MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 207–213

Congruence Subgroups of the Modular Group

By Morris Newman

Abstract. The congruence subgroups of the classical modular group which can be defined as the automorphs modulo q of some fixed matrix are studied, and their genera determined.

Let $\Gamma = SL(2, Z)$. A congruence subgroup of Γ is any subgroup containing a principal congruence subgroup $\Gamma(q)$, defined as the set of elements A of Γ such that $A \equiv I \bmod q$, where q is a positive integer. Of these one of the most important is the group $\Gamma_0(q)$, defined as the set of elements $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belonging to Γ such that $c \equiv 0 \bmod q$. It is known that

$$(\Gamma : \Gamma(q)) = q^3 \prod_{p \mid q} (1 - 1/p^2), \qquad (\Gamma : \Gamma_0(q)) = q \prod_{p \mid q} (1 + 1/p),$$

where p runs over the distinct primes dividing q.

Let $C = \{I, -I\}$ be the center of Γ, and $\bar{\Gamma} = \Gamma/C = PSL(2, Z)$. Then $\bar{\Gamma}$ is the classical modular group, and we will be interested here in the congruence subgroups of $\bar{\Gamma}$, which are the subgroups of $\bar{\Gamma}$ corresponding to the congruence subgroups of Γ under the natural homomorphism φ of Γ onto $\bar{\Gamma}$. In particular we will study those congruence subgroups which can be defined as the set of automorphs modulo q of some fixed 2×2 matrix over Z.

If Ω is a subgroup of Γ, then $\bar{\Omega}$ will denote the subgroup of $\bar{\Gamma}$ corresponding to Ω under φ. It is more convenient to study the problem for Γ and its subgroups, and then make the transition to $\bar{\Gamma}$ by means of Theorem 1 below. Also, we will choose q to be a prime > 3 for simplicity of exposition.

We first prove

THEOREM 1. *Let Ω be a subgroup of Γ. Then the subgroup $\bar{\Omega}$ of $\bar{\Gamma}$ corresponding to Ω under the natural homomorphism φ is*

$$\bar{\Omega} = \{\Omega, -I\}/C.$$

Thus

$$(\bar{\Gamma} : \bar{\Omega}) = \begin{cases} (\Gamma : \Omega), & -I \in \Omega, \\ \tfrac{1}{2}(\Gamma : \Omega), & -I \notin \Omega. \end{cases} \tag{1}$$

Proof. If G is any group and N a normal subgroup, then any subgroup H

Received February 15, 1974.
AMS (MOS) subject classifications (1970). Primary 10D05, 15A36, 20H05.
Key words and phrases. Automorphs, elliptic classes, finite fields, genus, modular group, natural homomorphism, parabolic classes.

Copyright © 1975, American Mathematical Society

of G is carried into HN/N under the natural homomorphism modulo N. Now $\Omega C = \Omega\{I, -I\} = \{\Omega, -I\}$, so that $\Omega C = \Omega$ if $-I \in \Omega$, and $\Omega C = \Omega + (-I)\Omega$ if $-I \notin \Omega$. Since

$$(\bar{\Gamma} : \bar{\Omega}) = (\Gamma/C : \Omega C/C) = (\Gamma : \Omega C) = (\Gamma : \Omega)/(\Omega C : \Omega),$$

the result follows.

As an illustration of this theorem, note that $-I \in \Gamma_0(q)$, but $-I \notin \Gamma(q)$, since $q > 2$. Hence

$$(\bar{\Gamma} : \bar{\Gamma}(q)) = \tfrac{1}{2}(\Gamma : \Gamma(q)), \qquad (\bar{\Gamma} : \bar{\Gamma}_0(q)) = (\Gamma : \Gamma_0(q)).$$

Throughout the following we put

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

Then every element A of Γ satisfies

$$ATA^T = T, \tag{2}$$

where A^T denotes the transpose of A. Indeed, (2) is satisfied if R is any commutative ring with identity, and A any element of $SL(2, R)$. A convenient way to think of $\bar{\Gamma}$ is as the set of elements of Γ in which a matrix is identified with its negative.

Let K denote an arbitrary 2×2 matrix over Z. The subgroup of Γ consisting of all matrices $A \in \Gamma$ such that $AKA^T \equiv K \mod q$, will be denoted by $\Gamma(K, q)$. It is clear that $\Gamma(K, q)$ is a congruence subgroup of Γ containing the principal congruence subgroup $\Gamma(q)$.

If R is any commutative ring with identity 1 and if M is any 2×2 matrix over R, the subgroup of $\Delta = SL(2, R)$ consisting of all matrices $A \in \Delta$ such that $AMA^T = M$, will be denoted by $\Delta(M, R)$. Since

$$\Gamma(K, q)/\Gamma(q) \cong \Delta(K, Z_q),$$

where $\Delta = SL(2, Z_q)$ and Z_q is the ring of integers modulo q (and so $GF(q)$ when q is prime), it will suffice to work with the latter group when this is desirable. The transition between the two depends on the result that if A is an integral matrix such that $\det A \equiv 1 \mod q$, then an integral matrix B exists such that $B \equiv A \mod q$ and $\det B = 1$ (see [2, pp. 36–37]).

We have the following:

LEMMA 1. *The groups* $\Gamma(K, q)$ *satisfy*

$$\Gamma(\alpha K, q) = \Gamma(K, q), \qquad \text{if } (\alpha, q) = 1, \tag{3}$$

$$\Gamma(BKB^T, q) = B\Gamma(K, q)B^{-1}, \quad \text{if } B \in \Gamma. \tag{4}$$

Proof. (3) is clear, since $A(\alpha K)A^T \equiv \alpha K \mod q$ if and only if $AKA^T \equiv K \mod q$, since $(\alpha, q) = 1$. As for (4), suppose that $A \in \Gamma(BKB^T, q)$. Then

$$ABKB^TA^T \equiv BKB^T \mod q,$$

so that

$$(B^{-1}AB)K(B^{-1}AB)^T \equiv K \mod q.$$

Hence $B^{-1}AB \in \Gamma(K, q)$, $A \in B\Gamma(K, q)B^{-1}$. Thus $\Gamma(BKB^T, q) \subset B\Gamma(K, q)B^{-1}$. The argument may be reversed to show that $B\Gamma(K, q)B^{-1} \subset \Gamma(BKB^T, q)$. Hence (4) holds and the proof is complete.

The next result, which we state in somewhat more general form, reduces the study of $\Gamma(K, q)$ to the case when K is symmetric:

THEOREM 2. *Let R be any commutative ring with identity 1 in which 2 is a unit. Put $\Delta = SL(2, R)$ and let $M = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ be any matrix over R. Then*

$$\Delta(M, R) = \Delta(M + M^T, R).$$

Proof. Suppose first that $A \in \Delta(M, R)$, so that $AMA^T = M$. Then also $AM^TA^T = M^T$, so that $A(M + M^T)A^T = M + M^T$. Hence $A \in \Delta(M + M^T, R)$ and so $\Delta(M, R) \subset \Delta(M + M^T, R)$.

Next suppose that $A \in \Delta(M + M^T, R)$ so that $A(M + M^T)A^T = M + M^T$. Then if x is any element of R,

$$A(M + M^T + xT)A^T = M + M^T + xT,$$

where $T = \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$, because of (2). Since $M - M^T = (\beta - \gamma)T$, the choice $x = \beta - \gamma$ implies that $A(2M)A^T = 2M$, so that $AMA^T = M$, since 2 is a unit of R. Hence $A \in \Delta(M, R)$, and so $\Delta(M + M^T, R) \subset \Delta(M, R)$.

It follows that $\Delta(M, R) = \Delta(M + M^T, R)$ and the proof is complete.

COROLLARY 1. *We have*

$$\Gamma(K, q) = \Gamma(K + K^T, q).$$

Proof. Since q is odd, 2 is a unit of Z_q and the theorem may be applied to $\Delta(K, Z_q)$ and so to $\Gamma(K, q)$.

Lemma 1 and Corollary 1 allow us to reduce the study of $\Gamma(K, q)$ to three simple types:

THEOREM 3. *The group $\Gamma(K, q)$ is either Γ or else is conjugate over Γ to one of the groups $\Gamma(K_n, q)$, where $K_n = \left(\begin{smallmatrix}1 & 0\\ 0 & n\end{smallmatrix}\right)$ and $n = 0, 1$, or some fixed non-square of Z_q.*

Proof. If K is skew-symmetric, Corollary 1 implies that

$$\Gamma(K, q) = \Gamma(K + K^T, q) = \Gamma(0, q) = \Gamma.$$

If K is not skew-symmetric, Corollary 1 implies that K may be taken symmetric and different from 0. We now work with $\Delta(K, Z_q)$. Since any symmetric matrix over a field of characteristic $\neq 2$ is congruent by a matrix of determinant 1 to a diagonal matrix (see [2, Chapter 4]) K may be taken diagonal, by (4) (replacing $\Delta(K, Z_q)$ by a conjugate group if necessary). Thus we may assume that $K = \left(\begin{smallmatrix}\alpha & 0\\ 0 & \delta\end{smallmatrix}\right)$,

where not both α and δ are 0, and so we may assume that $\alpha \neq 0$, and therefore 1, by property (3). If $\delta = 0$, then we obtain $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Suppose that $\delta \neq 0$. We may write $\delta = n/r^2$, where n is either 1 or some fixed nonsquare of Z_q and $r \in Z_q$. Then replacing K by rK we get $\left(\begin{smallmatrix} r & 0 \\ 0 & n/r \end{smallmatrix}\right)$. Since $n \neq 0$, we may determine $x, y \in Z_q$ so that $x^2 + ny^2 = r$. Then by virtue of the identity

$$\begin{pmatrix} r & 0 \\ 0 & n/r \end{pmatrix} = \begin{pmatrix} x & y \\ -ny/r & x/r \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} x & -ny/r \\ y & x/r \end{pmatrix}$$

we see that K may be replaced by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$. This completes the proof.

The important parameters associated with a subgroup of the classical modular group are the number of elliptic classes e_2 of period 2, the number of elliptic classes e_3 of period 3, the number of parabolic classes t, the index μ, and the genus g. These are related by the formula

$$g = 1 + \mu/12 - t/2 - e_2/4 - e_3/3.$$

We refer the reader to [2, Chapter 8], where these terms are defined and the principal facts about them given. We assume these known in what follows.

Our goal will be the calculation of these parameters for the groups $\overline{\Gamma}(K, q)$. Since conjugate groups have the same parameters, it is only necessary to consider the cases

$$K = K_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad K = K_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad K = K_n = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix},$$

where n is some nonsquare of Z_q, by virtue of Theorem 3.

Put $K_\delta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \delta \end{smallmatrix}\right)$, where $\delta = 0$, 1, or n, and let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Delta(K_\delta, Z_q)$. Then $AK_\delta A^T = K_\delta$, $K_\delta A^T = A^{-1} K_\delta$,

$$\begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}.$$

Hence $a = d$, $c = -b\delta$, so that

$$A = \begin{pmatrix} a & b \\ -b\delta & a \end{pmatrix}, \quad a^2 + \delta b^2 = 1. \tag{5}$$

Let χ be the Legendre symbol modulo q. Then the number of solutions of the congruence $x^2 \equiv a \bmod q$ is just $1 + \chi(a)$; and the value of the sum $\Sigma_{a \bmod q} \chi(x^2 - a)$ is -1 if $(a, q) = 1$ and $q - 1$ otherwise. It follows from (5) that the order of the group $\Delta(K_\delta, Z_q)$ is

$$\sum_{b \bmod q} \{1 + \chi(1 - \delta b^2)\} = q + \sum_{b \bmod q} \chi(1 - \delta b^2),$$

so that

$$(\Gamma(K_\delta, q) : \Gamma(q)) = \begin{cases} 2q, & \delta = 0, \\ q - \chi(-\delta), & \delta = 1, n. \end{cases}$$

Since $(\Gamma : \Gamma(q)) = q(q^2 - 1)$, this implies that

$$(\Gamma : \Gamma(K_\delta, q)) = \begin{cases} \tfrac{1}{2}(q^2 - 1), & \delta = 0, \\ q(q + \chi(-\delta)), & \delta = 1, n. \end{cases}$$

If we now note that $-I \in \Gamma(K, q)$, then Theorem 1 yields

LEMMA 2. *Let* $\mu(\delta)$ *be the index of* $\bar{\Gamma}(K_\delta, q)$ *in* $\bar{\Gamma}$. *Then*

$$\mu(\delta) = \begin{cases} \tfrac{1}{2}(q^2 - 1), & \delta = 0, \\ q(q + \chi(-\delta)), & \delta = 1, n. \end{cases}$$

The elements of period 2 of $\Gamma(K_\delta, q)$ correspond to the elements A of $\Delta(K_\delta, Z_q)$ satisfying $A^2 = -I$, or $\operatorname{tr} A = 0$. Then (5) implies that $a = 0$, so that

$$A = \begin{pmatrix} 0 & b \\ -\delta b & 0 \end{pmatrix}, \quad \delta b^2 = 1. \tag{6}$$

It follows that there are no elliptic elements of period 2 if $\delta = 0$ or n, and just 2 if $\delta = 1$, given by (6) with $b = \pm 1$. For these to be conjugate over $\Delta(K_1, Z_q)$, there must be an $A = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in \Delta(K_1, Z_q)$ such that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

which implies that $a = b = 0$, an impossibility. Hence we can conclude

LEMMA 3. *Let* $e_2(\delta)$ *be the number of classes of elliptic elements of period* 2 *of* $\bar{\Gamma}(K_\delta, q)$. *Then*

$$e_2(\delta) = \begin{cases} 0, & \delta = 0, \\ 1 + \chi(\delta), & \delta = 1, n. \end{cases}$$

The elements of period 3 of $\Gamma(K_\delta, q)$ correspond to the elements A of $\Delta(K_\delta, Z_q)$ satisfying $A^2 \pm A + I = 0$, or $\operatorname{tr} A = \pm 1$. Then (5) implies that $a = \pm \tfrac{1}{2}$, $\delta b^2 = \tfrac{3}{4}$. It follows that there are none if $\delta = 0$, or if $\chi(3\delta) = -1$. If $\chi(3\delta) = 1$, let θ be a solution of $\delta\theta^2 = \tfrac{3}{4}$. Then the elements of period 3 of $\Delta(K_\delta, Z_q)$ are given by

$$A_1 = \begin{pmatrix} \tfrac{1}{2} & \theta \\ -\delta\theta & \tfrac{1}{2} \end{pmatrix}, \quad A_2 = \begin{pmatrix} \tfrac{1}{2} & -\theta \\ \delta\theta & \tfrac{1}{2} \end{pmatrix},$$

$$A_3 = \begin{pmatrix} -\tfrac{1}{2} & \theta \\ -\delta\theta & -\tfrac{1}{2} \end{pmatrix}, \quad A_4 = \begin{pmatrix} -\tfrac{1}{2} & -\theta \\ \delta\theta & -\tfrac{1}{2} \end{pmatrix}.$$

Since $A_2 = A_1^{-1}, A_4 = A_3^{-1}$, it is only necessary to retain A_1 and A_3. Clearly,

A_1 and A_3 are not conjugate over $\Delta(K_\delta, Z_q)$, since $\operatorname{tr} A_1 = 1$, $\operatorname{tr} A_3 = -1$. Also $A_3^2 = A_3^{-1} = A_4$, so that A_1 and A_3^2 are also not conjugate over $\Delta(K_\delta, Z_q)$. Hence there are just two classes in this case.

Thus we have

LEMMA 4. *Let $e_3(\delta)$ be the number of classes of elliptic elements of period 3 of $\overline{\Gamma}(K_\delta, q)$. Then*

$$e_3(\delta) = \begin{cases} 0, & \delta = 0, \\ 1 + \chi(3\delta), & \delta = 1, n. \end{cases}$$

The computation of the parabolic class number of $\Gamma(K_\delta, q)$ depends on the following result, which is given in [1]:

THEOREM. *Let G, H be subgroups of finite index of the classical modular group, and assume that H is a normal subgroup of G. Let P_i, $1 \leqslant i \leqslant t$, be a complete set of parabolic representatives for G, and let e_i be the exponent of P_i modulo H, $1 \leqslant i \leqslant t$. Then the parabolic class number of H is given by*

$$\tau = \mu \sum_{i=1}^{t} \frac{1}{e_i},$$

where $\mu = (G : H)$. In particular, if every parabolic element of G is already in H, then $\tau = \mu t$.

The parabolic elements of $\Gamma(K_\delta, q)$ correspond to the elements A of $\Delta(K_\delta, Z_q)$ such that $\operatorname{tr} A = \pm 2$. Then (5) implies that $a = \pm 1$, $\delta b^2 = 0$. Hence if $\delta = 0$,

$$A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix};$$

and if $\delta \neq 0$, then $b = 0, A = \pm I$.

Suppose first that $\delta = 0$. Then $\overline{\Gamma}(K_0, q)$ is a normal subgroup of $\overline{\Gamma}_0(q)$ of index $\frac{1}{2}(q-1)$, and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ q & 1 \end{smallmatrix}\right)$ is a complete set of parabolic representatives for $\Gamma_0(q)$. Since each of these belongs to $\overline{\Gamma}(K_0, q)$, the previous theorem applies and we find that the parabolic class number is $\frac{1}{2}(q-1) \cdot 2 = q - 1$, in this case.

Next suppose that $\delta \neq 0$. Then $\overline{\Gamma}(q)$ is a normal subgroup of $\overline{\Gamma}(K_\delta, q)$ of index $\frac{1}{2}(q - \chi(-\delta))$. It is known that the parabolic class number of $\overline{\Gamma}(q)$ is $\frac{1}{2}(q^2 - 1)$. Since every parabolic element of $\overline{\Gamma}(K_\delta, q)$ is already in $\overline{\Gamma}(q)$, the previous theorem implies that

$$\tfrac{1}{2}(q^2 - 1) = \tfrac{1}{2}(q - \chi(-\delta))\tau, \qquad \tau = q + \chi(-\delta),$$

where τ is the parabolic class number of $\overline{\Gamma}(K_\delta, q)$.

Summarizing, we have proved

LEMMA 5. *Let $t(\delta)$ denote the number of parabolic classes of $\overline{\Gamma}(K_\delta, q)$. Then*

$$t(\delta) = \begin{cases} q - 1, & \delta = 0, \\ q + \chi(-\delta), & \delta = 1, n. \end{cases}$$

Lemmas 2, 3, 4, 5 now yield

THEOREM 4. *Let* $g(\delta)$ *denote the genus of* $\overline{\Gamma}(K_\delta, q)$. *Then*

$$g(\delta) = \begin{cases} \frac{1}{24}(q-5)(q-7), & \delta = 0, \\ \frac{1}{12}(q^2 - (6 - \chi(-\delta))q + 5 - 6\chi(-\delta) - 4\chi(3\delta) - 3\chi(\delta)), & \delta = 1, n. \end{cases}$$

Considering q modulo 12, we find the following explicit formulas for $g(1)$, $g(n)$:

$$g(1) = \begin{cases} (q^2 - 5q - 8)/12, & q \equiv 1 \bmod 12, \\ (q^2 - 5q)/12, & q \equiv 5 \bmod 12, \\ (q^2 - 7q + 12)/12, & q \equiv 7 \bmod 12, \\ (q^2 - 7q + 4)/12, & q \equiv 11 \bmod 12, \end{cases}$$

$$g(n) = \begin{cases} (q^2 - 7q + 18)/12, & q \equiv 1 \bmod 12, \\ (q^2 - 7q + 10)/12, & q \equiv 5 \bmod 12, \\ (q^2 - 5q - 2)/12, & q \equiv 7 \bmod 12, \\ (q^2 - 5q + 6)/12, & q \equiv 11 \bmod 12. \end{cases}$$

Finally, we note that $g(\delta) = 0$ for $\delta = 0, q = 5, 7; \delta = 1, q = 5$; and $\delta = n$, $q = 5$. $g(\delta)$ is also 0 for the excluded primes $q = 2, 3$, since $\Gamma(2), \Gamma(3)$ are of genus 0.

National Bureau of Standards
Washington, D. C. 20234

1. M. I. KNOPP & M. NEWMAN, "Congruence subgroups of positive genus of the modular group," *Illinois J. Math.*, v. 9, 1965, pp. 577–583. MR 31 #5902.

2. M. NEWMAN, *Integral Matrices*, Academic Press, New York, 1972.