ILLINOIS JOURNAL OF MATHEMATICS
Volume 26, Number 1, Spring 1982

THE CUSP AMPLITUDES OF THE CONGRUENCE SUBGROUPS OF THE CLASSICAL MODULAR GROUP

BY

H. LARCHER[1]

1. Introduction

The homogeneous modular group ${}_1\Gamma = SL(2, Z)$. If $A \in \Gamma_1$ and

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

then A induces the linear fractional substitution

$$z \to A(z), \quad \text{where } A(z) = (az + b)/(cz + d),$$

$z = x + iy$ and x, y real numbers. The group of all substitutions is known as the inhomogeneous modular group. A matrix $A \neq \pm I$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and the substitution $A(z)$ are called parabolic if, for a rational number ρ, or $\rho = \infty$, $A(\rho) = \rho$. We call ρ the fixed point of $A(z)$ and of A. For a parabolic matrix P with fixed point ρ there exist $B \in {}_1\Gamma$ and a rational integer $n \neq 0$ such that $P = \pm B^{-1}U^nB$, where

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and $\rho = B^{-1}(\infty)$. The modulus $|n|$ of n is called the amplitude of P. If Γ is a subgroup of ${}_1\Gamma$ and $P \in \Gamma$ then ρ is also referred to as a fixed point or a cusp of Γ. The cusp amplitude of ρ in Γ is the smallest positive rational integer k such that $\pm B^{-1}U^kB \in \Gamma$. Two cusps η and ρ are said to be equivalent under Γ, in which case we write $\eta \sim_\Gamma \rho$, if there is an $A \in \Gamma$ such that $\eta = A(\rho)$. Equivalent cusps in Γ have the same amplitudes. For $\Gamma \subset {}_1\Gamma$ we denote by $C(\Gamma)$ the subset of the set of all positive rational integers containing all different cusp amplitudes of Γ.

For a positive rational integer m,

$$\Gamma(m) = \{A \in {}_1\Gamma \mid A \equiv \pm I \pmod{m}\}$$

Received April 22, 1980.

[1] The publication of this paper is financially supported by the University of Maryland, European Division, Munich campus.

is known as the (homogeneous) principal congruence subgroup of ${}_1\Gamma$ of level m. A congruence group Γ of level m is a subgroup of ${}_1\Gamma$ such that $\Gamma \supset \Gamma(m)$, but $\Gamma \not\supset \Gamma(l)$ for $l < m$. Since a congruence group Γ is of finite index in ${}_1\Gamma$, the number of equivalence classes of cusps in Γ is finite, and hence $C(\Gamma)$ is a finite set.

In the following, all letters, if not otherwise stated, are rational integers, and it is understood that fractions of rational integers are in their lowest terms. We use g.c.d. and l.c.m. as the customary abbreviations for greatest common divisor and least common multiple, respectively. By $a|b$ we mean that a divides b. We let

$$(a, b) = \text{g.c.d. } \{a, b\} \quad \text{and} \quad [a, b] = \text{l.c.m. } \{a, b\},$$

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

and $P(a; b)$ stands for any one of the four parabolic matrices with fixed point $\rho = a/b$ and of amplitude 1; i.e.,

$$\pm \begin{pmatrix} 1 \pm ab & \mp a^2 \\ \pm b^2 & 1 \mp ab \end{pmatrix}.$$

The principal results of this paper are contained in the following three theorems.

THEOREM 1. *If Γ is a congruence subgroup of ${}_1\Gamma$ of level m and d and e are the respective amplitudes of ∞ and 0 in Γ then $de \equiv 0$ (mod m).*

THEOREM 2. *The least cusp amplitude d in Γ, a congruence subgroup of ${}_1\Gamma$ of level m, is the greatest common divisor of its cusp amplitudes.*

THEOREM 3. *A congruence subgroup Γ of ${}_1\Gamma$ of level m contains a cusp of amplitude m.*

It was Theorem 1 which gave impetus to this investigation. It seems that until now it has escaped being observed. Its content and a proof of it are suggested by the proof of the Theorem of Wohlfahrt [4] which says that for a congruence group of level m the least common multiple of its cusp amplitudes is m. This might be considered as the complementary theorem to our Theorem 2 and it is superseded by our Theorem 3. For this reason we shall not use the Theorem of Wohlfahrt in our proofs, though at times it would suggest alternative or shorter proofs.

The importance of the above results lies in the fact that they permit us to determine the set of cusp amplitudes $C(\Gamma)$ for any congruence group Γ.

2. Proofs of the main theorems

First we prove two lemmas which we use in the proofs of Theorems 1 and 3.

LEMMA 1. *If p is a prime and $(p^2, m) = p$ then*

$$\Gamma = \{\Gamma(m), U^{m/p}, W^{m/p}\} = \Gamma(m/p).$$

Proof. Let

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(m/p)$$

and let $\alpha \equiv 1 \pmod{m/p}$. We are going to show that $A \in \Gamma$. We may assume $(\gamma, p) = 1$. If it does not hold for A then, because $(\alpha, p) = 1$, it is true for $W^{m/p}A$. And $W^{m/p}A \in \Gamma$ implies $A \in \Gamma$. Now one easily checks that, for suitable j and k,

$$W^{km/p}U^{jm/p}(\alpha/\gamma) = \alpha'/\gamma',$$

where $\alpha' \equiv 1$ and $\gamma' \equiv 0 \pmod{m}$. Thus, for suitable β' and δ',

$$\begin{pmatrix} a' & \beta' \\ \gamma' & \delta' \end{pmatrix} \in \Gamma(m),$$

and hence $\alpha'/\gamma' \sim_{\Gamma(m)} \infty$. The last equivalence and $\alpha/\gamma \sim_{\Gamma} \alpha'/\gamma'$ imply $\alpha/\gamma \sim_{\Gamma} \infty$. There exist β'' and δ'' such that

$$B = \begin{pmatrix} \alpha & \beta'' \\ \gamma & \delta'' \end{pmatrix} \in \Gamma,$$

where $\beta'' \equiv 0 \pmod{m/p}$, since all elements of Γ have this property. But $B^{-1}A = U^{j'm/p}$ for a suitable j', and thus $A \in \Gamma$. If, in A, $\alpha \equiv -1 \pmod{m/p}$, then $-\alpha \equiv 1 \pmod{m/p}$; i.e., $-A \in \Gamma$. Since $-I \in \Gamma$, $A \in \Gamma$, completing the proof.

LEMMA 2. *If p is a prime, $(p^2, m) \mathrel{\hat{=}} p^2$, $(a, b) = (ab, p) = 1$ and $P = P(a; b)$, then*

$$\Gamma = \{\Gamma(m), U^{m/p}, W^{m/p}, P^{m/p}\} = \Gamma(m/p).$$

Proof. Clearly, $\Gamma(m/p) \supset \Gamma \supset \Gamma(m)$. It is well known that the index of $\Gamma(m)$ in ${}_1\Gamma$—usually denoted by $[{}_1\Gamma\colon \Gamma(m)]$—is

$$\mu(m) = (m^3/2) \prod_{p|m} (1 - 1/p^2) \quad \text{for } m > 2,\ \mu(2) = 6. \tag{1}$$

We know that $p^2 | m$ implies $[\Gamma(m/p)\colon \Gamma(m)] = p^3$ for $m > 4$, while $[\Gamma(2)\colon \Gamma(4)] = 4$. Also, if $p^2 | m$, then, for j, k, l arbitrary, $U^{jm/p}$, $W^{km/p}$, $P^{lm/p}$ commute with each other mod m, where

$$P^{m/p} = \begin{pmatrix} 1 + abm/p & -a^2m/p \\ b^2m/p & 1 - abm/p \end{pmatrix}.$$

We observe that $U^{jm/p} \equiv W^{km/p} \pmod{m}$ if and only if $j \equiv k \equiv 0 \pmod{p}$. Next we are going to show that for $m > 4$, and any j and k, $U^{jm/p}W^{km/p} \not\equiv \pm P^{m/p}$

(mod m). If the congruence were to hold with the plus sign it would imply that $abm/p \equiv 0 \pmod{m}$, and thus $ab \equiv 0 \pmod{p}$, contradicting the hypotheses. If it were to hold with the minus sign it would imply that $abm/p \equiv 2$ and $abm/p \equiv -2 \pmod{m}$. The last two congruences can only be satisfied provided $m = 4$ and $p = 2$. Thus, for $m = 4$,

$$\{\Gamma(4), U^2, W^2\} = \Gamma(2),$$

and the lemma holds. For $m > 4$, the p^3 matrices $U^{jm/p}W^{km/p}P^{lm/p}$ with $0 \leq j, k, l \leq p - 1$ are incongruent mod m, and hence $[\Gamma: \Gamma(m)] \geq p^3$. Since $[\Gamma(m/p): \Gamma(m)] = p^3$ the conclusion of the lemma follows. As to the content of this lemma see also M. Newman [2].

Proof of Theorem 1. Let $de = s$ and let us assume that $(s, m) \neq m$. First we consider the case $(s, m) = m/p$ for p prime, $p \mid m$. With $\Gamma' = \{\Gamma(m), U^d, W^e\}$, Γ in the hypotheses satisfies $\Gamma \supset \Gamma' \supset \Gamma(m)$. We are going to show that $\Gamma(m/p) \subset \Gamma'$, and thus $\Gamma(m/p) \subset \Gamma$, contradicting that m is the level of Γ. Now, $(s, m) = m/p$ implies $dp \mid m$ and $ep \mid m$; i.e., $U^{m/p}$ and $W^{m/p}$ are in Γ'. If $(p^2, m) = p$, $\Gamma(m/p) \subset \Gamma'$ by Lemma 1, and the proof is complete. If $p^2 \mid m$, by Lemma 2 the proof will be completed by showing that the parabolic matrix A with fixed point 1 and amplitude m/p is in Γ'. It is well known that if $(a, b) = (a', b') = 1$, and $a' \equiv a$ and $b' \equiv b \pmod{m}$, then $a'/b' \underset{\Gamma(m)}{\sim} a/b$. Using the latter and in addition

$$U^{jd}(a/b) = (a + jdb)/b \quad \text{and} \quad W^{ke}(a/b) = a/(b + kea),$$

we can show that, for suitable j and k, the following chain of equivalences under Γ' holds:

$$\infty \sim 1/e \sim (1 + dej)/e \sim (1 + m/p)/e \sim (1 + m/p)/(e + (1 + m/p)ek)$$
$$\sim (1 + m/p)/(m/p)$$

Observing that $W^e(\infty) = 1/e$, we have only to show the third and fifth equivalence. The congruence $1 + dej \equiv 1 + m/p \pmod{m}$ can be satisfied, since $js' \equiv 1 \pmod{p}$, where $s = s'm/p$, and necessarily $(s', p) = 1$, has a solution in j. Since $e \mid m/p$ and $p \mid m/p$ (by the assumption $p^2 \mid m$), it follows that, for any prime q such that $q \mid m/e$, $q \mid m/p$ as well. Hence $(1 + m/p, m/e) = 1$, so that for a suitable k,

$$e + (1 + m/p)ek \equiv m/p \pmod{m}.$$

From $\infty \underset{\Gamma'}{\sim} (1 + m/p)/(m/p)$, we deduce that there is a $B \in \Gamma'$ such that

$$B = \begin{pmatrix} 1 + m/p & \beta \\ m/p & \delta \end{pmatrix},$$

where $\beta \equiv 0 \pmod{d}$, a common property of the matrices in Γ'. As $(s, m) = m/p$ and $s = de$ imply $d \mid m/p$, if

$$A = \begin{pmatrix} 1 + m/p & -m/p \\ m/p & 1 - m/p \end{pmatrix}$$

then, for a suitable l, $B^{-1}A = U^{ld}$. Since B and $U^{ld} \in \Gamma'$, $A \in \Gamma'$, completing the proof when $(s, m) = m/p$.

If $(de, m) \neq m$ and $(de, m) \neq m/p$ we replace e by e', where $e \mid e'$ and $e' \mid m$, such that $(de', m) = m/p$ for some prime p. The remainder of the proof is evident.

COROLLARY 1. *If Γ is a congruence group of level m, and d and e are the respective amplitudes of ∞ and 0 in Γ, then*

(i) $de = m(d, e)/(m/d, m/e)$,

(ii) $(m/d, m/e) \mid (d, e)$.

Proof. Let $(m/d, m/e) = t$. Then $m(d, e) = tde$, implying part (i). Part (ii) is an immediate consequence of Theorem 1.

Next we prove three lemmas, the second of which is the main tool in the proof of Theorem 2.

LEMMA 3. *If $d \mid m$, $e \mid m$ and $de \equiv 0 \pmod{m}$ then*

$$\Gamma = \{\Gamma(m), U^d, W^e\} = \left\{A \in {}_1\Gamma \mid A \equiv \pm \begin{pmatrix} 1 & jd \\ ke & 1 \end{pmatrix} \pmod{m}\right\}.$$

Proof. One easily verifies that any matrix in Γ is of the form

$$\pm \begin{pmatrix} 1 + k_1 m & k_2 d \\ k_3 e & 1 + k_4 m \end{pmatrix}.$$

Conversely, if

$$A \equiv \pm \begin{pmatrix} 1 & jd \\ ke & 1 \end{pmatrix} \pmod{m}$$

then

$$A \equiv \pm W^{ke} U^{jd} \pmod{m}.$$

Hence for a suitable $B \in \Gamma(m)$, $A = W^{ke} U^{jd} B$.

The content of the next lemma is found also in [1].

LEMMA 4. *If $(a, b) = 1$, $(b, m/d) = m/d\sigma$, $P = P(a; b)$ and $\Gamma = \{\Gamma(m), U^d\}$, then*

(i) *the amplitude of a/b in Γ is $d\sigma$ (except when $m = 4$, $d = 1$ and $(b, 4) = 2$ in which case the amplitude is $d(\sigma/2)$), and*

(ii) *for a suitable $A \in \Gamma(m)$ and j with $(j, m/d\sigma) = 1$, $P^{d\sigma} = U^{jd\sigma} A$.*

Proof. Let ρ be the amplitude of a/b in Γ. From $[\Gamma : \Gamma(m)] = m/d$, we deduce $P^{\rho m/d} \in \Gamma(m)$, and thus $d \mid \rho$. Letting $\rho = d\sigma'$,

$$P^{d\sigma'} = \begin{pmatrix} 1 + abd\sigma' & -a^2 d\sigma' \\ b^2 d\sigma' & 1 - abd\sigma' \end{pmatrix}.$$

Applying Lemma 3 with $e = m$, we obtain $abd\sigma' \equiv 0$ and $b^2 d\sigma' \equiv 0 \pmod{m}$. The two congruences imply $b \equiv 0 \pmod{m/d\sigma'}$. From $(b, m/d) = m/d\sigma$ in the hypotheses, it follows that $m/d\sigma' \mid m/d\sigma$, and thus $\sigma \mid \sigma'$. Since, by Lemma 3, $P^{d\sigma} \in \Gamma$ and ρ is the amplitude of a/b in Γ, $\sigma' = \sigma$. It is straightforward to check that a $P^{d\sigma'}$, as defined above, satisfies $P^{d\sigma'} \equiv -U^{jd} \pmod{m}$ only provided $m = 4$, $d = 1$, $(b, 4) = 2$, and then $\sigma' = 1$.

To prove part (ii), we choose j such that $j \equiv -a^2 \pmod{m/d\sigma}$. Since $m/d\sigma \mid b$, $(a, m/d\sigma) = 1$, and thus $(j, m/d\sigma) = 1$. For this j, $U^{jd\sigma} \equiv P^{d\sigma} \pmod{m}$, and the conclusion follows.

Using W instead of U and working with a of the cusp a/b we have:

Lemma 4a. *If $(a, b) = 1$, $(a, m/e) = m/e\tau$, $P = P(a; b)$ and $\Gamma = \{\Gamma(m), W^e\}$, then*

(i) *the amplitude of a/b in Γ is $e\tau$ (except when $m = 4$, $e = 1$ and $(a, 4) = 2$ in which case the amplitude is $e(\tau/2)$), and*

(iii) *for suitable $A \in \Gamma(m)$ and k with $(k, m/e\tau) = 1$, $P^{e\tau} = W^{ke\tau}A$.*

Theorem 2 is a consequence of the following:

Theorem 4. *If r and s are cusp amplitudes in Γ, a congruence subgroup of ${}_1\Gamma$ of level m, then Γ has a cusp of amplitude $z \leq (r, s)$.*

Proof. We are going to show that Γ contains a parabolic matrix of amplitude (r, s). If the fixed point of this parabolic matrix has amplitude z in Γ then $z \leq (r, s)$.

We may assume that $U^r \in \Gamma$. Let a/b be a cusp of amplitude s in Γ and let $P = P(a; b)$. If $(r, s) = t$ we put $r = tr_1$ and $s = ts_1$, where necessarily $(r_1, s_1) = 1$. We consider the subgroup $\Gamma' = \{\Gamma(m), U^r, P^s\}$ of Γ. If $(b, m/r) = m/r\rho$ it follows, by Lemma 4, that $P^{r\rho} \in \Gamma'$, and hence $s \mid r\rho$. Thus $r\rho = t_1 r_1 s_1 \rho_1$, where we have put $\rho = s_1 \rho_1$. We pick

$$A = \begin{pmatrix} a & u \\ b & v \end{pmatrix} \in {}_1\Gamma,$$

where u and v are judiciously chosen later on. Let

$$\Gamma'' = \{\Gamma(m), P^s\} \quad \text{and} \quad \Gamma''_A = A^{-1}\Gamma''A = \{\Gamma(m), U^s\}.$$

In Γ''_A we consider the cusp α/β, where α and β are determined below. If y is the greatest divisor of ρ_1 such that $(y, s_1) = 1$, then $\rho_1 = xy$, where $(x, y) = 1$ and $(r_1, x) = 1$. Now we choose $\beta = m/sx$ and determine α suitably, subject to the condition $(\alpha, \beta) = 1$. For any α with $(\alpha, \beta) = 1$ and $Q = Q(\alpha; \beta)$, $Q^{sx} \in \Gamma''_A$ by Lemma 4. Then $AQ^{sx}A^{-1} = R^{sx}$ is in Γ'', and thus in Γ', where

$$R = R(a\alpha + u\beta;\, b\alpha + v\beta).$$

We observe that $(a\alpha + u\beta, b\alpha + v\beta) = 1$. Next we are going to show that for suitable choices of α and v, $R^{ry} \in \Gamma'$ also. Since $(sx, ry) = t = (r, s)$, this implies that $R^t \in \Gamma'$, and hence $R^t \in \Gamma$, completing the proof.

We consider the cusp $(a\alpha + u\beta)/(b\alpha + v\beta)$ in Γ'. We let $b = b_1 m/r\rho$ and observe that $(b_1, \rho) = 1$. Now

$$\begin{aligned}(b\alpha + v\beta, m/r) &= (m/r\rho)(b_1\alpha + r\rho v/sx, \rho)\\ &= (m/r\rho)(b_1\alpha + r_1 yv, s_1 xy)\\ &= m/ry_1,\end{aligned}$$

where $y_1 \mid y$, provided we can choose α suitably such that $(\alpha, \beta) = 1$ and $b_1\alpha + r_1 yv \equiv 0 \pmod{s_1 x}$. From $(b_1, \rho) = 1$, it follows that $(b_1, s_1 xy) = 1$, and thus the last congruence has the solutions $\alpha_i = \alpha_0 + s_1 xi$, i any integer. Hence it remains to show that for some i', $(\alpha_{i'}, \beta) = 1$. Clearly it suffices to show that we can choose α_0 such that $(\alpha_0, s_1 x) = 1$ and use Dirichlet's Theorem on primes in an arithmetic progression. Since $(r_1 y, s_1 x) = 1$, this can be done by choosing a v in the matrix A such that $(v, s_1 x) = 1$. Now all possible v's in A are of the form $v_k = v_0 + bk$, where $(v_0, b) = 1$ and k is any integer. Applying Dirichlet's Theorem once more for a suitable k', $(v_{k'}, s_1 x) = 1$. Thus R^{ry_1} and $R^{ry} \in \Gamma'$, and the proof is complete.

COROLLARY 2_1. Theorem 2.

COROLLARY 2_2. *Let Γ be a congruence group of level m and let d be the least cusp amplitude in Γ. If d and e are the respective cusp amplitudes of ∞ and 0 in Γ then $e = m/\delta$, where $\delta \mid (d, m/d)$.*

Proof. By Theorem 2, $d \mid e$ and $m \mid e \mid m/d$. Hence $(d, e) = d$ and $(m/d, m/e) = m/e$. Since $m/e \mid d$ by Corollary 1, $m/e \mid (d, m/d)$, and the conclusion follows.

COROLLARY 2_3. *Let d be the least cusp amplitude in Γ, a congruence group of level m. If d is the amplitude of ∞ and k is a rational integer, then the cusp amplitude of k in Γ is m/δ, where $\delta \mid (d, m/d)$.*

Proof. $\Gamma' = U^{-k}\Gamma U^k$ is a congruence group of level m with $U^d \in \Gamma'$. If e is the amplitude of 0 in Γ' then, by Corollary 2_2, $e = m/\delta$, where $\delta \mid (d, m/d)$. Now $\Gamma = U^k\Gamma' U^{-k}$ and $U^k W^e U^{-k} = P^e$, where $P = P(k; 1)$.

Corollaries 2_2 and 2_3 can be used to obtain a number of classes of congruence groups of level m which necessarily have a cusp of amplitude m. But these results are special cases of Theorem 3 which we are going to prove next.

Proof of Theorem 3. Let Γ be a congruence group of level m and let us suppose that all its cusp amplitudes are less than m. We are going to show that Γ is of level $m' < m$, a contradiction.

If d is the least cusp amplitude in Γ we may assume $U^d \in \Gamma$. Furthermore, we may assume that $(d, m/d) > 1$, since, by Corollary 2_3, $(d, m/d) = 1$ would imply that Γ has a cusp of amplitude m. For the amplitude e of 0 in Γ, we have $e = m/\delta_0$ for some $\delta_0 \mid (d, m/d)$ and $\delta_0 > 1$. If $\prod_{i=1}^{r} p_i^{\mu_i}$ is the canonical factorization of $(d, m/d)$ then $\delta_0 = \prod_{i=1}^{r} p_i^{v_i}$, where $0 \leq v_i \leq u_i$ $(1 \leq i \leq r)$ and at least one $v_i \geq 1$. We distinguish two cases.

(i) $v_i \geq 1$ for $1 \leq i \leq r$. By Corollary 2_3, the amplitude of the cusp 1 is $e_1 = m/\delta_1$, where $\delta_1 \mid (d, m/d)$ and $\delta_1 > 1$. Then $(\delta_1, \delta_0) > 1$, and hence there is a prime $p_i \mid (\delta_0, \delta_1)$. Furthermore, $p_i \mid m/d$ implies $d \mid m/p_i$. Thus $\Gamma \supset \Gamma'$, where

$$\Gamma' = \{\Gamma(m), U^{m/p_i}, W^{m/p_i}, P^{m/p_i}\}$$

and $P = P(1;1)$. By Lemmas 1 and 2, $\Gamma' = \Gamma(m/p_i)$, and Γ is of level $m' < m$.

(ii) Let $v_{i_1} = v_{i_2} = \cdots = v_{i_s} = 0$, where $1 \leq s < r$. Again, by Corollary 2_3, the cusp $a = p_{i_1} p_{i_2} \cdots p_{i_s}$ has amplitude $e' = m/\delta'$, where $\delta' \mid (d, m/d)$ and $\delta' > 1$. Either (a) $(\delta', \delta_0) > 1$, and the proof proceeds like in case (i), replacing the cusp 1 by the cusp a, or (b) $(\delta', \delta_0) = 1$. Then there is an h with $1 \leq h \leq s$ such that—letting $i_h = i'$—$Q^{m/p_{i'}} \in \Gamma$, where $Q = Q(a;\, 1)$. By Lemma 4*a*, for suitable j with $(j, p_{i'}) = 1$ and $A \in \Gamma(m)$, $Q^{m/p_{i'}} A = W^{jm/p_{i'}}$. Since W^{m/δ_0} and $W^{jm/p_{i'}}$ are in Γ and $(m/\delta_0, jm/p_{i'}) = m/\delta_0 p_{i'}$, we deduce that the amplitude of 0 in Γ is less than e, a contradiction. This completes the proof of Theorem 3.

A close look at the last proof yields:

COROLLARY 3_1. *If d is the least cusp amplitude of the congruence group Γ of level m and $U^d \in \Gamma$ then there is a rational integer whose amplitude in Γ is m.*

An immediate consequence of Theorem 3 is:

COROLLARY 3_2. *If Γ is a congruence subgroup of ${}_1\Gamma$ of level m then* $[{}_1\Gamma : \Gamma] \geq m$.

We note that equality in Corollary 3_2 holds for the cycloidal congruence groups only, i.e., congruence groups for which all cusps are equivalent under Γ. This latter class of congruence groups has been investigated by H. Petersson in [3].

In Corollary 2_3 we have shown that a lower bound for the cusp amplitude of any integer is $m/(d, m/d) = [d, m/d]$. This is a special case of the following theorem which gives lower bounds for the amplitudes of all cusps in Γ.

THEOREM 5. *Let d be the least cusp amplitude in Γ, a congruence subgroup of ${}_1\Gamma$ of level m, let $U^d \in \Gamma$, and let ρ be the amplitude of the cusp a/b in Γ. If v is the greatest divisor of m/d, with $(b, v) = 1$, then $[d, v] \mid \rho$.*

Proof. Let $P = P(a;\, b)$ and $\Gamma' = \{\Gamma(m), U^d, P^\rho\}$. The diophantine equation $av - bu = 1$ has the solutions

$$u_k = u_0 + ak \quad \text{and} \quad v_k = v_0 + bk,$$

where (u_0, v_0) is a solution of the equation and k is any integer. From $(b, v) = 1$ we deduce that, for a suitable k', $v' = v_0 + bk' \equiv 0 \pmod{v}$. Thus $(v', m/d) = v$ and, by Lemma 4, $Q^{m/v} \in \Gamma'$, where $Q = Q(u';\, v')$ and $u' = u_0 + ak'$. If

$$A = \begin{pmatrix} a & u' \\ b & v' \end{pmatrix}$$

and $\Gamma'' = A^{-1}\Gamma' A$, then U^{ρ} and $W^{m/v} \in \Gamma''$. The latter is a congruence group of level m which implies that $\rho m/v \equiv 0 \pmod{m}$ by Theorem 1, and thus $v \mid \rho$. By Theorem 2, $d \mid \rho$, and hence $[d, v] \mid \rho$.

In the case that m is square-free, i.e., m has no square factor greater than 1, Theorem 5 suffices to determine the amplitudes of all cusps of a congruence group of level m. For we have

COROLLARY 5. *If m is square-free, Γ a congruence group of level m with least cusp amplitude d, and $\Gamma \supset \Gamma' = \{\Gamma(m), U^d\}$, then the amplitudes of a cusp in Γ and Γ' are the same.*

Proof. We consider the cusp a/b. By Lemma 4, if $(b, m/d) = m/d\sigma$ the amplitude of a/b in Γ' is $d\sigma$. If ρ is the amplitude of a/b in Γ then $\rho \mid d\sigma$. If m is square-free then $v = \sigma$ and $[d, v] = d\sigma$. By Theorem 5, $d\sigma \mid \rho$, and thus $\rho = d\sigma$.

If m is square-free and Γ is a congruence group of level m with least cusp amplitude d then there is a $A \in {}_1\Gamma$ such that, if $A\Gamma A^{-1} = \Gamma_A$, $\Gamma_A \supset \Gamma' = \{\Gamma(m), U^d\}$. By Lemma 4, the amplitude of any cusp in Γ' is known. The same is true for Γ_A, by Corollary 5. Thus we can find the amplitude of any cusp in Γ. For any such Γ the set $C(\Gamma)$ of cusp amplitudes is

$$\{d\sigma\colon \sigma \mid m/d \text{ and } \sigma > 0\}.$$

We record this as our next theorem.

THEOREM 6. *Let m be square-free and let d be the least cusp amplitude of Γ, a congruence subgroup of ${}_1\Gamma$ of level m. Then its set of cusp amplitudes is*

$$C(\Gamma) = \{d\sigma\colon \sigma \mid m/d \text{ and } \sigma > 0\}.$$

Also, in the case that m is not square-free, the results of this paper are sufficient to determine, for any congruence group of level m, the amplitudes of its cusps. However the work is much more involved than in the "square-free" case, and the results will be published in another paper.

REFERENCES

1. J. LEWITTES, *Gaps at Weierstrass points for the modular group*, Bull. Amer. Math. Soc., vol. 69 (1963), pp. 578–582.
2. M. NEWMAN, *Normal congruence subgroups of the modular group*, Amer. J. Math., vol. 85 (1963), pp. 419–427.
3. H. PETERSSON, *Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe*, J. Reine Angew. Math., vol. 250 (1971), pp. 182–212.
4. K. WOHLFAHRT, *An extension of F. Klein's level concept*, Illinois J. Math., vol. 8 (1964), pp. 529–535.

UNIVERSITY OF MARYLAND, MUNICH CAMPUS,
MUNICH, GERMANY