CONGRUENCE SUBGROUPS OF POSITIVE GENUS OF THE MODULAR GROUP

BY

M. I. KNOPP AND M. NEWMAN

1. Introduction

Let $\Gamma$ be the modular group, consisting of all linear fractional transformations

$$\tau' = \frac{a\tau + b}{c\tau + d}$$

where $a, b, c, d$ are rational integers and $ad - bc = 1$. It is not difficult to construct a sequence of subgroups $G_n$ of finite index in $\Gamma$ such that $(\Gamma:G_n) \to \infty$ as $n \to \infty$, but such that the genus of $G_n$ is 0. (See papers [1], [4] and [6].) In conversation with the authors H. Rademacher conjectured that such a construction was not possible using congruence subgroups of $\Gamma$, and in fact that the number of congruence subgroups of $\Gamma$ having genus 0 is finite. Whether this conjecture is true or not we do not know. It is both plausible and difficult. In this note we make a contribution to this problem. In fact we prove that a free congruence subgroup of $\Gamma$ of level prime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ is necessarily of positive genus. We also prove inclusion theorems for certain subgroups of $\Gamma$ which are of independent interest.

2. Preliminary results and definitions

We find it convenient to work with the representation of $\Gamma$ as the multiplicative group of $2 \times 2$ rational integral matrices of determinant 1 modulo its centrum $\{\pm I\}$, where $I$ is the identity matrix. If $n$ is a positive integer, then $\Gamma(n)$ will denote the principal congruence subgroup of $\Gamma$ of level $n$, which consists of all elements of $\Gamma$ congruent modulo $n$ to $\pm I$. $\Gamma(n)$ is a normal subgroup of $\Gamma$. A subgroup of $\Gamma$ is a congruence subgroup if it contains a group $\Gamma(n)$; it is of level $n$ if $n$ is the least such integer. We set

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}. $$

Then $\Gamma$ may be generated by $S$ and $W$;

$$\Gamma = \{S, W\}.$$ 

An element of $\Gamma$ is parabolic if it is of trace $\pm 2$; it is then conjugate over $\Gamma$ to a power of $S$. If $M \in \Gamma$ and commutes with a non-trivial power of $S$ then $M$ itself is a power of $S$. 

Received March 28, 1964.