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}.