CONGRUENCE SUBGROUPS OF POSITIVE GENUS OF THE MODULAR GROUP

BY

M. I. Knopp and M. Newman

1. Introduction

Let Γ 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 Γ 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 Γ, and in fact that the number of congruence subgroups of Γ 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* Γ *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 Γ which are of independent interest.

2. Preliminary results and definitions

We find it convenient to work with the representation of Γ as the multiplicative group of 2×2 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 Γ of *level n*, which consists of all elements of Γ congruent modulo n to $\pm I$. $\Gamma(n)$ is a normal subgroup of Γ. A subgroup of Γ 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

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

Then Γ may be generated by S and W;

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

An element of Γ is *parabolic* if it is of trace ± 2; it is then conjugate over Γ 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.

Let G be a subgroup of Γ of finite index μ. By a *complete system of parabolic representatives*, abbreviated c.s.p.r., we understand a set of parabolic elements $P_1, P_2, \cdots, P_t$ of G such that

(1) every parabolic element of G is conjugate over G to some power of a P_i, $1 \leq i \leq t$;
(2) no non-trivial power of P_i is conjugate over G to a power of P_j, $1 \leq i$, $j \leq t$, $i \neq j$.

Then t is the number of *parabolic classes* of G.

(It is easy to see that for a subgroup of finite index in Γ, t is finite.)

It is an easy consequence of (1), (2) and of the properties of S that if $M \in G$ and commutes with some non-trivial power of P_i, it is itself a power of P_i, $1 \leq i \leq t$.

The group G is free if and only if it contains no elements of finite order (see 5]). In this case the genus g of G is given very simply by the formula

$$g = 1 + \mu/12 - t/2. \tag{3}$$

(This is a straightforward consequence of the "hyperbolic area formula", which in turn can be deduced from [3, p. 185, excercise 2].)

The congruence subgroup generated by S, $\Gamma(n)$ will be denoted by Γ_n :

$$\Gamma_n = \{S, \Gamma\ (n)\} = \textstyle\sum_{k=0}^{n-1} S^k\Gamma(n). \tag{4}$$

The congruence subgroup consisting of all elements $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of Γ such that $c \equiv 0 \pmod{n}$ will be denoted by $\Gamma_0(n)$, and the genus of $\Gamma_0(n)$ by g_n. The genus g_n has been computed explicitly (see [2]). We note only that if p is a prime, then

$$\begin{aligned} g_p &= (p - 13)/12, & p &\equiv 1 \pmod{12} \\ &= (p - 5)/12, & p &\equiv 5 \pmod{12} \\ &= (p - 7)/12, & p &\equiv 7 \pmod{12} \\ &= (p + 1)/12, & p &\equiv 11 \pmod{12}. \end{aligned} \tag{5}$$

Hence $g_p \geq (p - 13)/12$.

We set

$$\begin{aligned} \mu(n) = (\Gamma\!:\!\Gamma(n)) &= 6, & n &= 2 \\ &= \tfrac{1}{2}n^3 \textstyle\prod_{p|n} (1 - 1/p^2), & n &> 2. \end{aligned}$$

Then (4) implies that

$$(\Gamma\!:\!\Gamma_n) = \mu(n)/n.$$

If G, H are subgroups of finite index in Γ such that $G \supset H$, and if the genera of G, H are g, h respectively then the genus formula for subgroups (see [3, p. 260]) implies that $g \leq h$. In particular this implies that $g_d \leq g_n$, whenever $d|n$.

3. An inclusion theorem

In this section we prove an inclusion theorem for subgroups of Γ containing Γ_n, which is of interest in itself:

THEOREM 1. *Suppose that* $\Gamma \supset G \supset \Gamma_n$. *Then either* $G = \Gamma$ *or* $G \subset \Gamma_0(d)$ $d \mid n$, $d > 1$.

We break the proof up into a sequence of lemmas.

LEMMA 1. *Suppose that* $\Gamma \supset G \supset \Gamma_n$. *Suppose further that* G *contains an element*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $(c, n) = 1$. *Then* $G = \Gamma$.

Proof. We have

$$S^x M = \begin{pmatrix} a + xc & b + xd \\ c & d \end{pmatrix}.$$

Since $(c, n) = 1$, x may be chosen so that $a + xc \equiv 1 \pmod{n}$. Put $b_1 = b + x\,d$. Then

$$S^x M \equiv \begin{pmatrix} 1 & b_1 \\ c & 1 + b_1 c \end{pmatrix} \pmod{n},$$

$$S^x M \equiv W^c S^{b_1} \pmod{n}.$$

Hence $S^x M = W^c S^{b_1} M_1$, $M_1 \in \Gamma(n)$, and it follows that $W^c \in G$. Since $(c, n) = 1$ and $W^n \in G$, this implies that $W \in G$. Hence $G = \Gamma$, since $S, W \in G$ and are generators of Γ.

Lemma 1 implies

LEMMA 2. *Let* p *be a prime,* $\Gamma \supset G \supset \Gamma_p$. *Then either* $G = \Gamma$ *or* $G \subset \Gamma_0(p)$.

Lemma 2 is the case n prime of the lemma that follows:

LEMMA 3. *Suppose that* n *is square-free,* $\Gamma \supset G \supset \Gamma_n$. *Then either* $G = \Gamma$ or $G \subset \Gamma_0(d)$, $d \mid n$, $d > 1$.

Proof. The proof will be by induction on $\Omega(n)$, the number of primes dividing n. For $\Omega(n) = 0$ the lemma is trivial, and for $\Omega(n) = 1$ the lemma is true by Lemma 2. Assume the lemma proved for all square-free m such that $\Omega(m) < k$, and let n be square-free with $\Omega(n) = k$, $k \geq 2$. Let p be the smallest prime dividing n. Then $n/p > 2$ and

$$G\Gamma(n/p) \supset \Gamma_{n/p}.$$

Since $\Omega(n/p) = k - 1$, the induction hypothesis implies that either

$$G\Gamma(n/p) \subset \Gamma_0(d), \qquad d \mid n/p,\ d > 1 \tag{6}$$

or

$$G\Gamma(n/p) = \Gamma. \tag{7}$$

Since (6) implies that $G \subset \Gamma_0(d)$, where $d \mid n$, $d > 1$ we may assume that (7) holds. Then by one of the isomorphism theorems

$$\Gamma/\Gamma(n/p) \cong G/G \cap \Gamma(n/p). \tag{8}$$

Put $\mu = (\Gamma : G)$. Since

$$G \cap \Gamma(n/p) \supset \{S^{n/p}, \Gamma(n)\},$$

$(\Gamma : \{S^{n/p}, \Gamma(n)\}) = \mu(n)/p$, and $(p, n/p) = 1$, it follows from (8) that

$$\mu(n/p) \mid \frac{\mu(n)/p}{\mu},$$

$$\mu \mid p^2 - 1. \tag{9}$$

Now let q be the exponent of W modulo G. Since $W^n \in G$, $q \mid n$. Furthermore the cosets G, WG, W^2G, $\cdots$, $W^{q-1}G$ are distinct. Thus $q \leq \mu$. Combined with (9), this implies that $q \leq p^2 - 1$. Since n is square-free and since p is the smallest prime dividing n, q is either 1 or a prime. If $q = 1$ then $G = \Gamma$, since then W, $S \in G$ and W, S generate Γ. Suppose then that q is prime. Either $G \subset \Gamma_0(q)$, or there is an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ such that $(c, q) = 1$. Assume the latter. Then

$$W^{qx}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c + xqa & d + xqb \end{pmatrix},$$

and since $(c, qa) = 1$, x may be chosen so that $(c + xqa, n) = 1$ (for example, by Dirichlet's theorem on primes in arithmetic progressions). By Lemma 1, $G = \Gamma$. Hence in all cases we have shown that either $G = \Gamma$ or $G \subset \Gamma_0(d)$, $d \mid n$, $d > 1$ and the proof of the lemma is complete.

LEMMA 4. *Suppose that n is square-free, and suppose that m is an integer divisible only by primes dividing n. Then if*

$$\Gamma \supset G \supset \Gamma_{mn},$$

either $G = \Gamma$ or $G \subset \Gamma_0(d)$, $d \mid mn$, $d > 1$.

Proof. Assume that $G \neq \Gamma$. We have that

$$G\Gamma(n) \supset \Gamma_n.$$

By Lemma 3, either

$$G\Gamma(n) \subset \Gamma_0(d), \qquad d \mid n, d > 1 \tag{10}$$

or

$$G\Gamma(n) = \Gamma. \tag{11}$$

If (10) holds, then $G \subset \Gamma_0(d)$, $d \mid mn$, $d > 1$ and the proof of the lemma is concluded. We need only show that (11) cannot hold. Since $G \neq \Gamma$, it follows from Lemma 1 that if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G,$$

then $(c, mn) > 1$; and hence $(c\ n) > 1$ since every prime dividing m also divides n. Thus if $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G\Gamma(n)$ then $(\gamma, n) > 1$ and so (11) can not hold. The proof of the lemma is concluded.

Combining the previous lemmas, we obtain the theorem.

4. The parabolic class number formula

We are going to develop a formula involving parabolic class numbers for subgroups of the modular group. The formula actually holds for subgroups of finite index in an arbitrary H-group (see [3, p. 266] for the definition) but we content ourselves with the statement for the modular group. We will prove

THEOREM 2. *Let G, H be subgroups of finite index in Γ, H a normal subgroup of G, $(G:H) = \mu$. Let $P_1, P_2, \cdots, P_t$ be a c.s.p.r. for G, and suppose that P_i is of exponent m_i modulo H, $1 \leq i \leq t$. Then the number τ of parabolic classes of H is given by*

$$\tau = \mu \textstyle\sum_{i=1}^{t} 1/m_i .$$

Proof. Let P by any parabolic element of H. Since $P \in G$, $P = AP_i^{\alpha} A^{-1}$ where $A \in G$, α is a non-zero integer, and $1 \leq i \leq t$. Since H is a normal subgroup of G, $P_i^{\alpha} \in H$; and so $\alpha = \beta m_i$. Hence $P = AP_i^{\beta m_i}A^{-1}$. Now $AP_i^{\beta m_i}A^{-1}$ and $AP_i^{m_i}A^{-1}$ belong to the same parabolic class, since $AP_i^{m_i}A^{-1} \in H$. Thus we need only determine for each i, $1 \leq i \leq t$, the number of expressions

$$Q = AP_i^{m_i}A^{-1}, \qquad A \in G,$$

which are not conjugate over H. (Because of (2), two expressions Q corresponding to different subscripts i cannot be conjugate over G and so are certainly not conjugate over H.)

Suppose that

$$G = \textstyle\sum_{k=1}^{\mu} HR_k$$

is a right coset decomposition of G modulo H. Then A may be written as BR_k, where $B \in H$ and $1 \leq k \leq \mu$. Thus

$$Q = AP_i^{m_i} A^{-1} = BR_k P_i^{m_i}R_k^{-1}B^{-1},$$

and so Q is conjugate over H to

$$R_k P_i^{m_i}R_k^{-1}.$$

Furthermore the group G/H has the cyclic subgroup $K_i = \{HP_i\}$ of order m_i. Hence we can write

$$HR_k = HS_j P_i^{n_k}$$

where HS_j, $1 \leq j \leq \mu/m_i$ runs over the coset representatives of G/H modulo K_i and n_k is an integer. It follows that Q is conjugate over H to

$$S_j P_i^{m_i} S_j^{-1}, \qquad 1 \leq j \leq \mu/m_i. \tag{12}$$

The expressions (12) for a fixed i are not conjugate over H. For suppose that

$$S_j P_i^{m_i} S_j^{-1} = T S_l P_i^{m_i} S_l^{-1} T^{-1},$$

$T \in H$, $1 \leq j, l \leq \mu/m_i$. Put $M = S_j^{-1} T S_l$. Then M commutes with $P_i^{m_i}$ and so must be a power of P_i. Thus for some integer γ

$$TS_l = S_j P_i^{\gamma}.$$

But this implies that $j = l$, since the HS_j's are distinct modulo K_i. It follows that the number of parabolic classes in H arising from P_i is just μ/m_i, and the theorem follows by summation.

Easy corollaries of Theorem 2 for normal subgroups of Γ follows:

COROLLARY 1. *Let G be a normal subgroup of Γ such that $(\Gamma:G) = \mu$ and such that S is of exponent m modulo G. Then the number of parabolic classes t of G is given by $t = \mu/m$.*

COROLLARY 2. *The number of parabolic classes of $\Gamma(n)$ is $\mu(n)/n$.*

5. The principal results

We assume now that G is a congruence subgroup of Γ of level n. We continue to denote the number of parabolic classes of G by t, and $(\Gamma:G)$ by μ. Let $P_1, P_2, \cdots, P_t$ be a c.s.p.r. for G and assume that P_i is of exponent m_i modulo $\Gamma(n)$, $1 \leq i \leq t$. Then the results of Section 4 imply that

$$\frac{\mu(n)}{n} = \frac{\mu(n)}{\mu} \sum_{i=1}^{t} \frac{1}{m_i}, \qquad \mu = n \sum_{i=1}^{t} \frac{1}{m_i}. \tag{13}$$

Since the n-th power of *any* parabolic element of Γ is in $\Gamma(n)$, each m_i is a divisor of n. For each divisor d of n let $r(d)$ be the number of P_i for which $m_i = d$, $1 \leq i \leq t$. Then

$$\begin{aligned} \textstyle\sum_{d|n} r(n/d) &= t, \\ \textstyle\sum_{d|n} d r(n/d) &= \mu. \end{aligned} \tag{14}$$

Assume now that G is free. Then (3), (13) and (14) imply that the genus g of G is given by

$$g = (1/12) \textstyle\sum_{d|n} (d-6) r(n/d) + 1. \tag{15}$$

Assume further that $(n, 2.3.5) = 1$. Let q be the smallest prime dividing n. Suppose first that $r(n) = 0$. Then (15) implies that

$$g \geq 1 + (q-6)/12 = (q+6)/12.$$

Now suppose that $r(n) > 0$; i.e. that some conjugate of S, say ASA^{-1}, belongs to G. The groups G and $A^{-1}GA$ being conjugate subgroups of Γ are simultaneously free, of level n, and of the same genus. There is no loss of generality therefore in assuming that $S \in G$, so that $G \supset \Gamma_n$. Then Theorem 1 implies that $G \subset \Gamma_0(d)$, $d \mid n$, $d > 1$. Hence

$$g \geq g_d \geq \min_{p|n} g_p$$

and so by (5),

$$g \geq \min_{p|n} (p - 13)/12 = (q - 13)/12.$$

It follows that in either case

$$g \geq \min_{p|n} g_p \geq (q - 13)/12.$$

We have proved therefore

THEOREM 3. *Let G be a free congruence subgroup of Γ of level n, where $(n, 2 \cdot 3 \cdot 5) = 1$. Let q be the least prime dividing n. Then the genus g of G satisfies*

$$g \geq \min_{p|n} g_p \geq (q - 13)/12.$$

Theorem 3 and (5) readily imply the result mentioned in the introduction:

THEOREM 4. *A free congruence subgroup of Γ of level prime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ is of positive genus.*

REFERENCES

1. R. FRICKE, *Ueber die Substitutionsgruppen, welche zu den aus dem Legendre'schen Integralmodul $k^2(\omega)$ gezogen Wurzeln gehören*, Math. Ann., vol. 28 (1887), pp. 99–118.
2. E. HECKE, *Analytische Arithmetik der positiven quadratischen Formen*, Kungl. Danske Videnskabernes Selskab. Mathematisk-fysiske Meddelelser, vol. 17 (1940), p. 12.
3. J. LEHNER, *Discontinuous groups and automorphic functions*, Amer. Math. Soc. Mathematical Surveys, no. 8, 1964.
4. M. NEWMAN, *On a problem of G. Sansone*, Ann. Mat. Pura Appl. (4), vol. 65 (1964), pp. 27–34.
5. ———, *Free subgroups and normal subgroups of the modular group*, Illinois J. Math., vol. 8 (1964), pp. 262–265.
6. G. PICK, *Ueber gewisse ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen*, Math. Ann., vol. 28 (1887), pp. 119–124.

NATIONAL BUREAU OF STANDARDS
WASHINGTON, D.C.