4}{2p_{i+1} + \cfrac{\varepsilon_i}{2} + z}}}},$$

where $\varepsilon_s = 1$ or -1 $(s = 1, \dots, i)$, p_s $(s = 1, \dots, i+1)$ are arbitrary integers. Observe that

$$G(z) = \frac{1}{2} + \frac{2(a-c)z + 4b - d}{2(2cz+d)} = \frac{1}{2} + \frac{2R_0 z + B_0}{2(2R_{-1}z + B_{-1})} = \frac{1}{2} + \frac{-1/4}{\alpha_0},$$

where $R_{-1} = c$, $R_0 = a-c$, $B_{-1} = d$, $B_0 = 4b-\mathrm{d}$ and

$$\alpha_0 = -\frac{2R_{-1}z + B_{-1}}{2(2R_0 z + B_0)}.$$

It follows from the equation $ad-4bc = 1$ that a is odd and consequently R_{-1} and R_0 are neither even nor odd together. By the Lemma there is k such that $R_s \neq 0$ $(s = 1, \dots, k)$ and $R_{k+1} = 0$, where R_s is defined by (6).

Using (6) we get

$$\alpha_0 = (-1)\frac{2(2R_0 Q_1 + R_1)z + B_1}{2(2R_0 z + B_0)} = -Q_1 + \frac{-1/4}{\alpha_1},$$

where

$$\alpha_1 = (-1)^2 \frac{2R_0 z + B_0}{2(2R_1 z + B_1)}, \quad B_1 = B_{-1} - 2B_0 Q_1.$$

By induction we get

(9) $$\alpha_s = (-1)^{s+1}Q_{s+1} + (-1)^{s+1}\frac{2R_{s+1}z + B_{s+1}}{2(2R_s z + B_s)},$$

$$B_{s+1} = B_{s-1} - Q_{s+1}B_s \quad (s = 0, \dots, k).$$

In particular

$$(10)\qquad a_k=(-1)^{k+1}Q_{k+1}+(-1)^{k+1}\frac{B_{k+1}}{2(2R_kz+B_k)},\qquad B_{k+1}=B_{k-1}-2Q_{k+1}B_k,$$

since $R_{k+1}=0$.

It follows from (6) that R_k is a common divisor of R_{-1} and R_0, whence, in view of the equation $ad-4bc=1$, we get $|R_k|=1$.

Observe that, by (10), (6) and (9),

$$\begin{aligned}R_kB_{k+1}&=R_kB_{k-1}-2Q_{k+1}R_kB_k=R_kB_{k-1}-R_{k-1}B_k\\&=R_kB_{k-1}-R_{k-1}(B_{k-2}-2Q_kB_{k-1})=(R_k+2Q_kR_{k-1})B_{k-1}-R_{k-1}B_{k-2}\\&=R_{k-2}B_{k-1}-B_{k-2}R_{k-1}=(-1)(R_{k-1}B_{k-2}-R_{k-2}B_{k-1}).\end{aligned}$$

By induction we get

$$R_kB_{k+1}=(-1)^s(R_{k-s}B_{k-s-1}-R_{k-s-1}B_{k-s})\qquad(s=0,\dots,k)$$

whence

$$\begin{aligned}R_kB_{k-1}&=(-1)^k(R_0B_{-1}-R_{-1}B_0)=(-1)^k[(a-c)d-c(4b-d)]\\&=(-1)^k(ad-4bc)=(-1)^k\end{aligned}$$

and

$$R_{k-s}B_{k-s-1}-R_{k-s-1}B_{k-s}=(-1)^{k-s}\qquad(s=0,\dots,k).$$

Therefore

$$\frac{B_s}{R_s}-\frac{B_{s-1}}{R_{s-1}}=\frac{(-1)^{s-1}}{R_{s-1}R_s}\qquad(s=0,\dots,k),$$

whence

$$R_kB_k=\frac{B_k}{R_k}=\frac{d}{c}+\sum_{s=0}^{k}\frac{(-1)^{s-1}}{R_{s-1}R_s}.$$

Therefore a_k may be written in the form

$$a_k=(-1)^{k+1}Q_{k+1}+(-1)^{k+1}\frac{R_kB_{k+1}}{2(2z+R_kB_k)}=(-1)^{k+1}Q_{k+1}+\frac{-1/4}{B'_k+z},\qquad B'_k=\frac{1}{2}R_kB_k.$$

So G may be written in the form of the following continued fraction

$$(11)\qquad G(z)=\frac{1}{2}+\cfrac{-1/4}{-Q_1+\cfrac{-1/4}{Q_2+\ddots+\cfrac{-1/4}{Q_{k+1}(-1)^{k+1}+\cfrac{-1/4}{B'_k+z}}}}.$$

It may be easily checked that all the numbers

$$\varepsilon_0 = 1, \quad \varepsilon_i = (-1)^{\sum_{s=1}^{i}(1+Q_s)}, \quad p_i = \frac{1}{2}\left[(-1)^i Q_i - \frac{\varepsilon_{i-1}+\varepsilon_i}{2}\right] \quad (i = 1, \ldots, k+1),$$

are integers and that they satisfy the following equation

$$(-1)^i Q_i = 2p_i + \frac{\varepsilon_{i-1}+\varepsilon_i}{2} \quad (i = 1, \ldots, k+1). \tag{12}$$

Let us write the integer $R_k B_k$ first in the form

$$R_k B_k = 4p'_{k+2} + r \quad (0 \leqslant |r| < 4)$$

and next in the form

$$R_k B_k = (4p'_{k+2} + \varepsilon_{k+1}) + (r - \varepsilon_{k+1}). \tag{13}$$

Now in view of (8), (11), (12), and (13), the transformation G may be written in the form

$$G(z) = TS^{p_1}T^{\varepsilon_1} \ldots S^{p_{k+1}}T^{\varepsilon_{k+1}}S^{p'_{k+2}}L(z) = z + \frac{r-\varepsilon_{k+1}}{2}.$$

Since $L = S^{-p'_{k+2}}T^{-\varepsilon_{k+1}} \ldots T^{-1}G$ is a composition of even transformations, L itself has to be even. Therefore $L(z) = S^{(r-\varepsilon_{k+1})/4}$ and $G = TS^{p_1}T^{\varepsilon_1} \ldots T^{\varepsilon_{k+1}}S^{p_{k+2}}$, where

$$p_{k+2} = p'_{k+2} + \frac{r-\varepsilon_{k+1}}{4} = \frac{2B'_k - \varepsilon_{k+1}}{4} = \frac{1}{4}\left[\frac{d}{c} + \sum_{s=0}^{k} \frac{(-1)^{s-1}}{R_{s-1}R_s} - \varepsilon_{k+1}\right].$$

REFERENCES

[1] L. Ford, *Automorphic Functions*, New York 1929.

[2] F. Klein, *Vorlesungen über die Teorie der elliptischen Modulfunctionen*, Leipzig 1890.

[3] F. Leja, *Teoria funkcji analitycznych*, Warszawa 1957.

[4] H. Bateman, *Higher Transcendental Functions*, vol. 3, New York 1955.