MAXIMAL NORMAL SUBGROUPS OF THE MODULAR GROUP

MORRIS NEWMAN

1. **Introduction.** The purpose of this paper is to initiate the study of the maximal normal subgroups G of the modular group Γ; i.e. those normal subgroups G such that Γ/G is simple. The principal congruence subgroups $\Gamma(p)$ of prime level $p>3$ are such groups, since

$$\Gamma/\Gamma(p) \cong \mathrm{LF}(2, p).$$

However, these are not the only groups with quotient groups isomorphic to $\mathrm{LF}(2, p)$; and we shall show that for a given p there are in general many normal subgroups G of differing levels such that

$$\Gamma/G \cong \mathrm{LF}(2, p).$$

Furthermore, those of level $\neq p$ are not congruence groups. It is well known that Γ contains infinitely many normal subgroups of finite index which are not congruence groups; see for example papers [3], [4]. However, all of these groups have the common feature that they are "lattice subgroups" (in Rankin's terminology) of some normal congruence group, and so are not maximal. The results of this paper imply that Γ contains infinitely many maximal normal subgroups of finite index which are not congruence groups, a somewhat surprising fact.

The question which originally motivated this paper was the following: Which of the known simple groups have a representation as a modular quotient group, or equivalently, may be generated by two elements, one of period 2, the other of period 3? Call such a group a Γ-group. Then the groups $\mathrm{LF}(2, p)$ are certainly Γ-groups. However, it is not known for example when the alternating group is a Γ-group. In his lecture notes on Fuchsian groups [2], Macbeath poses a similar question for H-groups, and makes some remarks about the linear fractional groups which in fact form the basis of this paper, and which we are happy to acknowledge here.

2. **Definitions and notation.** The modular group Γ is the totality of linear fractional transformations

$$\tau' = (a\tau + b)/(c\tau + d) \tag{1}$$

where a, b, c, d are rational integers and $ad-bc=1$. It is known that

Received by the editors May 15, 1967.

$\Gamma = \{S, T\}$, the group generated by S and T, where

$$S\tau = \tau + 1, \qquad T\tau = -1/\tau$$

and in fact $\Gamma = \{T\} * \{TS\}$, the free product of the cyclic group $\{T\}$ of order 2 and the cyclic group $\{TS\}$ of order 3. If G is a normal subgroup of Γ of finite index, then the *level* of G is defined as the exponent of S modulo G; i.e. the least positive integer n such that $S^n\tau = \tau + n$ belongs to G. The *principal congruence subgroup* $\Gamma(n)$ of Γ is the totality of elements (1) of Γ such that $a \equiv d \equiv \pm 1 \bmod n$, $b \equiv c \equiv 0 \bmod n$. A *congruence subgroup* of Γ is one which contains a principal congruence subgroup.

In what follows p is a prime >3 and q a power of p. LF(2, q) has its customary meaning, and is best thought of as the group of 2×2 matrices of determinant 1 with entries from GF(q), in which a matrix and its negative are identified.

3. Preliminary results. In this section we prove some facts about GF(q) and LF(2, q) which will find later application.

LEMMA 1. *Let a, b, c be elements of* GF(q) *such that $b^2 - 4ac = \Delta \neq 0$. Then for any elements d, e, f of* GF(q) *the equation*

$$ax^2 + bxy + cy^2 = d + ex + fy \tag{2}$$

has solutions in GF(q).

PROOF. We first prove that for any element d of GF(q) the equation

$$x^2 - \Delta y^2 = d \tag{3}$$

has solutions in GF(q). Let θ be a primitive element of GF(q). Let Q be the set

$$Q = \{0, 1, \theta, \theta^2, \cdots, \theta^{(q-3)/2}\}.$$

The values assumed by x^2 for x in Q consist of $(q+1)/2$ distinct elements of GF(q), and the same is true of the values assumed by $\Delta y^2 + d$ for y in Q. Since GF(q) contains just q distinct elements, there must be elements x, y of Q such that $x^2 = \Delta y^2 + d$. Thus we have shown that (3) has solutions in GF(q).

We now show that (2) has solutions in GF(q). Suppose first that $a = c = 0$. Then $b \neq 0$, and (2) becomes

$$(x - f/b)(y - e/b) = d/b + ef/b^2$$

which clearly has solutions in GF(q). Now suppose that $a \neq 0$, say. Then (2) is equivalent to

$$(2ax + by - e)^2 - \Delta(y + (1/\Delta)(2af - eb))^2$$
$$= (1/\Delta)(e^2\Delta + 4ad\Delta - (2af - eb)^2),$$

which certainly has solutions in GF(q), since (3) has. This concludes the proof of the lemma.

LEMMA 2. *Let t_1, t_2, t be any elements of* GF(q). *Then there are elements A, B of* LF(2, q) *such that* $\mathrm{tr}(A) = t_1$, $\mathrm{tr}(B) = t_2$ *and* $\mathrm{tr}(AB) = t$.

PROOF. Suppose first that $t_1 \neq \pm 2$. By Lemma 1, elements x, y of GF(q) may be determined so that

$$x^2 + t_1xy + y^2 + t_2x + ty + 1 = 0,$$

since $\Delta = t_1^2 - 4 \neq 0$. If $y = 0$, then $x^2 + t_2x + 1 = 0$, and we choose

$$A = \begin{pmatrix} 0 & -1 \\ 1 & t_1 \end{pmatrix}, \qquad B = \begin{pmatrix} x + t_2 & t + t_1x \\ 0 & x \end{pmatrix}.$$

If $y \neq 0$, we choose

$$A = \begin{pmatrix} 0 & -1 \\ 1 & t_1 \end{pmatrix}, \qquad B = \begin{pmatrix} x + t_2 & -y \\ (x^2 + t_2x + 1)/y & -x \end{pmatrix}.$$

In each case it is readily verified that A and B satisfy the required conditions.

Suppose now that $t_1 = \pm 2$; say $t_1 = 2$. We choose

$$A = \begin{pmatrix} 1 & t - t_2 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & t_2 \end{pmatrix}.$$

Then A, B satisfy the required conditions, and the proof of the lemma is concluded.

As a corollary of Lemma 2, we have

COROLLARY 1. *Let t be any element of* GF(q). *Then there are elements A, B of* LF(2, q) *such that A is of period 2, B is of period 3, and* $\mathrm{tr}(AB) = t$.

PROOF. We choose $t_1 = 0$, $t_2 = 1$ in Lemma 2.

LEMMA 3. *Let t be any element of* GF(q) *other than* ± 2. *Let C be any element of* LF(2, q) *such that* $\mathrm{tr}(C) = t$. *Then C is conjugate over* LF(2, q) *to*

$$\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}.$$

PROOF. Put

$$C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad t = \operatorname{tr}(C) = a + d.$$

By Lemma 1, elements x, y of $\mathrm{GF}(q)$ may be determined so that

$$-bx^2 + (a - d)xy + cy^2 = 1,$$

since $\Delta = (a-d)^2+4bc = t^2-4 \neq 0$. Set

$$U = \begin{pmatrix} x & y \\ -ax - cy & -bx - dy \end{pmatrix}.$$

Then $U \in \mathrm{LF}(2, q)$ and

$$UCU^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix}.$$

This completes the proof of the lemma.

We remark that in the "parabolic" case ($t = \pm 2$, $C \neq \pm I$) the situation is slightly different. Here every element of trace 2 in $\mathrm{LF}(2, q)$ is conjugate over $\mathrm{LF}(2, q)$ to

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{or to} \quad \begin{pmatrix} 1 & \theta \\ 0 & 1 \end{pmatrix},$$

where θ is a primitive element of $\mathrm{GF}(q)$; and these are not conjugate over $\mathrm{LF}(2, q)$.

Lemma 3 implies that all elements of $\mathrm{LF}(2, q)$ with the same trace $t \neq \pm 2$ are conjugate over $\mathrm{LF}(2, q)$.

Combining these lemmas, we have

THEOREM 1. *Let C be any element of $\mathrm{LF}(2, q)$ other than $\pm I$. Then C may be written as*

$$C = AB,$$

where $A, B \in \mathrm{LF}(2, q)$ and A is of period 2, B of period 3.

PROOF. It is only necessary to show that this is so if $\operatorname{tr}(C) = \pm 2$, and in view of the preceding remarks it suffices to take

$$C = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \qquad b \neq 0.$$

But here we may choose

$$A = \begin{pmatrix} 0 & -b \\ 1/b & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & b \\ -1/b & -1 \end{pmatrix},$$

which completes the proof of the theorem.

We also require the following elementary group-theoretic result:

LEMMA 4. *Suppose that the group G is generated by two elements x, y such that x is of period m, y is of period n and xy is of period r, where $(m, n) = (m, r) = (n, r) = 1$. Then G is not solvable.*

PROOF. It is sufficient to show that $G = G'$ (the commutator subgroup of G). In G/G', we have $1 = (xy)^r = x^r y^r$ and taking mth powers, $y^{mr} = 1$. Since $(n, mr) = 1$ and $y^n = 1$, this implies that $y = 1$; and similarly, $x = 1$. Hence G/G' is trivial and the lemma is proved.

Lemma 4 is obviously true in the more general situation when $G = \{x_1, x_2, \cdots, x_k\}$, x_i is of period m_i, $1 \leqq i \leqq k$, $x_1 x_2 \cdots x_k$ is of period m, and the integers $m, m_1, m_2, \cdots, m_k$ are pairwise relatively prime.

4. **Principal results.** We now specialize to $q = p$, and assume in what follows that $p > 5$. The structure of $\mathrm{LF}(2, p)$ and its subgroups has been completely worked out by Gierster [1]. A proper subgroup of $\mathrm{LF}(2, p)$ is

(i) a tetrahedral, octahedral or icosahedral group,

(ii) a cyclic group of order m where $m = p$ or m is any divisor of $\frac{1}{2}(p \pm 1)$,

(iii) a dihedral group,

(iv) a metacyclic group.

All of these are solvable, with the exception of the icosahedral group of order 60. It follows that a nonsolvable subgroup of $\mathrm{LF}(2, p)$ whose order is not 60 must be $\mathrm{LF}(2, p)$ itself. This remark together with our previous information gives the following result:

THEOREM 2. *Suppose that the positive integer n satisfies*

(4) $n = p$ *or* $n \mid (p \pm 1)/2$,

(5) $(n, 6) = 1$,

(6) $n > 5$.

Then there are elements $A, B \in \mathrm{LF}(2, p)$ such that A is of period 2, B is of period 3, AB is of period n, and $\mathrm{LF}(2, p) = \{A, B\}$.

PROOF. By the results of Gierster quoted above, there is an element $C \in \mathrm{LF}(2, p)$ such that C is of period n, where n is any positive integer satisfying (4). By Theorem 1, elements A, B of $\mathrm{LF}(2, p)$ exist such that A is of period 2, B is of period 3, and $C = AB$. Since the integers 2, 3, n are pairwise relatively prime, by (5), Lemma 4 implies that the group $G = \{A, B\}$ is not solvable. Hence by Gierster's results, G is either an icosahedral group or else all of $\mathrm{LF}(2, p)$. The first possibility is ruled out by condition (6), and so $G = \mathrm{LF}(2, p)$, completing the proof.

Theorem 2 may readily be extended. It is not difficult to show by the same methods that if n_1, n_2, n_3 are integers >5 such that

$$n_i = p \quad \text{or} \quad n_i \mid (p \pm 1)/2, \qquad i = 1, 2, 3, \tag{7}$$

$$(n_1, n_2) = (n_1, n_3) = (n_2, n_3) = 1, \tag{8}$$

then elements A, B of $\mathrm{LF}(2, p)$ exist such that A is of period n_1, B is of period n_2, AB is of period n_3 and $\mathrm{LF}(2, p) = \{A, B\}$.

We now apply Theorem 2 to the proof of the following theorem.

THEOREM 3. *Suppose that n satisfies conditions* (4), (5), (6). *Then there is a maximal normal subgroup G_n of Γ such that G_n is of level n, and $\Gamma/G_n \cong \mathrm{LF}(2, p)$.*

PROOF. Determine elements A, B of $\mathrm{LF}(2, p)$ as described in Theorem 2. Then the homomorphism $\phi_n: \Gamma \to \mathrm{LF}(2, p)$ defined by

$$\phi_n: T \to A, \qquad \phi_n: TS \to B$$

is actually a homomorphism of Γ onto $\mathrm{LF}(2, p)$. Let G_n be the kernel of ϕ_n. Then G_n is a normal subgroup of Γ, and $\Gamma/G_n \cong \mathrm{LF}(2, p)$.

Since $\mathrm{LF}(2, p)$ is simple, G_n is a maximal normal subgroup of Γ. Furthermore the level of G_n, which is the exponent of S modulo G_n, is just n since $\phi_n: S \to AB$ and AB is of period n. This completes the proof.

The groups G_n are certainly distinct, being of different levels, but are all of index $\frac{1}{2}p(p^2-1)$ in Γ with common quotient group $\mathrm{LF}(2, p)$.

We now define a number-theoretic function $\zeta(p)$, as the number of values of n satisfying conditions (4), (5), (6):

$$\zeta(p) = 1 + \sum_{n \mid \frac{1}{2}(p-1);\ (n,6)=1;\ n>5} 1 + \sum_{n \mid \frac{1}{2}(p+1);\ (n,6)=1;\ n>5} 1. \tag{9}$$

We require the following lemma:

LEMMA 5. *The positive integers m such that $m(m+1) = 2^a \cdot 3^b$, $2^a \cdot 3^b \cdot 5$ are $m = 1, 2, 3, 4, 5, 8, 9, 15$.*

PROOF. The proof is a straightforward enumeration of possibilities. The problem is equivalent to finding all solutions of the six equations

$$3^b - 2^a = \pm 1, \qquad 3^b - 5 \cdot 2^a = \pm 1, \qquad 5 \cdot 3^b - 2^a = \pm 1.$$

Consider, for example, the equation $3^b - 2^a = 1$. If $a = 1$, we get the solution $3 - 2 = 1$. Suppose that $a > 1$. Then $(-1)^b \equiv 1 \bmod 4$, so that b is even. Put $b = 2c$, $c \geqq 1$. Then $(3^c+1)(3^c-1) = 2^a$, so that $3^c+1 = 2^r$, $3^c-1 = 2^s$, $r > s \geqq 1$, $r+s = a$. Thus $2^r - 2^s = 2$, $2^{r-1} - 2^{s-1} = 1$. This implies that $s = 1$, $r = 2$ giving the solution $9 - 8 = 1$. The remaining cases are disposed of similarly.

Lemma 5 implies that $\zeta(p)>1$ for $p\geqq 37$. We now prove

THEOREM 4. *For each prime $p\geqq 37$, there is a maximal normal subgroup of Γ of index $\frac{1}{2}p(p^2-1)$ which is not a congruence group, and therefore there are infinitely many maximal normal subgroups of Γ of finite index which are not congruence groups.*

PROOF. Since $p\geqq 37$, Lemma 5 implies that there is an n satisfying (4), (5), (6) such that $n\neq p$. The group G_n described by Theorem 3 is thus a maximal normal subgroup of Γ of index $\frac{1}{2}p(p^2-1)$, and we need only show that G_n is not a congruence group. Suppose the contrary. Then G_n, being of level n, would have to contain the principal congruence subgroup $\Gamma(n)$, by Wohlfahrt's theorem [5]. This would imply that $(\Gamma: G_n)\,|\,(\Gamma:\Gamma(n))$, or that

$$\tfrac{1}{2}p(p^2-1)\,\Big|\,\tfrac{1}{2}n^3\prod_{q|n}\left(1-\frac{1}{q^2}\right).$$

But this is false, since $n\,|\,\frac{1}{2}(p\pm 1)$ and so p cannot divide $(\Gamma:\Gamma(n))$. This concludes the proof of the theorem.

It is clear that the function $\zeta(p)$ assumes arbitrarily large values, and that in general there are many groups G_n of a given index $\frac{1}{2}p(p^2-1)$.

In conclusion, we mention that similar results may be obtained for such groups as LF(2, 8), LF(2, 16), etc., if use is made of their known presentations. For example, Burnside has shown that LF(2, 8) $=\{A, B\}$ with defining relations

$$A^7 = B^2 = (AB)^3 = (A^3BA^5BA^3B)^2 = 1.$$

This shows that $\Delta=\Delta(S^7,(S^3TS^5TS^3T)^2)$ (the normal closure in Γ of the indicated words) is a maximal normal subgroup of Γ of index 504 and level 7 such that $\Gamma/\Delta\cong$LF(2, 8). Furthermore Δ is not a congruence group, since Δ does not contain $\Gamma(7)$.

REFERENCES

1. J. Gierster, *Die Untergruppen der Galois'schen Gruppe der Modular-Gleichungen für den Fall eines primzahlen Transformation-grades*, Math. Ann. **18** (1881), 319–365.

2. A. M. Macbeath, *Fuchsian groups*, Lectures at Queen's College, Dundee.

3. M. Newman, *Normal subgroups of the modular group which are not congruence subgroups*, Proc. Amer. Math. Soc. **16** (1965), 831–832.

4. I. Reiner, *Normal subgroups of the unimodular group*, Illinois J. Math. **2** (1958), 142–144.

5. K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. **8** (1964), 529–535.

NATIONAL BUREAU OF STANDARDS, WASHINGTON, D. C.