

## Subgroups of the modular group defined by a single linear congruence

by

R. A. RANKIN (Glasgow)

*Dedicated to Professor C. L. Siegel on his 75th birthday*

1. We are concerned with certain subgroups of the modular group  $\Gamma(1)$ , i.e.  $SL(2, \mathbb{Z})$ ; this is the set of all matrices

$$(1) \quad T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with rational integral entries and determinant 1. We denote the identity element of  $\Gamma(1)$  by  $I$ .

Let  $q$  be any positive integer. Certain well known subgroups of  $\Gamma(1)$  have the property that they can be defined by a single linear congruence satisfied by the entries of their members, for example the groups

$$(2) \quad \Gamma_0(q) = \{T \in \Gamma(1) : c \equiv 0 \pmod{q}\}$$

and

$$(3) \quad \Gamma^0(q) = \{T \in \Gamma(1) : b \equiv 0 \pmod{q}\}.$$

These are conjugate subgroups of  $\Gamma(1)$  containing the principal congruence group

$$(4) \quad \Gamma(q) = \{T \in \Gamma(1) : T \equiv I \pmod{q}\}.$$

The object of this paper is to investigate when a single linear congruence

$$(5) \quad Aa + Bb + Cc + Dd \equiv 0 \pmod{q}$$

determines a subgroup of  $\Gamma(1)$ , where  $A, B, C$  and  $D$  are fixed integers and we consider matrices  $T$  whose entries satisfy (5). It is clear that we may assume that the highest common factor of  $A, B, C, D$  and  $q$  is unity; i.e.

$$(6) \quad (A, B, C, D, q) = 1.$$

The solution to this problem is given in Theorem 3 (§ 4). It turns out that when  $q$  is prime to 6 the only groups that arise in this way are conjugates of  $\Gamma_0(q)$ . When  $(q, 6) \neq 1$  a number of other groups exist and are found.

2. There is a more convenient way of expressing the congruence (5), but this was only discovered after a number of special cases had been considered. When  $q = 2, 3$  or 4, the number of sets of incongruent values  $A, B, C, D$  modulo  $q$  is small and it is a straightforward matter to determine those that give rise to subgroups of  $\Gamma(1)$ . These are now summarized, since they indicate the pattern of the more general results obtained later.

(i)  $q = 2$ . The only groups obtainable are the three conjugate groups  $\Gamma_0(2), \Gamma^0(2)$  and

$$(7) \quad \{T \in \Gamma(1): a + b + c + d \equiv 0 \pmod{2}\}.$$

This last group is the one corresponding to the theta function  $\vartheta_3$ , and the congruence representation (7) is known; see Petersson [2].

(ii)  $q = 3$ . The only groups obtainable are the four conjugate groups  $\Gamma_0(3), \Gamma^0(3)$ ,

$$(8) \quad \{T \in \Gamma(1): a + b - c - d \equiv 0 \pmod{3}\},$$

and

$$(9) \quad \{T \in \Gamma(1): a - b + c - d \equiv 0 \pmod{3}\}.$$

(iii)  $q = 4$ . Here things are more interesting. We obtain the three conjugate groups  $\Gamma_0(4), \Gamma^0(4)$  and

$$(10) \quad \{T \in \Gamma(1): a + b - c - d \equiv 0 \pmod{4}\} \\ = \{T \in \Gamma(1): a - b + c - d \equiv 0 \pmod{4}\},$$

which have index 2 in  $\Gamma_0(2), \Gamma^0(2)$  and (7), respectively. But we also obtain three further conjugate groups

$$(11) \quad \Gamma_0^*(4) = \{T \in \Gamma(1): 2b + c \equiv 0 \pmod{4}\},$$

$$(12) \quad \Gamma^{0*}(4) = \{T \in \Gamma(1): b + 2c \equiv 0 \pmod{4}\}$$

and

$$(13) \quad \{T \in \Gamma(1): a + b + c - d \equiv 0 \pmod{4}\} \\ = \{T \in \Gamma(1): a - b - c - d \equiv 0 \pmod{4}\}.$$

These also have index 2 in  $\Gamma_0(2), \Gamma^0(2)$  and (7), respectively. Moreover

$$[\Gamma_0(4) \cap \Gamma_0^*(4) : \Gamma(4)] = 2$$

and similar relations hold for  $\Gamma^0(4) \cap \Gamma^{0*}(4)$  and for the intersection of (10) and (13).

Further,  $\Gamma_0(4)/\Gamma(4)$  is a cyclic group of order 4, while  $\Gamma_0^*(4)/\Gamma(4)$  is isomorphic to the Klein 4-group.

From these examples it is not immediately clear why some values of  $A, B, C$  and  $D$  should give rise to groups and others not. However, if we regard  $A, B, C$  and  $D$  as entries of a matrix

$$(14) \quad M = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$$

(note unusual positions of  $B$  and  $C$ ), the congruence (5) takes the form

$$(15) \quad \text{tr } MT \equiv 0 \pmod{q},$$

and it turns out that the value of  $\det M$  is crucial in determining whether we get a group or not. Thus, we see that, when  $q = 4$ , groups arise if and only if  $\det M \equiv 0 \pmod{4}$  or  $\det M \equiv 2 \pmod{4}$ .

In the following sections we reformulate the problem in terms of the matrix  $M$ .

3. From now on  $M$  denotes a matrix (14) with integral entries satisfying (6), and we write

$$(16) \quad \mathcal{G}_q(M) = \{T \in \Gamma(1); \text{tr } MT \equiv 0 \pmod{q}\}.$$

We are interested in matrices  $M$  for which  $\mathcal{G}_q(M)$  is a group, and since  $\Gamma$  must therefore belong to  $\mathcal{G}_q(M)$  the condition

$$(17) \quad \text{tr } M = A + D \equiv 0 \pmod{q}$$

must be satisfied. It is then clear that

$$\Gamma(q) \subseteq \mathcal{G}_q(M),$$

so that our problem is really one concerning subsets of the modular group  $\Gamma(1)/\Gamma(q)$  satisfying (6), (15) and (17), where the entries of all the matrices considered belong to the ring  $\mathbb{Z}/q\mathbb{Z}$ ; here, as usual,  $\mathbb{Z}$  is the set of all rational integers. We shall, however, continue to work in terms of congruences.

THEOREM 1. Let  $M$  satisfy (6) and (17) and suppose that, for some integer  $d$  and  $2 \times 2$  matrix  $L$  with integral entries,

$$(d, q) = (\det L, q) = 1.$$

Then

$$(18) \quad \mathcal{G}_q(dM) = \mathcal{G}_q(M)$$

and

$$(19) \quad L^{-1}\mathcal{G}_q(M)L = \mathcal{G}_q(L^{-1}ML).$$

Proof. Clearly  $L^{-1}$  is defined modulo  $q$  and its entries may be taken to be integers. The theorem follows, since

$$\text{tr } dMT = d \text{tr } MT$$

and

$$\text{tr}(L^{-1}ML \cdot T) = \text{tr}(M \cdot LTL^{-1}).$$

THEOREM 2. Let  $M$  satisfy (6) and (17) and suppose that

$$q = rs, \quad \text{where } (r, s) = 1.$$

Then

$$(20) \quad G_q(M) = G_r(M) \cap G_s(M).$$

Further  $G_q(M)$  is a group if and only if  $G_r(M)$  and  $G_s(M)$  are groups.

Proof. Since (20) is obvious, we need only prove the last sentence. It suffices to assume that  $G_q(M)$  is a group and prove that  $G_r(M)$  is one also. Take any  $S$  and  $T$  in  $G_r(M)$  and choose  $S_1, T_1$  in  $I(1)$  so that

$$S_1 \equiv S \pmod{r}, \quad S_1 \equiv I \pmod{s},$$

and

$$T_1 \equiv T \pmod{r}, \quad T_1 \equiv I \pmod{s},$$

as is possible, since  $(r, s) = 1$ . Then

$$\text{tr } MS_1 = \text{tr } MT_1 \equiv 0 \pmod{q},$$

and so  $S_1, T_1 \in G_q(M) \subseteq G_r(M)$ . But  $ST \equiv S_1T_1 \pmod{r}$  and so  $ST \in G_r(M)$ . From this the required result follows.

4. Theorem 2 makes it clear that the problem of finding when  $G_q(M)$  is a group may be reduced to the case when  $q$  is a power of a prime.

THEOREM 3. Let  $q = p^n$ , where  $p$  is a prime and  $n$  a positive integer. Suppose also that  $M$  satisfies (6) and (17) and that  $\nu$  is the greatest integer for which  $p^\nu$  divides  $\det M$ . Then  $G_q(M)$  is a group only in the following cases:

(i)  $\det M \equiv 0 \pmod{q}$ . When this holds  $G_q(M)$  is conjugate in  $I(1)$  to  $\Gamma_0(q)$ .

(ii)  $p = 3$  and  $\nu = n - 1 \geq 1$ .

(iii)  $p = 2$  and either (a)  $\nu = n - 1 \geq 1$ , (b)  $\nu = n - 2 \geq 1$  or (c)  $\nu = n - 3 \geq 2$ .

Proof. It is clear from (15) that we need to find some relation connecting the traces of  $MS$ ,  $MT$  and  $MST$  for  $S$  and  $T$  in  $I(1)$ . There are several such relations, but the most convenient for our purpose is the following:

$$(21) \quad A \text{tr } MST = (Aa + C\gamma) \text{tr } MT - (Cc + Dd) \text{tr } MS + \\ + (\gamma b - \beta c) \det M + \{c(A\beta + C\delta) + d(B\beta + D\delta)\} \text{tr } M.$$

This holds for any three  $2 \times 2$  matrices  $M$ ,  $S$  and  $T$ , where  $M$  is given by (14),  $T$  by (1) and

$$(22) \quad S = \begin{bmatrix} a & \beta \\ \gamma & \delta \end{bmatrix}.$$

If we take  $L = I$  or

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

in Theorem 1, the first entry in  $L^{-1}ML$  is  $A$ ,  $A + C$  or  $A - B$ , respectively. Since  $p$  does not divide  $(A, B, C, D)$  and since  $D \equiv -A \pmod{p}$ , at least one of these three numbers is not divisible by  $p$ . It follows from Theorem 1 that, for the purpose of examining the conditions under which  $G_q(M)$  is a group, we may assume that  $p \nmid A$  and, in fact, by (18), that

$$(23) \quad A = -D = 1.$$

Then (21) takes the form

$$\text{tr } MST = (Aa + C\gamma) \text{tr } MT - (Cc + Dd) \text{tr } MS + (\gamma b - \beta c) \det M \pmod{q}.$$

Accordingly  $G_q(M)$  is a group if and only if

$$(24) \quad S \in G_q(M), T \in G_q(M) \Rightarrow (\gamma b - \beta c) \det M \equiv 0 \pmod{q}.$$

In particular,  $G_q(M)$  is a group whenever  $\det M \equiv 0 \pmod{q}$ .

Now take  $x \in \mathbb{Z}$  with  $p \nmid x$  and choose  $x'$  so that  $xx' \equiv 1 \pmod{q}$ . Then we can find  $S_x \in I(1)$  such that

$$(25) \quad S_x \equiv \begin{bmatrix} 0 & -x' \\ x & Cx - Bx' \end{bmatrix} \pmod{q}.$$

Since  $\text{tr } MS_x \equiv 0 \pmod{q}$ , it follows that  $S_x \in G_q(M)$ . In particular,  $S_1 \in G_q(M)$  and hence, by (24), the condition

$$(26) \quad (b + c) \det M \equiv 0 \pmod{q} \quad \text{for all } T \in G_q(M)$$

is necessary for  $G_q(M)$  to be a group. Moreover, since

$$\gamma b - \beta c = \gamma(b + c) - c(\beta + \gamma),$$

the condition (26) is, by (24), also sufficient. Further, if  $q$  is odd, we may take  $m = 2$  and  $T = S_2$  in (26) and deduce that

$$(27) \quad 3 \det M \equiv 0 \pmod{q} \quad (q \text{ odd})$$

is a necessary condition for  $G_q(M)$  to be a group.

If  $p > 3$ , (27) becomes

$$(28) \quad \det M \equiv 0 \pmod{q}.$$

We have therefore proved that, when  $p > 3$ ,  $G_q(M)$  is a group if and only if (28) holds.

We also observe that if, for any prime  $p$  and any matrix  $M$  satisfying (6) and (17) with  $q = p^n$ , the congruence (28) holds, then the group  $G_q(M)$  is conjugate to  $G_q(M_1)$ , where

$$M_1 = \begin{bmatrix} 1 & C_1 \\ B_1 & -1 \end{bmatrix}$$

and  $B_1$  and  $C_1$  are integers satisfying  $B_1 C_1 \equiv -1 \pmod{q}$ ; for in this application of Theorem 1 we have only used matrices  $L$  belonging to  $\Gamma(1)$ . We now apply Theorem 1 with

$$L = \begin{bmatrix} 1 & 0 \\ B_1 & 1 \end{bmatrix} \in \Gamma(1),$$

so that

$$L^{-1} M_1 L = \begin{bmatrix} 0 & C_1 \\ 0 & 0 \end{bmatrix}.$$

It follows that  $G_q(M_1)$ , and therefore  $G_q(M)$ , is conjugate to  $\Gamma_0(q)$ .

It now remains to consider the cases when  $p \leq 3$ , and from now on we may assume that (28) does not hold, so that  $\nu \leq n-1$ .

Suppose first that  $p = 3$ . If  $n = 1$ , so that  $q = 3$ , the work described in § 2 shows that there are no groups  $G_3(M)$  other than those that satisfy (28); we may therefore assume that  $n \geq 2$ . From (27) we deduce that

$$(29) \quad \det M \equiv 0 \pmod{3^{n-1}}$$

is a necessary condition for  $G_q(M)$  to be a group; it is equivalent to the condition  $\nu = n-1$ .

Conversely, assume that (29) holds. Then, by (23),

$$BC \equiv -1 \pmod{3^{n-1}},$$

so that  $3 \nmid B$ . We may then, by Theorem 1, replace  $M$  by  $L^{-1} M L$ , where

$$(30) \quad L = \begin{bmatrix} 1 & 0 \\ 0 & B \end{bmatrix},$$

so that  $M$  is replaced by

$$\begin{bmatrix} 1 & -1-3^{n-1}l \\ 1 & -1 \end{bmatrix},$$

where  $3 \nmid l$ . Thus the condition (15) becomes

$$a - d + b - c(1 + 3^{n-1}l) \equiv 0 \pmod{3^n}.$$

In particular,  $b - c \equiv d - a \pmod{3}$ , so that

$$\begin{aligned} (b+c)^2 &\equiv (b-c)^2 + 4bc \equiv (a-d)^2 + 4bc \\ &\equiv (a+d)^2 - 4 \equiv (a+d)^2 - 1 \pmod{3}. \end{aligned}$$

This is only possible if  $b+c \equiv 0 \pmod{3}$ . This must hold for all  $T \in G_q(M)$  and, accordingly, if also  $S \in G_q(M)$ , we have

$$\gamma b - \beta c \equiv -\beta(b+c) \equiv 0 \pmod{3}.$$

Then

$$(\gamma b - \beta c) \det M \equiv 0 \pmod{3^n}$$

and it follows from (24) that  $G_q(M)$  is a group.

It remains to consider the case when  $q = 2^n$ . If  $n = 1$ , there are, by § 2, no groups with  $\nu \leq n-1$ . If  $n = 2$ , there are exactly three and they satisfy part (iii) (a) of the theorem. We may therefore assume from now on that  $n \geq 3$ .

Take  $x = 3$  in (25) and put  $T = S_3$  in (26). Then, since  $x^2 - 1 = 8$ , a necessary condition for  $G_q(M)$  to be a group is that

$$\det M \equiv 0 \pmod{2^{n-3}},$$

and so

$$(31) \quad n-3 \leq \nu \leq n-1.$$

Now, by (15),

$$\begin{bmatrix} 1 & q/(B, q) \\ 0 & 1 \end{bmatrix} \in G_q(M).$$

If  $\nu = 0$ , (26) shows that  $(B, q) = 1$ , and, similarly,  $(C, q) = 1$ ; but then  $BC$  is odd and so  $\det M = -1 + BC \equiv 0 \pmod{2}$ , which is a contradiction. It follows that  $\nu$ , in addition to satisfying (31), is positive, and that  $B$  and  $C$  are odd.

Now, since  $B$  is odd, we can transform  $M$  by  $L$ , as given in (30), and so assume that  $B = 1$ ,  $C = -1 - 2^r l$ , where  $l$  is odd. Then (15) takes the form

$$(32) \quad a - d + b - c(1 + 2^r l) \equiv 0 \pmod{2^n}.$$

We show first that, if  $G_q(M)$  is a group, we cannot have  $\nu = n-3 = 1$ . For suppose that  $l \equiv \varepsilon \pmod{4}$ , where  $\varepsilon = \pm 1$ . Then, by (32),  $G_q(M)$  contains

$$\begin{bmatrix} 1 & -2\varepsilon \\ -2\varepsilon & 5 \end{bmatrix}.$$

But this matrix does not satisfy condition (26).

The only other case when  $\nu = 1$  is for  $n = 3$ . In this case  $G_q(M)$  is a group. For  $b - c$  cannot be odd as otherwise  $bc$  would be even and then  $ad$  would be odd and therefore  $a - d$  would be even; but, by (32),

$b-c$  and  $a-d$  cannot be of opposite parity. Hence both  $b+c$  and  $a+d$  are even. Now

$$\begin{aligned}(b+c)^2 &= (b-c)^2 + 4bc \\ &\equiv (a-d-2cl)^2 + 4bc \pmod{8} \\ &\equiv (a+d)^2 - 4 - 4cl(a-d) + 4c^2l^2 \pmod{8} \\ &\equiv (a+d-2c)^2 - 4 \pmod{8}.\end{aligned}$$

If  $b+c \equiv 2 \pmod{4}$ , it would follow that  $a+d \equiv 2c \pmod{4}$  and these congruences are easily seen to be inconsistent with  $ad-bc = 1$ . Hence

$$b+c \equiv 0 \pmod{4}$$

and so (26) holds and  $G_q(M)$  is a group.

We may therefore assume from now on that  $\nu \geq 2$  and we shall prove that

$$(33) \quad b+c \equiv 0 \pmod{2^{n-\nu}}$$

from which (26) will follow, so that  $G_q(M)$  is a group. Now, if  $x \equiv y \pmod{2^n}$ , then  $x^2 \equiv y^2 \pmod{2^{n+1}}$  and we deduce from (32) that, if  $T \in G_q(M)$ , then

$$(34) \quad \begin{aligned}(b+c)^2 &= (b-c)^2 + 4bc \\ &\equiv (a-d-2^{\nu}cl)^2 + 4bc \pmod{2^{n+1}} \\ &\equiv (a+d)^2 - 4 - 2^{\nu+1}cl(a-d) \pmod{16}.\end{aligned}$$

In particular,  $(b+c)^2 \equiv (a+d)^2 - 4 \pmod{8}$ , which shows that  $a+d$  and therefore  $a-d$  is even. Accordingly, we have

$$(b+c)^2 \equiv (a+d)^2 - 4 \pmod{16}$$

and this is only possible if  $b+c \equiv 0 \pmod{4}$  and  $a+d \equiv 2 \pmod{4}$ .

Accordingly, if  $\nu \geq n-2$ , (33) follows. We may therefore suppose that  $\nu = n-3 \geq 2$ . If  $c$  is even, we deduce from (34) that

$$(b+c)^2 \equiv (a+d)^2 - 4 \pmod{32},$$

and from this it follows that  $b+c \equiv 0 \pmod{8}$ , which gives (33). On the other hand, if  $c$  is odd it is easily seen that  $b+c \equiv 4 \pmod{8}$  implies that  $bc \equiv 3 \pmod{8}$ , and so  $ad \equiv 4 \pmod{8}$ ; this contradicts  $a+d \equiv 2 \pmod{4}$ . Hence in this case also we must have  $b+c \equiv 0 \pmod{8}$ , and therefore (33) holds.

We have therefore shown that, when  $q = 2^n$ ,  $G_q(M)$  is a group if and only if the conditions of part (iii) of the theorem hold.

5. In all the cases listed in Theorem 3 where  $G_q(M)$  is a group it can be shown that

$$[G_q(M) : \Gamma(q)] = [\Gamma_0(q) : \Gamma(q)].$$

This follows as a consequence of

THEOREM 4. Let  $q = p^n$ , where  $p$  is a prime and  $n \geq 1$ . Suppose that (6) and (17) hold and that  $\det M \equiv 0 \pmod{p}$ . Then the number of matrices in  $G_q(M)$  that are incongruent modulo  $q$  is equal to  $[\Gamma_0(q) : \Gamma(q)]$ .

Proof. In this theorem we do not assume that  $G_q(M)$  is a group.

By Theorem 3 and the particular cases described in § 2, the theorem is certainly true when  $n = 1$  for all primes  $p$ . We therefore assume its truth for  $q = p^n$ , where  $n \geq 1$ , and prove its truth for  $q = p^{n+1}$ .

Take any  $T_0 \in G_q(M)$  and write  $M_0 = MT_0$ , so that

$$\operatorname{tr} MT_0 = \operatorname{tr} M_0 = p^n t_0$$

for some integer  $t_0$ . We shall show that there are  $p^2$  incongruent matrices  $T$  modulo  $p^{n+1}$  such that  $T \in G_r(M)$ , where  $r = p^{n+1}$ , and such that

$$T \equiv T_0 \pmod{p^n}.$$

Every such matrix  $T$  can be written in the form

$$T = T_0(I + p^n T_1),$$

and it is enough to enumerate the number of incongruent matrices  $T_1$  modulo  $p$  for which

$$(35) \quad \operatorname{tr} MT = 0 \pmod{p^{n+1}}$$

and

$$(36) \quad \det(I + p^n T_1) \equiv 1 \pmod{p^{n+1}}.$$

It is clear that (36) is equivalent to

$$(37) \quad \operatorname{tr} T_1 \equiv 0 \pmod{p},$$

while (35) is equivalent to

$$0 \equiv \operatorname{tr} M_0(I + p^n T_1) \equiv p^n(t_0 + \operatorname{tr} M_0 T_1) \pmod{p^{n+1}},$$

i.e.

$$(38) \quad \operatorname{tr} M_0 T_1 \equiv -t_0 \pmod{p}.$$

Since  $\det M_0 \equiv \operatorname{tr} M_0 \equiv 0 \pmod{p}$  and  $M_0 \not\equiv 0 \pmod{p}$ , there exists a matrix  $L \in \Gamma(1)$  such that

$$L^{-1} M_0 L \equiv \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \pmod{p},$$

where  $p \nmid a$ . Write

$$T_2 = L^{-1} T_1 L = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}.$$

Then, by (38),

$$(39) \quad -t_0 \equiv \operatorname{tr} M_0 T_1 \equiv \operatorname{tr} L^{-1} M_0 L \cdot T_2 \equiv ac_2 \pmod{p}$$

and, by (37),

$$(40) \quad \operatorname{tr} T_2 = \operatorname{tr} T_1 \equiv 0 \pmod{p}.$$

We therefore have only to count the number of incongruent matrices  $T_2$  satisfying (39) and (40); this number is clearly  $p^2$ .

It follows that the number of matrices in  $G_p(M)$  that are incongruent modulo  $p^{n+1}$  is equal to

$$p^2 [\Gamma_0(p^n) : \Gamma(p^n)] = [\Gamma_0(p^{n+1}) : \Gamma(p^{n+1})]$$

and the theorem follows by induction.

6. The congruences that we have been considering are homogeneous. It is also possible in certain cases to define groups by inhomogeneous congruences. We give a few examples, omitting the proofs, which are straightforward.

$$(41) \quad \Gamma(2) = \{T \in \Gamma(1) : a + b + c \equiv 1 \pmod{2}\}$$

$$(42) \quad = \{T \in \Gamma(1) : b + c + d \equiv 1 \pmod{2}\},$$

$$(43) \quad \Gamma_0(4) = \{T \in \Gamma(1) : c + 2d \equiv 2 \pmod{4}\}$$

$$(44) \quad = \{T \in \Gamma(1) : c + 2a \equiv 2 \pmod{4}\},$$

$$(45) \quad \Gamma_0^*(4) = \{T \in \Gamma(1) : 2b + c + 2d \equiv 2 \pmod{4}\}$$

$$(46) \quad = \{T \in \Gamma(1) : 2a + 2b + c \equiv 2 \pmod{4}\}.$$

The conjugate groups to  $\Gamma_0(4)$  and  $\Gamma_0^*(4)$  can be defined similarly.

7. The asymmetrical relation (21) has been of basic importance in our discussion of  $G_d(M)$ . It is possible to derive other more symmetrical trace formulae.

Let  $M$ ,  $S$  and  $T$  be  $2 \times 2$  matrices over the complex field, the last two having determinant 1, and write

$$s, s_0, t, t_0, u, u_0$$

for the traces of the matrices

$$S, MS, T, MT, ST, MST,$$

respectively. Then

$$(47) \quad u_0^2 - (s_0 t + s t_0) u_0 + s_0^2 + t_0^2 + u s_0 t_0 = \det M \{2 - \text{tr}(STS^{-1}T^{-1})\}.$$

I have not come across this identity in the literature. It is, however, reminiscent of Fricke's identity [1].

$$(48) \quad s^2 + t^2 + u^2 = stu + 2 + \text{tr}(STS^{-1}T^{-1}).$$

#### References

- [1] R. Fricke, *Über die Theorie der automorphen Modulgruppen*, Nachr. Ges. Wiss. Göttingen (1896), pp. 91-101.  
 [2] H. Petersson, *Über die Kongruenzgruppen der Stufe 4*, J. für Math. 212 (1963), pp. 63-72.

UNIVERSITY OF GLASGOW  
Glasgow, Scotland

Received on 9. 11. 1972

(347)