ACTA ARITHMETICA
145.4 (2010)

Dimensions of spaces of modular forms for $\Gamma_H(N)$

by

Jordi Quer (Barcelona)

1. Introduction. All the basic facts and results about modular forms used in this paper can be found in Chapters 1 and 2 of Shimura's book [6].

Let Γ' be any subgroup of finite index of the group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, or more generally any Fuchsian group of the first kind $\Gamma' \subset \mathrm{SL}_2(\mathbb{R})$. Let $X(\Gamma') = \Gamma'\backslash\mathfrak{H}^*$ be the set of orbits endowed with the usual structure of compact Riemann surface, where $\mathfrak{H}^*$ denotes the union of the Poincaré upper half plane $\mathfrak{H}$ and the set of cusps of Γ' in $\mathbb{P}^1(\mathbb{R})$ (for subgroups of $\mathrm{SL}_2(\mathbb{Z})$ the set of cusps is $\mathbb{P}^1(\mathbb{Q})$).

In this situation, applying the Riemann–Roch theorem one obtains a formula for the dimensions of the spaces of modular and cuspidal forms of integer weight $k \geq 2$ for the group Γ' in terms of the following invariants: the genus g of the curve, the number ν_m of Γ'-orbits of elliptic points of every order m of the group Γ', and the number $\nu_\infty = \nu_\infty^{\mathrm{reg}} + \nu_\infty^{\mathrm{irr}}$ of its Γ'-orbits of regular and irregular cusps (cf. Theorems 2.23–2.25 in [6]).

In addition, in the case of a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, the genus of the curve $X(\Gamma')$ can be obtained by applying the Riemann–Hurwitz formula to the covering $X(\Gamma') \to X(\Gamma)$. Since the ramification of this covering is concentrated in the elliptic points and the cusps, the genus is a function of the degree ν_0 of the covering and the numbers of elliptic points and cusps.

Hence, for subgroups $\Gamma' \subseteq \Gamma$, the computation of the genus of the corresponding modular curve and of the dimensions of the spaces of modular and cuspidal forms is reduced to the computation of the following invariants:

- $\nu_0(\Gamma')$, the degree of the covering $X(\Gamma') \to X(\Gamma)$;
- $\nu_2(\Gamma')$ and $\nu_3(\Gamma')$, the numbers of Γ'-orbits of elliptic points of orders 2 and 3 of Γ';
- $\nu_\infty(\Gamma') = \nu_\infty^{\mathrm{reg}}(\Gamma') + \nu_\infty^{\mathrm{irr}}(\Gamma')$, the numbers of Γ'-orbits of regular and irregular cusps of Γ'.

2010 *Mathematics Subject Classification*: Primary 11F11.
Key words and phrases: modular forms, cusp forms, congruence subgroups.

DOI: 10.4064/aa145-4-4

Explicit formulas for these invariants for the congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(N)$ are a standard topic of the theory of modular forms, and can be found in many textbooks on the subject (e.g. in [6, 3, 5, 8] and many others). Using them, the computation of genera and dimensions has been implemented in several computer packages, including PARI, Magma and Sage.

The main objective of this paper is to give analogous formulas for all congruence subgroups $\Gamma_H(N)$ sitting between $\Gamma_1(N)$ and $\Gamma_0(N)$. Our interest (and need) for such formulas comes from work of the author and of William Stein towards the implementation of modular symbols computations for these groups in Sage and Magma. We remark that the values of the formulas can be easily computed in practice from the number N and the group H; the computations have been implemented by the author in Sage, Magma and Mathematica.

Formulas for the dimensions of the spaces of modular forms for $\Gamma_0(N)$ with Nebentypus character were given by Cohen and Oesterlé in their 1976 paper [1]. The paper does not contain proofs, and the authors say that these formulas "sont connues de beaucoup de gens et il existe plusieurs méthodes permettant de les obtenir (théorème de Riemann–Roch, application des formules de trace données par Shimura dans [7])." These formulas are also implemented as standard functions in some computer packages. In spite of the considerable literature on the subject published in the last three decades, including several textbooks containing detailed proofs of the formulas for the groups Γ_1 and Γ_0, and also the development of simplified formulas for the dimensions of newform subspaces (cf. [4]), no proof of the formula for the spaces with character seems to have been published. In this paper we obtain the same formula by a different procedure: we first deduce an expression for the dimensions of these spaces in terms of the dimensions of spaces for congruence subgroups $\Gamma_H(N)$, and then we use the formulas we obtained for these dimensions to transform this expression into the one given by Cohen and Oesterlé.

In Section 2 we recall some basic facts about congruence subgroups that will be used, especially those related to elliptic points and cusps, and we introduce some notation; in Section 3 we give explicit formulas for the invariants ν_0, ν_2, ν_3, ν_∞ and $\nu_\infty^{\mathrm{reg}}$ for all congruence subgroups $\Gamma_H(N)$; in Section 4 we obtain an expression for the dimensions of spaces of forms with character in terms of those invariants, and transform it to arrive at the Cohen–Oesterlé formulas.

2. The dimension formulas. From now on, let $\Gamma' \subseteq \Gamma = \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index (for instance, a congruence subgroup). This group

acts on $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ by linear fractional transformations

$$\gamma(z) = \frac{az+b}{cz+d}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma', \qquad z \in \mathfrak{H}^*.$$

We will denote by $\Gamma'^{\pm}$ the group $\{\pm 1\} \cdot \Gamma'$ and by $\overline{\Gamma'}$ the group $\Gamma'^{\pm}/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{Z})$ of linear fractional transformations of $\mathfrak{H}^*$ induced by elements of Γ'. We will denote by $\nu_0(\Gamma')$ the degree of the covering of Riemann surfaces $X(\Gamma') \to X(\Gamma)$; it is given by the index of the subgroup $\Gamma'^{\pm}$ in Γ:

$$\nu_0(\Gamma') = [\overline{\Gamma} : \overline{\Gamma'}] = [\Gamma : \Gamma'^{\pm}].$$

We recall that a point $z \in \mathfrak{H}$ is an *elliptic point* of Γ' if the isotropy subgroup $\Gamma'_z = \{\gamma \in \Gamma' \mid \gamma(z) = z\}$ contains non-scalar elements; in that case $\Gamma'^{\pm}_z$ is a cyclic group of order 4 or 6, and the elliptic point is said to be of *order* 2 or 3, respectively (in general, the order of an elliptic point z is defined as the order of the group $\overline{\Gamma'_z}$). The set of elliptic points is the union of a finite set of orbits for the action of Γ' on $\mathfrak{H}$, each of which corresponds to a point on the curve $X(\Gamma')$, also called an elliptic point. Let $\nu_2(\Gamma')$ and $\nu_3(\Gamma')$ denote the numbers of elliptic points of each order in the curve $X(\Gamma')$. For example, the curve $X(\Gamma)$ has two elliptic points: the orbit of $i = \sqrt{-1}$, of order 2, and the orbit of $\rho = e^{2\pi i/3}$, of order 3, and hence $\nu_2(\Gamma) = \nu_3(\Gamma) = 1$.

The points of $\mathbb{P}^1(\mathbb{Q})$ are the *cusps* of Γ', and they are the union of a finite set of orbits for that group: the cusps of the curve $X(\Gamma')$. For every cusp $z \in \mathbb{P}^1(\mathbb{Q})$ the isotropy subgroup $\Gamma'^{\pm}_z$ is of the form $\{\pm W^m \mid m \in \mathbb{Z}\}$ for some matrix $W \in \Gamma'^{\pm}$ of trace 2. If $-1 \notin \Gamma'$ then the isotropy subgroup Γ'_z is an infinite cyclic subgroup of index 2 in $\Gamma'^{\pm}_z$, and the cusp z is said to be *irregular* or *regular* depending on whether or not this subgroup contains ($\Leftrightarrow$ is generated by) a matrix of trace -2. The condition of regularity is an invariant of the Γ'-orbit, and hence one may speak of regular and irregular cusps of the curve $X(\Gamma')$. Let $\nu_\infty(\Gamma') = \nu_\infty^{\mathrm{reg}}(\Gamma') + \nu_\infty^{\mathrm{irr}}(\Gamma')$ denote the number of cusps of the curve $X(\Gamma')$, given as the sum of the number of regular and irregular ones for groups with $-1 \notin \Gamma'$.

Now, in terms of the invariants just described, the genus of the curve $X(\Gamma')$ and the dimensions of the spaces $M_k(\Gamma')$ of modular forms and $S_k(\Gamma')$ of cuspidal modular forms of weight $k \geq 2$ for the group Γ' are given in the following theorems (for proofs see for example Proposition 1.40 and Theorems 2.23, 2.24 and 2.25 of Shimura [6], or Theorems 3.1.1, 3.5.1 and 3.6.1 of Diamond–Shurman [3]).

THEOREM 2.1. *The genus of the curve $X(\Gamma')$ is*

$$g(X(\Gamma')) = 1 + \frac{\nu_0(\Gamma')}{12} - \frac{\nu_2(\Gamma')}{4} - \frac{\nu_3(\Gamma')}{3} - \frac{\nu_\infty(\Gamma')}{2}.$$

THEOREM 2.2. *If $k \geq 2$ is even, then*

$$\dim S_k(\Gamma') = \delta_{2,k} + \frac{k-1}{12}\nu_0(\Gamma') + \left(\left\lfloor \frac{k}{4} \right\rfloor - \frac{k-1}{4}\right)\nu_2(\Gamma') + \left(\left\lfloor \frac{k}{3} \right\rfloor - \frac{k-1}{3}\right)\nu_3(\Gamma') - \frac{\nu_\infty(\Gamma')}{2},$$

$$\dim M_k(\Gamma') = -\delta_{2,k} + \dim S_k(\Gamma') + \nu_\infty(\Gamma').$$

If $k \geq 3$ is odd and $-1 \notin \Gamma'$, then

$$\dim S_k(\Gamma') = \frac{k-1}{12}\nu_0(\Gamma') + \left(\left\lfloor \frac{k}{3} \right\rfloor - \frac{k-1}{3}\right)\nu_3(\Gamma') - \frac{\nu_\infty^{\mathrm{reg}}(\Gamma')}{2},$$

$$\dim M_k(\Gamma') = \dim S_k(\Gamma') + \nu_\infty^{\mathrm{reg}}(\Gamma'),$$

and the spaces $M_k(\Gamma')$ are trivial for k odd when $-1 \in \Gamma'$.

In the formulas of this theorem $\lfloor x \rfloor$ denotes the integral part of a rational number and $\delta_{i,j}$ is the Kronecker delta. Moreover, the coefficients of $\nu_2(\Gamma')$ and $\nu_3(\Gamma')$ are often replaced by the following expressions in the literature:

$$\gamma_4(k) = \begin{cases} -1/4 & \text{if } k \equiv 2 \pmod 4, \\ 1/4 & \text{if } k \equiv 0 \pmod 4, \\ 0 & \text{if } k \equiv 1 \pmod 2, \end{cases} \qquad \gamma_3(k) = \begin{cases} -1/3 & \text{if } k \equiv 2 \pmod 3, \\ 1/3 & \text{if } k \equiv 0 \pmod 3, \\ 0 & \text{if } k \equiv 1 \pmod 3. \end{cases} \tag{2.1}$$

The value of $\gamma_3(k)$ is always equal to $\lfloor k/3 \rfloor - (k-1)/3$, and $\gamma_4(k)$ coincides with $\lfloor k/4 \rfloor - (k-1)/4$ for k even (for k odd the number $\nu_2(\Gamma')$ does not appear in the dimension formula because the groups Γ' with $-1 \notin \Gamma'$ cannot have elliptic points of order 2); the need to define $\gamma_4(k)$ also for odd weights is because this coefficient appears in the formula of Theorem 2.3 below for all weights, but we remark that the value 0 assigned to it is completely irrelevant, since in that formula $\gamma_4(k)$ is the coefficient of $\nu_2(\varepsilon)$, which is equal to zero when k is odd.

We remark that even though the irregular cusps do appear in the formulas for odd weights given in Theorem 2.25 of [6] and Theorem 3.6.1 of [3], they are canceled when one replaces in those formulas the genus of the curve by its value as given by Theorem 2.1. For the groups Γ_0 and Γ_1 the distinction between regular and irregular cusps is almost never necessary because $-1 \in \Gamma_0(N)$, and even though $-1 \notin \Gamma_1(N)$ for $N > 2$, the unique group $\Gamma_1(N)$ having an irregular cusp is $\Gamma_1(4)$ (cf. Exercise 3.8.7 of [3]). On the contrary, many of the groups $\Gamma_H(N)$ that will be studied in the next section do have irregular cusps; in fact, for every N divisible by 4 there exist subgroups $H \subset (\mathbb{Z}/N\mathbb{Z})^*$ for which some of the cusps are irregular.

Dimensions of spaces of forms with character. We now recall the formula for the dimensions of spaces of modular forms of integral weight $k \geq 2$ with Nebentypus character, as given by Cohen and Oesterlé in [1, Théorème 1] (notice that in that paper they also give formulas for forms of half integral weight). We first introduce some notation and slightly adapt the formula of [1] to our notation and needs.

Let $N \geq 1$. We denote

$$\psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right) = |\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})|.$$

Let $A_4(N)$ and $A_3(N)$ be the sets of zeros modulo N of the 4th and the 3rd cyclotomic polynomials:

$$A_4(N) = \{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^2 + 1 \equiv 0 \pmod{N}\},$$
$$A_3(N) = \{a \in (\mathbb{Z}/N\mathbb{Z})^* \mid a^2 + a + 1 \equiv 0 \pmod{N}\}.$$

Let $k \geq 2$, and let $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character of the same parity as k, i.e. with $\varepsilon(-1) = (-1)^k$. Let $\mathfrak{f} \mid N$ be the conductor of ε. We denote $\nu_0(\varepsilon) = \psi(N)$,

$$\nu_2(\varepsilon) = \sum_{a \in A_4(N)} \varepsilon(a) \quad \text{and} \quad \nu_3(\varepsilon) = \sum_{a \in A_3(N)} \varepsilon(a), \tag{2.2}$$

and set

$$\nu_\infty(\varepsilon) = \sum_{\substack{d|N \\ (d,N/d)|N/\mathfrak{f}}} \varphi((d, N/d)).$$

Then the formula given in [1] reads

THEOREM 2.3 ([1, Théorème 1]). *Under the previous assumptions and notation,*

$$\dim S_k(N,\varepsilon) = \delta_{2,k\mathfrak{f}} + \frac{k-1}{12}\nu_0(\varepsilon) + \gamma_4(k)\nu_2(\varepsilon) + \gamma_3(k)\nu_3(\varepsilon) - \frac{\nu_\infty(\varepsilon)}{2},$$
$$\dim M_k(N,\varepsilon) = -\delta_{2,k\mathfrak{f}} + \dim S_k(N,\varepsilon) + \nu_\infty(\varepsilon),$$

with γ_4 and γ_3 given in (2.1) *and $\delta_{i,j}$ the Kronecker delta.*

For the computation of $\nu_\infty(\varepsilon)$ in practice the following multiplicative expression is very useful (also given in [1]):

$$\nu_\infty(\varepsilon) = \prod_{p|N} \lambda(v_p(N), v_p(\mathfrak{f}), p), \tag{2.3}$$

with

$$\lambda(r,s,p) = \begin{cases} p^{r'} + p^{r'-1} & \text{if } 2s \leq r = 2r', \\ 2p^{r'} & \text{if } 2s \leq r = 2r'+1, \\ 2p^{r-s} & \text{if } 2s > r, \end{cases} \tag{2.4}$$

for integers $r \geq 1, s \geq 0$, and $r \geq s$, and a prime number p.

In Lemma 4.4 of Section 4 we shall give an expression for the values of $\nu_2(\varepsilon)$ and $\nu_3(\varepsilon)$ that is much better for practical computation than using (2.2) directly.

3. Computation of invariants for the groups $\Gamma_H(N)$. From now on we focus on the congruence subgroups $\Gamma' \subseteq \Gamma = \mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma' = \Gamma_H(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \pmod{N},\ a, d \in H \right\}$$

for H a subgroup of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. This includes the two extreme cases $\Gamma_1(N)$ and $\Gamma_0(N)$ corresponding to the subgroups $H = \{1\}$ and $H = (\mathbb{Z}/N\mathbb{Z})^*$. We observe that the group $\Gamma_H(N)^{\pm} = \{\pm 1\} \cdot \Gamma_H(N)$ is just $\Gamma_{H^{\pm}}(N)$ for the subgroup $H^{\pm} \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ defined in the analogous way, i.e. $H^{\pm} = \{\pm 1\} \cdot H$.

We denote $X = X(\Gamma)$ and $X_H(N) = X(\Gamma')$.

For a fixed N the modular curves $X_H(N)$ are in bijective correspondence with the subcovers of the Galois cover $X_1(N) \to X_0(N)$. If $f \in S_2(N, \varepsilon)$ is a newform for $\Gamma_0(N)$ with Nebentypus ε, then the abelian variety A_f attached to it by Shimura (cf. [6, Theorem 7.14]) is isogenous to a factor of the Jacobian variety $J_H(N) = \mathrm{Jac}(X_H(N))$ for all subgroups $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ contained in $\ker \varepsilon$. A package for explicit computations with these varieties, based on modular symbols for $\Gamma_0(N)$ with Nebentypus, was implemented by William Stein in Magma, and he has also been implementing this kind of computations in Sage. For many purposes it is desirable to have a description of A_f as a subvariety or a quotient of a Jacobian of a curve, and in this respect the curves $X_H(N)$ are of great interest, because if one restricts to work only with the family of Jacobians $J_1(N)$, which in some sense would be enough since all A_f are quotients of some of them, one major drawback is that the dimensions of these Jacobians grow very fast and the computations become unfeasible even for relatively small values of N (a few hundred). On the contrary, if one works with the subcovers $X_H(N)$ then the varieties A_f for forms with Nebentypus character having large kernel (i.e. small order) can be handled in practice for very large values of N (up to several thousand).

The need to do explicit computations with modular symbols for congruence groups $\Gamma_H(N)$ and with modular curves $X_H(N)$ was our motivation to develop the genus and dimension formulas that will be given in this section.

The rest of the section is devoted to obtaining formulas for the invariants ν_0, ν_2, ν_3, ν_∞ and $\nu_\infty^{\mathrm{reg}}$ for the groups $\Gamma_H(N)$.

Degree of the covering. For a subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ let

$$\mathbb{P}_H(N) = \{(c, d) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid (c, d, N) = 1\}/\sim$$

where

$$(c,d) \sim (c',d') \;\Leftrightarrow\; c' = hc \text{ and } d' = hd \text{ for some } h \in H.$$

We remark that for $H = (\mathbb{Z}/N\mathbb{Z})^*$ this set is the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, and that $|\mathbb{P}_H(N)| = \psi(N)\varphi(N)/|H|$ with φ being the Euler totient function.

LEMMA 3.1. *The map* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto (c,d)$ *induces a well defined bijection between the set of right cosets* $\Gamma_H(N)\gamma \in \Gamma_H(N)\backslash\Gamma$ *and the set* $\mathbb{P}_H(N)$.

Proof. The proof is straightforward. Cf. also Proposition 2.2.1 of [2], where an equivalent formulation of this lemma is proved for the group $\Gamma_0(N)$. ∎

As an immediate consequence we obtain

PROPOSITION 3.2. *The degree of the covering* $X_H(N) \to X(\Gamma)$ *is*

$$\nu_0(\Gamma_H(N)) = [\Gamma : \Gamma_{H^\pm}(N)] = \psi(N)\varphi(N)/|H^\pm|.$$

Number of elliptic points. The counting of elliptic points on the curves $X_0(N)$ is performed in [6] and in [3] by counting ideals in the orders $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$. Instead, we use a simpler argument inspired by Proposition 14 of [5]. Let S and U be the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

The isotropy subgroups of the elliptic points $i = \sqrt{-1}$ and $\rho = e^{2\pi i/3}$ in the group Γ are $\Gamma_i = \langle S \rangle = \{\pm 1, \pm S\}$ and $\Gamma_\rho = \langle -U \rangle = \{\pm 1, \pm U, \pm U^2\}$. We have

LEMMA 3.3. *Let* $\Gamma' \subseteq \mathrm{SL}_2(\mathbb{Z})$ *be any finite index subgroup. Let* $\{\gamma_1, \ldots, \gamma_\nu\}$ *be a full set of representatives of the right cosets of* $\Gamma'^{\pm}$ *in* Γ. *Then the map* $\gamma_j \mapsto \gamma_j(i)$ (*resp.* $\gamma_j \mapsto \gamma_j(\rho)$) *is a bijection between the set of* γ_j *such that* $\gamma_j S \gamma_j^{-1} \in \Gamma'$ (*resp.* $\gamma_j U \gamma_j^{-1} \in \Gamma'$) *and the set of elliptic points of order* 2 (*resp. order* 3) *for* Γ'.

Proof. The elliptic points in $\mathfrak{H}$ of order 2 (resp. order 3) for Γ' belong to the Γ-orbit of i (resp. of $\rho = e^{2\pi i/3}$). Let $\gamma \in \Gamma$. The condition that the isotropy subgroup of $\gamma(i)$ (resp. $\gamma(\rho)$) with respect to Γ' contains a non-scalar matrix is that $\gamma S \gamma^{-1} \in \Gamma'$ (resp. $\gamma U \gamma^{-1} \in \Gamma'$), and two such elements belong to the same Γ'-orbit if, and only if, the corresponding γ belong to the same right coset with respect to $\Gamma'^{\pm}$. ∎

PROPOSITION 3.4. *The numbers of elliptic points of order* 2 *and* 3 *in the curve* $X_H(N)$ *are given by*

$$\nu_2(\Gamma_H(N)) = \frac{\varphi(N)}{|H^\pm|}\,|A_4(N) \cap H^\pm|, \qquad \nu_3(\Gamma_H(N)) = \frac{\varphi(N)}{|H^\pm|}\,|A_3(N) \cap H^\pm|.$$

Proof. We apply the previous lemma to our group $\Gamma_H(N)$. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then the matrix

$$\gamma \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} ac+bd & -(a^2+b^2) \\ c^2+d^2 & -(ac+bd) \end{pmatrix}$$

belongs to $\Gamma_H(N)$ if, and only if, the following two conditions are satisfied:

$$c^2 + d^2 \equiv 0 \pmod{N} \quad \text{and} \quad ac + bd \in H.$$

Notice that these conditions only depend on the entries of the matrix viewed modulo N. The congruence $c^2+d^2 \equiv 0 \pmod{N}$ implies $(c, N) = (d, N) = 1$. On the set $\mathbb{P}_H(N)$ representing the cosets of the group $\Gamma_H(N)$, a full set of representatives for the pairs (c, d) corresponding to matrices such that the congruence is satisfied is constructed in the following way. Fix elements $c_j \in (\mathbb{Z}/N\mathbb{Z})^*$ that are a set of representatives of the quotient $(\mathbb{Z}/N\mathbb{Z})^*/H^{\pm}$, with $j = 1, \ldots, \varphi(N)/|H^{\pm}|$, and then take all pairs (c_j, d) for $d \in \mathbb{Z}/N\mathbb{Z}$ such that $(c_j, d) = (d, N) = 1$. Then, among these (c_j, d), the pairs satisfying the congruence are those with $(d/c_j)^2 \equiv -1 \pmod{N} \Leftrightarrow d = ac_j$ for some $s \in (\mathbb{Z}/N\mathbb{Z})^*$ with $s^2 \equiv -1 \pmod{N}$. Hence, a full set of representatives of the $(c, d) \in \mathbb{P}_H(N)$ satisfying $c^2 + d^2 \equiv 0 \pmod{N}$ is

$$(c_j, sc_j) \quad \text{for } j = 1, \ldots, \varphi(N)/|H^{\pm}| \text{ and } s \in A_4(N).$$

Now a short computation using the fact that $ad - bc = 1$ shows that for the matrices corresponding to these pairs we have $ad + bc \equiv s \pmod{N}$, so that those for which $\gamma(i)$ is an elliptic point are the ones having $s \in H = H^{\pm}$.

The argument for cusps of order 3 is analogous: for a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as before one has

$$\gamma \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \gamma^{-1} = \gamma \begin{pmatrix} bc-bd-ac & a^2-ab+b^2 \\ -(c^2-cd+d^2) & ac-ad+bd \end{pmatrix}$$

and again the condition $c^2 - cd + d^2 \equiv 0 \pmod{N}$ implies that $(c, N) = (d, N) = 1$. Let the pairs (c_j, d) be as before; they satisfy the congruence when $(c_j/d)^2 - c_d + 1 \equiv 0 \pmod{N}$. A full set of representatives of these pairs is

$$(c_j, -sc_j) \quad \text{for } j = 1, \ldots, \varphi(N)/|H^{\pm}| \text{ and } s \in A_3(N),$$

and among them one has $bc - bd - ac \equiv s^2 \pmod{N}$. Hence we also obtain a full set of representatives as in the previous lemma by taking the pairs with $s \in H^{\pm}$. ∎

Number of cusps. In order to simplify many expressions, from now on we will use the following notation. For every divisor $d \,|\, N$ we denote $N_d = [d, N/d]$ the least common multiple of d and N/d (notice that $N/N_d = (d, N/d)$ and that N_d is divisible by all prime factors of N) and we denote

by $H_d = \{a \pmod{N_d} \mid a \in H\}$ the subgroup of $(\mathbb{Z}/N_d\mathbb{Z})^*$ that is the image of the subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ under reduction modulo N_d.

Set

$$\mathbb{S}_H(N,d) = \{(p,q) \in (\mathbb{Z}/d\mathbb{Z})^* \times (\mathbb{Z}/(N/d)\mathbb{Z})^*\}/\sim$$

where

$$(p,q) \sim (p',q') \;\Leftrightarrow\; p' = hp \text{ and } q' = h^{-1}q \text{ for some } h \in H$$

(notice that the reduction of elements of H modulo d and modulo N/d is well defined), and let $\mathbb{S}_H(N) = \bigcup_{d|N} \mathbb{S}_H(N,d)$ be the union of all these sets. We observe that the elements $h \in H$ for which $hp = p$ and $h^{-1}q = q$ are the $h \equiv 1 \pmod{N_d}$, and this implies that the number of elements in each set $\mathbb{S}_H(N,d)$ is $\varphi(d)\varphi(N/d)/|H_d|$.

Proposition 3.5. *For cusps $p/q \in \mathbb{P}^1(\mathbb{Q})$ with $(p,q) = 1$, the map $p/q \mapsto (p, q/(q,N))$ induces a well defined bijection between the set of cusps on the curve $X_H(N)$ and the set $\mathbb{S}_{H^\pm}(N)$. If $-1 \notin H$ then under this bijection the regular and irregular cusps correspond, respectively, to the subsets*

$$\bigcup_{\substack{d|N \\ -1 \notin H_d}} \mathbb{S}_{H^\pm}(N,d) \quad \text{and} \quad \bigcup_{\substack{d|N \\ -1 \in H_d}} \mathbb{S}_{H^\pm}(N,d).$$

Proof. The proof of the first statement is easily obtained following the same arguments as in Proposition 2.2.3 of [2], where an equivalent statement for the group $\Gamma_0(N)$ is proved.

Assume $-1 \notin H$. Let $s = p/qd$ be a cusp, given as a quotient of integers with $(s, qd) = 1$, $d \mid N$ and $(q, N/d) = 1$. The isotropy subgroup of s in Γ is

$$\Gamma_s = \left\{ \pm \begin{pmatrix} 1 + pqdt & -p^2 t \\ q^2 d^2 t & 1 - pqdt \end{pmatrix} \;\middle|\; t \in \mathbb{Z} \right\},$$

and $\Gamma_H(N)_s = \Gamma_s \cap \Gamma_H(N)$. This group contains a matrix of trace -2 if, and only if, there is an integer $t \in \mathbb{Z}$ such that

$$q^2 d^2 t \equiv 0 \pmod{N} \quad \text{and} \quad -1 - pqdt \in H.$$

The first congruence is equivalent to t being divisible by $(N/d)/(d, N/d) = N_d/d$; if we put $t = t_0 N_d/d$, the second condition becomes $-1 - pqN_d t_0 \in H$ for some $t_0 \in \mathbb{Z}$. If this condition is satisfied then $-1 \in H_d$. Conversely, assume that $-1 \in H_d$; then there exists an integer $m \in \mathbb{Z}$ such that $-1 + N_d m \in H$. For any given cusp corresponding to an element of $\mathbb{S}_{H^\pm}(N,d)$ there are representatives of the form p/qd with p and q relatively prime to any given number, and in particular we may assume that they are odd; then, since $N_d^2 \equiv 0 \pmod{N}$, the integer $(-1 + N_d m)^{pq}$ is congruent modulo N to $-1 + N_d pqm$. By the previous criterion it follows that the cusp is irregular. ∎

As an immediate consequence we obtain

PROPOSITION 3.6. *The number of cusps in the curve $X_H(N)$ is*

$$\nu_\infty(\Gamma_H(N)) = \sum_{d|N} \frac{\varphi(d)\varphi(N/d)}{|H_d^{\pm}|}.$$

If $-1 \notin H$ the number of regular and irregular ones is given by the sums over the divisors d for which $-1 \notin H_d$ and $-1 \in H_d$, respectively.

Concerning the existence of irregular cusps, the following information can be useful.

PROPOSITION 3.7. *Assume $-1 \notin H$. Then for every divisor $d \,|\, N$ with $(d, N/d)$ odd one has $-1 \notin H_d$. It follows that if $4 \nmid N$ then all the cusps for the group $\Gamma_H(N)$ are regular.*

Proof. Assume that $-1 \in H_d$ and $(d, N/d)$ is odd. Then $-1 + N_d m \in H$ for some integer m and $-1 \equiv (-1 + N_d m)^{(d,N/d)} \pmod N$, which is a contradiction. The congruence may be deduced from the binomial theorem, by noticing that $(d, N/d)N_d = N$ and that $N_d^2 \equiv 0 \pmod N$.

The greatest common divisor $(d, N/d)$ is even for some divisor $d \,|\, N$ if, and only if, $4 \,|\, N$. ∎

A practical formula for the number of cusps. To use the formula of Proposition 3.6 in practice would require to compute the number of elements of each group H_d for all divisors d of N. We will see that in fact this number of elements can be obtained if we just know the number of elements of the reduction H_0 of the group H modulo a single divisor N_0 of N, and then derive from this fact a formula for the number of cusps depending on a multiplicative expression as a product of terms similar to (2.4), which we introduce now: for integers $r \geq 1, s \geq 0$, and $r \geq s$, and a prime number p, we define

(3.1)
$$\ell(r,s,p) = \begin{cases} p^{3r'-s-2}(p^2-1) & \text{if } 2s \geq r = 2r', \\ 2p^{3r'-s}(p-1) & \text{if } 2s \geq r = 2r'+1, \\ p^{r-2}(p-1)(2p+(p-1)(r-2s-1)) & \text{if } 2s < r. \end{cases}$$

For every integer $N \geq 1$ we define the integer N_0 to be

$$N_0 = \begin{cases} \prod_{p|N} p & \text{if } 8 \nmid N, \\ 2\prod_{p|N} p & \text{if } 8 \,|\, N. \end{cases} \tag{3.2}$$

It is essentially the radical of N, except that when N is divisible by 8 then it has the prime 2 twice. For any subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^*$ we denote by H_0 the subgroup of $(\mathbb{Z}/N_0\mathbb{Z})^*$ obtained by reduction of the elements of H modulo N_0. We have an exact sequence

$$1 \to K_0 \to H \to H_0 \to 1$$

with $K_0 = \{h \in H \mid h \equiv 1 \pmod{N_0}\}$, the kernel of the reduction map. For every divisor $d \mid N$ we have an analogous exact sequence $1 \to K_d \to H \to H_d \to 1$ corresponding to the reduction map modulo N_d, and one has

LEMMA 3.8. *Let* $\mathfrak{k} = |K_0| = |H|/|H_0|$. *Then for every* $d \mid N$ *one has* $|H_d| = |H_0|\mathfrak{k}/(\mathfrak{k}, N/N_d)$; *moreover,*

$$\sum_{d|N} \frac{\varphi(d)\varphi(N/d)}{|H_d|} = \frac{1}{|H_0|} \prod_{p|N} \ell(v_p(N), v_p(\mathfrak{k}), p). \tag{3.3}$$

Proof. Consider the exact sequence corresponding to the reduction modulo N_0 map,

$$1 \to C_0 \to (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N_0\mathbb{Z})^* \to 1.$$

Then, from the definition of N_0, and taking into account the structure of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$ as the product of the groups $(\mathbb{Z}/p^e\mathbb{Z})^*$ for the prime-power factors of N, it follows that the group C_0 is cyclic of order $\varphi(N)/\varphi(N_0) = N/N_0$. Let g be a generator of it. For every $d \mid N$ reduction modulo N_d gives an analogous exact sequence with kernel C_d being a subgroup of C_0 of order $\varphi(N)/\varphi(N_d) = N/N_d$, hence generated by the (N_d/N_0)th power of g.

The group $K_0 = C_0 \cap H$ is generated by the smallest power of g belonging to H, which by the definition of $\mathfrak{k}$ is $(N/N_0)/\mathfrak{k}$. For every divisor N_d of N (in fact, for every divisor of N that is divisible by N_0), the group $K_d = C_d \cap H$ is the subgroup of C generated by the smallest power of g that belongs to H and C_d, and hence its exponent must be a multiple of the least common divisor $[N_d/N_0, N/(\mathfrak{k}N_0)]$. Thus, the group K_d has order $(N/N_0)/[N_d/N_0, N/(\mathfrak{k}N_0)]$. A short computation shows that this number is equal to $(\mathfrak{k}, N/N_d)$. The identity relating $|H_d|$ and $|H_0|$ in the statement of the lemma is then obtained by just expressing the numbers of elements of the groups H_d and H_0 in terms of $|H|$ and of $|K_d|$ and $|K_0|$.

Now we observe that the factor $(\mathfrak{k}, N/N_0) = (\mathfrak{k}, d, N/d)$ of $|H_d|$ is multiplicative, in the sense that for every decomposition $N = N_1N_2$ into a product of relatively prime factors one has $(\mathfrak{k}, d, N/d) = (\mathfrak{k}_1, d_1, N_1/d_1)(\mathfrak{k}_2, d_2, N_2/d_2)$ with $\mathfrak{k}_i = (\mathfrak{k}, N_i)$ and $d_i = (d, N_i)$. Taking out the common factor $1/|N_0|$ in the sum on the left of (3.3), we get a sum over the divisors of N of an expression that is multiplicative with respect to factorizations of N as a product of coprime factors. Then an easy but tedious computation of the sums for prime-power divisors, similar to the one needed to obtain (2.3), gives us the expression of this sum as a product of the $\ell(r, s, p)$. ∎

We obtain the following formula that essentially reduces the practical computation of the number of cusps to the knowledge of the number of elements of the group H_0, and of whether or not the condition $-1 \in H_0$ is satisfied for the distinction between regular and irregular ones.

COROLLARY 3.9. *For every subgroup $\Gamma_H(N)$, let $\mathfrak{k} = |H^{\pm}|/|H_0^{\pm}|$. Then the number of cusps of $X_H(N)$ is given by*

$$\nu_\infty(\Gamma_H(N)) = \frac{1}{|H_0^{\pm}|}\prod_{p|N}\ell(v_p(N), v_p(\mathfrak{k}), p).$$

Assume that $-1 \notin H$. Then if $-1 \notin H_0$ all the cusps are regular, and if $-1 \in H_0$ the number of regular cusps of $X_H(N)$ is

$$\nu_\infty^{\mathrm{reg}}(\Gamma_H(N)) = \frac{\ell(v_2(N), v_2(\mathfrak{k})-1, 2) - \ell(v_2(N), v_2(\mathfrak{k}), 2)}{|H_0^{\pm}|}\prod_{\substack{p|N\\ p\neq 2}}\ell(v_p(N), v_p(\mathfrak{k}), p).$$

Proof. Indeed, the first formula is simply obtained by applying the formula of Proposition 3.6 and the expression obtained in Lemma 3.8.

Assume that $-1 \notin H$, which is equivalent to $|H^{\pm}| = 2|H|$. The regular cusps are obtained as the sum of Proposition 3.6 restricted to the divisors $d \mid N$ for which $-1 \notin H_d$. As N_0 divides N_d for all d, we see that $-1 \notin H_0 \Rightarrow -1 \notin H_d$ for all d and all cusps are regular. Assume that $-1 \in H_0$. Then, for every divisor $d \mid N$, one has

$$-1 \in H_d \;\Leftrightarrow\; |H_d^{\pm}| = |H_d| \quad \text{and} \quad -1 \notin H_d \;\Leftrightarrow\; |H_d^{\pm}| = 2|H_d|.$$

It follows that the number of regular cusps is

$$\sum_{\substack{d|N\\ -1\notin H_d}}\frac{\varphi(d)\varphi(N/d)}{|H_d^{\pm}|} = \frac{1}{2}\sum_{\substack{d|N\\ -1\notin H_d}}\frac{\varphi(d)\varphi(N/d)}{|H_d|} = \sum_{d|N}\frac{\varphi(d)\varphi(N/d)}{|H_d|} - \sum_{d|N}\frac{\varphi(d)\varphi(N/d)}{|H_d^{\pm}|}, \tag{3.4}$$

and the formula in the statement of the lemma is obtained by just applying Lemma 3.8 to the two sums in this last expression. ∎

4. Dimensions of spaces of modular forms with Nebentypus. Let $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character, and let $M_k(N,\varepsilon)$ and $S_k(N,\varepsilon)$ be the spaces of modular and cuspidal forms for $\Gamma_0(N)$ with Nebentypus character ε. An application of the Möbius inversion formula gives the following expression for the dimensions of these spaces in terms of the dimensions of spaces of modular forms for congruence subgroups $\Gamma_H(N)$.

THEOREM 4.1. *Let ε be a Dirichlet character of order n. Then*

$$\dim S_k(N,\varepsilon) = \frac{1}{\varphi(n)}\sum_{\delta|n}\mu(\delta)\dim S_k(\Gamma_{\ker(\varepsilon^\delta)}(N)),$$

where μ is the Möbius function, and the analogous formula holds for the spaces M_k.

Proof. The standard decomposition of $S_k(\Gamma_1(N))$ into spaces of forms with Nebentypus,

$$S_k(\Gamma_1(N)) \simeq \bigoplus_{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*} S_k(N, \varepsilon),$$

induced by the action of the diamond operators $\langle a \rangle$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^*$ yields analogous decompositions of the spaces of modular forms for congruence subgroups $\Gamma_H(N)$: the action of the diamond operator $\langle a \rangle$ on $S_k(\Gamma_H(N))$ depends only on $a \in (\mathbb{Z}/N\mathbb{Z})^*/H$, and one obtains a decomposition involving only the Dirichlet characters with kernel containing the group H,

$$S_k(\Gamma_H(N)) \simeq \bigoplus_{\substack{\varepsilon:(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^* \\ H \subseteq \ker \varepsilon}} S_k(N, \varepsilon).$$

Consider the case $H = \ker \varepsilon$. For this subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ of cyclic cokernel the characters whose kernels contain it are the powers of ε. Grouping them by conjugacy classes, and observing that the dimensions of $S_k(N, {}^\sigma\varepsilon)$ are the same for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\dim S_k(\Gamma_{\ker(\varepsilon)}(N)) = \sum_{m=0}^{n-1} \dim S_k(N, \varepsilon^m) = \sum_{\delta | n} \varphi(\delta) \dim S_k(N, \varepsilon^{n/\delta}).$$

Applying the Möbius inversion formula to the functions defined for divisors δ of n by

$$f(\delta) = \varphi(\delta) \dim S_k(N, \varepsilon^{n/\delta}) \quad \text{and} \quad g(\delta) = \dim S_k(\Gamma_{\ker(\varepsilon^{n/\delta})}(N)),$$

we obtain

$$\varphi(n) \dim S_k(N, \varepsilon) = \sum_{\delta | n} \mu(\delta) \dim S_k(\Gamma_{\ker(\varepsilon^\delta)}(N)),$$

and we deduce the formula in the statement. ∎

Now, a proof of the formula by Cohen and Oesterlé is provided by the following

THEOREM 4.2. *For every N, k and ε the formulas of Theorems* 2.3 *and* 4.1 *give the same value.*

The rest of this section is devoted to a proof of Theorem 4.2. The proof will be obtained by showing the identity between each "ν-component" of the formula of Theorem 4.1 with the dimensions $\dim S_k(\Gamma_{\ker(\varepsilon^\delta)}(N))$ replaced by their expression in Theorem 2.2, and the corresponding ν-component of the formula of Theorem 2.3; specifically, in Propositions 4.3, 4.6 and 4.8 we will

see that

$$\sum_{\delta|n}\mu(\delta)\nu(\Gamma_{\ker(\varepsilon^\delta)}(N))=\varphi(n)\nu(\varepsilon)\quad\text{ for }\nu=\nu_0,\nu_2,\nu_3,\nu_\infty,$$

with the appropriate interpretation for each ν and taking into account the following remark: the case of odd character corresponds to odd weight, and in this case the dimensions of the spaces $S_k(\Gamma_{\ker(\varepsilon^\delta)}(N))$ are zero when $-1\in\ker(\varepsilon^\delta)$ and are given by the formula of Theorem 2.2 when $-1\notin\ker(\varepsilon^\delta)$; since this last condition is equivalent to δ being odd, only the odd divisors of n must be taken into account for odd characters ε.

There is also a zero-or-one summand $\delta_{2,k}$ and $\delta_{2,k\mathfrak{f}}$ in the formulas of Theorems 2.2 and 2.3 that needs to be considered (only for the even weight formulas). The corresponding identity is obtained as an immediate consequence of the basic property of the Möbius function saying that $\sum_{\delta|n}\mu(n)$ is the characteristic function of the set containing only the number one:

$$\begin{aligned}\sum_{\delta|n}\mu(\delta)\delta_{2,k}&=\delta_{2,k}\sum_{\delta|n}\mu(\delta)\\&=\left.\begin{cases}1 & \text{if } k=2 \text{ and } n=1\ (\Leftrightarrow \varepsilon \text{ is trivial})\\ 0 & \text{otherwise.}\end{cases}\right\}=\varphi(n)\delta_{2,k\mathfrak{f}}.\end{aligned}$$

Here the double use of δ to denote a divisor of n and the Kronecker delta should not lead to confusion.

Proposition 4.3 (Equality for ν_0). *If ε is even, then*

$$\sum_{\delta|n}\mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N))=\varphi(n)\nu_0(\varepsilon),$$

and if ε is odd, then

$$\sum_{\substack{\delta|n\\ \delta\ odd}}\mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N))=\varphi(n)\nu_0(\varepsilon).$$

Proof. Recall that $\nu_0(\varepsilon)=\psi(N)$. Assume first that ε is even. Then $-1\in\ker(\varepsilon^\delta)$ for all δ, hence $\ker(\varepsilon^\delta)^\pm=\ker(\varepsilon^\delta)$, and since ε^δ has order n/δ, which is the order of the image $\varepsilon^\delta((\mathbb{Z}/N\mathbb{Z})^*)\subset\mathbb{C}^*$, we have $|\ker(\varepsilon^\delta)|=\varphi(N)/(n/\delta)$ and using the formula of Proposition 3.2 and the Möbius inversion formula, we obtain

$$\begin{aligned}\sum_{\delta|n}\mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N))&=\sum_{\delta|n}\mu(\delta)\psi(N)\frac{\varphi(N)}{|\ker(\varepsilon^\delta)|}\\&=\psi(N)\sum_{\delta|n}\mu(\delta)\frac{n}{\delta}=\psi(N)\varphi(n).\end{aligned}$$

Let now ε be an odd character. In this case we have to prove that

$$\sum_{\substack{\delta|n\\ \delta\,\text{odd}}} \mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N)) = \varphi(n)\nu_0(\varepsilon).$$

Since $\varepsilon(-1) = -1$ the order n must be even. Let $n = 2^v n_0$ for an odd integer n_0 and exponent $v \geq 1$. In this case $|\ker(\varepsilon^\delta)^{\pm}| = 2|\ker(\varepsilon^\delta)|$ for odd divisors $\delta \,|\, n$ and we have

$$\begin{aligned}\sum_{\substack{\delta|n\\ \delta\,\text{odd}}} \mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N)) &= \sum_{\delta|n_0} \mu(\delta)\nu_0(\Gamma_{\ker(\varepsilon^\delta)}(N))\\ &= \sum_{\delta|n_0} \mu(\delta)\psi(N)\frac{\varphi(N)}{2|\ker(\varepsilon^\delta)|} = \psi(N)\sum_{\delta|n_0}\mu(\delta)\frac{n}{2\delta}\\ &= \psi(N)\frac{n}{2n_0}\sum_{\delta|n_0}\mu(\delta)\frac{n_0}{\delta} = \psi(N)2^{v-1}\varphi(n_0) = \psi(N)\varphi(n). \ \blacksquare\end{aligned}$$

A formula for $\nu_2(\varepsilon)$ and $\nu_3(\varepsilon)$. We now give a formula for the values $\nu_2(\varepsilon)$ and $\nu_3(\varepsilon)$; apart from it being useful for the computation of these numbers in practice, the formula will be needed in the proof of the identity corresponding to the numbers of elliptic points.

For a Dirichlet character ε modulo N and a prime number $p \,|\, N$, we will denote by ε_p the "local component" of N at p corresponding to the decomposition of $(\mathbb{Z}/N\mathbb{Z})^*$ into the product of groups $(\mathbb{Z}/p^e\mathbb{Z})^*$. These characters correspond, under the identification between primitive Dirichlet characters and characters of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ provided by class field theory, to the restrictions to decomposition groups.

The set $A_4(N)$ is non-empty exactly when $4 \nmid N$ and all odd prime factors of N are $\equiv 1 \pmod 4$, in which case it contains 2^t elements, with t the number of odd prime factors; the set $A_3(N)$ is non-empty exactly when $9 \nmid N$ and all prime factors of N different from 3 are $\equiv 1 \pmod 3$, in which case it contains 2^t elements, with t the number of prime divisors $p \neq 3$. When these sets are non-empty, we have

LEMMA 4.4. *Assume that* $|A_4(N)| = 2^t > 0$. *Then*

$$\nu_2(\varepsilon) = \begin{cases} \varepsilon_0(-1)2^t \in \{\pm 2^t\} & \text{if } \varepsilon = \varepsilon_0^2,\\ 0 & \text{otherwise.}\end{cases}$$

Assume that $|A_3(N)| = 2^t > 0$. *Then*

$$\nu_3(\varepsilon) = (-1)^{t_0}2^{t_1}$$

where t_1 (*resp.* t_0) *is the number of local components* ε_{p_i} *that are cubes* (*resp. non-cubes*) *of Dirichlet characters modulo* $p_i^{e_i}$, *for the prime factors* $p_i \equiv 1 \pmod 3$ *of* N.

Proof. Fix $a_0 \in A_4(N)$. Let $N = 2^{r_0} p_1^{r_1} \cdots p_t^{r_t}$ be the factorization of N, with $r_0 \in \{0,1\}$ and $p_i \equiv 1 \pmod 4$ for all $i = 1, \ldots, t$. Then there are 2^t zeros of X^2+1 modulo N, and they form a coset of the 2-torsion subgroup $(\mathbb{Z}/N\mathbb{Z})^*[2] = \{\zeta \in (\mathbb{Z}/N\mathbb{Z})^* \mid \zeta^2 = 1\}$. Since this subgroup is the product of all the 2-torsion subgroups $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*[2]$, which are contained in the kernel of ε_{p_i} if and only if this character is a square, and from the observation that ε is a square if and only if all its local components are squares, we deduce that $(\mathbb{Z}/N\mathbb{Z})^*[2] \subseteq \ker \varepsilon$ exactly when ε is the square of some Dirichlet character ε_0.

If ε is not a square (this includes the case where $\varepsilon(-1) = -1$) then $\ker(\varepsilon)[2] = (\mathbb{Z}/N\mathbb{Z})^*[2] \cap \ker(\varepsilon)$ is a subgroup of index 2 of the full 2-torsion. Let ζ_0 be a representative of the non-trivial coset, for which necessarily $\varepsilon(\zeta_0) = -1$. Then

$$\sum_{a \in A_4(N)} \varepsilon(a) = \varepsilon(a_0) \sum_{\zeta \in (\mathbb{Z}/N\mathbb{Z})^*[2]} \varepsilon(\zeta) = \sum_{\zeta \in \ker(\varepsilon)[2]} (\varepsilon(\zeta) + \varepsilon(\zeta_0\zeta)) = 0.$$

Suppose now that $\varepsilon = \varepsilon_0^2$. Then $(\mathbb{Z}/N\mathbb{Z})^*[2] \subseteq \ker(\varepsilon)$ and

$$\sum_{a \in A_4(N)} \varepsilon(a) = \varepsilon(a_0) \sum_{\zeta \in (\mathbb{Z}/N\mathbb{Z})^*[2]} \varepsilon(\zeta) = \varepsilon_0^2(a_0) 2^t = \varepsilon_0(-1) 2^t.$$

Now consider the case $A_3(N) \neq \emptyset$. Let $N = 3^{r_0} p_1^{r_1} \cdots p_t^{r_t}$ with $p_i \equiv 1 \pmod 3$. The 3-torsion $(\mathbb{Z}/N\mathbb{Z})^*[3]$ decomposes as the product of the 3-torsions for the (cyclic) multiplicative groups modulo $p_i^{r_i}$ for $1 \leq i \leq t$ and, under this decomposition, the elements of $A_3(N)$ correspond to the t-tuples of elements of order 3 modulo $p_i^{r_i}$ for every i. Let $a = (a_i)$ with $a_i \in (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ be one of such elements. Then

$$\sum_{a \in A_3(N)} \varepsilon(a) = \sum_{e_i \in \{1,2\}} \prod_{i=1}^{t} \varepsilon_{p_i}(a_i^{e_i}) = \prod_{i=1}^{t} (\varepsilon_{p_i}(a_i) + \varepsilon_{p_i}(a_i^2)).$$

The group of Dirichlet characters modulo $p_i^{r_i}$ is cyclic generated by some character that on the order 3 element a_i takes the value $e^{2\pi i/3}$. Hence, for every character ε_{p_i}, the value $\varepsilon_{p_i}(a_i)$ is 1 or $e^{\pm 2\pi i/3}$ depending on whether the character is the cube of some character or not, and the sum $\varepsilon_{p_i}(a_i) + \varepsilon_{p_i}(a_i)^2$ is 2 or -1 depending on whether the character is a cube or a non-cube. ∎

LEMMA 4.5. *Let χ be a Dirichlet character modulo N. If $A_4(N) \neq \emptyset$, then*

$$|A_4(N) \cap \ker(\chi)| = \begin{cases} 0 & \text{if } \chi(-1) = -1, \\ \frac{1}{2}|A_4(N)| & \text{if } \chi \neq \chi_0^2 \text{ and } \chi(-1) = 1, \\ |A_4(N)| & \text{if } \chi = \chi_0^2 \text{ and } \chi_0(-1) = 1, \\ 0, & \text{if } \chi = \chi_0^2 \text{ and } \chi_0(-1) = -1. \end{cases}$$

If $A_3(N) \neq \emptyset$ and t_0, t_1 are as in the previous lemma, then

$$|A_3(N) \cap \ker(\chi)| = \frac{2}{3}(2^{t_0-1} - (-1)^{t_0-1})2^{t_1}.$$

Proof. Let $a_0 \in A_4(N)$ be any fixed element, so that $A_4(N) = \{a_0\zeta \mid \zeta \in (\mathbb{Z}/N\mathbb{Z})^*[2]\}$. If $\chi(-1) = -1$ then $\chi(a) \neq 1$ for all $a \in A_4(N)$ and the first case follows. The condition of χ being a square is equivalent to the inclusion $(\mathbb{Z}/N\mathbb{Z})^*[2] \subseteq \ker(\chi)$. Consider the case $\chi \neq \chi_0$ but $\chi(-1) = 1$. Then $\chi(a) \in \{\pm 1\}$ for all $a \in A_4(N)$ and $\ker(\chi) \cap (\mathbb{Z}/N\mathbb{Z})^*[2]$ is a subgroup of index two of the 2-torsion $(\mathbb{Z}/N\mathbb{Z})^*[2]$; if ζ_0 is a representative of the non-trivial coset one has $\chi(a_0\zeta_0\zeta) = -\chi(a_0\zeta)$ for all $\zeta \in \ker(\chi) \cap (\mathbb{Z}/N\mathbb{Z})^*[2]$, and hence $\chi(a) = 1$ for exactly half of the elements of $A_4(N)$. Assume now that $\chi = \chi_0^2$. Then, for every $a \in A_4(N)$, $\chi(a) = \chi(a_0) = \chi_0^2(a_0) = \chi_0(-1)$, from which the last two cases follow.

Let $t = t_0 + t_1$ be the number of prime factors of N different from 3, with t_0 (resp. t_1) being the number of local characters χ_p that are cubes (resp. non-cubes). Then $t_0 = 0$ is equivalent to χ being a cube, and in this case one checks that the formula gives the correct value 2^t. Let $p_1, \ldots, p_{t_0}, p_{t_0+1}, \ldots, p_t$ be the list of prime divisors of N different from 3, the first t_0 being those for which the local character χ_{p_i} is a non-cube. Let $\zeta_i \in (\mathbb{Z}/N\mathbb{Z})^*$ be an element of order 3 modulo the largest power of p_i dividing N and congruent to one modulo all other prime power factors. Then $(\mathbb{Z}/N\mathbb{Z})^*[3]$ is the cyclic group of order 3^t generated by the ζ_i, and the elements of $A_3(N)$ are the $\zeta = \prod_{i=1}^t \zeta_i^{x_i}$ with all exponents relatively prime to 3. The character χ sends such an element to the power of $e^{2\pi i/3}$ with exponent given by a linear form $\sum_{i=1}^t a_i x_i$, with a_i integers such that $a_1, \ldots, a_{t_0}$ are not divisible by 3 and the remaining $a_{t_0+1}, \ldots, a_t$ are divisible by 3. Hence the elements $\zeta = \prod \zeta_i^{x_i} \in A_3(N)$ with $\chi(\zeta) = 1$ can have arbitrary exponents on the last t_1 factors while the first t_0 exponents must satisfy $\sum_{i=1}^{t_0} a_i x_i \equiv 0 \pmod 3$. We see that $|A_3(N) \cap \ker(\chi)|$ is 2^{r_1} times the number of vectors $(x_1, \ldots, x_m) \in \mathbb{F}_3^m$ in the $\mathbb{F}_3$-vector space of dimension $m = t_0$ with all $x_i \neq 0$ and with $\sum a_i x_i = 0$. This number, call it w_m, can be computed recursively by reducing the problem in $\mathbb{F}^{m+1}$ to the m-dimensional subspace of vectors with zero first coordinate. We find that $w_1 = 0$ and $w_{m+1} = 2^m - w_m$ for $m \geq 1$, and hence the numbers w_i satisfy $w_{m+2} = w_{m+1} + 2w_m$; solving the corresponding recurrence equation we obtain the expression $w_m = \frac{2}{3}(2^{m-1} - (-1)^{m-1})$ and the formula follows. ∎

Proposition 4.6 (Equality for ν_2 and ν_3). *If ε is even, then*

$$\sum_{\delta|n} \mu(\delta)\nu_i(\Gamma_{\ker(\varepsilon^\delta)}(N)) = \varphi(n)\nu_i(\varepsilon) \quad \text{for } i = 2, 3,$$

and if ε is odd, then

$$\sum_{\substack{\delta\mid n\\ \delta\ odd}} \mu(\delta)\nu_2(\Gamma_{\ker(\varepsilon^\delta)}(N)) = \varphi(n)\nu_2(\varepsilon) \quad \textit{for } i = 2, 3.$$

Proof. We begin by considering the identities corresponding to ν_2. Assume that $A_4(N) \neq \emptyset$ since otherwise the identities are obvious because everything is zero on both sides.

Consider first the case of an even Dirichlet character ε. Then all its powers are even and $\ker(\varepsilon^\delta)^\pm = \ker(\varepsilon^\delta)$ for all $\delta \mid N$. For every odd value of δ, the character ε^δ is a square if, and only if, ε is a square. Assume that ε is not a square. Then its order is even and we can write $n = 2^v n_0$ with n_0 odd and $v \geq 1$. Discarding the divisors δ that are multiples of four and using the previous lemma we obtain

$$\begin{aligned}\sum_{\delta\mid n} \mu(\delta)\nu_2(\Gamma_{\ker(\varepsilon^\delta)}(N)) &= \sum_{\delta\mid n_0} \mu(\delta)\nu_2(\Gamma_{\ker(\varepsilon^\delta)}(N)) + \sum_{\delta\mid n_0} \mu(2\delta)\nu_2(\Gamma_{\ker(\varepsilon^{2\delta})}(N))\\ &= \sum_{\delta\mid n_0} \mu(\delta)\frac{\varphi(N)}{|\ker(\varepsilon^\delta)|}\cdot\frac{1}{2}|A_4(N)| + \sum_{\delta\mid n_0} \mu(2\delta)\frac{\varphi(N)}{|\ker(\varepsilon^{2\delta})|}\cdot|A_4(N)| = 0.\end{aligned}$$

Assume now that $\varepsilon = \varepsilon_0^2$. If $\varepsilon_0(-1) = 1$ then ε^δ is always the square of an even character and

$$\begin{aligned}\sum_{\delta\mid n} \mu(\delta)\nu(\Gamma_{\ker(\varepsilon^\delta)}(N)) &= \sum_{\delta\mid n} \mu(\delta)\frac{\varphi(N)}{|\ker(\varepsilon^\delta)|}\cdot|A_4(N)|\\ &= |A_4(N)|\sum_{\delta\mid n}\mu(\delta)\frac{n}{\delta} = \varphi(n)|A_4(N)|.\end{aligned}$$

If ε_0 is odd, then its order must be a multiple of 4 because $\varepsilon_0(a_0)$ is a 4th root of unity. Hence ε has even order, say $n = 2^v n_0$. Each power ε^δ is the square of the character ε_0^δ, which has the same parity of δ. Discarding the divisors that are multiples of 4 we obtain

$$\begin{aligned}&\sum_{\delta\mid n_0} \mu(\delta)\nu_2(\Gamma_{\ker(\varepsilon^\delta)}(N)) + \sum_{\delta\mid n_0} \mu(2\delta)\nu_2(\Gamma_{\ker(\varepsilon^{2\delta})}(N))\\ &\quad= 0 + \sum_{\delta\mid n_0} \mu(2\delta)\frac{\varphi(N)}{|\ker(\varepsilon^{2\delta})|}\cdot|A_4(N)| = -|A_4(N)|\sum_{\delta\mid n_0}\mu(\delta)\frac{n}{2\delta}\\ &\quad= -|A_4(N)|\frac{n}{2n_0}\sum_{\delta\mid n_0}\mu(\delta)\frac{n_0}{\delta} = -|A_4(N)|2^{v-1}\varphi(n_0) = -\varphi(n)|A_4(N)|.\end{aligned}$$

Consider finally the case of an odd character ε, when we have $\nu_2(\varepsilon) = 0$. Since every power ε^δ with odd exponent is also an odd character we have always $|A_4(N) \cap \ker(\varepsilon^\delta)| = 0$ and the identity follows.

Let us now consider the equalities corresponding to ν_3, and assume that $A_3(N) \neq \emptyset$ since otherwise the identities are trivially true. Let $t = t_0 + t_1$ be the numbers of local factors of the character that are cubes and non-cubes as before.

Given a Dirichlet character ε, all powers ε^δ are cubes if $3 \mid \delta$ and have the same number of local factors that are cubes and non-cubes as ε for all exponents prime to 3. Consider first the case of an even character; then all its powers are even and $\ker(\varepsilon^\delta)^\pm = \ker(\varepsilon^\delta)$. Assume first that ε is a cube, i.e. $r_0 = 0$. Then $|A_3(N) \cap \ker(\varepsilon^\delta)| = 2^t$ for all δ and the equality of the statement follows immediately. Assume that $r_0 \geq 1$. Then n must be divisible by 3 and we write $n = 3^v n_0$ with $v \geq 1$ and $3 \nmid n_0$. Discarding the divisors divisible by 9 and summing separately over the divisors prime to 3 and divisible by 3 we obtain

$$\begin{aligned}
&\sum_{\delta \mid n_0} \mu(\delta)\nu_3(\Gamma_{\ker(\varepsilon^\delta)}(N)) + \sum_{\delta \mid n_0} \mu(3\delta)\nu_3(\Gamma_{\ker(\varepsilon^{3\delta})}(N)) \\
&\qquad = \sum_{\delta \mid n_0} \mu(\delta)\frac{n}{\delta}|A_3(N) \cap \ker(\varepsilon^\delta)| - \sum_{\delta \mid n_0} \mu(\delta)\frac{n}{3\delta}2^t \\
&\qquad = \frac{n}{n_0}\varphi(n_0)\frac{2}{3}(2^{t_0-1} - (-1)^{r_0-1})2^{r_1} - \frac{n}{3n_0}\varphi(n_0)2^t \\
&\qquad = \varphi(n)2^{t_1}(2^{t_0-1} - (-1)^{t_0-1} - 2^{t_0-1}) = \varphi(n)2^{t_1}(-1)^{t_0} = \varphi(n)\nu_3(\varepsilon).
\end{aligned}$$

Let now ε be an odd character. Let $n = 2^u n_0$ with $u > 0$ and n_0 odd. Then all powers ε^δ with odd exponent are odd and since $\ker(\varepsilon^\delta)^\pm = \ker(\varepsilon^{2\delta})$ one has $|A_3 \cap \ker(\varepsilon^\delta)^\pm| = |A_3 \cap \ker(\varepsilon^\delta)|$. After these remarks, the identity can be checked exactly as in the case of even characters by considering separately the cases of ε being a cube or not. ∎

Before proving the identity corresponding to ν_∞ we state a technical result that will be used there.

LEMMA 4.7. *Let $N = 2^r M$ with M odd and $r \geq 4$. For every odd Dirichlet character χ modulo N of conductor $\mathfrak{f}$ divisible by 4 there exists an element $a \in (\mathbb{Z}/N\mathbb{Z})^*$ such that*

$$a \equiv -1 \pmod{2^{v_2(\mathfrak{f})-1}M} \quad \textit{and} \quad a \in \ker(\chi).$$

Proof. Let $\chi = \chi_2\chi'$ with χ' the product of the local components of χ at the odd prime divisors of N. A Dirichlet character χ_2 modulo a power of 2 is determined by its values at -1 and 5, since these numbers generate $(\mathbb{Z}/2^r\mathbb{Z})^*$. Moreover, if χ_2 has conductor $\mathfrak{f}_2 > 4$ then the image of 5 is a primitive $2^{\mathfrak{f}_2/4}$th root of unity, and hence $\chi_2(5)^{\mathfrak{f}_2/8} = -1$.

If $v_2(\mathfrak{f}) = 2$ then χ_2 is the unique non-trivial character modulo 4, which is odd, and this implies that χ' must be even. Then an integer $a \equiv 1 \pmod 4$ and $a \equiv -1 \pmod M$ satisfies the conditions.

If $v_2(\mathfrak{f}) > 2$ then an integer $a \equiv -5^{v_2(\mathfrak{f})-3} \pmod{2^{v_2(\mathfrak{f})}}$ and $a \equiv -1 \pmod{M}$ satisfies the conditions because $-5^{v_2(\mathfrak{f})-3} \equiv -1 \pmod{2^{v_2(\mathfrak{f})-1}}$ and

$$\begin{aligned}\chi(a) &= \chi_2(a)\chi'(a) = \chi_2(-5^{v_2(\mathfrak{f})-3})\chi'(-1)\\ &= \chi_2(5)^{v_2(f)-3}\chi_2(-1)\chi'(-1) = -\chi(-1) = 1. \ \blacksquare\end{aligned}$$

PROPOSITION 4.8 (Equalities for ν_∞). *If ε is even, then*

$$\sum_{\delta|n} \mu(\delta)\nu_\infty(\Gamma_{\ker(\varepsilon^\delta)}(N)) = \varphi(n)\nu_\infty(\varepsilon),$$

and if ε is odd, then

$$\sum_{\substack{\delta|n\\ \delta \text{ odd}}} \mu(\delta)\nu_\infty^{\mathrm{reg}}(\Gamma_{\ker(\varepsilon^\delta)}(N)) = \varphi(n)\nu_\infty(\varepsilon).$$

Proof. Consider first the case of ε even. In this case, the identity to prove is

$$\sum_{\delta|n} \mu(\delta) \sum_{d|N} \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d^{\pm}|} = \varphi(n) \sum_{\substack{d|N\\ (d,N/d)|N/\mathfrak{f}}} \varphi((d, N/d)),$$

and it will be obtained as a consequence of the equality between the summands corresponding to each divisor $d \,|\, N$ on both sides. Since all powers of ε are also even, always $\ker(\varepsilon^\delta)_d^{\pm} = \ker(\varepsilon^\delta)_d$. The condition $(d, N/d) \,|\, N/\mathfrak{f}$ is equivalent to $\mathfrak{f} \,|\, [d, N/d] = N_d$, and in the sum on the right only these divisors d contribute a non-zero value. Hence we must show that for every $d \,|\, N$,

$$\sum_{\delta|n} \mu(\delta) \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} = \begin{cases} \varphi(n)\varphi((d, N/d)) & \text{if } \mathfrak{f} \,|\, N_d,\\ 0 & \text{otherwise.}\end{cases}$$

Consider first the summands with $\mathfrak{f} \,|\, N_d$. In this case, since the character ε takes the same values of a character defined modulo N_d (which has the same order n), say ε_0, then $\ker(\varepsilon)_d = \ker(\varepsilon_0)$ and hence $|\ker(\varepsilon)_d| = (1/n)\varphi(N_d)$. For every δ one has also $\varepsilon^\delta = \varepsilon_0^\delta$ and in the same way $|\ker(\varepsilon^\delta)_d| = (\delta/n)\varphi(N_d)$. Then

$$\sum_{\delta|n} \mu(\delta) \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} = \sum_{\delta|n} \mu(\delta) \frac{n}{\delta} \frac{\varphi(d)\varphi(N/d)}{\varphi(N_d)} = \varphi(n)\varphi((d, N/d)).$$

Now we consider the summands corresponding to the case $\mathfrak{f} \nmid N_d$. Consider the exact sequence

$$1 \to K_d(\varepsilon) \to \ker(\varepsilon) \to \ker(\varepsilon)_d \to 1,$$

which is the case $H = \ker(\varepsilon)$ of the sequence already considered in the arguments of the end of the previous section, with cyclic kernel $K_d(\varepsilon) = \{a \in \ker(\varepsilon) \mid a \equiv 1 \pmod{N_d}\}$.

Take a prime p with $v_p(\mathfrak{f}) > v_p(N_d)$. Then the analogous cyclic group

$$K_d(\varepsilon^p) = \{a \in \ker(\varepsilon^p) \mid a \equiv 1 \pmod{N_d}\}$$

has elements of order p. Indeed, assume for simplicity that p is odd (the case $p = 2$ is analogous) and let g be an integer that is a generator of $(\mathbb{Z}/p^r\mathbb{Z})^*$ for all exponents e and that is congruent to 1 modulo all other prime powers dividing N. Let $a_0 = g^{(p-1)p^{v_p(\mathfrak{f})-2}}$. Then $\varepsilon(a_0) \neq 1$ and $a_0 \equiv 1 \pmod{N_d}$, so if $a = a_0^{p^e}$ is the largest power such that $\varepsilon(a) \neq 1$, the element a is of order p in the group $K_d(\varepsilon^p)$. Since the groups $K_d(\varepsilon) \subset K_d(\varepsilon^p)$ are cyclic and $K_d(\varepsilon^p)^p \subseteq K_d(\varepsilon)$, we deduce that $|K_d(\varepsilon^p)| = p|K_d(\varepsilon)|$. The fact that $\mathrm{ord}_p(\mathfrak{f}) \geq 2$ also implies that the order of ε is divisible by p and hence

$$|\ker(\varepsilon^p)| = \frac{\varphi(N)}{n/p} = p\frac{\varphi(N)}{n} = |\ker(\varepsilon)|.$$

Combining the two identities it follows that

$$|\ker(\varepsilon)_d| = |\ker(\varepsilon^p)_d|.$$

Now we observe that all the previous arguments only depend on the condition $v_p(\mathfrak{f}) \leq v_p(N_d)$. When the p-factor of the conductor of a character has valuation $v_p(\mathfrak{f}) \geq 2$, this valuation does not change by raising the character to a prime-to-p power; this implies that the equality

$$|\ker(\varepsilon^\delta)_d| = |\ker(\varepsilon^{\delta p})_d|$$

is also true for all integers δ prime to p. So, if $n_0 = \mathrm{rad}(n)$ is the product of the prime divisors of n, summing over the squarefree divisors of n we obtain

$$\begin{aligned}\sum_{\delta|n} \mu(\delta)\frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} &= \sum_{\delta|n_0} \mu(\delta)\frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} \\ &= \sum_{\delta|(n_0/p)} \mu(\delta)\frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} + \sum_{\delta|n_0/p} \mu(p\delta)\frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{p\delta})_d|} \\ &= \sum_{\delta|n_0/p} (\mu(\delta) - \mu(\delta))\frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d|} = 0.\end{aligned}$$

For odd characters we have to prove the identity

$$\sum_{\substack{\delta|n \\ \delta \text{ odd}}} \mu(\delta) \sum_{\substack{d|N \\ -1\notin\ker(\varepsilon^\delta)_d}} \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^\delta)_d^{\pm}|} = \varphi(n) \sum_{\substack{d|N \\ (d,N/d)|N/\mathfrak{f}}} \varphi((d, N/d)).$$

We remark that since we sum only over odd δ, all the characters ε^δ involved in the formula are odd, and for all odd characters one has $\ker(\varepsilon^\delta)^{\pm} = \ker(\varepsilon^{2\delta})$. Let $n = 2^t n_0$ with n_0 odd and $t \geq 1$. Let N_0 be the divisor of N defined in (3.2). In order to sum over the regular cusps, we will consider two

cases as in the proof of Corollary 3.9. We have

$$-1 \in \ker(\varepsilon)_0 \;\Leftrightarrow\; -1 \in \ker(\varepsilon^\delta)_0 \text{ for all } \delta.$$

If this condition is not satisfied, then all the cusps for all groups $\Gamma_{\ker(\varepsilon^\delta)}(N)$ are regular and the identity to be proved becomes

$$\sum_{\delta \mid n_0} \mu(\delta) \sum_{d \mid N} \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{2\delta})_d|} = \varphi(n) \sum_{\substack{d \mid N \\ (d,N/d) \mid N/\mathfrak{f}}} \varphi((d, N/d)),$$

and is proved by showing that for every $d \mid N$,

$$\sum_{\delta \mid n_0} \mu(\delta) \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{2\delta})_d|} = \begin{cases} \varphi(n)\varphi((d, N/d)) & \text{if } \mathfrak{f} \mid N_d, \\ 0 & \text{otherwise.} \end{cases}$$

For the divisors d such that $\mathfrak{f} \mid N_d$ the identity is proven exactly in the same way as in the previous case. If there is an odd prime p with $v_p(\mathfrak{f}) > v_p(N_d)$ then also the same proof given before shows that the sum on the left is zero. This completes the proof by observing that if $v_2(\mathfrak{f}) > v_2(N_d)$ but $v_p(\mathfrak{f}) \le v_p(N_d)$ for all other primes then the previous lemma would imply that $-1 \in \ker(\varepsilon)_d$, in contradiction with our assumption that $-1 \notin \ker(\varepsilon)_0$.

Suppose now that $-1 \in \ker(\varepsilon^\delta)_0$. In this case the number of regular cusps for all groups $\Gamma_{\ker(\varepsilon^\delta)}(N)$ can be obtained using the formula (3.4), and the identity to be proved becomes

$$\sum_{\delta \mid n_0} \mu(\delta) \left(\sum_{d \mid N} \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{\delta})_d|} - \sum_{d \mid N} \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{2\delta})_d|} \right) = \varphi(n) \sum_{\substack{d \mid N \\ (d,N/d) \mid N/\mathfrak{f}}} \varphi((d, N/d)),$$

and is proved by showing that for every $d \mid N$,

$$\sum_{\delta \mid n_0} \mu(\delta) \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{\delta})_d|} - \sum_{\delta \mid n_0} \mu(\delta) \frac{\varphi(d)\varphi(N/d)}{|\ker(\varepsilon^{2\delta})_d|} = \begin{cases} \varphi(n)\varphi((d, N/d)) & \text{if } \mathfrak{f} \mid N_d, \\ 0 & \text{otherwise.} \end{cases}$$

Now again in the case $\mathfrak{f} \mid N_d$ the identity is proven with the same computation as in the previous cases. Also if there is an odd prime p with $v_p(\mathfrak{f}) > v_p(N_d)$ then one sees that the two sums on the left of the equality are both zero with the same argument as before. Finally assume that $v_2(\mathfrak{f}) > v_2(N_d)$. Observing that this condition will also be satisfied by the conductors of all characters ε^δ, the previous lemma ensures that $-1 \in \ker(\varepsilon^\delta)_d$ and hence the terms of each sum on the left of the equality corresponding to the same δ are equal, which implies that the difference is zero. ∎

Acknowledgements. This research was partly supported by grants MTM2009–13060–C02–01 and 2009 SGR 1220.

References

[1] H. Cohen and J. H. Oesterlé, *Dimensions des espaces de formes modulaires*, in: Modular Functions of One Variable, VI (Bonn, 1976), Lecture Notes in Math. 627, Springer, Berlin, 1977, 69–78.

[2] J. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, 1997 (available online).

[3] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, New York, 2005.

[4] G. Martin, *Dimensions of the spaces of cuspforms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$*, J. Number Theory 112 (2005), 298–331.

[5] A. Ogg, *Modular Forms and Dirichlet Series*, W. A. Benjamin, New York, 1969.

[6] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan 11, Kanô Memorial Lectures 1, Princeton Univ. Press, Princeton, NJ, 1994.

[7] —, *On the trace formula for Hecke operators*, Acta Math. 132 (1974), 245–281.

[8] W. Stein, *Modular Forms: A Computational Approach*, Grad. Stud. in Math. 79, Amer. Math. Soc., 2007 (available online).

Jordi Quer
Dept. Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Jordi Girona 1–3
08034 Barcelona, Spain
E-mail: jordi.quer@upc.edu

Received on 13.5.2009
and in revised form on 2.3.2010 (6027)