ILLINOIS JOURNAL OF MATHEMATICS
Volume 28, Number 2, Summer 1984

THE CUSP AMPLITUDES OF THE CONGRUENCE SUBGROUPS OF THE CLASSICAL MODULAR GROUP (II)

BY

H. LARCHER

1. Introduction

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

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

then A induces the linear fractional substitution $z \to A(z)$, where

$$A(z) = (az + b)/(cz + d), z = x + iy,$$

where x and y are 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 ζ or $\zeta = \infty$, $A(\zeta) = \zeta$. We call ζ the fixed point of $A(z)$ and of A. For a parabolic matrix P with fixed point ζ there exist $B \in {}_1\Gamma$ and a rational integer $n \neq 0$ such that

$$P = \pm B^{-1}U^nB \quad \text{where } U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \zeta = B^{-1}(\infty).$$

The modulus $|n|$ of n is called the amplitude of P. If Γ is a subgroup of ${}_1\Gamma$ and $P \in \Gamma$ then ζ is also referred to as a fixed point or a cusp of Γ. The cusp amplitude of ζ in Γ is the smallest positive rational integer k such that

$$\pm B^{-1}U^kB \in \Gamma.$$

Two cusps η and ζ are said to be eqivalent under Γ, for which we write $\eta \sim_\Gamma \zeta$, if there is a $A \in \Gamma$ such that $\eta = A(\zeta)$. 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.

Received December 11, 1981.

For a positive rational integer m,

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

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 $\Gamma \not\supset \Gamma(k)$ for $k < m$. As 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. All this is found in [2], which represents the principal source of reference.

Notation. If not otherwise stated, all letters 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. Furthermore,

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

By $a|b$ we mean that a divides b and $a > 0$. We let

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

and $P(a; b)$ stands for either of the two parabolic matrices with fixed point $\zeta = a/b$ and of amplitude 1; i.e.,

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

By $\text{amp}(a, b, \Gamma) = r$ we mean that the cusp a/b has amplitude r in Γ. For $d \mid m$,

$$\Gamma(m; m/d) = \{\Gamma(m), U^d\},$$

and for $\Gamma' \subset \Gamma$, $[\Gamma:\Gamma']$ is the index of Γ' in Γ. The determinant and the trace of a matrix A are denoted by $\det A$ and $\text{tr}(A)$, respectively.

In [3] we obtained new results for the cusp amplitudes of congruence groups and with their aid we were able to determine $C(\Gamma)$ for any congruence group of level m in the case that m is square-free; i.e., m has no square factor greater than one. The scope of this paper is to extend those results to any congruence group of level m when m has square factors greater than one. Actually, the results of this paper comprise the square-free m's as special cases. The principal results obtained are summarized in the following three theorems.

THEOREM A. *Let $d|m$, $m/d = h_d^2 n_d$ with square-free n_d, $\varepsilon \mid h_d$,*

$$\chi \mid (d\varepsilon, m/d\varepsilon^2)$$

and $\tau \in R$, where all letters are positive rational integers and R is a reduced residue system mod χ. *Then the groups*

$$\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi) = \Bigg\{ A \in {}_1\Gamma \;\Bigg|\; A = \pm\begin{pmatrix} 1 + k_1(m/\varepsilon\chi) & k_2 d \\ k_3(m/\chi) & 1 + k_4(m/\varepsilon\chi) \end{pmatrix}, \quad k_3 \equiv \tau k_1 \pmod{\chi} \Bigg\},$$

with the exceptions $\Gamma_1(4; 2, 1, 2)$ and $\Gamma_1(8; 8, 2, 2)$, *are congruence subgroups of* ${}_1\Gamma$ *of level m such that*

(i) *d is the least cusp amplitude, and*
(ii) *d and m are the respective cusp amplitudes of* ∞ *and* 0.

Theorem B. *If* $(\varepsilon, 2^{e+1}) = 2^e$ *and* $(m/d, 2^{f+1}) = 2^f$, *where the rational integers e and f are non-negative, then*

$$C(\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi))$$
$$= \{d\,\rho \geqslant 1 \mid (\varepsilon^2, m/d\rho)$$
$$= t^2,\ \rho \text{ and } t \text{ rational integers and } \rho \neq ((\varepsilon, \chi, 2) - 1)2^{f-2\varepsilon}\rho' \text{ with odd } \rho'\},$$

save $C(\Gamma(4; 4)) = C(\Gamma_1(8; 8, 2, 2)) = \{1, 4\}$ *and* $C(\Gamma_1(4; 2, 1, 2)) = \{2\}$.

Theorem C. *If* Γ *is a congruence subgroup of* ${}_1\Gamma$ *of level m then*

(i) $C(\Gamma) = C(\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi))$ *for suitable* d, ε, χ *and* τ, *and*
(ii) $C(\Gamma)$ *is closed under the operations g.c.d. and l.c.m.*

We mention that Theorem A comprises congruence groups which we believe to be new, although it also contains well known groups (e.g., what usually is denoted by $\Gamma_m = \Gamma_1(m;\, m,\, 1,\, 1)$). The importance of Theorem A lies in the fact that, subject to our normalization as stated in part (ii), there are no other congruence groups of level m which can be obtained from $\Gamma(m)$ by lowering the amplitudes of cusps. Thus, we are able to determine the set of cusp amplitudes for any congruence group as follows from Theorem B and part (i) of Theorem C. Part (ii) of Theorem C, rather interesting in itself, will often prove to be useful in showing that a subgroup of ${}_1\Gamma$ is not a congruence group.

Next we give a summary of a few results with proofs or references which are repeatedly used in the paper. It is understood that $m \geqslant 1$ and $d \mid m$.

(1) (i) If $(b, m/d) = m/d\sigma$, or equivalently $\sigma = m/(db, m)$, and $b = b_1 m/d\sigma$ then $(b_1, \sigma) = 1$.

(ii) For any a with $(a, b) = 1$, $\mathrm{amp}(a, b, \Gamma(m; m/d)) = dm/(db, m)$, except when $m = 4$, $d = 1$ and $(b, 4) = 2$ in which case the amplitude is 1 instead of 2.

(iii) $C(\Gamma(m;\ m/d)) = \{d\sigma{:}\sigma|m/d\}$, except $C(\Gamma(4;\ 4)) = \{1,\ 4\}$.
(iv) $[\Gamma(m;\ m/d){:}\Gamma(m)] = m/d$.
(v) If $m > 4$, p a prime and $p^2 \mid m$ then

$$[\Gamma(m/p){:}\Gamma(m)] = p^3; \quad [\Gamma(2){:}\Gamma(4)] = 4.$$

Proofs or references.

(i) $m/d\sigma = (b,\ m/d) = (b_1 m/d\sigma,\ m/d) = (m/d\sigma)(b_1,\ \sigma)$, implying $(b_1,\ \sigma) = 1$.

(ii) See [4] or Lemma 4 of [3]. There it is shown that if

$$(b,\ m/d) = m/d\sigma$$

then $\mathrm{amp}(a,\ b,\ \Gamma(m;\ m/d)) = d\sigma = dm/(db,\ m)$. The exception is dealt with in Lemma 4 of [3].

(iii) By (ii), for any $\sigma \mid m/d$, $\mathrm{amp}(1,\ m/d\sigma,\ \Gamma(m;\ m/d)) = d\sigma$, except for $\Gamma(4;\ 4)$ when $C(\Gamma(4;\ 4)) = \{1,\ 4\}$.

(iv) $\Gamma(m)$ is normal in $\Gamma(m;\ m/d) = \{\Gamma(m),\ U^d\}$.

(v) It follows from the well known formula for the index of $\Gamma(m)$ in ${}_1\Gamma$ (see [1]):

$$[{}_1\Gamma{:}\Gamma(m)] = \mu(m) = (m^3/2)\prod_{p|m}(1 - 1/p^2) \quad \text{for } m > 2, \text{ and } \mu(2) = 6.$$

2. The Congruence Groups $\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi)$

We investigate the existence of congruence groups of level m with least cusp amplitude d, which can be obtained from $\Gamma(m;\ m/d)$ by lowering the amplitudes of cusps. Ignoring $\Gamma(4;\ 4)$, if a/b is a cusp with $\sigma = m/(db,\ m)$ then, by (1)(ii), $\mathrm{amp}(a,\ b,\ \Gamma(m;\ m/d)) = d\sigma$. As we want d to be the least cusp amplitude of the groups to be studied, by Theorem 2 of [3], all cusp amplitudes must be multiples of d. Hence we are going to investigate for which λ's with $\lambda \mid \sigma$,

$$\Gamma = \{\Gamma(m;\ m/d),\ P^{d\sigma/\lambda}\}, \text{ where } P = P(a;\ b),$$

are congruence groups of level m. From Theorem 5 of [3] it follows that $\lambda > 1$ can exist only if m has square factors greater than one. For by this theorem, if p is a prime, $p \mid \sigma$ and $p^2 \nmid m$ then $\Gamma = \{\Gamma(m;\ m/d),\ P^{d\sigma/p}\}$ is not a congruence group of level m. This result appears as Lemma 1 below. Throughout this paper $P = P(a;\ b)$, and we write down for future reference

$$P^{ds} = \begin{pmatrix} 1 + abds & -a^2ds \\ b^2ds & 1 - abds \end{pmatrix}. \tag{2}$$

LEMMA 1. *If $\sigma = m/(db,\ m)$, $P = P(a;\ b)$ and p is a prime such that $p \mid \sigma$ and $p^2 \nmid m$ then $\Gamma = \{\Gamma(m;\ m/d),\ P^{d\sigma/p}\}$ is not a congruence group of level m.*

Proof. By (1)(ii), $\operatorname{amp}(a, b, \Gamma(m; m/d)) = d\sigma$. If ν is the greatest divisor of m/d with $(b, \nu) = 1$ then $p \mid \nu$, since by the hypotheses $(b, m/d) = m/d\sigma$, $p \mid \sigma$ and $p^2 \nmid m$. Hence $[d, \nu] \nmid d\sigma/p$, and, by Theorem 5 of [3], Γ is not a congruence group of level m.

THEOREM 1. *If*

$$\sigma = m/(db, m),\ \lambda \mid (\sigma, db^2) \quad \textit{and} \quad P = P(a; b)$$

then

(i)
$$\begin{aligned}\Gamma &= \{\Gamma(m; m/d), P^{d\sigma/\lambda}\}\\ &= \left\{ A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + k_1(a, \lambda)m/\lambda & k_2 d \\ k_3(b, \lambda)m/\lambda & 1 + k_4(a, \lambda)m/\lambda \end{pmatrix},\right.\\ &\qquad\qquad\qquad \left. a(b, \lambda)k_3 \equiv b(a, \lambda)k_1 \pmod{\lambda} \right\}\end{aligned}$$

and

(ii) $[\Gamma : \Gamma(m; m/d)] = \lambda$.

Proof. It is straightforward to check that the set of all matrices A under matrix multiplication is a group Γ'. We only point out that (a) since $\det A = 1$ we have the congruence

$$(k_1 + k_4)b(a, \lambda) \equiv 0 \pmod{\lambda},$$

showing that $A^{-1} \in \Gamma'$, (b) $\lambda \mid (\sigma, db^2)$ implies $\lambda \mid (\sigma, m^2/d\sigma^2)$ by (1)(i), and (c) $(a, \lambda) \mid d$, since $(a, b) = 1$. Next, it is easily checked that $P^{d\sigma/\lambda}$, using (2) with $s = \sigma/\lambda$, U^d and each matrix in $\Gamma(m)$ are of the form A. Thus $\Gamma' \supset \Gamma$. We complete the proof of part (i) by showing that also $\Gamma \supset \Gamma'$. The latter will hold, if we can find j, k and $B \in \Gamma(m)$ such that $A = BP^{jd\sigma/\lambda}U^{kd}$. This implies that for suitable j,

$$A(\infty) \sim_{\Gamma(m)} P^{jd\sigma/\lambda}(\infty).$$

Using the fact that if $(u, v) = (u', v') = 1$ and $u' \equiv u$ and $v' \equiv v \pmod{m}$ then $u'/v' \sim_{\Gamma(m)} u/v$, if we let $b = b_1 m/d\sigma$ then the equivalence holds if the following congruences have a solution j:

$$(a/(a, \lambda))b_1(m/\lambda)(a, \lambda)j \equiv k_1(a, \lambda)m/\lambda \pmod{m}$$

$$b_1(b/(b, \lambda))(m/\lambda)(b, \lambda)j \equiv k_3(b, \lambda)m/\lambda \pmod{m}$$

or

$$(a/(a, \lambda))b_1 j \equiv k_1 \pmod{\lambda/(a, \lambda)},$$

$$b_1(b/(b, \lambda))j \equiv k_3 \pmod{\lambda/(b, \lambda)}$$

By (1) (i), $(b_1, \sigma) = 1$, and, by hypotheses, $\lambda \mid \sigma$, $(b_1, \lambda) = 1$. Hence a solution of the congruences exists if

$$(a/(a, \lambda))k_3 \equiv (b/(b, \lambda))k_1 \pmod{\lambda/(a, \lambda), \lambda/(b, \lambda)},$$

or, since $(a, b) = 1$ implies $(\lambda/(a, \lambda), \lambda/(b, \lambda)) = \lambda/((a, \lambda)(b, \lambda))$,

$$a(b, \lambda)k_3 \equiv b(a, \lambda)k_1 \pmod{\lambda}.$$

Thus, for suitable j and $B \in \Gamma(m)$, $A(\infty) = BP^{jd\sigma/\lambda}(\infty)$, or

$$A^{-1}BP^{jd\sigma/\lambda} = U^{-kd}$$

for suitable k, since all matrices on the left are elements of $\Gamma(d)$. Hence $A = BP^{jd\sigma/\lambda}U^{kd}$, implying that $\Gamma \supset \Gamma'$ and that $[\Gamma:\Gamma(m; m/d)] = \lambda$.

Theorem 1 defines a class of congruence groups the elements of whose matrices depend on the fixed point and the amplitude of the parabolic matrix used to generate Γ. It is to be expected that certain other parabolic elements would generate one and the same group. Thus we are going to characterize the class of groups, defined in Theorem 1, by matrices whose elements depend on m and d only. As a first step we determine the λ's for all different parabolic matrices which may be used to generate a Γ.

LEMMA 2. *Let $m = h^2n$ with square-free n and*

$$mn/(m, dh) = u^3v$$

with cube-free v. Then $e \mid (m/d)$ and $e^3 \mid (m^2/d)$ if and only if

$$e \mid (m/d, h)u.$$

Proof. One easily verifies that

$$m^2/d = [(hn, d)h/d]^3(hn^2/(hn, d))d^2/(hn, d)^2.$$

As $hn^2/(hn, d) = mn/(m, dh)$, and, by hypotheses, $mn/(m, dh) = u^3v$, where v is cube-free, we obtain

$$m^2/d = [(hn, d)hu/d]^3vd^2/(hn, d)^2 \tag{3}$$

The expression (3) suggests we put

$$m/d = ((hn, d)h/d)(hn/(hn, d)).$$

Since $u^3 v = mn/(m, dh) = hn^2/(hn, d)$ and n is square-free by hypotheses, we deduce that $u \mid hn/(hn, d)$. Thus,

$$m/d = [(hn, d)hu/d]hn/((hn, d)u). \tag{4}$$

Since $(hn/(hn, d), d/(hn, d)) = 1$, and, by hypotheses, v is cube-free, from (3) and (4) we conclude that $e \mid m/d$ and $e^3 \mid m^2/d$ if and only if $e \mid (hn, d)hu/d$. Since $(hn, d)hu/d = (m/d, h)u$, the proof is complete.

THEOREM 2. *If* $m = h^2n$ *with square-free* n *and*

$$mn/(m, dh) = u^3v$$

with cube-free v *then*

(i) $(\sigma, db^2) = (\sigma, m^2/d\sigma^2)$ *for* $\sigma = m/(db, m)$,
(ii) $(\sigma, m^2/d\sigma^2) \mid (m/d, h)u$ *for* $\sigma \mid m/d$,

and

(iii) $\max_{\sigma \mid m/d}(\sigma, m^2/d\sigma^2) = (m/d, h)u$.

Proof. (i) Putting $b = b_1m/d\sigma$ and observing that $(b_1, \sigma) = 1$ by (1)(i), we have $(\sigma, db^2) = (\sigma, b_1^2m^2/d\sigma^2) = (\sigma, m^2/d\sigma^2)$.

(ii) We set $(\sigma, m^2/d\sigma^2) = e$ and observe that $e|m/d$ and $e^3|m^2/d$. The conclusion follows from Lemma 2.

(iii) With $\sigma = e$ and $e = (m/d, h)u$, by Lemma 2, $\sigma \mid m/d$ and $\sigma^3 \mid m^2/d$. Thus $(\sigma, m^2/d\sigma^2) = \sigma = (m/d, h)u$.

We define $S(b) = \{\lambda : \lambda|(m/(db, m), db^2)\}$ and $S = \cup_{b \in Z} S(b)$, where Z denotes the set of rational integers; i.e., S is the set of all λ's which may appear in the matrices of the congruence groups defined in Theorem 1.

COROLLARY 2_1. *If* $m = h^2n$ *with square-free* n *and*

$$mn/(m, dh) = u^3v$$

with cube-free v *then* $S = \{\lambda : \lambda|(m/d, h)u\}$.

Proof. If $\lambda \in S(b)$ then

$$\lambda \mid (m/(db, m), db^2).$$

By Theorem 2, if $\sigma = m/(db, m)$, $\lambda \mid (\sigma, m^2/d\sigma^2)$ and $\lambda \mid (m/d, h)u$. Conversely, if $\lambda \mid (m/d, h)u$ then, by Lemma 2, $\lambda \mid m/d$ and $\lambda^3 \mid m^2/d$, and thus $(\lambda, m^2/d\lambda^2) = \lambda$. We put $b' = m/d\lambda$ and obtain $\lambda = m/(db', m)$. Hence

$$\lambda = (\lambda, m^2/d\lambda^2) = (m/(db', m), db'^2),$$

showing that λ lies in $S(b')$ and in S.

An immediate consequence of Lemma 2 and Theorem 2 is:

COROLLARY 2_2. *If* $\sigma = m/(db, m)$ *and* $\lambda \mid (\sigma, db^2)$ *then* $\lambda^3 \mid m^2/d$.

To make further progress, Theorem 1 would suggest determining the possible (a, λ) and (b, λ) with $\lambda \mid(m/d, h)u$. Although this could be done, we find it more advantageous to proceed differently.

First we are going to study the groups of Theorem 1 for which $(b, \lambda) = \lambda$. From $b = b_1m/d\sigma$ where $(b_1, \sigma) = 1$, by (1) (i), and $\lambda \mid \sigma$, it follows that $\lambda = (b, \lambda) = (b_1m/d\sigma, \lambda) = (m/d\sigma, \lambda)$, and thus $\lambda \mid (\sigma, m/d\sigma)$. We put $\lambda = \varepsilon$ and denote this class of groups by $\Gamma(m; m/d, \varepsilon)$. Clearly

$(a, \lambda) = 1$, and the congruence condition for the elements of the matrices in Theorem 1 is trivially satisfied. Hence we obtain

$$(5)\qquad \Gamma(m; m/d, \varepsilon) = \left\{A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + k_1m/\varepsilon & k_2d \\ k_3m & 1 + k_4m/\varepsilon \end{pmatrix}\right\}.$$

Evidently another parabolic element with fixed point a'/b' such that $\sigma' = m/(db', m)$ and $\varepsilon \mid (\sigma', b')$ generates together with $\Gamma(m; m/d)$ the same group. The question as to the class of all groups of type (5) is answered by the following lemma.

Lemma 3. *If $m = h^2n$ with square-free n then*

(i) $(x, m/x) \mid h$ if $x \mid m$, *and*
(ii) $\max_{x|m}(x, m/x) = h$.

Proof. Using the fact that for square-free s, $(r^2, s) = (r, s)$ we have

$$\begin{aligned} x(x, m/x) &= (x^2, h^2n) \\ &= (x^2, h^2)(x^2/(x^2, h^2), n) \\ &= (x, h)^2(x/(x, h), n) \\ &= (x(x, h), n(x, h)^2) \\ &= (x^2, xh, m) \\ &= x(x, h, m/x). \end{aligned}$$

Thus $(x, m/x) = (x, h, m/x)$, proving part (i). Part (ii) follows from $(h, m/h) = h$.

In the introductory remarks to (5) we have seen that

$$\varepsilon \mid (\sigma, m/d\sigma).$$

Clearly, for each $\sigma \mid m/d$ there exists a cusp a/b such that

$$(b, m/d) = m/d\sigma.$$

Putting $m/d = h_d^2n_d$ with square-free n_d, by Lemma 3, the ε's in $\Gamma(m; m/d, \varepsilon)$ are the divisors of h_d. Observing that

$$(\sigma, m/d\sigma) = (\sigma, b)$$

by (1) (i), we have:

Theorem 3. *If $m/d = h_d^2n_d$ with square-free n_d and $\varepsilon \mid h_d$ then*

(i)

$$\Gamma(m; m/d, \varepsilon) = \left\{A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + k_1m/\varepsilon & k_2d \\ k_3m & 1 + k_4m/\varepsilon \end{pmatrix}\right\}$$

and

(ii)

$$\Gamma(m; m/d, \varepsilon) = \{\Gamma(m; m/d), P^{d\sigma/\varepsilon}\}$$

for any parabolic matrix $P = P(a; b)$ *for which* $\sigma = m/(db, m)$ *and* $\varepsilon \mid (\sigma, b)$.

COROLLARY 3_1. *$\Gamma(m; m/d, \varepsilon)$ is a congruence group of level m.*

Proof. If

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

then the smallest $r > 0$ for which $W^r \in \Gamma(m; m/d, \varepsilon)$ *is* $r = m$.

(1)(ii) gives the amplitude of any cusp in $\Gamma(m; m/d)$. Among the latter groups $\Gamma(4; 4)$ shows an exceptional behavior as noted in (1)(ii) and in (1)(iii). Thus we take a closer look at $\Gamma(4; 4, 2)$ and obtain a result which we need for later reference.

COROLLARY 3_2. $\Gamma(4; 4, 2) = \Gamma(4; 4)$.

Proof. $\Gamma(4; 4, 2)$ is Theorem 3 with $m = 4$, $d = 1$, $h_1 = 2$, $n_1 = 1$ and $\varepsilon = 2$. By Theorem 3, $\varepsilon \mid (\sigma, b)$, so we have to choose a cusp a/b for which $(b, 4) = 2$. From Theorem 3 with $P = P(a; b)$ it follows that $\Gamma(4; 4, 2) = \{\Gamma(4; 4), P\} = \Gamma(4; 4)$, since by (1)(ii) $P \in \Gamma(4; 4)$.

Next we investigate the groups in Theorem 1 for which $(b, \lambda) \neq \lambda$. We put $\lambda = \varepsilon\chi$, where $(b, \lambda) = \varepsilon$, and we note that $(b/\varepsilon, \chi) = 1$. As $\lambda \mid (\sigma, db^2)$ by Theorem 1, $\chi \mid (\sigma/\varepsilon, db^2/\varepsilon)$. Since

$$(b/\varepsilon, \chi) = 1 \quad \text{and} \quad (\sigma/\varepsilon, db^2/\varepsilon) = (\sigma/\varepsilon, d\varepsilon(b/\varepsilon)^2)$$

we conclude that the divisors χ of $(\sigma/\varepsilon, db^2/\varepsilon)$ and of $(\sigma/\varepsilon, d\varepsilon)$ satisfying $(\chi, b/\varepsilon) = 1$ are the same. Letting $(a, \chi) = \chi_1$, from Theorem 1, we have:

LEMMA 4. *If* $\sigma = m/(db, m)$, $\varepsilon \mid (\sigma, b)$, $\chi \mid (\sigma/\varepsilon, d\varepsilon)$ *such that*

$$(\chi, b/\varepsilon) = 1, \quad (a, \chi) = \chi_1 \quad \text{and} \quad P = P(a; b)$$

then

$$\begin{aligned} \Gamma &= \{\Gamma(m; m/d), P^{d\sigma/\varepsilon\chi}\} \\ &= \left\{ A \in {}_1\Gamma \,\middle|\, A = \pm\begin{pmatrix} 1 + k_1(m/\varepsilon\chi)\chi_1 & k_2 d \\ k_3 m/\chi & 1 + k_4(m/\varepsilon\chi)\chi_1 \end{pmatrix}, \right. \\ &\qquad\qquad \left. a\varepsilon k_3 \equiv b\chi_1 k_1 \pmod{\varepsilon\chi} \right\}. \end{aligned}$$

Using Lemma 4 we determine all possible χ's for $\varepsilon \mid h_d$. We define

$$T_\varepsilon(b) = \{\chi : \chi | (\sigma/\varepsilon, d\varepsilon), \sigma = m/(db, m), \varepsilon \mid (\sigma, b) \text{ and } (\chi, b/\varepsilon) = 1\}$$

and $T_\varepsilon = \cup^*_{b \in Z} T_\varepsilon(b)$, where the symbol $\cup^*$ indicates that b runs through those rational integers in Z for which $\varepsilon \mid (\sigma, b)$.

Lemma 5. *If* $\varepsilon \mid h_d$, $T_\varepsilon = \{\chi : \chi | (d\varepsilon, m/d\varepsilon^2)\}$.

Proof. Let $T = \{\chi : \chi | \ (d\varepsilon, m/d\varepsilon^2)\}$. We consider a $T_\varepsilon(b)$ and show that $T_\varepsilon(b) \subset T$. Since $\varepsilon \mid (\sigma, b)$ and

$$(\sigma, b) = (\sigma, b_1 m/d\sigma) = (\sigma, m/d\sigma),$$

and, by (1)(i), $(b_1, \sigma) = 1$, it follows that $\varepsilon \mid m/d\sigma$, or $\sigma \mid m/d\varepsilon$. Thus

$$(\sigma/\varepsilon, d\varepsilon) \mid (m/d\varepsilon^2, d\varepsilon),$$

implying $T_\varepsilon(b) \subset T$. Conversely, let $\chi \in T$. Now we are going to show that for suitable b', $\chi \in T_\varepsilon(b')$. We choose $b' = \varepsilon$. Then, since $\varepsilon \mid h_d$, $(b', m/d) = \varepsilon$, and $\sigma' = m/(db', m) = m/d\varepsilon$. Thus,

$$(\sigma', b') = (m/d\varepsilon, \varepsilon) = \varepsilon;$$

i.e., $\varepsilon \mid (\sigma', b')$. Since $(\sigma'/\varepsilon, d\varepsilon) = (m/d\varepsilon^2, d\varepsilon)$ and $\chi \in T$, we conclude that $\chi \mid (\sigma'/\varepsilon, d\varepsilon)$. Also $(\chi, b'/\varepsilon) = (\chi, 1) = 1$, showing that $\chi \in T_\varepsilon(b')$. Hence $T \subset T_\varepsilon$, which together with $T_\varepsilon \subset T$ proves the lemma.

Lemma 6. *For* $\varepsilon \mid h_d$ *and* $\chi \mid (d\varepsilon, m/d\varepsilon^2)$ *the possible* χ_1'*s in Lemma 4 are the divisors* χ' *of* χ *for which* $(\chi', \varepsilon) = 1$.

Proof. Let a/b be a cusp, as in Lemma 4, for which

$$\varepsilon \mid (\sigma, b), \quad \varepsilon\chi \mid (\sigma, db^2) \quad \text{and} \quad (\chi, b/\varepsilon) = 1,$$

where $\sigma = m/(db, m)$. Since $\varepsilon \mid b$ and $(a, b) = 1$, $(a, \varepsilon) = 1$. Thus, if $(a, \chi) = \chi'$ then $(\chi', \varepsilon) = 1$. Conversely, if $\chi' \mid \chi$ and $(\chi', \varepsilon) = 1$ then $(\chi', b) = 1$, since $(\chi, b/\varepsilon) = 1$. Hence there exists a such that $(a, b) = 1$ and $(a, \chi) = \chi'$.

What remains to be looked at is the congruence satisfied by the elements of the matrices in Lemma 4. By the hypotheses of Lemma 4, $a\varepsilon k_3 \equiv b\chi_1 k_1$ (mod $\varepsilon\chi$) if and only if

$$(a/\chi_1)k_3 \equiv (b/\varepsilon)k_1 \pmod{\chi/\chi_1}.$$

Since $(a/\chi_1, \chi/\chi_1) = (b/\varepsilon, \chi) = 1$, $k_3 \equiv (a/\chi_1)^{-1}(b/\varepsilon)k_1$ (mod χ/χ_1), where $(a/\chi_1)^{-1}$ is an inverse unit of a/χ_1 mod χ/χ_1, showing that $(a/\chi_1)^{-1}b/\varepsilon$ is a reduced residue mod χ/χ_1. Conversely, if τ is a reduced residue mod χ/χ_1 then

$$\tau \equiv (b/\varepsilon)\tau_1 \pmod{\chi/\chi_1}$$

for a suitable reduced residue τ_1 mod χ/χ_1, since $(b/\varepsilon, \chi) = 1$. If τ_1^{-1} is an inverse unit of τ_1 mod χ/χ_1 then

$$(\tau_1^{-1}, \chi/\chi_1) = 1,$$

and thus, by Dirichlet's Theorem on the number of primes in an arithmetic progression, for a suitable j,

$$(\tau_1^{-1} + j\chi/\chi_1, b) = 1.$$

Putting $(\tau_1^{-1} + j\chi/\chi_1)\chi_1 = a'$, we have a cusp a'/b such that

$$(a', \chi) = \chi_1 \quad \text{and} \quad k_3 \equiv \tau k_1 \pmod{\chi/\chi_1},$$

or

$$(a'/\chi_1)k_3 \equiv (b/\varepsilon)k_1 \pmod{\chi/\chi_1}.$$

We have shown that in Lemma 4, for a fixed b and distinct a's with $(a, b) = 1$ and $(a, \chi) = \chi_1$, the congruence condition for the elements of the matrices is of the form $k_3 \equiv \tau k_1 \pmod{\chi/\chi_1}$, and τ assumes all values of a reduced residue system mod χ/χ_1.

From the last paragraph, together with Theorem 1 and Lemmas 4, 5 and 6, we have:

THEOREM 4. *Let $d \mid m$, $m/d = h^2{}_d n_d$ with square-free n_d, $\varepsilon \mid n_d$,*

$$\chi \mid (d\varepsilon, m/d\varepsilon^2),$$

$\chi_1 \mid \chi$ such that $(\chi_1, \varepsilon) = 1$, and $\tau \in R$, a reduced residue system mod *χ/χ_1. Then*

$$\Gamma = \left\{A \in {}_1\Gamma \,\middle|\, A = \pm\begin{pmatrix} 1 + k_1(m/\varepsilon\chi)\chi_1 & k_2 d \\ k_3 m/\chi & 1 + k_4(m/\varepsilon\chi)\chi_1 \end{pmatrix}, \right.$$
$$\left. k_3 \equiv \tau k_1 \pmod{\chi/\chi_1} \right\}$$

is generated by $\Gamma(m)$, U^d and one other suitably chosen parabolic matrix.

The groups $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ are the groups of Theorem 4 for which $\chi_1 = 1$. Now, for any Γ of Theorem 4 there exists an r such that

$$U^r \Gamma U^{-r} = \Gamma_\tau(m; m/d, \varepsilon, \chi)$$

for a suitable $\tau \in R'$, where R' is a reduced residue system mod χ. For if

$$\Gamma = \{\Gamma(m; m/d), P^{dp}\} \quad \text{where } P = P(a; b) \text{ and } (a, \chi) = \chi_1 > 1,$$

then $U^r\Gamma(m; m/d)U^{-r} = \Gamma(m; m/d)$ and

$$U^r P^{dp} U^{-r} = Q^{dp} \quad \text{with } Q = Q(a + rb; b).$$

Since $(a, b) = 1$, by Dirichlet's Theorem on the number of primes in an arithmetic progression, for a suitable r, $(a + rb, \chi) = 1$. As the main thrust of the paper is to find $C(\Gamma)$ for any congruence group and $C(B\Gamma B^{-1}) = C(\Gamma)$ for any $B \in {}_1\Gamma$, we work with the $\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi)$ from here on. Thus we have

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) = \left\{ A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + k_1 m/\varepsilon\chi & k_2 d \\ k_3 m/\chi & 1 + k_4 m/\varepsilon\chi \end{pmatrix}, \quad k_3 \equiv \tau k_1 \pmod{\chi} \right\}. \tag{6}$$

We point out that we have chosen the notation in such a way that

(i) $\Gamma_1(m;\, m/d,\, \varepsilon,\, 1) = \Gamma(m;\, m/d,\, \varepsilon)$,
(ii) $\Gamma_1(m;\, m/d,\, 1,\, 1) = \Gamma(m;\, m/d,\, 1) = \Gamma(m;\, m/d)$, and
(iii) $\Gamma(m;\, 1) = \Gamma(m)$.

In order to show that, with two exceptions, the groups

$$\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi)$$

are congruence groups of level m we determine the amplitudes of their cusps. The exceptions arise when $m/\varepsilon\chi = 2$ and $\chi > 1$, as we shall see below. But first we give an example to present the idea used in the proof of the next lemma. For this we use $\Gamma(4;\, 4)$ whose cusp amplitudes show an irregular behavior as noted in (1)(ii) and (1)(iii):

$$\Gamma(4; 4) = \left\{ A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + 4k_1 & k_2 \\ 4k_3 & 1 + 4k_4 \end{pmatrix} \right\}.$$

Using the plus sign and the matrices A with $\operatorname{tr}(A) = 2$,

$$P^2 = \begin{pmatrix} 1 + 2 \cdot 2 & -2 \\ 4 \cdot 2 & 1 - 2 \cdot 2 \end{pmatrix} \in \Gamma(4; 4),$$

where $P = P(1;\, 2)$. Also

$$B = \begin{pmatrix} 1 - 4 & 1 \\ -4 & 1 \end{pmatrix} \in \Gamma(4; 4)$$

and $\operatorname{tr}(B) = -2$. Since

$$B = -\begin{pmatrix} 1 + 2 \cdot 1 & -1 \\ 4 \cdot 1 & 1 - 2 \cdot 1 \end{pmatrix} = -P,$$

$\operatorname{amp}(1,\, 2,\, \Gamma(4;\, 4)) = 1$.

LEMMA 7. *If* $\sigma = m/(db,\, m)$ *and*

$$\operatorname{amp}(a,\, b,\, \Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi)) = d\rho$$

then $\rho = \sigma/(\sigma,\, \varepsilon\chi,\, b - \tau a\varepsilon)$, *except for* $\Gamma(4;\, 4)$ *and possibly when* $m/\varepsilon\chi = 2$ *with* $\varepsilon\chi > 1$.

Proof. (i) We work with only those matrices A in (6) which have a plus sign and for which $\operatorname{tr}(A) = 2$. For $P = P(a; b)$,

$$P^{d\rho} = \begin{pmatrix} 1 + abd\rho & -a^2d\rho \\ b^2d\rho & 1 - abd\rho \end{pmatrix},$$

and we determine the smallest $\rho > 0$ such that $P^{d\rho} = A$. For this to hold, by (6), ρ must be the smallest positive integer such that $(abd\rho\varepsilon\chi)/m = k_1$ and $(b^2d\rho\chi)/m = k_3$ are integers satisfying

$$(b^2d\rho\chi)/m \equiv \tau(abd\rho\varepsilon\chi)/m \pmod{\chi},$$

or, after putting $b = b_1m/d\sigma$,

$$(b_1b\rho\chi)/\sigma \equiv \tau(ab_1\rho\varepsilon\chi)/\sigma \pmod{\chi}.$$

This implies that $\sigma \mid (b_1b\rho\chi, ab_1\rho\varepsilon\chi)$. Since

$$(b_1b\rho\chi, ab_1\rho\varepsilon\chi) = b_1\rho\chi(b, a\varepsilon) = b_1\rho\chi(b, \varepsilon) = b_1\rho\varepsilon'\chi(b, \varepsilon)/\varepsilon',$$

where $\varepsilon' = (\varepsilon, \sigma, b)$, and since $(b_1, \sigma) = 1$ by (1)(i), it follows that $\sigma \mid \rho\varepsilon'\chi$. We multiply the last congruence by ε' and obtain

$$(b - \tau a\varepsilon)b_1(\rho\varepsilon'\chi)/\sigma \equiv 0 \pmod{\varepsilon'\chi}.$$

First, dividing $\varepsilon'\chi$ on top and σ on bottom of the fraction by $(\sigma, \varepsilon'\chi)$ and then dividing the congruence by $\varepsilon'\chi/(\sigma, \varepsilon'\chi)$ yields

$$\rho/(\sigma/(\sigma, \varepsilon'\chi))(b - \tau a\varepsilon)b_1 \equiv 0 \pmod{(\sigma, \varepsilon'\chi)}.$$

As $(\sigma, b_1) = 1$ by (1)(i), the smallest $\rho > 0$ satisfying the last congruence is $\rho = \sigma/(\sigma, \varepsilon'\chi, b - \tau a\varepsilon)$. Since $\varepsilon' = (\varepsilon, \sigma, b)$, the expression for ρ in the lemma follows from

$$\begin{aligned}(\sigma, \varepsilon\chi, b - \tau a\varepsilon) &= \varepsilon'(\sigma/\varepsilon', \chi\varepsilon/\varepsilon', (b/\varepsilon') - \tau a\varepsilon/\varepsilon') \\ &= \varepsilon'(\sigma/\varepsilon', \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon') \\ &= (\sigma, \varepsilon'\chi, b - \tau a\varepsilon).\end{aligned}$$

(ii) We work with the matrices A in (6) which have a plus sign and for which $\operatorname{tr}(A) = -2$. Again we consider the cusp a/b and we determine the smallest $\rho' > 0$ such that with $P = P(a; b)$,

$$P^{d\rho'} \in \Gamma_\tau(m; m/d, \varepsilon, \chi).$$

For a ρ' to exist such that $\rho' < \rho$, where ρ has been found in part (i), we must have

$$\begin{aligned}P^{d\rho'} &= \begin{pmatrix} 1 + abd\rho' & -a^2d\rho' \\ b^2d\rho' & 1 - abd\rho' \end{pmatrix} \\ &= -\begin{pmatrix} 1 + k_1m/\varepsilon\chi & k_2d \\ k_3m/\chi & 1 + k_4m/\varepsilon\chi \end{pmatrix} \\ &= -A\end{aligned}$$

for suitable k_i $(i = 1, 2, 3, 4)$ and $k_3 \equiv \tau k_1 \pmod{\chi}$. Clearly $\rho' = \rho/2$, since $\operatorname{tr}(A^2) = 2$, and thus A^2 has been considered in part (i). Since $\operatorname{tr}(P^{d\rho'}) = \operatorname{tr}(-A)$, it follows that

$$(k_1 + k_4)m/\varepsilon\chi = -4.$$

It is easily checked that $\det A = 1$ implies $d\varepsilon \mid (k_1 + k_4)$, and thus $d\varepsilon(m/\varepsilon\chi) \mid 4$. We distinguish three cases.

(a) $d\varepsilon = 1$. Since $\chi \mid (d\varepsilon, m/d\varepsilon^2)$ by Theorem 4, this implies $\chi = 1$. This case has been dealt with in Lemma 4 of [3]. It is the exceptional behavior of $\Gamma(4; 4)$ as noted in (1)(ii) and (1)(iii).

(b) $d\varepsilon = 4$. This implies that $m/\varepsilon\chi = 1$. From $\chi \mid (d\varepsilon, m/d\varepsilon^2)$, by Theorem 4 it follows that $d\varepsilon \mid (d^2\varepsilon^2/\chi, m/\varepsilon\chi)$, eliminating this case.

(c) $d\varepsilon = 2$. By the same argument as in (b) one sees that $m/\varepsilon\chi = 2$. Here again, $\varepsilon\chi = 1$ is excluded by Lemma 4 of [3]. Thus $m/\varepsilon\chi = 2$, and $\varepsilon\chi > 1$ is a necessary condition for the conclusion of the lemma not to hold.

This completes the proof of Lemma 7.

For the possible exceptions to Lemma 7 we have:

LEMMA 8. *The groups* $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ *with* $\varepsilon\chi > 1$ *and* $m/\varepsilon\chi = 2$ *are* $\Gamma(4; 4, 2)$, $\Gamma_1(4; 2, 1, 2)$ *and* $\Gamma_1(8; 8, 2, 2)$.

Proof. By Theorem 4 with $\chi_1 = 1$,

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) = \{\Gamma(m; m/d), P^{d\sigma/\lambda}\}$$

for a suitable $P = P(a; b)$, where $\sigma = m/(db, m)$ and $\lambda = \varepsilon\chi$. By Theorem 1, $\lambda \mid (\sigma, db^2)$ and by Corollary 2_2, $\lambda^3 \mid m^2/d$. The hypothesis $m/\varepsilon\chi = 2$ implies $\lambda = m/2$, and thus $(m/2)^3 \mid m^2/d$, or $dm \mid 8$. In the proof of Lemma 7, part (ii)(c), we have seen that $m/\varepsilon\chi = 2$ is possible only provided $d\varepsilon = 2$, so the solutions are

(i) $d = 1, \varepsilon = 2, m = 4, \chi = 1$, i.e., $\Gamma(4; 4, 2)$,
(ii) $d = 2, \varepsilon = 1, m = 4, \chi = 2$, i.e., $\Gamma_1(4; 2, 1, 2)$, and
(iii) $d = 1, \varepsilon = 2, m = 8, \chi = 2$, i.e., $\Gamma_1(8; 8, 2, 2)$.

Of the three groups in Lemma 8 only the last two show an irregular behavior with regard to the cusp amplitudes among the groups $\Gamma_\tau(m; m/d, \varepsilon, \chi)$. We list the cusp amplitudes of all three groups in the next theorem, since in the remainder of the paper we frequently adopt the restriction $m/\varepsilon\chi > 2$, in order not to have to consider the exceptional cases separately. In the next theorem, $\Gamma_0(4)$ is the well known congruence group of level 4.

THEOREM 5. (i) $\Gamma(4; 4, 2) = \Gamma(4; 4)$ and $C(\Gamma(4; 4, 2)) = \{1, 4\}$.

(ii) $\Gamma_1(4; 2, 1, 2) = \Gamma(2)$ *and* $C(\Gamma_1(4; 2, 1, 2)) = \{2\}$.

(iii) $\Gamma_1(8; 8, 2, 2) = \Gamma(4; 4, 2) = \Gamma_0(4)$ *and* $C(\Gamma_1(8; 8, 2, 2)) = \{1, 4\}$.

Proof. (i) See Corollary 3_2 and (1)(iii).

(ii) As $d = 2$, $\Gamma_1(4; 2, 1, 2) \subset \Gamma(2)$. By (1)(v),

$$[\Gamma(2):\Gamma(4)] = 4 \text{ and } [\Gamma_1(4; 2, 1, 2):\Gamma(4)] = 4,$$

so the conclusion follows.

(iii) By (6),

$$\Gamma_1(8; 8, 2, 2) = \left\{A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + 2k_1 & k_2 \\ 4k_3 & 1 + 2k_4 \end{pmatrix},\ k_3 \equiv k_1 \,(\mathrm{mod}\ 2)\right\}.$$

The congruence condition says that k_1 and k_3 are both either even or odd. Let us assume that in the following matrix, k_1 and k_3 are even. Then

$$-\begin{pmatrix} 1 + 2k_1 & k_2 \\ 4k_3 & 1 + 2k_4 \end{pmatrix} = \begin{pmatrix} 1 - 2(k_1 + 1) & -k_2 \\ -4k_3 & 1 - 2(k_4 + 1) \end{pmatrix}$$
$$= \begin{pmatrix} 1 + 2k_1' & k_2' \\ 4k_3' & 1 + 2k_4' \end{pmatrix},$$

where k_1' is odd and k_3' is even. Hence

$$\Gamma_1(8; 8, 2, 2) = \left\{A \in {}_1\Gamma \;\middle|\; A = \pm\begin{pmatrix} 1 + 2k_1 & k_2 \\ 4k_3 & 1 + 2k_4 \end{pmatrix}\right\};$$

i.e., by Theorem 3, $\Gamma_1(8; 8, 2, 2) = \Gamma(4; 4, 2) = \Gamma_0(4)$. The last equality holds, since one may drop the negative sign with the matrices.

Combining Lemmas 7 and 8 and Theorem 5 we obtain:

THEOREM 6. *If* $\sigma = m/(db, m)$ *and*

$$\mathrm{amp}(a, b, \Gamma_\tau(m; m/d, \varepsilon, \chi)) = d\rho$$

then

$$\rho = \sigma/(\sigma, \varepsilon\chi, b - \tau a\varepsilon) = m/(m, db(\varepsilon\chi, b - \tau a\varepsilon)),$$

except for $\Gamma(4; 4)$, $\Gamma_1(4; 2, 1, 2)$ *and* $\Gamma_1(8; 8, 2, 2)$.

COROLLARY 6_1. *The congruence groups* $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ *are of level* m, *except* $\Gamma_1(4; 2, 1, 2)$ *and* $\Gamma_1(8; 8, 2, 2)$.

Proof. We apply Theorem 6 to the cusp $0 = 0/1$, i.e., $a = 0$ and $b = 1$. Since $\sigma = m/(db, m) = m/(d, m) = m/d$ and

$$\rho = (m/d)/(m/d, \varepsilon\chi, 1) = m/d,$$

$\mathrm{amp}(0, 1, \Gamma_\tau(m; m/d, \varepsilon, \chi) = m$, implying that the level is m. The exceptions follow from Theorem 5.

COROLLARY 6_2. *If* $\sigma = m/(db, m)$ *and* $(a, b) = 1$ *then, excepting* $\Gamma(4; 4)$, $\Gamma_1(4; 2, 1, 2)$ *and* $\Gamma_1(8; 8, 2, 2)$,

(i) $$\operatorname{amp}(a, b, \Gamma(m; m/d, \varepsilon)) = d\sigma/\varepsilon'$$

with $\varepsilon' = (\varepsilon, \sigma, b) = (\varepsilon, \sigma, m/d\sigma)$, *and*

(ii) $$\operatorname{amp}(a, b, \Gamma_\tau(m; m/d, \varepsilon, \chi)) = d\sigma/\varepsilon' \chi'$$

with $\varepsilon' = (\varepsilon, \sigma, b) = (\varepsilon\chi', \sigma, b)$ *and* $\chi' = (\sigma/\varepsilon', \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon')$.

Proof. (i) Using Theorem 6 with $\chi = 1$ and $\tau = 1$ we obtain

$$(\sigma, \varepsilon, b - a\varepsilon) = (\sigma, \varepsilon, b) = \varepsilon'.$$

Also $(\sigma, \varepsilon, b) = (\sigma, \varepsilon, m/d\sigma)$, since, by (1)(i), if $b = b_1 m/d\sigma$, $(b_1, \sigma) = 1$.

(ii) Applying Theorem 6 again and using the fact that $(\varepsilon, \sigma, b) = \varepsilon'$, we have

$$\begin{aligned}(\sigma, \varepsilon\chi, b - \tau a\varepsilon) &= \varepsilon'(\sigma/\varepsilon', \chi\varepsilon/\varepsilon', (b/\varepsilon') - \tau a\varepsilon/\varepsilon') \\ &= \varepsilon'(\sigma/\varepsilon', \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon') \\ &= \varepsilon'\chi'.\end{aligned}$$

From the last equality, it follows that $(\chi', b/\varepsilon') = 1$, showing that $\varepsilon' = (\varepsilon\chi', \sigma, b)$.

COROLLARY 6_3. *Let* $P = P(a; b)$ *and* $\sigma = m/(db, m)$. *Then*

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) = \{\Gamma(m; m/d), P^{d\sigma/\varepsilon\chi}\}$$

if and only if

$$\operatorname{amp}(a, b, \Gamma_\tau(m; m/d, \varepsilon, \chi)) = d\sigma/\varepsilon\chi.$$

Proof. If $\operatorname{amp}(a, b, \Gamma_\tau(m; m/d, \varepsilon, \chi)) = d\sigma/\varepsilon\chi$ then, by Theorem 6,

$$\Gamma = \{\Gamma(m; m/d), P^{d\sigma/\varepsilon\chi}\} \subset \Gamma_\tau(m; m/d, \varepsilon, \chi),$$

and, by Theorem 1 with $\lambda = \varepsilon\chi$,

$$[\Gamma_\tau(m; m/d, \varepsilon, \chi):\Gamma(m; m/d)] = \varepsilon\chi.$$

By hypotheses and (1)(ii),

$$\operatorname{amp}(a, b, \Gamma(m; m/d)) = d\sigma, \ [\Gamma:\Gamma(m; m/d)] \geqslant \varepsilon\chi,$$

implying equality of the two groups. The converse is trivial.

From Theorem 4 with $\chi_1 = 1$ and (6) it follows that

$$\Gamma = \Gamma_\tau(m; m/d, \varepsilon, \chi) \subset \Gamma(d).$$

Since $U^d \in \Gamma$, d is the least cusp amplitude and is the amplitude of ∞ in Γ. By the proof of Corollary 6_1, with the two exceptions noted, the amplitude of 0 in Γ is m. Thus, from Theorem 4 with $\chi_1 = 1$, and (6), we obtain Theorem A in the introduction.

Next we are going to show that the groups $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ are the only congruence groups of level m which, subject to the normalization as contained in part (ii) of Theorem A, may be obtained from $\Gamma(m)$ by lowering the amplitudes of cusps.

THEOREM 7. *If* $(\varepsilon\chi, \varepsilon'\chi') = 1$ *then*

$$\Gamma_{\tau''}(m;\, m/d,\, \varepsilon\varepsilon',\, \chi\chi') = \Gamma_{\tau}(m;\, m/d,\, \varepsilon,\, \chi) \cup \Gamma_{\tau'}(m;\, m/d,\, \varepsilon',\, \chi')$$

for suitable reduced residues τ mod χ *and* τ' mod χ'.

Proof. We denote the three respective groups by Γ'', Γ and Γ'. By Theorem 4, for suitable $P = P(a;\, b)$ with $\sigma = m/(db, m)$,

$$\Gamma'' = \{\Gamma(m;\, m/d),\, P^{d\sigma/\varepsilon\varepsilon'\chi\chi'}\},$$

and $(\sigma,\, \varepsilon\varepsilon'\chi\chi',\, b - \tau''a\varepsilon\varepsilon') = \varepsilon\varepsilon'\chi\chi'$ by Corollary 6_3. Since

$$(\varepsilon', \chi) = (\tau'', \chi\chi') = 1,$$

$\tau = \tau''\varepsilon'$ is a reduced residue mod χ, implying that

$$(\sigma,\, \varepsilon\chi,\, b - \tau a\varepsilon) = \varepsilon\chi;$$

i.e., $\{\Gamma(m;\, m/d),\, P^{d\sigma/\varepsilon\chi}\} = \Gamma$ by Corollary 6_3. Correspondingly, with $\tau' = \tau''\varepsilon$, $\{\Gamma(m;\, m/d),\, P^{d\sigma/\varepsilon'\chi'}\} = \Gamma'$. The hypothesis $(\varepsilon\chi, \varepsilon'\chi') = 1$ implies

$$P^{d\sigma/\varepsilon\varepsilon'\chi\chi'} \in \Gamma \cup \Gamma^1,$$

showing that $\Gamma \cup \Gamma' = \Gamma''$.

In Theorem 1 we introduced for $\lambda \mid db^2$ the groups

$$\Gamma = \{\Gamma(m;\, m/d),\, P^{d\sigma/\lambda}\},$$

and in the succeeding work we have put $\lambda = \varepsilon\chi$. From Corollary 6_1 we know that almost all these groups are congruence groups of level m. Now we are going to show that if $\lambda \mid \sigma$ and $\lambda \nmid db^2$ then Γ is not of level m. In fact, we shall immediately prove a more general result by investigating what happens to $\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi)$ when lowering the amplitude of any of its cusps by a prime p, provided, of course, its amplitude is divisible by dp. Because of Theorem 7, it suffices to work with the groups

$$\Gamma_\tau(m;\, m/d,\, p^i,\, p^k),$$

where p is a prime and $i, k \geqslant 0$. We can smoothe the presentation by disregarding the exceptional cases and $\Gamma(4;\, 4, 2)$, and thus in the following we assume $m/\varepsilon\chi > 2$.

LEMMA 9. *If, for a prime* p,

$$\Gamma = \Gamma_\tau(m;\, m/d,\, p^i,\, p^k) \quad \textit{with } i + k \geqslant 1 \textit{ and } m/p^{i+k} > 2,$$

and $\Gamma' = \{\Gamma, \Gamma(m/p)\}$ *then*

(i) $\Gamma' = \Gamma_\tau(m/p;\, (m/p)/d,\, p^i,\, p^{k-1})$ *or* $\Gamma(m/p;\, (m/p)/d,\, p^{i-1})$ *depending whether* $k \geqslant 1$ *or* $k = 0$, *and*

(ii) $[\Gamma':\Gamma] = p$.

Proof. (i) By Theorem 4, $\Gamma = \{\Gamma(m; m/d), P^{d\sigma/p^j}\}$ for suitable $P = P(a; b)$, where $\sigma = m/(db, m)$ and $j = i + k$. Thus

$$\Gamma' = \{\Gamma(m/p; (m/p)/d), P^{d\sigma/p^j}\},$$

since $j \geqslant 1$ in the hypotheses implies $p \mid m/d$. Since $j \geqslant 1$, it also follows that $(b, (m/p)/d) = (m/p)/(d\sigma/p)$; i.e.,

$$\operatorname{amp}(a, b, \Gamma(m/p; (m/p)/d) = d\sigma/p$$

by (1)(ii). By Theorem 1, $p^j \mid (\sigma, db^2)$, and hence $p^{j-1} \mid (\sigma/p, db^2)$, showing that

$$[\Gamma' : \Gamma(m/p; (m/p)/d)] = p^{j-1}$$

by Theorem 1. Since $(\sigma, p^j, b - \tau a p^i) = p^j$ by Corollary 6_3,

$$(\sigma/p, p^{j-1}, b - \tau a p^i) = p^{j-1}$$

(we point out that the last still holds when $k = 0$) implying, by Corollary 6_3, the conclusion of part (i).

(ii) The hypotheses $m/p^j > 2$ and $j \geqslant 1$ imply $m > 4$ by Lemma 8. We use the following schema in the proof, where necessarily $p^2 \mid m$ by Lemma 1:

$$\tag{7} \begin{array}{ccccc} \Gamma(m) & \overset{m/d}{\subset} & \Gamma(m; m/d) & \overset{p^j}{\subset} & \Gamma \\ p^3 \cap & & p^2 \cap & & p \cap \\ \Gamma(m/p) & \underset{m/dp}{\subset} & \Gamma(m/p;\ (m/p)/d) & \underset{p^{j-1}}{\subset} & \Gamma'. \end{array}$$

The expressions with the symbol "$\subset$" are the respective indices. While the first four indices from the left follow from (1)(iv) and (1)(v), the remaining three are consequences of the proof of part (i) and Theorem 1.

LEMMA 10. *Let* Γ *and* Γ' *be defined as in Lemma 9*, $j = i + k \geqslant 1$, $m/p^j > 2$, $\sigma = m/(db, m)$, $\operatorname{amp}(a, b, \Gamma) = d\rho$, $\rho = \sigma/p^{j'}$ *and* $p \mid \rho$. *If* $j' < j$ *then* $\operatorname{amp}(a, b, \Gamma') = d\rho/p$,

Proof. By the hypotheses, and Theorem 6 applied to Γ, we have

$$(\sigma, p^j, b - \tau a p^i) = p^{j'}.$$

The hypothesis $p \mid \rho$ implies $(b, (m/p)/d) = (m/p)/(d\sigma/p)$ and, by (1)(ii),

$$\operatorname{amp}(a, b, \Gamma(m/p; (m/p)/d)) = d\sigma/p.$$

Theorem 6 applied to Γ', and the hypotheses $p \mid \rho$ and $j' < j$ imply, by part (i) of Lemma 9, that

$$(\sigma/p, p^{j-1}, b - \tau a p^i) = p^{j'};$$

i.e., $\operatorname{amp}(a, b, \Gamma') = d\sigma/p^{j'+1} = d\rho/p$.

LEMMA 11. *Let $m > 4$, $\sigma = m/(db, m)$, $p^{j+1} \mid \sigma$, where p is a prime and $j \geqslant 0$, $(p^{j+1}, \sigma, db^2) = p^j$ and $P = P(a; b)$. If*

$$\Gamma = \{\Gamma(m; m/d), P^{d\sigma/p^j}\}, \quad \Gamma_1 = \{\Gamma, P^{d\sigma/p^{j+1}}\}, \quad \Gamma' = \{\Gamma, \Gamma(m/p)\}$$

and

$$\Gamma_1' = \{\Gamma_1, \Gamma(m/p)\}$$

then

(i) $[\Gamma_1:\Gamma] > p$, *and*
(ii) $[\Gamma_1':\Gamma'] = p$ *when* $j \geqslant 1$, *and* $[\Gamma_1':\Gamma'] = 1$ *when* $j = 0$.

Proof. (i) From (2) with $s = \sigma/p^{j+1}$ it follows that

$$P^{d\sigma/p^{j+1}} U^d P^{-d\sigma/p^{j+1}} = Q^d,$$

where $Q = Q(a'; b')$ with

$$a' = 1 + abd\sigma/p^{j+1} \quad \text{and} \quad b' = b^2 d\sigma/p^{j+1};$$

i.e., $\text{amp}(a', b', \Gamma_1) = d$. Now we are going to show that

$$\text{amp}(a', b', \Gamma) = dp.$$

Letting $b = b_1 m/d\sigma$, where $(b_1, \sigma) = 1$ by (1)(i), we obtain

$$(b^2 d\sigma/p^{j+1}, m/d) = (m/dp^{j+1})(db, p^{j+1})$$

and, by (1)(i) and (1)(ii),

(8) $$\text{amp}(a', b', \Gamma(m; m/d)) = dp^{j+1}/(db, p^{j+1}).$$

We let $(p^j, b) = p^i$ and $j = i + k$. Since by hypotheses $p^j \mid (\sigma, db^2)$, from Theorem 1 and Corollaries 6_2 and 6_3 it follows that, for suitable τ with $(\tau, p) = 1$, $\Gamma = \Gamma_\tau(m; m/d, p^i, p^k)$, where

(9) $$(\sigma, p^j, b - \tau a p^i) = p^j.$$

We use Theorem 6 to find $\text{amp}(a', b', \Gamma)$. We have

$$\begin{aligned}
&(p^{j+1}/(db, p^{j+1}), p^j, b' - \tau a' p^i) \\
&\qquad = (p^{j+1}/(db, p^{j+1}), p^j, bd(\sigma/p^{j+1})(b - \tau a p^i) - \tau p^i) \\
&\qquad = (p^{j+1}/(db, p^{j+1}), p^i(p^k, bd(\sigma/p^{j+1})(b/p^i - \tau a) - \tau)) \\
&\qquad = (p^{j+1}/(db, p^{j+1}), p^i),
\end{aligned}$$

since $(p, \tau) = 1$ and (9) imply that $p^k \mid (b/p^i - \tau a)$. The hypotheses and $(p^j, b) = p^i$ imply

$$p^j = (p^{j+1}, db^2) = p^i(p^{k+1}, db).$$

Thus, $(p^{j+1}, db) = p^k$ and $(p^{j+1}/(db, p^{j+1}), p^i) = p^i$. This shows that the right side of (8) is dp^{i+1}, and hence

$$\text{amp}(a', b', \Gamma) = dp.$$

The latter result together with $\mathrm{amp}(a', b', \Gamma_1) = d$, shown above, can be used to prove that $[\Gamma_1{:}\Gamma] > p$. We assume that $[\Gamma_1{:}\Gamma] = p$. Then $\Gamma_1 = \Sigma_{r=1}^{p} Q^{dr}\Gamma$, and for a suitable $A \in \Gamma$ and r with $1 \leqslant r \leqslant p - 1$, $Q^{dr}\mathrm{A} = \mathrm{P}^{d\sigma/p^{j+1}}$. This would imply

$$Q^{dr}A(\infty) = a'/b'$$

and, since $Q = Q(a'; b')$, $A(\infty) = a'/b'$, or $a'/b' \sim_{\Gamma} \infty$. The last equivalence would imply that $\mathrm{amp}(a', b', \Gamma) = d$, a contradiction.

(ii) By hypothesis,

$$\Gamma_1' = \{\Gamma(m/p; (m/p)/d), P^{d\sigma/p^{j+1}}\}.$$

The hypotheses $p \mid \sigma$ and $\sigma = m/(db, m)$ imply that

$$(b, (m/p)/d) = (m/p)/(d\sigma/p),$$

and thus, by (1)(ii), $\mathrm{amp}(a, b, \Gamma(m/p; (m/p)/d)) = d\sigma/p$. From the hypotheses $p^{j+1} \mid \sigma$ and $(p^{j+1}, \sigma, db^2) = p^j$, it follows that

$$p^j \mid (\sigma/p, db^2).$$

Hence, by Theorem 1,

$$[\Gamma_1'{:}\Gamma(m/p; (m/p)/d)] = p^j \quad \text{and} \quad [\Gamma'{:}\Gamma(m/p; (m/p)/d)] = p^{j-1},$$

proving part (ii) when $j \geqslant 1$. For $j = 0$,

$$\mathrm{amp}(a, b, \Gamma') = \mathrm{amp}(a, b, \Gamma_1') = d\sigma/p,$$

implying $\Gamma' = \Gamma_1'$.

The last three lemmas enable us to prove the principal result which we set out to show and which is contained in:

THEOREM 8. *If, for a prime p,*

$$\Gamma = \Gamma_\tau(m; m/d, p^i, p^k),$$

$(a, b) = 1$, $\mathrm{amp}(a, b, \Gamma) = d\rho$, $p \mid \rho$, $P = P(a; b)$ *and* $\Gamma_1 = \{\Gamma, P^{d\rho/p}\}$, *then either*

(i) $\Gamma_1 = \Gamma_{\tau'}(m; m/d, p^{i'}, p^{k'})$ *for suitable* τ' *and* $i', k' \geqslant 0$, *or*

(ii) Γ_1 *is not a congruence group of level* m.

Proof. The theorem holds for $\Gamma_1(4; 2, 1, 2)$ and $\Gamma_1(8; 8, 2, 2)$, since, by Theorem 5, their respective levels are 2 and 4. Since

$$[\Gamma(2; 2){:}\Gamma(4; 4)] = [\Gamma(2; 1){:}\Gamma(4; 2)] = 2$$

it follows that the theorem also holds for $\Gamma(4; 4)$ and $\Gamma(4; 2)$. Thus, in the following we may assume $m > 4$. Because of Lemma 1 we may also assume $p^2 \mid m$. If $\sigma = m/(db, m)$ and $j = i + k$,

$$(\sigma, p^j, b - \tau a p^i) = p^{j'} \quad \text{with } 0 \leqslant j' \leqslant j,$$

and thus, by Theorem 6, $\rho = \sigma/p^{j'}$. We distinguish the cases $j' < j$ and $j' = j$.

(i) Suppose $j' < j$. Now we are going to show that Γ_1 is a group of level m/p. Since $m > 4$ and $p^2 \mid m$, $[\Gamma(m/p):\Gamma(m)] = p^3$ by (1) (v). Observing that $j' < j$ implies $j \geqslant 1$, we use schema (7):

$$\begin{tikzcd}
\Gamma \arrow[r, hook, "x"] \arrow[d, hook, "p"'] & \Gamma_1 \arrow[dl, hook] \\
\Gamma^1 &
\end{tikzcd}$$

where $\Gamma' = \{\Gamma, \Gamma(m/p)\}$. By Lemma 10, the hypothesis $p \mid \rho$ implies that

$$\operatorname{amp}(a, b, \Gamma') = d\rho/p.$$

Since $x \geqslant p$ $\Gamma_1 = \Gamma'$; i.e., Γ_1 is a congruence group of level m/p.

(ii) Suppose $j' = j$. By Corollary 6_3, $\Gamma = \{\Gamma(m;\, m/d),\, P^{d\sigma/p^j}\}$ *and* $\rho = \sigma/p^j$. If $p^{j+1} \mid db^2$ then, by Theorem 1 and Theorem 4,

$$\Gamma_1 = \Gamma_{\tau'}(m;\, m/d,\, p^{i'},\, p^{k'})$$

for suitable τ' and i', $k' \geqslant 0$. If $p^{j+1} \nmid db^2$ we use again schema (7):

$$\begin{tikzcd}
\Gamma(m; m/d) \arrow[r, hook, "p^j"] \arrow[d, hook, "p^2"'] & \Gamma \arrow[r, hook, "x"] \arrow[d, hook, "p"'] & \Gamma_1 \arrow[d, hook, "y"'] \\
\Gamma(m/p; (m/p)/d) \arrow[r, hook, "p^{j-1}"'] & \Gamma' \arrow[r, hook, "p"'] & \Gamma_1',
\end{tikzcd}$$

where

$$\Gamma' = \{\Gamma, \Gamma(m/p)\} \quad \text{and} \quad \Gamma_1' = \{\Gamma_1, \Gamma(m/p)\},$$

and, by Lemma 11, $[\Gamma_1:\Gamma] = x > p$ and $[\Gamma_1':\Gamma'] = p$ for $j \geqslant 1$. If $j = 0$, $\Gamma = \Gamma(m;\, m/d)$, and, by Lemma 11, $\Gamma_1' = \Gamma' = \Gamma(m/p;\, (m/p)/d)$. In both cases $xy = p^2$, and, since $x > p$, $y = 1$, showing that Γ_1 is a group of level m/p.

The next two results are immediate consequences of Theorems 7 and 8. In particular, the first corollary follows from Theorem 1 and the proof of Theorem 8.

Corollary 8_1. *Let* $\sigma = m/(db, m)$, $\lambda \mid \sigma$, $P = P(a;\, b)$ *and* $m/\lambda > 2$. *Then* $\Gamma = \{\Gamma(m;\, m/d),\, p^{d\sigma/\lambda}\}$ *is a congruence group of level m if and only if* $\lambda \mid db^2$.

Corollary 8_2. *The groups* $\Gamma_\tau(m;\, m/d,\, \varepsilon,\, \chi)$ *for all admissible* d, ε, χ *and* τ, *comprise all congruence groups of level m which, subject to our normalization, may be obtained from* $\Gamma(m)$ *by lowering the amplitudes of cusps.*

In the following final section we are going to determine the set of cusp amplitudes for any congruence group.

3. The Cusp Amplitudes of a Congruence Group

Let Γ be a congruence group of level m, d the least cusp amplitude in Γ, and α/β a cusp with $\operatorname{amp}(\alpha, \beta, \Gamma) = d$. As $(\alpha, \beta) = 1$, there is a matrix

$$A = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in {}_1\Gamma$$

such that $U^d \in \Gamma' = A^{-1}\Gamma A$. By Corollary 3_1 of [3], there is a rational integer k with $\operatorname{amp}(k, 1, \Gamma') = m$. Thus $\Gamma'' = U^{-k}\Gamma' U^k$ is a congruence group of level m having the properties:

(i) its least cusp amplitude is d,
(ii) $\operatorname{amp}(\infty, \Gamma'') = d$, and
(iii) $\operatorname{amp}(0, 1, \Gamma'') = m$.

By Corollary 8_2, for suitable ε, χ and τ, $\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi)$ is a congruence group having the properties:

(i) $\Gamma'' \supset \Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi)$ and
(ii) $\operatorname{amp}(a, b, \Gamma'') = \operatorname{amp}(a, b, \Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi))$ for any cusp a/b or ∞.

It is easily seen that for a parabolic matrix P of amplitude one and $A \in {}_1\Gamma$, $A^{-1}P^sA = Q^s$, where s is any rational integer and Q a suitable parabolic matrix of amplitude one. Thus, if $C(\Gamma)$ is the set of cusp amplitudes of Γ as defined in the introduction then $C(A^{-1}\Gamma A) = C(\Gamma)$ for any $A \in {}_1\Gamma$. We have proved the following theorem which appears also as part (i) of Theorem C in the introduction.

THEOREM 9. *For a congruence subgroup* Γ *of* ${}_1\Gamma$ *of level* m,

$$C(\Gamma) = C(\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi))$$

for suitable $d \mid m$, $\varepsilon \mid h_d$, $\chi \mid (d\varepsilon, m/d\varepsilon^2)$ *and* $\tau \in R$, *where* $m/d = h_d^2 n_d$ *with square-free* n_d *and* R *is a reduced residue system* mod χ.

The remainder of the paper deals with finding

$$C(\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi))$$

and with proving the properties of the cusp amplitudes as stated in part (ii) of Theorem C. To save in writing, we shall frequently use the abbreviations $\Gamma\langle\varepsilon\rangle$ and $\Gamma\langle\varepsilon, \chi\rangle$ for the respective groups $\Gamma(m;\ m/d,\ \varepsilon)$ and $\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi)$. The next theorem characterizes the cusp amplitudes of $\Gamma\langle\varepsilon\rangle$ and is in the case $\varepsilon = 1$ a restatement of (1)(iii).

THEOREM 10. *With the exception of* $\Gamma(4;\ 4)$, $d\rho \geq 1$ *is a cusp amplitude of* $\Gamma(m;\ m/d,\ \varepsilon)$ *if and only if* $(\varepsilon^2, m/d\rho)$ *is a perfect square.*

Proof. Save $\Gamma(4;\ 4) = \Gamma(4;\ 4,\ 1)$, for $\sigma = m/(db, m)$ and a with $(a, b) = 1$,

$$\operatorname{amp}(a, b, \Gamma(m; m/d)) = d\sigma$$

by (1)(ii). Thus, by (1)(iii), the theorem holds for $\varepsilon = 1$. By Corollary 6_2, $\operatorname{amp}(a, b, \Gamma\langle\varepsilon\rangle) = d\rho$, where $\rho = \sigma/\varepsilon'$ and $\varepsilon' = (\varepsilon, \sigma, b)$. Now we are going to show that $(\varepsilon^2, m/d\rho)$ is a perfect square. Since for $(r, s) = 1$, $(rs, t) = (r, t)(s, t)$, it suffices to prove it for $\varepsilon = p^k$, where p is a prime and $k \geqslant 1$. If

$$(p^k, \sigma, b) = (p^k, \sigma, m/d\sigma) = p^l,$$

where $b = b_1 m/d\sigma$ and we use the fact that $(b_1, \sigma) = 1$ by (1)(i), and $\sigma = \rho p^l$, then $(p^{k-l}, \rho, m/(d\rho p^{2l})) = 1$. Thus, for some $u \geqslant 0$,

$$(p^{k-l}, m/d\rho p^{2l}) = p^u.$$

We distinguish the two cases $u = 0$ and $u > 0$.

(i) Suppose $u = 0$. Then $(p^{k+l}, m/d\rho) = p^{2l}$, and, since $l \leqslant k$,

$$(p^{2k}, m/d\rho) = p^{2l},$$

a perfect square.

(ii) Suppose $u > 0$. Then $(\rho, p) = 1$. From $m/d = h_d^2 n_d$ and $\varepsilon \mid h_d$, by Theorem 3 it follows that $p^{2k} \mid m/d$. Thus $p^{2k} \mid m/d\rho$, and

$$(p^{2k}, m/d\rho) = p^{2k},$$

a perfect square.

Conversely, if $\rho \mid m/d$ and $(\varepsilon^2, m/d\rho) = \varepsilon'^2$ then $d\sigma = d\rho\varepsilon'$ is the amplitude of some cusp a/b in $\Gamma(m; m/d)$ whose amplitude in $\Gamma\langle\varepsilon\rangle$ is $d\rho$. For, from $(\varepsilon^2, m/d\rho) = \varepsilon'^2$ we obtain

$$(\varepsilon\varepsilon', m/d\rho) = \varepsilon'^2, \quad (\varepsilon, \rho\varepsilon', m/d\rho\varepsilon') = \varepsilon' \quad \text{and} \quad (\varepsilon, \sigma, m/d\sigma) = \varepsilon'.$$

The conclusion follows from Corollary 6_2 and the observation that, by (1)(iii) ($\Gamma(4; 4)$ excepting), for any $\sigma \mid m/d$, $d\sigma$ is a cusp amplitude in $\Gamma(m; m/d)$.

The following lemmas serve to characterize the cusp amplitudes of $\Gamma\langle\varepsilon, \chi\rangle$. First we take a closer look at χ' in Corollary 6_2.

LEMMA 12. *If* $\sigma = m/(db, m)$, $(a, b) = 1$, $\varepsilon' = (\varepsilon, \sigma, b)$ *and*

$$(\sigma/\varepsilon', \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon') = \chi'$$

then $(\chi', b/\varepsilon') = (\chi', \tau a\varepsilon/\varepsilon') = 1$.

Proof. Since $(\chi, \tau) = 1$, $(\chi', \tau) = 1$. Suppose $(\chi', a\varepsilon/\varepsilon') = \chi_1 > 1$. This implies $\chi_1 \mid b/\varepsilon'$, since $\chi_1 \mid (b/\varepsilon' - \tau a\varepsilon/\varepsilon')$. From $(a, b) = 1$ in the hypotheses we deduce $\chi_1 \mid \varepsilon/\varepsilon'$. This contradicts $(\varepsilon, \sigma, b) = \varepsilon'$, since by hypotheses $\chi_1 \mid \sigma/\varepsilon'$. Similarly, if one assumes $(\chi', b/\varepsilon') = \chi_2 > 1$.

In the following we put down again the restriction $m/\varepsilon\chi > 2$, in order not to have to consider the exceptional cases separately.

LEMMA 13. *For $m/\varepsilon\chi > 2$, $C(\Gamma_\tau(m; m/d, \varepsilon, \chi)) \subset C(\Gamma(m; m/d, \varepsilon))$.*

Proof. We consider the cusp a/b, which satisfies the hypotheses of Lemma 12. Suppose $d\rho$ and $d\rho'$, where by Corollary 6_2, $\rho = \sigma/\varepsilon'$ and $\rho' = \rho/\chi'$, are the respective amplitudes of a/b in $\Gamma\langle\varepsilon\rangle$ and in $\Gamma\langle\varepsilon, \chi\rangle$. We are going to show that $d\rho' \in C(\Gamma\langle\varepsilon\rangle)$. By Theorem 10, for a suitable t,

$$(\varepsilon^2, m/d\rho) = t^2.$$

As $\varepsilon' = (\varepsilon, \sigma, m/d\sigma)$ by Corollary 6_2 and $m/d\sigma = m/d\rho\varepsilon'$,

$$(\varepsilon\varepsilon', \rho\varepsilon'^2, m/d\rho) = \varepsilon'^2,$$

implying that $\varepsilon' \mid t$. Hence

$$((\varepsilon/\varepsilon')^2, m/d\rho\varepsilon'^2) = (t/\varepsilon')^2.$$

Since $(\chi', \varepsilon/\varepsilon') = 1$ by Lemma 12, $((\varepsilon/\varepsilon')^2, m/d\rho'\varepsilon'^2) = (t/\varepsilon')^2$, and thus $(\varepsilon^2, m/d\rho') = t^2$, showing that $d\rho' \in C(\Gamma\langle\varepsilon\rangle)$ by Theorem 10.

LEMMA 14. *Let*

$$\Gamma = \Gamma_\tau(m; m/d, \varepsilon, \chi),$$

$m/\varepsilon\chi > 2$, $\sigma \mid m/d$, $(\varepsilon, \sigma, m/d\sigma) = \varepsilon'$, $\rho = \sigma/\varepsilon'$ and let χ_1 be the greatest divisor of (ρ, χ) such that $(\chi_1, \varepsilon/\varepsilon') = (\chi_1, m/d\sigma\varepsilon') = 1$. If $(\varepsilon', \chi_1, 2) = 1$ then $d\rho$ lies in $C(\Gamma(m; m/d, \varepsilon))$ and in $C(\Gamma)$.

Proof. By (1)(iii), for any $\sigma \mid m/d$, $d\sigma \in C(\Gamma(m; m/d))$, so

$$d\rho \in C(\Gamma(m; m/d, \varepsilon))$$

by Corollary 6_2. Using Corollary 6_2 once more, the proof will be completed by showing that for suitable b_1 and a such that $(b_1, \sigma) = 1$, $b = b_1 m/d\sigma$ and $(a, b) = 1$, $(\rho, \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon') = 1$. We put $r = m/d\rho\varepsilon'^2$ and $s = \tau\varepsilon/\varepsilon'$ and observe that, by hypotheses, $(r, \chi_1) = (s, \chi_1) = 1$. The solutions of

$$xr/(r, s) \equiv 1 \pmod{\chi_1}$$

are $x_j = x_0 + j\chi_1$, where x_0 is a solution and j any integer. As $(x_0, \chi) = 1$, by Dirichlet's Theorem on the number of primes in an arithmetic progression, for a suitable j, $x_0 + j\chi_1 = p$, p a prime satisfying $(p, \sigma) = 1$. Correspondingly, $y_0 + k\chi_1$ are the solutions of $ys/(r, s) \equiv -1 \pmod{\chi_1}$. Hence, for a suitable k, $y_0 + k\chi_1 = q$, q a prime satisfying $(q, p) = (q, m/d\sigma) = 1$. Now $(\varepsilon', \chi_1, 2) = 1$ in the hypotheses may be broken down into the two cases $2 \nmid \chi_1$, and $2 \mid \chi_1$ and $2 \nmid \varepsilon'$, which we treat separately.

(i) Suppose $2 \nmid \chi_1$. Then $pr - qs \equiv 2(r, s) \pmod{\chi_1}$. The hypotheses $2 \nmid \chi_1$, $(r, \chi_1) = (s, \chi_1) = 1$ and Lemma 12 imply $(\rho, \chi, p(m/d\rho\varepsilon'^2) - \tau q\varepsilon/\varepsilon') = 1$; i.e., the cusp $q/(pm/d\sigma)$ has amplitude $d\rho$ in $\Gamma\langle\varepsilon\rangle$ and in $\Gamma\langle\varepsilon, \chi\rangle$.

(ii) Suppose $2 \mid \chi_1$ and $2 \nmid \varepsilon'$. Then $pr + 2qs \equiv -(r, s) \pmod{\chi_1}$. The hypotheses $2 \mid \chi_1$, $2 \nmid \varepsilon'$ and $(\chi_1, m/d\rho\varepsilon'^2) = 1$ imply $2 \nmid (m/d\rho\varepsilon')$, and thus $(2, m/d\sigma) = 1$. Hence, as in case (i), the cusp $-2q/(pm/d\sigma)$ has amplitude $d\rho$ in $\Gamma\langle\varepsilon\rangle$ and in $\Gamma\langle\varepsilon, \chi\rangle$.

Lemma 14 does not hold when $(\varepsilon', \chi_1, 2) = 2$. For then $m/d\sigma\varepsilon'$ and ε/ε' are odd. Since $2 \mid \varepsilon'$ implies $2 \mid \sigma$ and $(b_1, \sigma) = 1$ by (1)(i), b_1 is odd. Thus $b_1 m/d\sigma\varepsilon' = b/\varepsilon'$ is odd. From $2 \mid \varepsilon'$ and $(a, b) = 1$ we deduce that a is odd. It follows from $\chi_1 \mid \chi$ and $(\chi, \tau) = 1$ that τ is odd. Thus $2 \mid (b/\varepsilon' - \tau a\varepsilon/\varepsilon')$, the difference of two odd integers, and hence,

$$2 \mid (\rho, \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon'),$$

since $2 \mid \chi_1$ and $\chi_1 \mid (\rho, \chi)$ by the hypotheses of Lemma 14; i.e., while $\operatorname{amp}(a, b, \Gamma\langle\varepsilon\rangle) = d\rho$, $\operatorname{amp}(a, b, \Gamma\langle\varepsilon, \chi\rangle) = d\rho_1$, where $2\rho_1 \mid \rho$. This is part of the proof of:

LEMMA 15. *If*

$$\Gamma = \Gamma_\tau(m; m/d, \varepsilon, \chi),$$

$m/\varepsilon\chi > 2$, $\sigma \mid m/d$, $(\varepsilon, \sigma, m/d\sigma) = \varepsilon'$, $\rho = \sigma/\varepsilon'$, χ_1 *is the greatest divisor of* (ρ, χ) *such that*

$$(\chi_1, \varepsilon/\varepsilon') = (\chi_1, m/d\sigma\varepsilon') = 1,$$

and $(\varepsilon', \chi_1, 2) = 2$ *then*

(i) $\rho = 2^{f-2e}\rho'$, *where* ρ' *is odd*, $(m/d, 2^{f+1}) = 2^f$ *and* $(\varepsilon, 2^{e+1}) = 2^e$ *with* $e, f \geqslant 1$, *and*

(ii) $d\rho \in C(\Gamma(m; m/d, \varepsilon))$ *and* $d\rho \notin C(\Gamma)$.

Proof. (i) The hypotheses $(\varepsilon', \chi_1, 2) = 2$, $(\chi_1, \varepsilon/\varepsilon') = 1$ and $(\varepsilon, 2^{e+1}) = 2^e$ imply $2^e \mid \varepsilon'$. From the hypotheses $(\varepsilon', \chi_1, 2) = 2$, $(\chi_1, m/d\sigma\varepsilon') = 1$ and $(m/d, 2^{f+1}) = 2^f$ it follows that $2^f \mid \sigma\varepsilon'$, or $2^f \mid \rho\varepsilon'^2$. Thus $2^{f-2e} \mid \rho$ and $\rho = 2^{f-2e}\rho'$ for suitable odd ρ'. Note that necessarily $f - 2e > 0$.

(ii) By Corollary 6_2, $d\rho \in C(\Gamma\langle\varepsilon\rangle)$. By the introductory remarks to Lemma 15, all cusp amplitudes $d\rho$ with $\rho = 2^{f-2e}\rho'$ and odd ρ' are lowered under χ to $d\rho_1$, where $2\rho_1 \mid \rho$. Thus the proof of part (ii) will be completed by showing that no cusp amplitude in $\Gamma\langle\varepsilon\rangle$ is lowered under χ to $d2^{f-2e}\rho'$ for some odd ρ'. Suppose that $d2^g\rho''$ with $g > f - 2e$ and odd ρ'' has the latter property. Although for $\rho = 2^g\rho''$ the corresponding ε' and χ_1 are different from those defined in the hypotheses, we still use the same notation. Since ρ is not of the form $2^{f-2e}\rho'$, by part (i) $(\varepsilon', \chi_1, 2) = 1$. If

$$(2^g\rho'', \chi, (b/\varepsilon') - \tau a\varepsilon/\varepsilon') = \chi',$$

where a/b is a cusp with $\operatorname{amp}(a, b, \Gamma\langle\varepsilon\rangle) = d2^g\rho''$, the proof will be completed by showing that $2 \nmid \chi'$. We break $(\varepsilon', \chi_1, 2) = 1$ down into two cases.

(a) If $2 \nmid \chi_1$ then, by Lemma 12, $2 \nmid \chi'$.

(b) It is impossible to have $2 \mid \chi_1$ and $2 \nmid \varepsilon'$ since $2^e \mid \varepsilon$ and $e \geqslant 1$ by hypotheses imply $2 \mid \varepsilon/\varepsilon'$, contradicting $(\chi_1, \varepsilon/\varepsilon') = 1$.

Combining Theorem 10 and Lemmas 13, 14 and 15 we obtain:

THEOREM 11. *If* $(m/d, 2^{f+1}) = 2^f$ *and* $(\varepsilon, 2^{e+1}) = 2^e$ *with* $e, f \geqslant 0$ *then*

$$C(\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi)) = \{d\rho \geqslant 1 \mid (\varepsilon^2, m/d\rho) = t^2 \text{ and } \rho \neq ((\varepsilon, \chi, 2) - 1)2^{f-2e}\rho' \text{ with odd } \rho'\},$$

except for $\Gamma(4;\ 4)$, $\Gamma_1(4;\ 2,\ 1,\ 2)$ *and* $\Gamma_1(8;\ 8,\ 2,\ 2)$.

From Theorem 11 together with Theorem 5 we have Theorem B in the introduction.

Example. We determine $C(\Gamma(48;\ 24,\ 2))$ and $C(\Gamma_1(48;\ 24,\ 2,\ 2))$. For the meanings of the letters used, see Theorems 4 and 11. We have $m/d = 48/2 = 24 = 2^2 \cdot 6$, implying $h_2 = 2$ and $n_2 = 6$. Thus $\varepsilon \mid 2$, and we have to choose $\varepsilon = 2$. Since

$$(d\varepsilon,\ m/d\varepsilon^2) = (4,\ 48/2 \cdot 2^2) = (4,\ 6) = 2,$$

$\chi \mid 2$ and we have to choose $\chi = 1$ and $\chi = 2$ for the respective groups

$$\Gamma(48;\ 24,\ 2) \quad \text{and} \quad \Gamma_1(48;\ 24,\ 2,\ 2),$$

where necessarily $\tau = 1$. Since $(\varepsilon^2, m/d\rho) = (4, 24/\rho)$ it follows, by Theorem 11, that the solutions of $(4, 24/\rho) = 1^2$ are $\rho = 8, 24$, and the solutions of $(4, 24/\rho) = 2^2$ are $\rho = 1, 2, 3, 6$. Hence

$$C(\Gamma(48;\ 24,\ 2)) = \{2, 4, 6, 12, 16, 48\}.$$

From $m/d = 48/2 = 24 = 2^3 \cdot 3$ and $\varepsilon = 2$, it follows that $f = 3$ and $e = 1$, and thus $f - 2e = 1$. Since $(\varepsilon, \chi, 2) = (2, 2, 2) = 2$, we obtain

$$C(\Gamma_1(48;\ 24,\ 2,\ 2))$$

by removing from $C(\Gamma(48;\ 24,\ 2))$ those cusp amplitudes 2ρ for which $\rho = 2\rho'$ with odd ρ'; namely $\rho = 2$ and $\rho = 6$. Thus,

$$C(\Gamma_1(48;\ 24,\ 2,\ 2)) = \{2, 6, 16, 48\}.$$

Finally, we prove a result which, we presume, anyone sufficiently familiar with congruence groups suspected of being true and which, as far as the g.c.d. is concerned, also was raised as a question by K. Wohlfahrt in a letter to the author. The theorem appears also as part (ii) of Theorem C in the introduction.

THEOREM 12. $C(\Gamma_\tau(m;\ m/d,\ \varepsilon,\ \chi))$ *is closed under the operations* g.c.d. *and* l.c.m.

Proof. It certainly holds for the three exceptional cases whose cusp amplitudes are listed in Theorem 5. Else, let $d\rho$ and $d\rho'$ be two elements of $C(\Gamma\langle\varepsilon, \chi\rangle)$. By Theorem 10 and Lemma 13, $(\varepsilon^2, m/d\rho) = t^2$ and $(\varepsilon^2, m/d\rho') = t'^2$ for suitable $t, t' \geqslant 1$. Thus,

$$\begin{aligned}[t, t']^2 &= [t^2, t'^2] \\ &= [(\varepsilon^2, m/d\rho), (\varepsilon^2, m/d\rho')] \\ &= (\varepsilon^2, [m/d\rho, m/d\rho']) \\ &= (\varepsilon^2, m/d(\rho, \rho'))\end{aligned}$$

and

$$\begin{aligned}(t, t')^2 &= (t^2, t'^2) \\ &= ((\varepsilon^2, m/d\rho), (\varepsilon^2, m/d\rho')) \\ &= (\varepsilon^2, (m/d\rho, m/d\rho')) \\ &= (\varepsilon^2, m/d[\rho, \rho']).\end{aligned}$$

By Theorem 11,

$$d(\rho, \rho') = (d\rho, d\rho') \quad \text{and} \quad d[\rho, \rho'] = [d\rho, d\rho']$$

are in $C(\Gamma\langle\varepsilon, \chi\rangle)$, since, in the case $(\varepsilon, \chi, 2) = 2$, if ρ and ρ' are not of the form $2^{f-2e}\rho''$ with odd ρ'', the same holds for (ρ, ρ') and $[\rho, \rho']$.

With the results of this paper, the principal problem remaining is to find for $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ all congruence groups Γ of level m such that

(i) $\Gamma_\tau(m; m/d, \varepsilon, \chi) \subset \Gamma \subset {}_1\Gamma$ and
(ii) $C(\Gamma) = C(\Gamma_\tau(m; m/d, \varepsilon, \chi))$.

References

1. R. C. Gunning, *Lectures on modular forms,* Princeton University Press, Princeton, New Jersey, 1962.

2. F. Klein and R. Fricke, *Vorlesungen Über die Theorie der elliptischen Modulfunktionen,* 2 Bde, Leipzig, 1890.

3. H. Larcher, *The cusp amplitudes of the congruence subgroups of the classical modular group,* Illinois J. Math., vol. 26 (1982), pp. 164–172.

4. J. Lewittes, *Gaps at Weierstrass points for the modular group,* Bull. Amer. Math. Soc., vol. 69 (1963), pp. 578–582.

University of Maryland, Munich Campus
Munich, Germany