ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 43, Number 1, 2013

ON THE SIGNATURE OF A CLASS OF CONGRUENCE SUBGROUPS

C.J. CUMMINS AND N.S. HAGHIGHI

ABSTRACT. We find explicit formulas for the signatures of a large family of congruence subgroups of $\mathrm{SL}(2,\mathbf{Z})$. The family depends upon five parameters and includes a family of groups first introduced by Larcher. Larcher showed that every (regular) congruence subgroup G contains at least one subgroup H from this family, such that G and H have the same parabolic elements. Thus, every congruence subgroup contains a "large" Larcher subgroup. These facts were used by Sebbar to classify the torsion-free, genus-zero congruence subgroups of $\mathrm{PSL}(2,\mathbf{R})$. The results of this paper have been used by one of the authors to classify the torsion-free, genus-one congruence subgroups of $\mathrm{PSL}(2,\mathbf{R})$.

1. Introduction. Let $\Gamma := \mathrm{SL}(2,\mathbf{Z})$, and define a subgroup H of Γ to be a congruence subgroup if it contains one of the principal congruence subgroups:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid (a-1) \equiv (d-1) \equiv b \equiv c \equiv 0 \pmod N \right\}.$$

The smallest N such that $\Gamma(N)$ is contained in H is called the level of H.

Let $\mathfrak{H}$ be the complex upper half-plane and $\mathfrak{H}^* = \mathfrak{H} \cup \mathbf{Q}^*$ where $\mathbf{Q}^* = \mathbf{Q} \cup \{\infty\}$. If H is a subgroup of Γ, then H acts on both $\mathbf{Q}^*$ and $\mathfrak{H}^*$ by fractional linear transformations. If H is a finite index subgroup of Γ, then the number of orbits of H acting on $\mathbf{Q}^*$ is called the cusp number of H. For each $\alpha \in \mathbf{Q}^*$, let H_α be the stabilizer of α in H. The set of cusp widths of H is defined to be $C(H) = \{\mathrm{Index}\,(\overline{\Gamma_\alpha} : \overline{H_\alpha}) \mid \alpha \in \mathbf{Q}^*\}$ where $\overline{\Gamma_\alpha}$ and $\overline{H_\alpha}$ are the images of Γ_α and H_α in $\overline{\Gamma} := \mathrm{PSL}\,(2,\mathbf{Z})$, respectively.

It is a surprising fact that, for any congruence subgroup H, the set of cusp widths $C(H)$ is closed under taking greatest common divisors and

Received by the editors on December 11, 2009, and in revised form on April 15, 2010.

DOI:10.1216/RMJ-2013-43-1-83

least common multiples. To establish this result, Larcher in [**3**] defined the following congruence subgroups of level m:

$$\Gamma_\tau(m;m/d,\varepsilon,\chi)$$
$$=\left\{A\in\Gamma \mid A=\pm\begin{pmatrix}1+k_1(m/\varepsilon\chi) & k_2d\\ k_3(m/\chi) & 1+k_4(m/\varepsilon\chi)\end{pmatrix},\ k_3\equiv\tau k_1 \pmod{\chi}\right\},$$

where d divides m, $m/d=h^2n$, with n square-free, ε divides h and χ divides $\gcd(d\varepsilon, m/d\varepsilon^2)$.

Larcher showed that the set of cusp widths of this class of congruence subgroups is closed under taking greatest common divisors and least common multiples. He then proved, for any congruence subgroup H of level m, that the set of its cusp widths, $C(H)$, coincides with the set of cusp widths $C(\Gamma_\tau(m;m/d,\varepsilon,\chi))$ for suitable d,ε,χ and τ, and hence every congruence subgroup has the required property. In fact, his result is somewhat stronger, since he shows that every (regular) congruence subgroup H contains at least one Larcher subgroup L with the property that, if h is an element of H which stabilizes some α in $\mathbf{Q}^*$, then h is also an element of L, so that L is a "large" subgroup of H.

Sebbar [**6**] made use of Larcher's results to classify the torsion-free, genus-zero congruence subgroups of $\mathrm{PSL}(2,\mathbf{R})$. The results of this paper have also been used by one of us [**2**] to classify the torsion-free, genus-one congruence subgroups of $\mathrm{PSL}(2,\mathbf{R})$. Recently, Mason and Schweizer have extended Larcher's results to congruence subgroups of $\mathrm{SL}(2,D)$, where D is any Dedekind ring [**4**].

Although these results indicate the importance of Larcher's family of subgroups, some of their basic properties have not been studied. In this paper we consider a somewhat larger set of congruence subgroups:

$$H(p,q,r;\chi,\tau)$$
$$=\left\{\begin{pmatrix}1+ap & bq\\ cr & 1+dp\end{pmatrix}\in\Gamma \mid a,b,c,d\in\mathbf{Z},\ c\equiv\tau a \pmod{\chi}\right\},$$

where p divides qr and χ divides $\gcd(p, qr/p)$. These groups include $\Gamma(N)=H(N,N,N,1,1)$, $\Gamma_0(N)=H(1,1,N,1,1)$ and $\Gamma_1(N)=H(N,1,N,1,1)$. The main result of this paper will be simple formulas for the signatures of this family of groups. We find it remarkable that an explicit result of this type exists for such a large family.

To state our results we first give some notation.

We will call a subgroup of Γ a regular subgroup if it contains -1_2 where 1_2 is the identity in Γ. If a subgroup is not regular, we will call it irregular. In general, the group $H(p,q,r;\chi,\tau)$ is irregular, and so we will also consider the associated regular subgroup $\pm H(p,q,r;\chi,\tau)$. Larcher's subgroups are special cases of this set of subgroups since $\Gamma_\tau(m;m/d,\varepsilon,\chi) = \pm H(m/\varepsilon\chi, d, m/\chi;\chi,\tau)$ (see Lemma 2.8).

Let H be one of the groups $H(p,q,r;\chi,\tau)$ or $\pm H(p,q,r;\chi,\tau)$. We compute the signature $(\mu,\nu_2,\nu_3,\nu_\infty,\nu'_\infty)$ of H where μ is the index of $\overline{H}$ in $\overline{\Gamma}$, ν_2 and ν_3 are the number of inequivalent elliptic fixed points of order 2 and 3, respectively, ν_∞ is the number of inequivalent regular cusps and ν'_∞ is the number of inequivalent irregular cusps of H. See Section 4 for the definitions. Note that these data determine the genus of H. See, for example, [**8**, Proposition 1.40].

For integers a and b, we say that a exactly divides b if a divides b and $\gcd(a,b/a)=1$. In this case we write $a||b$.

For a positive integer N, define $\nu_2(N)$ and $\nu_3(N)$ to be the number of inequivalent elliptic fixed points of order 2 and 3, respectively, of $\Gamma_0(N)$. Explicitly, these are given by the following expressions (see, for example, [**8**, Proposition 1.43]):

$$\nu_2(N) = \begin{cases} 0 & \text{if } N \text{ is divisible by } 4, \\ \prod_{p|N}\left(1+\left(\frac{-1}{p}\right)\right) & \text{otherwise,} \end{cases}$$
$$\nu_3(N) = \begin{cases} 0 & \text{if } N \text{ is divisible by } 9, \\ \prod_{p|N}\left(1+\left(\frac{-3}{p}\right)\right) & \text{otherwise,} \end{cases}$$

where $\left(\frac{-}{p}\right)$ is the extended quadratic residue symbol:

$$\left(\frac{-1}{p}\right) = \begin{cases} 0 & \text{if } p=2, \\ 1 & \text{if } p\equiv 1 \pmod 4, \\ -1 & \text{if } p \equiv 3 \pmod 4, \end{cases}$$
$$\left(\frac{-3}{p}\right) = \begin{cases} 0 & \text{if } p=3, \\ 1 & \text{if } p\equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

We will also require the following definitions and lemma. Let $H(p,N;\chi) = H(p,N,1;\chi,1)$, for integers p, N and χ such that $p|N$ and $\chi|\gcd(p,N/p)$.

Lemma 1.1. *Suppose p,q,r,χ and τ are positive integers such that $p|qr$ and $\chi|\gcd(p,qr/p)$. Let $g = \gcd(\chi,\tau)$. Then the groups $H(p,q,r;\chi,\tau)$ and $H(p,gqr;\chi/g)$ have the same signature.*

Let $k = \operatorname{lcm}[\gcd(p^2,N)\chi, N]$, and define $c(p,N;\chi)$ as follows:

$$c(p,N;\chi) = \frac{\chi N\phi(p)}{\phi(N)} \sum_{d|k/\chi} \frac{\phi(d)\phi(d')}{\operatorname{lcm}[d,d',pk/N]},$$

where $d\,d' = k/\chi$ and ϕ is Euler's function. In Section 7, we will show that $c(p,N;\chi)$ is the number of orbits of $H(p,N;\chi)$ acting on a set related to the cusps of $\Gamma(N)$.

Our main results are as follows:

Theorem 1.2. *Suppose p,N and χ are positive integers such that $p \mid N$ and $\chi \mid \gcd(p,N/p)$. Let $c = c(p,N;\chi)$ and $\psi(N) = N\prod_{p|N,p \text{ prime}}(1+\frac{1}{p})$. The signature $(\mu,\nu_2,\nu_3,\nu_\infty,\nu'_\infty)$ of $H(p,N;\chi)$ is*:

$$\mu = \begin{cases} \chi\phi(p)\psi(N), & \textit{if } p=2 \textit{ and } \chi=1, \\ & \textit{or } p=1, \\ \frac{1}{2}\chi\phi(p)\psi(N), & \textit{otherwise.} \end{cases}$$

$$\nu_2 = \begin{cases} \nu_2(N) & \textit{if } p=1, \\ & \textit{or } p=2 \textit{ and } 2||N, \\ 0 & \textit{otherwise.} \end{cases}$$

$$\nu_3 = \begin{cases} \nu_3(N) & \textit{if } p=1, \\ & \textit{or } p=3 \textit{ and } 3||N, \\ 0 & \textit{otherwise.} \end{cases}$$

$$(\nu_\infty, \nu'_\infty) = \begin{cases} (c, 0) & \textit{if } p = 2 \textit{ and } \chi = 1, \\ & \textit{or } p = 1, \\ \left(\frac{2}{5}c, \frac{1}{5}c\right) & \textit{if } p = 2,\ \chi = 2,\ 2 \,||\, (N/p), \\ \left(\frac{1}{4}c, \frac{1}{2}c\right) & \textit{if } p = 2,\ \chi = 2,\ 2^k \,||\, (N/p),\ k \textit{ odd, } k > 1, \\ \left(\frac{1}{3}c, \frac{1}{3}c\right) & \textit{if } p = 2,\ \chi = 2,\ 2^k \,||\, (N/p),\ k \textit{ even,} \\ \left(\frac{2}{5}c, \frac{1}{5}c\right) & \textit{if } p = 4,\ 2 \nmid (N/p),\ (\textit{so } \chi = 1), \\ \left(\frac{1}{2}c, 0\right) & \textit{otherwise.} \end{cases}$$

The signature of $\pm H$ *is* $(\mu, \nu_2, \nu_3, \nu_\infty + \nu'_\infty, 0)$.

In Section 2 the index formula will be derived. The number of inequivalent elliptic fixed points is found in Section 3. To compute the cusp number, we first find the number of orbits of (a conjugate of) $H(p, q, r; \chi, \tau)$ acting on the subset of $(\mathbf{Z}/N\mathbf{Z})^2$ consisting of elements of additive order N where $N = qrg$ and $g = \gcd(\chi, \tau)$. This is the expression $c(p, N; \chi)$ above. The virtue of working with this expression is that it is "multiplicative" in the generalized sense of Selberg [**7**], as shown in Section 6. This reduces the calculation to the case that the level is a prime power. The number of orbits is given by the Cauchy-Frobenius formula. This initial expression is quite complex, and we do not have an explanation as to why the final expression for $c(p, N; \chi)$ is so simple. Having found the expression for $c(p, N; \chi)$, the task of computing the cusp numbers involves a detailed analysis of the action of -1_2, which is done in Section 7 using results from Section 6.

2. The index formulas. In this section we compute the indices of $H(p, q, r; \chi, \tau)$ and $\pm H(p, q, r; \chi, \tau)$ in Γ and also the indices of their images in $\overline{\Gamma}$.

We first recall the following easy proposition. For positive integers p,q and r such that $p|qr$, it is straightforward to verify that

$$H(p, q, r) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \mid \alpha - 1 \equiv \delta - 1 \equiv 0 \pmod{p}, \right. \\ \left. \beta \equiv 0 \pmod{q}, \gamma \equiv 0 \pmod{r} \right\},$$

is a subgroup of Γ, and we have

Proposition 2.1.

$$\begin{aligned}\mathrm{Index}\,(\Gamma : H(p,q,r)) &= pqr \prod_{\substack{\ell \mid qr \\ \ell \text{ prime}}} \left(1+\frac{1}{\ell}\right) \prod_{\substack{\ell \mid p \\ \ell \text{ prime}}} \left(1-\frac{1}{\ell}\right) \\ &= \phi(p)\psi(qr).\end{aligned}$$

Now define $\rho : H(p,q,r) \to \mathbf{Z}/g\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ by $\rho\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) = ((\alpha-1)/p, \beta/q, \gamma/r)$, where $g = \gcd(p, qr/p)$. It is not difficult to verify that ρ is a group homomorphism.

Lemma 2.2. *The homomorphism ρ is surjective.*

Proof. First note that $\rho(\left(\begin{smallmatrix}1 & q \\ 0 & 1\end{smallmatrix}\right)) = (0,1,0)$, and $\rho(\left(\begin{smallmatrix}1 & 0 \\ r & 1\end{smallmatrix}\right)) = (0,0,1)$, so to show that ρ is surjective, it is sufficient to find $m = \left(\begin{smallmatrix}1+ap & bq \\ cr & 1+dp\end{smallmatrix}\right) \in H(p,q,r)$ such that a is coprime to g. Set $s = qr/p$, and choose $a = 1+wp$ where w is a positive integer chosen such that $1+ap = 1+p+wp^2$ is a prime number coprime to s. This is possible since $1+p$ and p^2 are coprime, so by Dirichlet's theorem there are infinitely many primes in the sequence $1+p+wp^2$, $w = 1,2,3,\ldots$. Note that this choice of a implies a is coprime to p and hence also coprime to g. We must now show that we can choose b, c and d such that m is in $H(p,q,r)$. First, set $c=1$, and then choose b to be any solution to the congruence $sb \equiv a \pmod{1+ap}$. This is possible since s is coprime to $1+ap$. This implies that $bcs - a$ is divisible by $1+ap$, and so we set $d = (bcs-a)/(1+ap)$. With this choice of a, b, c and d we can check that m has determinant 1 and so is in $H(p,q,r)$, as required. □

Proposition 2.3. *The kernel of ρ is $H(gp, pq, pr)$.*

Proof. First note that gp divides p^2qr so that the group $H(gp,pq,pr)$ exists. Then $m = \left(\begin{smallmatrix}1+ap & bq \\ cr & 1+dp\end{smallmatrix}\right) \in H(p,q,r)$ is in $\ker(\rho)$ if and only if $a \equiv 0 \pmod{g}$, $b \equiv 0 \pmod{p}$, $c \equiv 0 \pmod{p}$ if and only if $m \in H(gp,pq,pr)$. For the last step, we have used the fact that $\det(m) = 1$ implies that $d \equiv -a \pmod{g}$. □

Definition 2.4. Let S be a subgroup of $\mathbf{Z}/g\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Then we define $H(p,q,r;S)$ to be the preimage of S under ρ.

Proposition 2.5.

$$\begin{aligned} &\operatorname{Index}(\Gamma : H(p,q,r;S)) \\ &\qquad = |S|^{-1} g p^3 q r \prod_{\substack{\ell \mid qr \\ \ell \ prime}} \left(1 + \frac{1}{\ell}\right) \prod_{\substack{\ell \mid p \\ \ell \ prime}} \left(1 - \frac{1}{\ell}\right) \\ &\qquad = |S|^{-1} g p^2 \phi(p) \psi(qr). \end{aligned}$$

Proof. From Proposition 2.3, we have $\operatorname{Index}(\Gamma : H(p,q,r;S)) = \operatorname{Index}(\Gamma : \Gamma(gp,pq,pr))/|S|$. The formula now follows from Proposition 2.1 by noting that a prime divides gp if and only if it divides p, since g divides p and similarly a prime divides p^2qr if and only if it divides qr. □

Let χ be a divisor of g and τ any integer. Let T be the subgroup of $(\mathbf{Z}/\chi\mathbf{Z})^2$ generated by $(1,\tau)$, so $|T| = \chi$. Define $\mu : \mathbf{Z}/g\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \to (\mathbf{Z}/\chi\mathbf{Z})^2$ by $\mu(a,b,c) = (a,c)$. Define $H(p,q,r;\chi,\tau) = H(p,q,r;\mu^{-1}(T))$. Since $|\mu^{-1}(T)| = gp^2/\chi$, we have from Proposition 2.5:

Proposition 2.6.

$$\operatorname{Index}(\Gamma : H(p,q,r;\chi,\tau)) = \chi \phi(p) \psi(qr).$$

Proposition 2.7.

$$\begin{aligned} &H(p,q,r;\chi,\tau) \\ &\quad = \left\{ \begin{pmatrix} 1+ap & qb \\ rc & 1+dp \end{pmatrix} \in \Gamma \mid a,b,c,d \in \mathbf{Z}, \quad c \equiv \tau a \pmod{\chi} \right\}. \end{aligned}$$

Proof. If $m = \left(\begin{smallmatrix} 1+ap & qb \\ rc & 1+dp \end{smallmatrix}\right) \in \Gamma$ with $a,b,c,d \in \mathbf{Z}$, then $m \in H(p,q,r)$. Moreover, we have $\mu(\rho(m)) = (a,c) = (a,\tau a)$ since $c \equiv \tau a$

$\pmod{\chi}$, so $m \in H(p,q,r;\chi,\tau)$. Conversely, if $m \in H(p,q,r)$, then $m = \left(\begin{smallmatrix} 1+ap & qb \\ rc & 1+dp \end{smallmatrix}\right)$, with $a,b,c,d \in \mathbf{Z}$. If also $m \in H(p,q,r;\chi,\tau)$, then since $\mu(\rho(m)) = (a,c) \in T$, we must have $c \equiv \tau a \pmod{\chi}$. □

Lemma 2.8. *Larcher's congruence subgroups satisfy:*

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) = \pm H(m/\varepsilon\chi, d, m/\chi; \chi, \tau).$$

Proof. The only part which is not straightforward to verify is $\chi | \gcd(d\varepsilon, m/d\varepsilon^2)$ implies $\chi | g$, where $g = \gcd(m/\varepsilon\chi, d(m/\chi)(\varepsilon\chi/m)) = \gcd(m/\varepsilon\chi, d\varepsilon)$. However, if $\chi|\gcd(d\varepsilon, m/d\varepsilon^2)$, then $d\varepsilon = k\chi$ for some integer k. So $\gcd(d\varepsilon, m/d\varepsilon^2) = \gcd(d\varepsilon, m/k\varepsilon\chi)$ which divides $\gcd(m/\varepsilon\chi, d\varepsilon)$, so $\chi|g$ as required. □

To compute the index of the image of $H(p,q,r;\chi,\tau)$ in $\overline{\Gamma}$, we need to know when -1_2 is in $H(p,q,r;\chi,\tau)$. This information is provided by the following proposition:

Proposition 2.9. *The cases when $H(p,q,r;\chi,\tau)$ contains -1_2 are*:

(1) $p = 2$, $\chi = 2$, τ *even.*

(2) $p = 2$, $\chi = 1$.

(3) $p = 1$.

Proof. By Proposition 2.7, an element of $H(p,q,r;\chi,\tau)$ must have the form $\left(\begin{smallmatrix} 1+ap & qb \\ rc & 1+dp \end{smallmatrix}\right)$ with $c \equiv \tau a \pmod{\chi}$. Thus, if $-1_2 \in H(p,q,r;\chi,\tau)$, we have $ap = -2$ and $c = 0$. So either $p = 1$ which is case (3), or $p = 2$. Suppose $p = 2$; then χ is either 1 or 2. If $\chi = 1$, then we are in case (2). If $\chi = 2$, then $0 \equiv \tau(-1) \pmod{2}$, and so τ is even, which is case (1). Conversely, if $p = 1$ or $p = 2$, then from the definition we have $-1_2 \in H(p,q,r)$. If $\chi = 1$, then the group T, defined above, is trivial. It follows that $\mu(\rho(-1_2)) \in T$. Hence, $-1_2 \in H(p,q,r;\chi,\tau)$ in cases (2) and (3) since $\chi = 1$ in both cases. If $\chi = 2$ and τ is even, then T is the subgroup $\{(0,0),(1,0)\}$. So, since $\mu(\rho(-1_2)) = (1,0)$ we also have $-1_2 \in H(p,q,r;\chi,\tau)$ in case (1). □

Propositions 2.6 and 2.9 now yield the expression for μ in Theorem 1.2 which is the index of $\overline{H(p,q,r;\chi,\tau)}$ in $\overline{\Gamma}$. Since $\pm H(p,q,r;\chi,\tau)$ contains -1_2, μ is also the index of $\pm H(p,q,r;\chi,\tau)$ in Γ and $\overline{\pm H(p,q,r;\chi,\tau)}$ in $\overline{\Gamma}$. These propositions yield the equality of the indices in Lemma 1.1.

3. The elliptic fixed points of $H(p,q,r;\chi,\tau)$. In this section we determine ν_2 and ν_3, the number of inequivalent elliptic fixed points of order two and three, respectively, of $H(p,q,r;\chi,\tau)$. These are also the number of inequivalent elliptic fixed points of order two and three of $\pm H(p,q,r;\chi,\tau)$. We can use the fact that the signature is invariant under conjugation to reduce the cases we have to consider. This will also be useful later when we compute the cusp numbers.

Proposition 3.1. *Let p, q, r, χ and τ be positive integers such that $p|qr$ and $\chi|\gcd(p, qr/p)$. Let $g = \gcd(\chi,\tau)$. Then the groups $H(p,q,r;\chi,\tau)$ and $H(p,qrg,1;\chi/g,\tau/g)$ are conjugate in $\mathrm{GL}^+(2,\mathbf{Q})$ which is the group of nonsingular 2×2 rational matrices of positive determinant.*

Proof. $H(p,q,r;\chi,\tau)$ has a conjugate which is contained in $H(p,qr,1;\chi,\tau)$ since

$$\begin{pmatrix}1 & 0\\ 0 & 1/r\end{pmatrix}\begin{pmatrix}1+ap & bq\\ cr & 1+dp\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & r\end{pmatrix}\begin{pmatrix}1+ap & bqr\\ c & 1+dp\end{pmatrix}.$$

The inverse conjugation gives the reverse inclusion, so that $H(p,q,r;\chi,\tau)$ and $H(p,qr,1;\chi,\tau)$ are conjugate in $\mathrm{GL}^+(2,\mathbf{Q})$.

Next we have that $H(p,N,1;\chi,\tau)$ is equal to $H(p,Ng,1;\chi/g,\tau/g)$, where $g=\gcd(\chi,\tau)$. To see this, suppose $\left(\begin{smallmatrix}1+ap & bN\\ c & 1+dp\end{smallmatrix}\right)\in H(p,N,1;\chi,\tau)$, so $c\equiv a\tau \pmod{\chi}$, and therefore $g \mid c$. We have $c=c'g$ where $c'\equiv a\tau/g \pmod{\chi/g}$. Hence, $H(p,N,1;\chi,\tau)$ is contained in $H(p,N,g;\chi/g,\tau/g)$. Similarly, every element of $H(p,N,g;\chi/g,\tau/g)$ is in $H(p,N,1;\chi,\tau)$ so that $H(p,N,1;\chi,\tau) = H(p,N,g;\chi/g,\tau/g)$. Applying the conjugation above now gives us the desired result. □

By Proposition 3.1, when computing the number of inequivalent elliptic fixed points and cusp numbers, one only needs to consider the groups $H(p,N,1;\chi,\tau)$ where $(\chi,\tau)=1$. We will use this fact in the proof of the following:

Proposition 3.2. *Let p, N, χ and τ be positive integers such that $p|N$, $\chi|gcd(p,N/p)$ and* $\gcd(\chi,\tau)=1$. *The values of ν_2 and ν_3 are given by*:

$$\nu_2=\begin{cases}\nu_2(N) & \text{if } p=1,\\ & \text{or } p=2 \text{ and } 2||N,\\ 0 & \text{otherwise,}\end{cases}$$

$$\nu_3=\begin{cases}\nu_3(N) & \text{if } p=1,\\ & \text{or } p=3 \text{ and } 3||N,\\ 0 & \text{otherwise.}\end{cases}$$

Proof. Let $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$ be an elliptic element of $H(p,N,1;\chi,\tau)$. Then we have $|a+d|<2$. So there is no such element if $p\geqq 4$ since $a+d\equiv 2 \pmod p$. So it is enough to consider the three following cases.

If $p=1$, then $H(p,N,1;\chi,\tau)=\Gamma^0(N)$ where

$$\Gamma^0(N)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathrm{SL}\,(2,\mathbf{Z}) \mid b\equiv 0 \pmod N\right\}.$$

As $\Gamma^0(N)$ is a conjugate of $\Gamma_0(N)$, the number of inequivalent elliptic fixed points is given by $\nu_2(N)$ and $\nu_3(N)$ as defined in the introduction.

For $p=2$, we assert that there is no elliptic element if $2\mid(N/2)$. To see this, suppose that $\left(\begin{smallmatrix} 1+2a & bN\\ c & 1+2d\end{smallmatrix}\right)$ is an elliptic element of $H(2,N,1;\chi,\tau)$. Then $(1+2a)(1+2d)\equiv 1 \pmod N$, and so $1+2(a+d)+4ad\equiv 1 \pmod N$. If $2\mid(N/2)$, then $2\mid(a+d)$, and this contradicts the trace condition $|2+2(a+d)|<2$.

If $p=3$, as in the previous case, it can be proved that there are no elliptic elements if $3\mid(N/3)$.

Finally, we have to consider the two cases $p=2$, $2||N$ and $p=3$, $3||N$. In both cases we must have $\chi=1$. Now $H(p,N,1;1,\tau)=H(p,N,1)\subset\Gamma^0(N)$, and this inclusion implies

$$H(2,N,1;1,\tau)=H(2,N,1)=\Gamma^0(N),$$

since both have the same index in Γ by Proposition 2.1. Thus, if $p = 2$ and $2||N$, the number of inequivalent fixed points is given by $\nu_2(N)$ and $\nu_3(N)$. However, since $2|N$, in this case, we have $\nu_3(N) = 0$ from the formula given for $\nu_3(N)$ in the introduction. Similarly,

$$\overline{H(3, N, 1; 1, \tau)} = \overline{H(3, N, 1)} = \overline{\Gamma^0(N)},$$

since they have the same index in $\overline{\Gamma}$ by Proposition 2.1 and Proposition 2.9. So, in the cases $p = 3$ and $3||N$, the number of inequivalent elliptic fixed points is given by $\nu_2(N)$ and $\nu_3(N)$. However, since $3|N$, in this case we have $\nu_2(N) = 0$ from the formula given for $\nu_2(N)$ in the introduction.

This accounts for all the cases listed in the proposition. □

This completes the proof of the expressions for μ, ν_2 and ν_3 in Theorem 1.2. So it remains to compute the cusp numbers. We start in the next three sections by developing the necessary machinery. The computation of the cusp numbers is contained in the final section.

As the expressions for ν_2 and ν_3 in Proposition 3.2 are independent of τ, it follows that Propositions 3.1 and 3.2 establish the equality of ν_2 and ν_3 in Lemma 1.1.

4. Double cosets and the number of inequivalent regular and irregular cusps. We first recall some standard facts about group actions and cusps of finite index subgroups of Γ. The treatment in this section and the next is based on that of Miyake [**5**], in particular subsection 4.2 in which Miyake computes the signatures of $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$.

Lemma 4.1. *Let a group G act transitively on a set S, and let H be a finite index subgroup of G. Fix $s \in S$, and write G_s for the stabilizer of s in G. Then the map $\phi : H\backslash G/G_s \to H\backslash S$ defined by $HgG_s \mapsto Hg(s)$ is bijective. We adopt the notation $H\backslash S$ for the orbits of S under the left action of H, and $H\backslash G/G_s$ for the orbits of $H\backslash G$ under the right action of G_s. In particular, $|H\backslash S| = |H\backslash G/G_s|$.*

Lemma 4.2. *Under the assumptions of Lemma* 4.1, *we have*

$$\text{Index}\,(G_{g(s)} : H_{g(s)}) = \text{Index}\,(G_s : (G_s)_{Hg}) = \text{Index}\,(G_s : G_s{\cap}g^{-1}Hg),$$

where $(G_s)_{Hg}$ is the stabilizer of Hg under the action of G_s acting from the right on $H\backslash G$.

Now, let $S = \mathbf{Q} \cup \{\infty\} = \mathbf{Q}^*$ be the set of cusps of Γ, i.e., the fixed points of parabolic elements of Γ acting on $\mathfrak{H}^*$ by fractional linear transformations. By [**8**, Proposition 1.30], if G and G' are mutually commensurable discrete subgroups of $\mathrm{SL}(2, \mathbf{R})$, that is to say, if

$$\mathrm{Index}\,(G : G \cap G') < \infty \quad \text{and} \quad \mathrm{Index}\,(G' : G \cap G') < \infty,$$

then they have the same set of cusps. In particular, the cusp set of any finite index subgroup of Γ is $\mathbf{Q}^*$. For a finite index subgroup H of Γ, $|H\backslash\mathbf{Q}^*|$ is the cusp number of H.

Note that the stabilizer subgroup of ∞ in Γ is

$$\Gamma_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbf{Z} \right\}.$$

It follows from Lemma 4.1 that

Theorem 4.3. *Suppose that H is a finite index subgroup of Γ. Then a bijective map $\phi : H\backslash\Gamma/\Gamma_\infty \to H\backslash\mathbf{Q}^*$ exists defined by $H\alpha\Gamma_\infty \mapsto H\alpha(\infty)$, and therefore $|H\backslash\mathbf{Q}^*| = |H\backslash\Gamma/\Gamma_\infty|$.*

Definition 4.4. Let x be a cusp of a subgroup H of Γ and σ an element of Γ such that $\sigma x = \infty$. Then $n > 0$ exists so that

$$\sigma H_x \sigma^{-1}\{\pm 1_2\} = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}^m \,\middle|\, m \in \mathbf{Z} \right\}.$$

If $-1_2 \notin H$, $\sigma H_x \sigma^{-1}$ contains either $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right)$, but not both, and the cusp x is called *regular* or *irregular*, respectively.

The (ir)regularity of a cusp x of H is independent of the choice of σ. See, for example, [**5**, Lemma 1.5.6].

To distinguish regular and irregular cusps of H, we put

$$\Gamma_\infty^+ = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \,\middle|\, n \in \mathbf{Z} \right\}$$

and define a map $\eta : H\backslash\Gamma/\Gamma_\infty^+ \to H\backslash\Gamma/\Gamma_\infty$ by $H\alpha\Gamma_\infty^+ \mapsto H\alpha\Gamma_\infty$. Note that Index $(\Gamma_\infty : \Gamma_\infty^+) = 2$.

Lemma 4.5. *If H is regular, then η is a bijection.*

Proof. By construction, η is surjective. If $\eta(H\alpha\Gamma_\infty^+) = \eta(H\beta\Gamma_\infty^+)$, then there are $h \in H$ and $t \in \Gamma_\infty^+$ such that either $\beta = h\alpha t$ or $\beta = h\alpha(-t)$. In the first case, $\beta \in H\alpha\Gamma_\infty^+$, while in the second case $\beta = (-h)\alpha t$. Since H is regular $-h \in H$ and so in the second case also $\beta \in H\alpha\Gamma_\infty^+$, η is injective. □

Lemma 4.6. *If H is an irregular subgroup of Γ, then with the notation as above, we have $\eta^{-1}(H\alpha\Gamma_\infty) = \{H\alpha\Gamma_\infty^+, H(-\alpha)\Gamma_\infty^+\}$.*

Proof. $H\alpha\Gamma_\infty = H(-\alpha)\Gamma_\infty$ since $-1_2 \in \Gamma_\infty$, and so $\{H\alpha\Gamma_\infty^+, H(-\alpha)\Gamma_\infty^+\} \subset \eta^{-1}(H\alpha\Gamma_\infty)$. For the inverse inclusion, suppose that $\eta(H\beta\Gamma_\infty^+) = \eta(H\alpha\Gamma_\infty^+)$ and suppose that $H\beta\Gamma_\infty^+ \neq H\alpha\Gamma_\infty^+$. Then, since $H\beta\Gamma_\infty = H\alpha\Gamma_\infty$, we must have $\beta = h\alpha \left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right)$, for some $n \in \mathbf{Z}$, and therefore $\beta = h(-\alpha) \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right)$. This implies that $H\beta\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+$. □

Theorem 4.7. *For H an irregular subgroup of Γ and $\alpha \in \Gamma$, the following are equivalent*:

(1) $\alpha(\infty)$ *is an irregular cusp of* H.

(2) $|\eta^{-1}(H\alpha\Gamma_\infty)| = 1$.

(3) Index $(\Gamma_{\infty(H\alpha)} : \Gamma_{\infty(H\alpha)}^+) = 2$.

(4) Index $(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) =$ Index $(\Gamma_\infty^+ : \Gamma_{\infty(H\alpha)}^+)$.

Proof. From the last lemma, (2) is equivalent to $H\alpha\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+$. On the other hand, one observes that

$$\begin{aligned} H\alpha\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+ &\iff -\alpha \in H\alpha\Gamma_\infty^+ \\ &\iff -1_2 \in \alpha^{-1}H\alpha\Gamma_\infty^+ \\ &\iff \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} \in \alpha^{-1}H\alpha \quad \text{for some } n \in \mathbf{Z} \end{aligned}$$

$$\Longleftrightarrow \alpha(\infty) \quad \text{is an irregular cusp.}$$

This shows that (1) and (2) are equivalent. To see the equivalence between (3) and (4), consider the action of Γ_∞^+ on the cosets $H \setminus \Gamma$. Then we have the following diagram:

$$\begin{tikzcd}
& \Gamma_\infty \arrow[dl, dash] \arrow[dr, dash, "2"] & \\
\Gamma_{\infty(H\alpha)} \arrow[dr, dash] & & \Gamma_\infty^+ \arrow[dl, dash] \\
& \Gamma^+_{\infty(H\alpha)} &
\end{tikzcd}$$

where $\Gamma_{\infty(H\alpha)}$ and $\Gamma^+_{\infty(H\alpha)}$ are the stabilizer subgroups of the cosets $H\alpha$ in Γ_∞ and Γ_∞^+, respectively. This diagram implies

$$\begin{aligned} \operatorname{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) &= \operatorname{Index}(\Gamma_\infty^+ : \Gamma^+_{\infty(H\alpha)}) \\ &\Longleftrightarrow \operatorname{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 2. \end{aligned}$$

This shows that (3) and (4) are equivalent.

Finally, we show that (1) and (4) are equivalent. Since H is irregular, we must have $H\alpha(-1_2) \neq H\alpha$. This implies $-1_2 \notin \Gamma_{\infty(H\alpha)}$. It follows that $\Gamma_{\infty(H\alpha)}$ is a cyclic subgroup generated either by $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ or by $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right)$ for some $n > 0$. In the former case, $\operatorname{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) = 2n$, $\operatorname{Index}(\Gamma_\infty^+ : \Gamma^+_{\infty(H\alpha)}) = n$ and $\operatorname{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 1$, while, in the latter case, $\operatorname{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) = 2n$, $\operatorname{Index}(\Gamma_\infty^+ : \Gamma^+_{\infty(H\alpha)}) = 2n$ and $\operatorname{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 2$. This shows that (4) is equivalent to the statement that $\Gamma_{\infty(H\alpha)}$ contains $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right)$ for some $n > 0$ since, if (4) holds, then we have just shown that $\Gamma_{\infty(H\alpha)}$ is generated by an element of this type. Conversely, if (4) does not hold, then $\Gamma_{\infty(H\alpha)}$ is generated by an element of the form $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for some $n > 0$.

Finally, $\Gamma_{\infty(H\alpha)}$ contains an element of the form $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right)$ for some $n > 0$ if and only if $\left(\begin{smallmatrix} -1 & n \\ 0 & -1 \end{smallmatrix}\right) \in \alpha^{-1}H\alpha$, which means that (1) is equivalent to (4) and this completes the proof. □

An analogous theorem can also be stated for regular cusps.

Theorem 4.8. *For $\alpha \in \Gamma$ and H an irregular subgroup of Γ, the following statements are equivalent*:

(1) $\alpha(\infty)$ *is a regular cusp of H.*

(2) $|\eta^{-1}(H\alpha\Gamma_\infty)| = 2$.

(3) $\operatorname{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 1$.

(4) $\operatorname{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) = 2\operatorname{Index}(\Gamma^+_\infty : \Gamma^+_{\infty(H\alpha)})$.

Corollary 4.9. *Suppose H is an irregular subgroup of Γ, and let ν_∞ and ν'_∞ be the number of inequivalent regular and irregular cusps of H, respectively. Then $2\nu_\infty + \nu'_\infty = |H\backslash\Gamma/\Gamma^+_\infty|$ and $\nu_\infty + \nu'_\infty$ is the cusp number of H in this case.*

Corollary 4.10. *If H is a regular subgroup of Γ, then all the cusps are regular and $\nu_\infty = |H\backslash\Gamma/\Gamma^+_\infty| = |H\backslash\Gamma/\Gamma_\infty|$.*

This section gives us a characterization of the regular and irregular cusps of an irregular congruence subgroup in terms of double cosets. However, we will need a more concrete description which will be derived in the next section.

5. The action of congruence subgroups on M_N.

We set

$$M_N = \left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in (\mathbf{Z}/N\mathbf{Z})^2 \mid \gcd(\alpha, \beta, N) = 1 \right\}.$$

Consider the faithful action of $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$ on M_N, given by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}.$$

If H is a subgroup of Γ and H contains $\Gamma(N)$, then H acts on M_N via the surjective map $\varphi_N : \Gamma \to \mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$. Moreover, the image $\varphi_N(H)$ is isomorphic to $H/\Gamma(N)$.

Remark. To simplify notation, we will not distinguish between an integer a and the corresponding equivalence class $\overline{a}$ in $\mathbf{Z}/N\mathbf{Z}$ as the meaning will be clear from the context.

Theorem 5.1. *Suppose H is a subgroup of Γ which contains $\Gamma(N)$. Define*

$$\psi : H\backslash\Gamma/\Gamma_\infty^+ \longrightarrow H\backslash M_N$$
$$H\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma_\infty^+ \longmapsto \mathcal{O}_{\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)}$$

where $\mathcal{O}_{\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)}$ is the orbit of the action of H on M_N containing $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. Then ψ is well defined and is a bijection. So, in particular, $|H\backslash\Gamma/\Gamma_\infty^+| = |H\backslash M_N|$.

Proof. ψ is well defined because, if $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in H\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\Gamma_\infty^+$, then $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) = h\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ for some $h \in H$, and so $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) \in \mathcal{O}_{\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)}$.

ψ is surjective. One way to see this is that if we have two integers a and c such that $0 \le a,\ c < N$ and $\gcd(a, c, N) = 1$, then by Dirichlet's theorem the sequence $c+kN$, $k = 0, 1, 2, \ldots$ will contain infinitely many terms of the form $\gcd(c, N)\ell$ where ℓ is prime. Thus, for a suitable choice of k, we can find a and c' with $\gcd(a, c') = 1$ such that $c' \equiv c \pmod{N}$. We can then find b and d such that $m = \left(\begin{smallmatrix} a & b \\ c' & d \end{smallmatrix}\right)$ is in Γ and by construction satisfies $\psi(Hm\Gamma_\infty^+) = \mathcal{O}_{\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)}$. To prove its injectivity, suppose $\psi(H\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\Gamma_\infty^+) = \psi(H\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)\Gamma_\infty^+)$. So we have $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) \in \mathcal{O}_{\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)}$, and therefore $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) \equiv h\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \pmod{N}$ for some $h \in H$. By [**8**, Lemma 1.41], $g \in \Gamma(N)$ exists such that $\left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) = gh\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. We also know that, for any matrix $\left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right) \in \Gamma$, a $\gamma \in \Gamma_\infty^+$ exists such that $\left(\begin{smallmatrix} a & * \\ c & * \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\gamma$. These imply that $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = gh\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\gamma$, and this completes the proof. □

Next observe that the image of -1_2 under the map φ_N is a central element of $\mathrm{SL}(2, \mathbf{Z}/N\mathbf{Z})$. Thus, there is an action of -1_2 on $H\backslash M_N$ given by $-1_2 \cdot H\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) = H\left(\begin{smallmatrix} -a \\ -c \end{smallmatrix}\right)$. Let $\mathcal{O}$ be an element of $H\backslash M_N$; then either $-1_2 \cdot \mathcal{O} = \mathcal{O}$ or $-1_2 \cdot \mathcal{O} \neq \mathcal{O}$. In the first case, $\{\mathcal{O}\}$ is an orbit of length 1, and in the second, $\{\mathcal{O}, -\mathcal{O}\}$ is an orbit of length 2. If $-1_2 \in H$, all orbits of -1_2 have length 1. We make the following definition:

Definition 5.2. Let H be a congruence subgroup of Γ of level M and $M|N$. If H is regular, we say that all the orbits of H on M_N are regular. If H is irregular, we call an orbit $\mathcal{O}$ of H on M_N irregular if $-1_2 \cdot \mathcal{O} = \mathcal{O}$ and regular if $-1_2 \cdot \mathcal{O} \neq \mathcal{O}$.

The motivation for this definition is given by the following result:

Theorem 5.3. *The map*

$$w = \phi \circ \eta \circ \psi^{-1} : H \backslash M_N \to H \backslash \mathbf{Q}^*$$

maps regular orbits to (*classes of*) *regular cusps and irregular orbits to* (*classes of*) *irregular cusps. If H is regular, then w is a bijection. If H is irregular, then if a/c represents a regular cusp and* $\gcd(a, c) = 1$, *then* $w^{-1}(a/c) = \left\{\mathcal{O}_{\binom{a}{c}}, \mathcal{O}_{\binom{-a}{-c}}\right\}$, *and these two elements are distinct, and if a/c represents an irregular cusp, then* $w^{-1}(a/c) = \left\{\mathcal{O}_{\binom{a}{c}}\right\}$.

Proof. If H is regular, then by Theorems 4.3, 5.1 and Lemma 4.5, the map w is a bijection. Since H is regular all cusps are regular, and by Definition 5.2, all orbits of H on M_N are regular and are fixed by -1_2.

Suppose next that H is irregular. Note that there is an action of -1_2 on $H \backslash \Gamma / \Gamma_\infty^+$ given by $-1_2 \cdot H\alpha\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+$. By Theorems 4.7 and 4.8, an orbit of -1_2 acting on $H \backslash \Gamma / \Gamma_\infty^+$ maps to a class of irregular cusps under the composition $\phi \circ \eta$ if and only if the orbit has length 1. Similarly, it maps to a class of regular cusps if and only if the orbit has length 2. Since the actions of -1_2 on $H \backslash \Gamma / \Gamma_\infty^+$ and $H \backslash M_N$ satisfy $-1_2 \circ \psi = \psi \circ -1_2$ and ψ is a bijection, we obtain the required result. □

Theorem 5.3 gives an explicit construction which allows the determination of the regular and irregular cusps of a given irregular congruence subgroup. However, to prove the remaining parts of Theorem 1.2, we will require some "multiplicative decomposition" results which will be derived in the next section.

6. Multiplicativity and the action of -1_2. In [**7**], Selberg gives a general definition of a multiplicative function as follows:

Let $n = \prod_\ell \ell^a$ where the product extends over all primes (so that all but a finite number of a are zero). Let there be defined for each ℓ a function $f_\ell(a)$ on the non-negative integers such that $f_\ell(0) = 1$ except for at most finitely many ℓ. Then

$$f(n) = \prod_\ell f_\ell(a)$$

defines a multiplicative function. If $f(1) = 1$, Selberg calls $f(n)$ normal. The class of multiplicative functions defined by the standard definition coincides with the class of normal multiplicative functions according to the new definition.

Selberg's new definition can be used to define multiplicative functions of several variables. He uses the notation $\{n\}_r$ for an r-tuple of positive integers $n_1, n_2, \dots, n_r$ and writes

$$\{n\}_r = \prod_\ell \ell^{\{a\}_r}$$

to denote that

$$n_i = \prod_\ell \ell^{a_i} \quad \text{for} \quad i = 1, \dots, r.$$

Then a function $f(n_1, \dots, n_r) = f(\{n\}_r)$ is multiplicative if it has the form

$$f(\{n\}_r) = \prod_\ell f_\ell(\{a\}_r),$$

where the functions $f_\ell(\{a\}_r)$ satisfy the condition that, for each ℓ, $f_\ell(a_1, \dots, a_r)$ is defined on r-tuples of non-negative integers and is such that $f_\ell(0, \dots, 0) = 1$ except for at most finitely many ℓ. Again, if $f(1) = 1$, call f normal.

In this section we shall prove that the function $c(p, N; \chi)$ is a normal multiplicative function in Selberg's sense. We also analyze the action of -1_2 which will allow us in the next section to compute the number of inequivalent regular and irregular cusps of $H(p, N; \chi)$. We start with a technical lemma:

Lemma 6.1. *Let N, p and χ be positive integers. Suppose $N = N_1N_2$ with $\gcd(N_1, N_2) = 1$. Suppose p divides N, and let p_1 and p_2 be such that $p = p_1p_2$ and $p_1|N_1$ and $p_2|N_2$. Suppose also that $\chi|\gcd(N, N/p)$ with $\chi = \chi_1\chi_2$ with $\chi_1|N_1$ and $\chi_2|N_2$. Then*

$$H(p, N, 1; \chi, 1) \cap \Gamma(N_1) = H(p_2N_1, N, N_1; \chi_2, p_1'),$$

where p_1' is any integer such that $p_1p_1' \equiv 1 \pmod{\chi_2}$.

Proof. If $m \in H(p_2N_1, N, N_1; \chi_2, p_1')$, then $m = \left(\begin{smallmatrix} 1+ap_2N_1 & bN \\ cN_1 & 1+dp_2N_1 \end{smallmatrix}\right)$ with $c \equiv p_1'a \pmod{\chi_2}$ and $\det(m) = 1$. As $N_1|N$, we have $m \in \Gamma(N_1)$. Also $ap_2N_1 = (aN_1/p_1)p$, $a(N_1/p_1) \equiv N_1c \pmod{\chi_2}$ and also $a(N_1/p_1) \equiv N_1c \equiv 0 \pmod{\chi_1}$, so $a(N_1/p_1) \equiv N_1c \pmod{\chi}$. It follows that $m \in H(p, N, 1; \chi, 1)$, and therefore

$$H(p_2N_1, N, N_1; \chi_2, p_1') \subseteq H(p, N, 1; \chi, 1) \cap \Gamma(N_1).$$

If $m \in H(p, N, 1; \chi, 1) \cap \Gamma(N_1)$, then $m \in H(p, N, 1) \cap H(N_1, N_1, N_1) = H(p_2N_1, N, N_1)$. So $m = \left(\begin{smallmatrix} 1+ap_2N_1 & bN \\ cN_1 & 1+dp_2N_1 \end{smallmatrix}\right)$. Moreover, since $m \in H(p, N, 1; \chi, 1)$, we have $a(N_1/p_1) \equiv N_1c \pmod{\chi}$, and this implies that $a(N_1/p_1) \equiv N_1c \pmod{\chi_2}$ and so $ap_1' \equiv c \pmod{\chi_2}$. Thus, $H(p, N, 1; \chi, 1) \cap \Gamma(N_1) \subseteq H(p_2N_1, N, N_1; \chi_2, p_1')$, and combined with the reverse inclusion above, we have the required equality. □

In particular, Lemma 6.1 shows that $\Gamma(N)$ is a subgroup of $H(p, N; \chi)$. We shall use this fact shortly.

Now suppose G is a subgroup of Γ containing $\Gamma(N)$ and, as above, $N = N_1N_2$ with $(N_1, N_2) = 1$. Denote by G_1 and G_2 the inverse images of $\psi_1 \circ \varphi_N(G)$ and $\psi_2 \circ \varphi_N(G)$, respectively, where

$$\Gamma \xrightarrow{\varphi_N} \mathrm{SL}\left(2, \frac{\mathbf{Z}}{N\mathbf{Z}}\right) \xrightarrow{\psi_i} \mathrm{SL}\left(2, \frac{\mathbf{Z}}{N_i\mathbf{Z}}\right), \quad \text{for } i = 1, 2.$$

It follows that $G_i = G\Gamma(N_i)$, the group generated by G and $\Gamma(N_i)$ for $i = 1, 2$. We next show that, in the case that $G = H(p, N; \chi)$, the groups G_1 and G_2 are related in a simple way to $H(p_1, N_1; \chi_1)$ and $H(p_2, N_2; \chi_2)$:

Lemma 6.2. *With the notation as above, the images of $\varphi_{N_i}(H(p_i, N_i; \chi_i))$ and $\varphi_{N_i}(G_i)$ where $G_i = H(p, N; \chi)\Gamma(N_i)$ are conjugate in $\mathrm{GL}\,(2, \mathbf{Z}/N_i\mathbf{Z})$ for $i = 1, 2$. Moreover, $H(p_i, N_i; \chi_i)$ and G_i have the same number of inequivalent regular cusps and the same number of inequivalent irregular cusps for $i = 1, 2$.*

Proof. We give the proof for $i = 1$ as the proof for $i = 2$ is essentially identical. Let $\left(\begin{smallmatrix} a & 0 \\ c & d \end{smallmatrix}\right) \in \varphi_{N_1}(G_1)$; then

$$\begin{pmatrix} 1 & 0 \\ 0 & p_2 \end{pmatrix}\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p_2^{-1} \end{pmatrix} = \begin{pmatrix} a & 0 \\ cp_2 & d \end{pmatrix} \in \varphi_{N_i}(H(p_1, N_1; \chi_1)),$$

where the final inclusion follows from the congruence conditions on a, c and d. Now, we prove that both images have the same cardinality. By Lemma 6.1,

$$H(p, N; \chi) \cap \Gamma(N_1) = H(p_2N_1, N, N_1; \chi_2, p_1').$$

So

$$\frac{G_1}{\Gamma(N_1)} \simeq \frac{H(p, N; \chi)}{H(p, N; \chi) \cap \Gamma(N_1)} = \frac{H(p, N; \chi)}{H(p_2N_1, N, N_1; \chi_2, p_1')},$$

and hence by Proposition 2.6,

$$\left|\frac{G_1}{\Gamma(N_1)}\right| = \left|\frac{H(p, N; \chi)}{H(p_2N_1, N, N_1; \chi_2, p_1')}\right| = \frac{N_1\phi(N_1)}{\chi_1\phi(p_1)},$$

which, again by Proposition 2.6, is the same as $|H(p_1, N_1; \chi_1)/\Gamma(N_1)|$, as required.

The conjugation above induces a bijection between the orbits of the two groups acting on M_{N_1}. Moreover, the conjugations commute with the action of -1_2, and so by Theorem 5.3, the number of inequivalent regular and irregular cusps is the same for the two groups. □

In general, the homomorphism $\psi_1 \times \psi_2 : G/\Gamma(N) \to G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$ is injective (by the Chinese remainder theorem) but is not necessarily surjective. However, we have the following proposition:

Proposition 6.3. *With notation as above, if $G = H(p, N; \chi)$, then the map $\psi_1 \times \psi_2$ is surjective. In particular, $G/\Gamma(N)$ is isomorphic to $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$.*

Proof. By Proposition 2.6, the order of $G/\Gamma(N)$ is $N\phi(N)/\chi\phi(p)$. But, by Lemma 6.2, this is the order of $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$, and so $\psi_2 \times \psi_2$ from $G/\Gamma(N)$ to $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$ is an isomorphism. □

We will also have to consider the action of -1_2. The next lemma gives a general result.

Lemma 6.4. *Suppose G and H are subgroups of groups A and B with -1_G and -1_H involutions in A and B which centralize G and H, respectively. Let $\pm G = \langle -1_G, G\rangle$ and $\pm H = \langle -1_H, H\rangle$. Suppose there is an isomorphism $\gamma : \pm G \to \pm H$ such that $\gamma(G) = H$ and $\gamma(-1_G) = -1_H$. Suppose X is a set with an action of $\pm G$ and Y is a set with an action of $\pm H$ and that there is a bijection ϕ from X to Y which intertwines the actions of $\pm G$ and $\pm H$. In other words, for all $g \in \pm G$ and all x in X, we have $\phi(g \cdot x) = \gamma(g) \cdot \phi(x)$. Then there is an action of -1_G on $G\backslash X$ given by $(-1_G) \cdot \mathcal{O}_x = \mathcal{O}_{-x}$ where $-x = (-1_G) \cdot x$ for x in X, and similarly there is an action of -1_H on $H\backslash Y$. The bijection ϕ between X and Y induces a bijection $\overline{\phi}$ between $G\backslash X$ and $H\backslash Y$ which intertwines the actions of -1_G and -1_H. In other words, $\overline{\phi}((-1_G) \cdot \mathcal{O}_x) = (-1)_H \cdot \overline{\phi}(\mathcal{O}_x)$.*

Proof. Let $\mathcal{O}_x$ be the element of $G\backslash X$ containing the element x of X and define $\mathcal{O}_y$ similarly. The action of -1_G on $G\backslash X$ is well defined since -1_G centralizes the action of G. Similarly -1_H has a well defined action on $H\backslash Y$.

Define $\overline{\phi} : G\backslash X \to H\backslash Y$ by $\overline{\phi}(\mathcal{O}_x) = \mathcal{O}_{\phi(x)}$. This is well defined since ϕ intertwines the actions of G and H. Surjectivity of $\overline{\phi}$ follows from that of ϕ. It is also injective since, if $\mathcal{O}_{\phi(x)} = \mathcal{O}_{\phi(x')}$, then $\phi(x) = h \cdot \phi(x')$ for some h in H. This implies $\phi(x) = \gamma(g)\phi(x')$ for some g in G and so $x = g \cdot x'$ as ϕ is a bijection. Thus, $\mathcal{O}_x = \mathcal{O}_{x'}$ as required.

Finally, $\overline{\phi}((-1_G) \cdot \mathcal{O}_x) = \overline{\phi}(\mathcal{O}_{-x}) = \mathcal{O}_{\phi(-x)} = \mathcal{O}_{-\phi(x)} = (-1)_H \cdot \mathcal{O}_{\phi(x)} = (-1)_H \cdot \overline{\phi}(\mathcal{O}_x)$, as required.

Note that we allow for the possibility that -1_G is an element of G. By the properties of γ, this is the case if and only if -1_H is an element of H. So, if -1_G is an element of G, then the actions of -1_G and -1_H are both trivial. □

Applying this general result in this case yields:

Corollary 6.5. *With the notation as above, there is a bijection between $H(p,N;\chi)\backslash M_N$ and $H(p_1,N_1;\chi_1)\backslash M_{N_1}\times H(p_2,N_2;\chi_2)\backslash M_{N_2}$. There is an action of -1_2 on $H(p,N;\chi)\backslash M_N$ given by $-1_2\cdot\mathcal{O}_x=\mathcal{O}_{-x}$ and also an action of -1_2 on $H(p_1,N_1;\chi_1)\backslash M_{N_1}\times H(p_2,N_2;\chi_2)\backslash M_{N_2}$, given by $-1_2\cdot(\mathcal{O}_{x_1},\mathcal{O}_{x_2})=(\mathcal{O}_{-x_1},\mathcal{O}_{-x_2})$. The bijection intertwines these two actions. As a consequence, the function $c(p,N;\chi)$, which is the cardinality of $H(p,N;\chi)\backslash M_N$, is a multiplicative function.*

Proof. Let $G=H(p,N;\chi)$. The groups $\mathrm{SL}(2,\mathbf{Z}/N\mathbf{Z})$ and $\mathrm{SL}(2,\mathbf{Z}/N_1\mathbf{Z})\times\mathrm{SL}(2,\mathbf{Z}/N_2\mathbf{Z})$ are isomorphic by the map $\psi_1\times\psi_2$. The map γ between M_N and $M_{N_1}\times M_{N_2}$ given by restriction modulo N_1 and N_2 is a bijection which intertwines the actions of $\mathrm{SL}(2,\mathbf{Z}/N\mathbf{Z})$ and $\mathrm{SL}(2,\mathbf{Z}/N_1\mathbf{Z})\times\mathrm{SL}(2,\mathbf{Z}/N_2\mathbf{Z})$. By Proposition 6.3, these restrict to an isomorphism of $G/\Gamma(N)$ and $G_1/\Gamma(N_1)\times G_2/\Gamma(N_2)$, and a bijection which intertwines the actions on M_N and $M_{N_1}\times M_{N_2}$.

Let -1 be the image of -1_2 in $\mathrm{SL}(2,\mathbf{Z}/N\mathbf{Z})$ and, for convenience, we use the same notation for the image of -1_2 in $\mathrm{SL}(2,\mathbf{Z}/N_1\mathbf{Z})$ and $\mathrm{SL}(2,\mathbf{Z}/N_2\mathbf{Z})$. Then the image of -1 under $\psi_1\times\psi_2$ is $(-1,-1)$. The elements -1 and $(-1,-1)$ are involutions which centralize $G/\Gamma(N)$ and $G_1/\Gamma(N_1)\times G_2/\Gamma(N_2)$, respectively. The isomorphism $\psi_1\times\psi_2$ maps $G/\Gamma(N)$ to $G_1/\Gamma(N_1)\times G_2/\Gamma(N_2)$ and maps -1 to $(-1,-1)$. The bijection γ intertwines the corresponding actions on M_N and $M_{N_1}\times M_{N_2}$. By Lemma 6.2, the actions of G_i on M_{N_i} are conjugate in $\mathrm{GL}\,(2,\mathbf{Z}/N_i\mathbf{Z})$ to the actions of $H(p_i,N_i;\chi_i)$, $i=1,2$, and this conjugation commutes with the action of -1. Thus, composing $\psi_1\times\psi_2$ and γ with these conjugations we obtain an isomorphism and a bijection which intertwine the action of -1 Thus, applying Lemma 6.4, we obtain the required bijection $\overline{\phi}$ between the orbit spaces which intertwines the actions of -1 and $(-1,-1)$, as required.

It follows that the number of elements of $G\backslash M_N$ is $c(p_1,N_1;\chi_1)c\,(p_2,N_2;\chi_2)$. By induction on the number of primes dividing N, the function $c(p,N;\chi)$ is multiplicative (and normal) in the sense of Selberg. □

Finally, we find the relationship between the number of inequivalent regular and irregular cusps of $H(p,N;\chi)$ and those of $H(p_1,N_1,\chi_1)$

and $H(p_2, N_2; \chi_2)$. If -1_2 is an element of G, then by Proposition 2.9 it is also an element of $H(p_1, N_1; \chi_1)$ and $H(p_1, N_1; \chi_2)$, and so in this case the actions of -1 and $(-1, -1)$ in Corollary 6.5 are both trivial.

If $H(p_1, N_1; \chi_1)$ and $H(p_1, N_1; \chi_2)$ are both regular, then by Lemma 6.2 $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$ contains $(-1, -1)$. So, by Proposition 6.3, it follows that $-1_2 \in H(p, N; \chi)$ and so $H(p, N; \chi)$ is also regular. This leaves the four cases described in the following corollary.

Corollary 6.6. *Suppose $G = H(p, N; \chi)$, and let $H_1 = H(p_1, N_1; \chi_1)$ and $H_2 = H(p_2, N_2; \chi_2)$ with other notation as above. Let ν_∞ and ν'_∞ be the number of inequivalent regular and irregular cusps of G. Let ν_1 and ν_2 be the number of inequivalent regular cusps of H_1 and H_2, respectively, and ν'_1 and ν'_2 be the number of inequivalent irregular cusps. Then we have the following four cases*:

G	H_1	H_2		
regular	regular	regular	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = 0$
irregular	irregular	regular	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = \nu'_1\nu_2$
irregular	regular	irregular	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = \nu_1\nu'_2$
irregular	irregular	irregular	$\nu_\infty = 2\nu_1\nu_2 + \nu_1\nu'_2 + \nu'_1\nu_2$	$\nu'_\infty = \nu'_1\nu'_2$

Proof. By Corollary 6.5, there is a bijection between the orbits of G on M_N and the orbits of $H_1 \times H_2$ on $M_{N_1} \times M_{N_2}$. Recall from Section 5 that, for a regular group containing $\Gamma(N)$, the cusp number is equal to the number of orbits on M_N, and there are no irregular cusps. Thus, when G, H_1 and H_2 are all regular, we have $\nu_\infty = \nu_1\nu_2$ and $\nu'_\infty = 0$.

Next suppose that G is irregular. If one of H_1 and H_2 is regular, then, as discussed above, the other is irregular. So suppose H_1 is irregular and H_2 is regular. Recall again, from Section 5, that an orbit $\mathcal{O}$ of G on M_N is irregular if $-1_2 \cdot \mathcal{O} = \mathcal{O}$ and regular if $-1_2 \cdot \mathcal{O} \neq \mathcal{O}$. Also, ν_∞ is equal to half the number of regular orbits and ν'_∞ is equal to the number of irregular orbits. By Corollary 6.5, $\mathcal{O}$ is irregular if and only if it corresponds to $\mathcal{O}_1 \times \mathcal{O}_2$ where $\mathcal{O}_1$ is an irregular orbit of G_1 on M_{N_1} and $\mathcal{O}_2$ is an orbit of G_2 on M_{N_2}, so that $\nu'_\infty = \nu'_1\nu_2$. Similarly, $\mathcal{O}$ is regular if and only if it corresponds to $\mathcal{O}_1 \times \mathcal{O}_2$ where $\mathcal{O}_1$ is regular. The number of such pairs of orbits is $\nu_1\nu_2$, and so $\nu_\infty = \nu_1\nu_2$. Alternatively, we can use the fact that the number of orbits is given both by $2\nu_\infty + \nu'_\infty$ and $(2\nu_1 + \nu'_1)(\nu_2)$ and then that $\nu'_\infty = \nu'_1\nu_2$ to reach the same conclusion.

The case that G is regular, G_1 is regular and G_2 is irregular just exchanges the roles of G_1 and G_2.

Finally, if all three groups are irregular, we have that $-1_2 \cdot \mathcal{O} = \mathcal{O}$ if and only if $-1_2 \cdot \mathcal{O}_1 = \mathcal{O}_1$ and $-1_2 \cdot \mathcal{O}_2 = \mathcal{O}_2$ where $\mathcal{O}$ corresponds to $\mathcal{O}_1 \times \mathcal{O}_2$ as before. This implies that $\nu'_\infty = \nu'_1\nu'_2$. Finally, the total number of orbits is given by both $2\nu_\infty + \nu'_\infty$ and $(2\nu_1 + \nu_1)(2\nu_2 + \nu'_2)$. Using $\nu'_\infty = \nu'_1\nu'_2$ then gives $\nu_\infty = 2\nu_1\nu_2 + \nu_1\nu'_2 + \nu'_1\nu_2$, as required. □

7. The cusp number of $H(p, N; \chi)$. In this section we compute the cusp number of $H(p, q, r; \chi, \tau)$. We first observe that it suffices to compute the cusp number of $H(p, N; \chi)$ where $p \mid N$ and $\chi \mid \gcd(N, N/p))$. This simplification is based upon Proposition 3.1 and the following

Lemma 7.1. *If* $\gcd(\chi, \tau) = 1$*, then* $H(p, N, 1; \chi, \tau)$ *and* $H(p, N, 1; \chi, 1)$ *contain* $\Gamma(N)$*, the images of the groups under* φ_N *are conjugate and the two groups have the same number of regular and irregular orbits on* M_N*, and hence the same number of inequivalent regular and irregular cusps.*

Proof. That the two groups contain $\Gamma(N)$ follows, for example, from Lemma 6.1, or by a straightforward verification from their definitions. Let $m = \left(\begin{smallmatrix} 1+ap & 0 \\ c & 1+dp \end{smallmatrix}\right) \in \varphi_N(H(p, N, 1; \chi, \tau))$. Since $\gcd(\chi, \tau) = 1$, a $k \in \mathbf{N}$ exists such that $\gcd(\tau + k\chi, N) = 1$, so $(\tau + k\chi)^m \equiv 1 \pmod{N}$ for some m. Now we have

$$\begin{pmatrix} 1 & 0 \\ 0 & (\tau + k\chi)^{m-1} \end{pmatrix} \begin{pmatrix} 1 + ap & 0 \\ c & 1 + dp \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (\tau + k\chi) \end{pmatrix} = \begin{pmatrix} 1 + ap & 0 \\ c(\tau + k\chi)^{m-1} & 1 + dp \end{pmatrix}$$

where $c(\tau + k\chi)^{m-1} \equiv a\tau(\tau + k\chi)^{m-1} \equiv a(\tau + k\chi)^m \equiv a \pmod{\chi}$, and so m is in $\varphi_N(H(p, N, 1; \chi, 1)$. Conversely, suppose that $\left(\begin{smallmatrix} 1+ap & 0 \\ c & 1+dp \end{smallmatrix}\right) \in \varphi_N(H(p, N, 1; \chi, 1))$; then, applying the inverse of the conjugation given above, we have $\left(\begin{smallmatrix} 1+ap & 0 \\ c(\tau+k\chi) & 1+dp \end{smallmatrix}\right) \in \varphi_N(H(p, N, 1; \chi, \tau))$, because $c(\tau + k\chi) \equiv a\tau \pmod{\chi}$. Thus, the two images are conjugate.

Finally, note that, as in Proposition 6.2, -1 commutes with the conjugation and so the two groups have the same number of regular and irregular orbits on M_N and hence the same number of inequivalent regular and irregular cusps. □

We start by computing

$$\begin{aligned} c(p,N;\chi) &:= |(H(p,N;\chi)\backslash M_N| \\ &= \begin{cases} 2\nu_\infty + \nu'_\infty & -1 \notin H(p,N;\chi), \\ \nu_\infty & -1 \in H(p,N;\chi), \end{cases} \end{aligned}$$

and then find ν_∞ and ν'_∞, the number of inequivalent regular and irregular cusps of $H(p,N;\chi)$.

7.1. Computing $c(p,N;\chi)$. A key theorem here is the Cauchy-Frobenius formula, so we recall its statement.

Theorem 7.2. *Let a group G act on a set X with both G and X finite. Then the total number, n, of orbits is given by*

$$n = \frac{1}{|G|}\sum_{x\in X}|G_x|.$$

To apply the Cauchy-Frobenius formula, we observe first that the number of elements of $\varphi_N(H(p,N;\chi))$ is

$$\frac{\text{Index}\,(\Gamma:\Gamma(N))}{\text{Index}\,(\Gamma:H(p,N;\chi))} = \frac{\phi(N)\psi(N^2)}{\chi\phi(P)\psi(N)} = \frac{N\phi(N)}{\chi\phi(p)}.$$

If the stabilizer of $\binom{\alpha}{\beta} \in M_N$ in $\varphi_N(H(p,N;\chi))$ is denoted by $H_{\binom{\alpha}{\beta}}$ then the Cauchy-Frobenius formula implies that

$$c(p,N;\chi) = \frac{\chi\phi(p)}{N\phi(N)}\sum_{\binom{\alpha}{\beta}\in M_N}\left|H_{\binom{\alpha}{\beta}}\right|. \tag{1}$$

In order to compute $\left|H_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)}\right|$, we also need the following form of the Chinese remainder theorem:

Lemma 7.3. *Suppose $A \mid N$ and $B \mid N$. Then the system of equations*

$$\begin{cases} x \equiv a \pmod{A} \\ x \equiv b \pmod{B} \end{cases}$$

has solutions in $\frac{\mathbf{Z}}{N\mathbf{Z}}$ if and only if $a \equiv b \pmod{(A,B)}$. If the condition is satisfied, then the number of solutions is $\frac{N}{[A,B]}$.

(A,B) (respectively, $[A,B]$) here represents the greatest common divisor (respectively, the least common multiple) of A and B.

Computing $|\mathbf{H}_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)}|$. Now we choose $\left(\begin{smallmatrix} x^{-1} & 0 \\ y & x\end{smallmatrix}\right) \in H_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)}$. It follows from the definition of $H(p,N;\chi)$ that

$$x \equiv 1 \pmod{p}, \tag{2}$$

$$y \equiv \frac{1-x}{p} \pmod{\chi}. \tag{3}$$

We must also have

$$\begin{pmatrix} x^{-1} & 0 \\ y & x \end{pmatrix}\begin{pmatrix}\alpha \\ \beta\end{pmatrix} \equiv \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \pmod{N}$$

or

$$x^{-1}\alpha \equiv \alpha \pmod{N} \tag{4}$$

$$y\alpha + x\beta \equiv \beta \pmod{N}. \tag{5}$$

To apply the Cauchy-Frobenius formula, we need to calculate, for given p, N, χ, α and β, the number of solutions for x and y of the congruences (2), (3), (4) and (5). We shall do this by finding an equivalent "triangular" system of congruences.

Observe first that

$$(4) \Longleftrightarrow x^{-1} \equiv 1 \left(\operatorname{mod} \frac{N}{(N,\alpha)}\right) \Longleftrightarrow x \equiv 1 \left(\operatorname{mod} \frac{N}{(N,\alpha)}\right),$$

$$(5) \Longleftrightarrow -\beta(x-1) \equiv y\alpha \pmod{N},$$

and, since $((N,\alpha),\beta)=1$, we infer that $(N,\alpha)\mid(x-1)$ or, equivalently, $x\equiv 1 \pmod{(N,\alpha)}$. The latter condition on x, together with the congruence equation (5) imply that

$$y\equiv\left(\frac{\alpha}{(N,\alpha)}\right)^{-1}(-\beta)\,\frac{x-1}{(N,\alpha)}\left(\operatorname{mod}\frac{N}{(N,\alpha)}\right). \tag{6}$$

Now we apply Lemma 7.3 to the following system of equations in order to find condition(s) on x which guarantees the existence of a solution for y.

$$\begin{cases} y\equiv \frac{1-x}{p} \pmod{\chi} \\ y\equiv\left(\frac{\alpha}{(N,\alpha)}\right)^{-1}(-\beta)\frac{x-1}{(N,\alpha)}\left(\operatorname{mod}\frac{N}{(N,\alpha)}\right). \end{cases} \tag{7}$$

This system has solutions if and only if $\frac{1-x}{p}\equiv(\frac{\alpha}{(N,\alpha)})^{-1}(-\beta)\frac{x-1}{(N,\alpha)}$ $(\operatorname{mod}(\frac{N}{(N,\alpha)},\chi))$. That is equivalent to $(1-x)\frac{\alpha}{(N,\alpha)}\equiv -p\beta\frac{x-1}{(N,\alpha)}$ $(\operatorname{mod}(p(\frac{N}{(N,\alpha)},\chi)))$, or to $(1-x)\alpha\equiv -p\beta(x-1)(\operatorname{mod}(p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)))$. Finally, we have

$$(x-1)(\alpha-p\beta)\equiv 0\left(\operatorname{mod}\left(p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)\right).$$

The last condition is satisfied if and only if

$$x\equiv 1\left(\operatorname{mod}\frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta,p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right).$$

So, we have the following conditions to be satisfied by x:

$$\begin{aligned} &x\equiv 1 \pmod{p},\\ &x\equiv 1 \pmod{(N,\alpha)},\\ &x\equiv 1\left(\operatorname{mod}\frac{N}{(N,\alpha)}\right),\\ &x\equiv 1\left(\operatorname{mod}\frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta,p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right). \end{aligned} \tag{8}$$

Note that, in the modulus of the last congruence, the denominator has a factor of (α, p) and since χ divides $\frac{N}{p}$, we deduce that the whole modulus divides $(\frac{pN}{(\alpha,p)}, \frac{(N,\alpha)N}{(\alpha,p)})$; since $(\frac{p}{(\alpha,p)}, \frac{(N,\alpha)}{(\alpha,p)}) = 1$, it follows that this modulus divides N.

As we have just seen, any solution for x and y to congruences (2), (3), (4) and (5) gives rise to a solution to congruences (7) and (8). Conversely, it is clear that any solution to (7) and (8) will satisfy (2), (3) and (4), and a solution to (7), and hence (6), gives a solution to (5). Thus, the two sets of congruences are equivalent.

By applying Lemma 7.3, we find the number of solutions for x of the congruences (8) is

$$\frac{N}{\left[p, (N,\alpha), \frac{N}{(N,\alpha)}, \frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta, p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right]}.$$

For each given x satisfying (8), there are unique values of $\frac{1-x}{p} \pmod{\chi}$ and $\frac{x-1}{(N,\alpha)} \pmod{\frac{N}{(N,\alpha)}}$. Moreover, each such x satisfies the consistency condition for (7). Thus, we can count the number of solutions (7) using Lemma 7.3, which gives $\frac{N}{[\frac{N}{(N,\alpha)},\chi]}$. Therefore,

$$\left|H_{\binom{\alpha}{\beta}}\right| = \frac{N}{\left[p, (N,\alpha), \frac{N}{(N,\alpha)}, \frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta, p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right]} \frac{N}{\left[\frac{N}{(N,\alpha)}, \chi\right]}, \tag{9}$$

and, by substituting $|H_{\binom{\alpha}{\beta}}|$ in formula (1), we get

$$\begin{aligned} c(p,N;\chi) &= \frac{\chi\phi(p)}{N\phi(N)} \\ &\sum_{\binom{\alpha}{\beta}\in M_N} \frac{N}{\left[p, (N,\alpha), \frac{N}{(N,\alpha)}, \frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta, p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right]} \frac{N}{\left[\frac{N}{(N,\alpha)}, \chi\right]} \\ &= \frac{\chi\phi(p)N}{\phi(N)} \\ &\sum_{\binom{\alpha}{\beta}\in M_N} \frac{1}{\left[p, (N,\alpha), \frac{N}{(N,\alpha)}, \frac{p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)}{\left(\alpha-p\beta, p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)}\right]} \frac{N}{\left[\frac{N}{(N,\alpha)}, \chi\right]}. \end{aligned} \tag{10}$$

Although (10) is somewhat unwieldy, we shall show that it reduces to the following remarkably simple expression:

Theorem 7.4.

$$c(p,N;\chi) = \frac{N\chi\phi(p)}{\phi(N)} \sum_{d|\frac{k}{\chi}} \frac{\phi(d)\phi(d')}{[d,d',\frac{pk}{N}]}, \tag{11}$$

where $k = [(p^2,N)\chi, N]$ and $dd' = k/\chi$.

The difficulty in a direct approach is the additive term $\alpha - p\beta$, which makes a direct simplification problematic. Our strategy will be to invoke multiplicativity of $c(p,N;\chi)$ and then do a case-by-case verification that (10) and (11) are equal. We start with the following special case:

Lemma 7.5.

$$c(p,N;1) = \frac{N\phi(p)}{\phi(N)} \sum_{d|N} \frac{\phi(d)\phi(\frac{N}{d})}{[d,\frac{N}{d},p]}.$$

Proof. Let $\begin{pmatrix} a^{-1} & 0 \\ b & a \end{pmatrix} \in H_{\binom{\alpha}{\beta}}$, where $a \equiv 1 \pmod p$. Now we have the following system of congruences to be satisfied by a and b:

$$\begin{aligned} a^{-1}\alpha &\equiv \alpha \pmod N, \\ b\alpha + a\beta &\equiv \beta \pmod N. \end{aligned}$$

In this case, the conditions on a and b are given by

$$\begin{aligned} a &\equiv 1 \pmod p, \\ a &\equiv 1 \pmod{(N,\alpha)}, \\ a &\equiv 1 \left(\bmod\ \frac{N}{(N,\alpha)}\right), \end{aligned}$$

and $b \equiv (\frac{\alpha}{(N,\alpha)})^{-1}(-\beta)\frac{a-1}{(N,\alpha)} \pmod{\frac{N}{(N,\alpha)}}$. These conditions, as in the general case, imply that $|H_{\binom{\alpha}{\beta}}| = (N,\alpha)\frac{N}{[(N,\alpha),\frac{N}{(N,\alpha)},p]}$, and the main formula (11) becomes

$$\begin{aligned} c(p,N;1) &= \frac{\phi(p)}{N\phi(N)} \sum_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)\in M_N} (N,\alpha)\frac{N}{\left[(N,\alpha),\frac{N}{(N,\alpha)},p\right]} \\ &= \frac{\phi(p)}{\phi(N)} \sum_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)\in M_N} \frac{(N,\alpha)}{\left[(N,\alpha),\frac{N}{(N,\alpha)},p\right]}. \end{aligned}$$

Now it is not difficult to show that $\sum_{\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)\in M_N} 1 = \frac{N}{d}\phi(d)\phi(\frac{N}{d})$, where the sum is over all $\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)$ with $(N,\alpha)=d$ with d fixed. Thus, we have

$$c(p,N;1) = \frac{N\phi(p)}{\phi(N)} \sum_{d|N} \frac{\phi(d)\phi(\frac{N}{d})}{[d,\frac{N}{d},p]}. \qquad \square$$

Since $c(p,N;\chi)$ is a multiplicative function in the sense of Selberg [**7**], as shown in Section 6, it will suffice to prove Theorem 7.4 in the case where $N=l^a$ is a prime power. Note that this assumption implies that $p=l^b$ and $\chi=l^c$ so that

$$b \le a \quad \text{and} \quad c \le \min(a-b,b).$$

Lemma 7.6. *Let l be a prime number. Then*

$$c(l^b,l^a;l^c) = \begin{cases} c(l^{b+c},l^a;1) & a \le 2b \\ l^c\ c(l^b,l^{a-c};1) & 2b+c \le a \\ l^{a-2b}\ c(l^{3b+c-a},l^{2b};1) & 2b < a < 2b+c. \end{cases}$$

Proof. (Case $a \le 2b$). The equality in this case follows from the fact that $H(l^b,l^a;l^c)$ and $H(l^{b+c},l^a;1)$ are conjugate.

If
$$\begin{pmatrix} 1+ul^b & vl^a \\ w & 1+xl^b \end{pmatrix} \in H(l^b,l^a;l^c),$$

then $(1+ul^b)(1+xl^b)-vwl^a=1$ and $u\equiv w \pmod{l^c}$, and so $l^c \mid (w+x)$. Now consider the relation

$$\begin{pmatrix}1 & -l^b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1+ul^b & vl^a\\ w & 1+xl^b\end{pmatrix}\begin{pmatrix}1 & l^b\\ 0 & 1\end{pmatrix}$$
$$=\begin{pmatrix}1+(u-w)l^b & (u-w-x)l^{2b}+vl^a\\ w & 1+(w+x)l^b\end{pmatrix}.$$

Therefore,

$$\begin{pmatrix}1+(u-w)l^b & (u-w-x)l^{2b}+vl^a\\ w & 1+(w+x)l^b\end{pmatrix}\in H(l^{b+c},l^a;1).$$

So $H(l^b,l^a;l^c)$ is conjugate to a subgroup of $H(l^{b+c},l^a;1)$ and, by Proposition 2.6, $H(l^b,l^a;l^c)$ and $H(l^{b+c},l^a;1)$ have the same index in Γ which implies that they are conjugate.

(Cases $2b+c\leq a$ and $2b<a<2b+c$). Before proceeding, we first show that

$$\left(\alpha-p\beta,p(N,\alpha)\left(\frac{N}{(N,\alpha)},\chi\right)\right)=(p,(N,\alpha)), \tag{12}$$

where all parameters are as above, but with the extra condition that the common prime divisors of p and (N,α) do not have the same multiplicities. It is easy to see that the right hand side is a divisor of the left hand side. Conversely, in order to show that $(\alpha-p\beta,p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)) \mid (p,(N,\alpha))$, let $q^s\|(\alpha-p\beta,p(N,\alpha)(\frac{N}{(N,\alpha)},\chi))$ where q is a prime number, and also suppose that $q^t\|p$ and $q^{t'}\|(N,\alpha)$ so that $t\neq t'$. Then $q^s \mid q^{\min(t,t')}(\frac{\alpha}{q^{\min(t,t')}}-\beta\frac{p}{q^{\min(t,t')}})$, where $(\frac{\alpha}{q^{\min(t,t')}}-\beta\frac{p}{q^{\min(t,t')},q})=1$. This proves $q^s \mid (p,(N,\alpha))$, and hence our statement.

Now we can apply equality (11) to simplify the formula for $c(l^b,l^a;l^c)$ where $\alpha=ul^m$ so that $m\neq b$ and $(u,l)=1$. To do so, the sum in

$c(l^b, l^a; l^c)$ is broken into the following sums:

$$\begin{aligned} c(l^b, l^a; l^c) &= \frac{l^c\phi(l^b)l^a}{\phi(l^a)} \\ &\quad \sum_{\binom{\alpha}{\beta}\in M_{l^a}} \frac{1}{\left[l^b, (l^a, \alpha), \frac{l^a}{(l^a,\alpha)}, \frac{l^b(l^a,\alpha)(\frac{l^a}{(l^a,\alpha)},l^c)}{\left(\alpha - l^b\beta, l^b(l^a,\alpha)\left(\frac{l^a}{(l^a,\alpha)},l^c\right)\right)}\right]\left[\frac{l^a}{(l^a,\alpha)}, l^c\right]} \\ &= \frac{l^c\phi(l^b)l^a}{\phi(l^a)} \left\{ \sum_{\substack{m=0\\ m\neq b}}^{a} \frac{\phi(l^m)\phi(l^{a-m})l^{a-m}}{\left[l^b, l^m, l^{a-m}, \frac{l^{b+m}(l^{a-m},l^c)}{(l^b,l^m)}\right]\left[l^{a-m}, l^c\right]} s \right. \\ &\quad \left. + \sum_{\substack{(\beta,l)=1\\ u}} \frac{1}{\left[l^b, l^{a-b}, \frac{l^{2b}(l^{a-b},l^c)}{l^b(u-\beta,l^b(l^{a-b},l^c))}\right]\left[l^{a-b}, l^c\right]} \right\}. \end{aligned}$$

It is convenient to further split these two sums into three terms S_1, S_2 and S_3 corresponding to those α's such that $0 \le m \le b-1$, $m = b$ and $b+1 \le m \le a$, respectively. S_1 and S_3 can be written as

$$S_1 = \sum_{0\le m\le b-1} \frac{\phi(l^m)\phi(l^{a-m})}{[l^{a-m}, l^{b+c}]} \quad \text{since } m < b \text{ and } 2b \le a$$

$$S_3 = \sum_{b+1\le m\le a} \frac{\phi(l^m)\phi(l^{a-m})l^{a-m}}{[l^{a-m}, (l^a, l^{m+c})][l^{a-m}, l^c]} \quad \text{since } m > b,$$

and S_2 splits into the following sums

$$S_2 = \sum_{\substack{(l,\beta)=1\\ u}} \frac{1}{\left[l^{a-b}, l^b, \frac{l^{2b}(l^{a-b},l^c)}{l^b(u-\beta,l^b(l^{a-b},l^c))}\right]\left[l^{a-b}, l^c\right]}$$

$$\begin{aligned} S_2 &= \frac{(\phi(l^a) - l^{a-1})\phi(l^{a-b})}{[l^{a-b}, l^b(l^{a-b}, l^c)][l^{a-b}, l^c]} \\ &\quad + \sum_{m=1}^{b+c} \frac{\phi(l^{a-m})\phi(l^{a-b})}{\left[l^{a-b}, l^b, \frac{l^{b+c}}{l^m}\right]\left[l^{a-b}, l^c\right]} + \frac{l^{a-b-c-1}\phi(l^{a-b})}{[l^{a-b}, l^b][l^{a-b}, l^c]}. \end{aligned}$$

If $(u - \beta, l^a) = l^m$, then these three terms correspond to $m = 1$, $1 < m \le b+c$ and $b+c < m \le a$, respectively.

By considering the two cases $2b+c \leq a$ and $2b < a < 2b+c$, we can simplify S_1, S_2 and S_3 as follows:

(Case $2b+c \leq a$). What we want to prove is

$$S_1 + S_2 + S_3 = \sum_{m=0}^{a-c} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}. \tag{13}$$

It is not difficult to see

$$S_1 = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{a-m})}{l^{a-m}} = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}, \tag{14}$$

and also

$$\begin{aligned} S_3 &= \sum_{m=b+1}^{a} \frac{\phi(l^m)\phi(l^{a-m})l^{a-m}}{[l^{a-m}, (l^a, l^{m+c})][l^{a-m}, l^c]} \\ &= \sum_{m=b+1}^{a-c-1} \frac{\phi(l^m)\phi(l^{a-m})}{[l^{a-m}, l^{m+c}]} \\ &\quad + \sum_{m=a-c}^{a} \frac{\phi(l^m)\phi(l^{a-m})l^{a-m}}{l^{a+c}}. \end{aligned}$$

The first sum can be rewritten as

$$\sum_{m=b+1}^{a-c-1} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}, \tag{15}$$

and the second sum is simplified to $\frac{1}{l^c}(1-\frac{1}{l})\sum_{m=a-c}^{a} \phi(l^{a-m})$, or

$$\frac{1}{l^c}\left(1-\frac{1}{l}\right)^2 \sum_{a-c}^{a-1}(l^{a-m}) + \frac{1}{l^c}\left(1-\frac{1}{l}\right) = 1 - \frac{1}{l}. \tag{16}$$

Now, by the assumption $2b+c \leq a$, so S_2 can be written as

$$\begin{aligned} S_2 &= \frac{\phi(l^{a-b})}{l^{a-b}}\left\{\frac{l^a - 2l^{a-1}}{l^{a-b}} + \frac{(1-\frac{1}{l})}{l^{a-b}}\sum_{m=1}^{b+c} l^{a-m} + \frac{1}{l^{c+1}}\right\} \\ &= \left(1-\frac{1}{l}\right)(l^b - l^{b-1}). \end{aligned} \tag{17}$$

Statement (13) follows from (14)–(17).

(Case $2b < a < 2b+c$). In this case the statement we want to show is

$$S_1 + S_2 + S_3 = \sum_{m=0}^{2b} \frac{\phi(l^m)\phi(l^{2b-m})}{[l^m, l^{2b-m}, l^{3b+c-a}]}. \tag{18}$$

S_1 can be written as $S_1 = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{a-m})}{[l^{a-m}, l^{b+c}]}$, or

$$S_1 = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{2b-m})}{[l^m, l^{2b-m}, l^{3b+c-a}]}.$$

We can split S_3 into the following sums:

$$S_3 = \sum_{m=b+1}^{a-c} \frac{\phi(l^m)\phi(l^{a-m})}{[l^{a-m}, l^{m+c}]} + \sum_{m=a-c+1}^{a} \frac{\phi(l^m)\phi(l^{a-m})l^{a-m}}{l^{a+c}},$$

and it can be simplified to

$$S_3 = \sum_{b+1}^{a} \frac{\phi(l^m)\phi(l^{a-m})}{l^{m+c}} = \phi(l^{a-b-c-1}).$$

Finally, the simplification of S_2 in this case is given by:

$$\begin{aligned} S_2 = \frac{\phi(l^{a-b})}{l^{a-b}} \Bigg\{ \frac{l^a - 2l^{a-1}}{l^{b+c}} &+ \sum_{m=1}^{2b+c-a} \frac{\phi(l^{a-m})}{l^{b+c-m}} \\ &+ \sum_{2b+c-a+1}^{b+c} \frac{\phi(l^{a-m})}{l^{a-b}} + \frac{1}{l^{c-1}} \Bigg\} \\ = \left(1 - \frac{1}{l}\right) \Bigg\{ l^{a-b-c} &- 2l^{a-b-c-1} \\ &+ (2b+c-a)\left(1 - \frac{1}{l}\right) l^{a-b-c} + l^{a-b-c-1} \Bigg\} \\ = \left(1 - \frac{1}{l}\right) \left\{ (2b+c-a+1)\phi(l^{a-b-c}) \right\}. \end{aligned}$$

It is easy to verify that the right hand side of (18) is

$$\begin{aligned}S_1 + \sum_{m=b}^{3b+c-a} \frac{\phi(l^m)\phi(l^{2b-m})}{l^{3b+c-a}} &+ \sum_{m=3b+c-a+1}^{2b} \frac{\phi(l^m)\phi(l^{2b-m})}{l^m} \\ &= S_1 + \left(1 - \frac{1}{l}\right)\left\{(2b+c-a+1)\phi(l^{a-b-c}) + l^{a-b-c-1}\right\} \\ &= S_1 + S_2 + S_3.\end{aligned}$$

This completes the proof. □

Finally observe that Lemmas 7.5 and 7.6 show that Theorem 7.4 holds for the prime power case and so the general case of Theorem 7.4 now follows from the multiplicativity of $c(p, N; \chi)$.

7.2. The number of inequivalent regular and irregular cusps. By Theorem 5.3, if $H(p, N; \chi)$ is regular, then $\nu_\infty = c(p, N; \chi)$ and $\nu'_\infty = 0$, and so, by Theorem 7.4 and Proposition 2.9, the first case of the formula for $(\nu_\infty, \nu'_\infty)$ in Theorem 1.2 is proved. In this subsection we give the proof of the remaining cases of Theorem 1.2, giving the number of inequivalent regular and irregular cusps where $H(p, N; \chi)$ is irregular. We start with the following lemma

Lemma 7.7. *If p has a nontrivial odd divisor and $H(p, N; \chi)$ is irregular, then $H(p, N; \chi)$ has no irregular cusps and $\nu_\infty = \frac{c(p,N;\chi)}{2}$.*

Proof. Suppose the contrary, so $H(p, N; \chi)$ has an irregular cusp. Then, by Theorem 5.3, the action of $H(p, N; \chi)$ on M_N has an irregular orbit. Let $\left(\begin{smallmatrix}\alpha \\ \beta\end{smallmatrix}\right) \in M_N$ be an element of this irregular orbit. Since the action of -1 maps this orbit to itself, it follows that there is an element $\left(\begin{smallmatrix}1+px & Nz \\ y & 1+pt\end{smallmatrix}\right) \in H(p, N; \chi)$ such that

$$\begin{pmatrix} 1+px & Nz \\ y & 1+pt \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \equiv \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix} \pmod{N}.$$

This gives rise to the following system of congruences:

$$\begin{cases} (1+px)\alpha \equiv -\alpha \pmod{N} \\ y\alpha + (1+pt)\beta \equiv -\beta \pmod{N}. \end{cases}$$

The first equation implies that $px \equiv -2 \pmod{N/(N,\alpha)}$. Hence,

$$2 \equiv 0 \pmod{(N/(N,\alpha),p)}. \tag{19}$$

Since p has an odd divisor, say $q \neq 1$, this shows that $q \mid (N,\alpha)$. On the other hand, the second equation can be rewritten as

$$(2+pt)\beta \equiv -y\alpha \pmod{N}.$$

From this and the fact that $((N,\alpha),\beta)=1$, we deduce that $(N,\alpha) \mid 2+pt$, and therefore $q \mid 2+pt$. This is a contradiction, since q is a nontrivial odd divisor of p. The second part of the lemma now follows from Theorem 5.3, since the preimage of a class of regular cusps consists of a pair of (distinct) regular orbits on M_N. □

Note that the previous lemma proves the final case of Theorem 1.2 except the case when p is a power of 2 greater than or equal to 4.

Lemma 7.8. *Suppose $N = 2^a$ for some $a \geq 1$ and $H(p,N;\chi)$ is irregular. Let $c = c(p,N;\chi)$. Then:*

If $p=2$, then $\chi = 2$ and

$$\begin{cases} \nu_\infty = (2/5)c & \nu'_\infty = (1/5)c \quad \textit{if } a = 2, \\ \nu_\infty = (1/4)c & \nu'_\infty = (1/2)c \quad \textit{if } a > 2 \textit{ is even}, \\ \nu_\infty = (1/3)c & \nu'_\infty = (1/3)c \quad \textit{if } a > 1 \textit{ is odd}. \end{cases}$$

If $p=4$, then $a=2$, $\chi=1$ and $\nu_\infty = (2/5)c$, $\nu'_\infty = (1/5)c$.

Otherwise, there are no irregular cusps for $H(p,N;\chi)$, and therefore $\nu_\infty = (1/2)c$ and $\nu'_\infty = 0$.

Proof. If $N = 2^a$, then $p = 2^b$ for some $b \leq a$. Now suppose that $\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right) \in M_{2^a}$ is an irregular cusp of $H(2^b,2^a;\chi)$, and therefore

$$\begin{pmatrix} 1+2^b x & 2^a z \\ y & 1+2^b t \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -\alpha \\ -\beta \end{pmatrix},$$

for some $\left(\begin{smallmatrix} 1+2^b x & 2^a z \\ y & 1+2^b t \end{smallmatrix}\right) \in H(2^b,2^a;\chi)$. So

$$\begin{cases} (1+2^b x)\alpha \equiv -\alpha \pmod{2^a} \\ y\alpha + (1+2^b t)\beta \equiv -\beta \pmod{2^a}. \end{cases}$$

An argument similar to the one we used to conclude (19) implies that

$$2 \equiv 0 \biggl(\operatorname{mod} \left(\frac{2^a}{(2^a, \alpha)}, 2^b\right)\biggr). \tag{20}$$

We now consider the following cases:

Case I. $b \geq 2$. The congruence (20) implies that $(2^a, \alpha) = 2^a$ or $(2^a, \alpha) = 2^{a-1}$. If $(2^a, \alpha) = 2^a$, then $2^b t\beta \equiv -2\beta \pmod{2^a}$, and this contradicts the assumption that $2 \nmid \beta$. If $(2^a, \alpha) = 2^{a-1}$, then

$$2^b t\beta \equiv -2\beta \pmod{2^{a-1}}. \tag{21}$$

Subcase. $b = 2$. In this case, since $2 \nmid \beta$, we have $a = 2$ and immediately $\chi = 1$. This is the case $H(4, 4; 1)$ which is conjugate to $\Gamma_1(4)$. One knows that $\Gamma_1(4)$ has one inequivalent irregular and two inequivalent regular cusps. As $c(4, 4, 1) = 5$, the result follows in this case.

Subcase. $b > 2$. In this case (21) contradicts $(2, \beta) = 1$; thus, there is no irregular cusp in this case and the number of inequivalent regular cusps is given by $\nu_\infty = \frac{c}{2}$.

Case II. $b = 1$. In this case the assumption $-1_2 \notin H(2, 2^a; \chi)$ implies that $\chi = 2$, and therefore $a \geq 2$.

Subcase. $a = 2$. The group $H(2, 4; 2)$ is conjugate to $H(4, 4; 1)$ by the first case of Lemma 7.6, and so it has the same number or inequivalent regular and irregular cusps as $\Gamma_1(4)$. As $c(2, 4, 2) = 5$, the result follows in this case.

Subcase. $a \geq 3$. The vector $\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$ is an element of an irregular orbit of $H(2, 2^a; 2)$ if and only if x, y and t exist satisfying

$$(1 + 2x)\alpha \equiv -\alpha \pmod{2^a} \tag{22}$$

$$y\alpha + (1 + 2t)\beta \equiv -\beta \pmod{2^a} \tag{23}$$

$$x \equiv y \pmod{2} \tag{24}$$

$$(1 + 2x)(1 + 2t) \equiv 1 \pmod{2^a}. \tag{25}$$

We shall now prove that such x, y and t exist if and only if α is of the form $u2^m$, where u is odd and $a \geq m > \frac{a-1}{2}$, and β is odd. First we prove that α must be even. If not, by congruence (22), $x\alpha \equiv -\alpha \pmod{2^{a-1}}$, and hence x is odd and so is y. But congruence (23) can be reduced to $y\alpha + 2t\beta \equiv -2\beta \pmod{2^a}$, which shows that $y\alpha$ is even, which is a contradiction. Thus, $\alpha = u2^m$ for some u odd and $a \geq m \geq 1$.

Next, we show that no solutions exist for the system of congruence equations above if $m \leq \frac{a-1}{2}$. By substituting $\alpha = u2^m$ where $a \geq m$ in (22), we have $2x \equiv -2 \pmod{2^{a-m}}$. Then (25) gives $2t \equiv -2 \pmod{2^{a-m}}$. These combined with (23) yield $yu2^m \equiv 0 \pmod{2^{a-m}}$. If $m \leq (a-1)/2$, then $a-m \geq (a+1)/2$. Since $a \geq 3$, the congruence $2x \equiv -2 \pmod{2^{a-m}}$ implies that x is odd, and hence y is odd. Also, $m \leq (a-1)/2$ implies $m < a/2$ and so $m < a-m$. Since u is odd, the congruence $yu2^m \equiv 0 \pmod{2^{a-m}}$ then yields a contradiction, and so $m > (a-1)/2$.

Any $\binom{\alpha}{\beta} \in M_{2^a}$, where β is odd and $\alpha = u2^m$ such that $a \geq m > \frac{a-1}{2}$ and where u is an odd number, is an element of an irregular orbit of $H(2, 2^a; 2)$, since it is easily checked that

$$\begin{aligned} x &= -1 + 2^{m-1} - 2^m + 2^{2m-1} \\ t &= -1 + 2^{m-1} \\ y &= -u^{-1}\beta \quad \text{where } uu^{-1} \equiv 1 \pmod{2^a} \end{aligned}$$

is a solution to the congruences (22)–(25).

By the Cauchy-Frobenius formula and Theorem 5.3, the number of irregular orbits and the number of inequivalent irregular cusps is given by

$$\nu'_\infty = \frac{\chi\phi(p)}{N\phi(N)} \sum_{\binom{\alpha}{\beta}} \left|H_{\binom{\alpha}{\beta}}\right| = \frac{1}{2^{2a-2}} \sum_{\binom{\alpha}{\beta}} \left|H_{\binom{\alpha}{\beta}}\right|,$$

where the sum is taken over all α and β such that β is odd and $\alpha = u2^m$ with $a \geq m > \frac{a-1}{2}$. Using the expression for $|H_{\binom{\alpha}{\beta}}|$ from equation (9) gives

$$\nu'_\infty = 4 \sum_{\binom{\alpha}{\beta}} \frac{1}{(2^a, 2^{m+1})[2^{a-m}, 2]}.$$

This simplifies to

$$\nu'_\infty = 4 \sum_{m=a/2}^{a} \frac{\phi(2^m)\phi(2^{a-m})2^{a-m}}{(2^a, 2^{m+1})[2^{a-m}, 2]} \quad \text{if } a \text{ is even,}$$

$$\nu'_\infty = 4 \sum_{m=(a+1)/2}^{a} \frac{\phi(2^m)\phi(2^{a-m})2^{a-m}}{(2^a, 2^{m+1})[2^{a-m}, 2]} \quad \text{if } a \text{ is odd.}$$

Evaluating these sums gives $\nu'_\infty = 2^{a/2}$ where a is even and $a > 2$ and $\nu'_\infty = 2^{(a-1)/2}$ where a is odd and $a > 1$. Using Theorem 7.4 to compute $c(2, 2^a; 2)$ when $a \geq 3$ gives

$$c(2, 2^a; 2) = \begin{cases} 2^{\frac{a}{2}+1} & \text{if } a \text{ is even,} \\ 3 \times 2^{\frac{a-1}{2}} & \text{if } a \text{ is odd.} \end{cases}$$

Comparing this with the number of inequivalent irregular cusps computed above gives $\nu'_\infty = (1/2)c$ where a is even and $a > 2$ and $\nu'_\infty = (1/3)c$ if a is odd and $a > 1$. Finally, Corollary 4.9 and Theorem 5.1 give $\nu_\infty = (1/4)c$ if a is even and $a > 2$ and $\nu_\infty = (1/3)c$ if a is odd and $a > 1$, which completes the proof. □

The above two lemmas combined with Corollary 6.6 give the following proposition to obtain the number of inequivalent regular and irregular cusps for $H(p, N; \chi)$ in the case $H(p, N; \chi)$ is irregular.

Proposition 7.9. *Let $N = 2^a N_1$, $p = 2^b$ and $\chi = 2^c$ where N_1 is an odd number. Suppose $H(p, N; \chi)$ is irregular. Then there are no irregular cusps for $H(p, N; \chi)$, and therefore $\nu_\infty = \frac{c(p,N;\chi)}{2}$, except in the following cases*:

If $p = 2$, then $\chi = 2$ and

$$\begin{cases} \nu_\infty = \frac{2c(p,N;\chi)}{5} & \nu'_\infty = \frac{c(p,N;\chi)}{5} & \text{if } a = 2, \\ \nu_\infty = \frac{c(p,N;\chi)}{4} & \nu'_\infty = c(p, N; \chi)2 & \text{if } a > 2 \text{ is even,} \\ \nu_\infty = \frac{c(p,N;\chi)}{3} & \nu'_\infty = \frac{c(p,N;\chi)}{3} & \text{if } a > 1 \text{ is odd.} \end{cases}$$

If $p = 4$, then $a = 2$, $\chi = 1$ and

$$\nu_\infty = \frac{2c(p, N; \chi)}{5} \quad \nu'_\infty = \frac{c(p, N; \chi)}{5}.$$

Proof. If $H(p, N; \chi)$ is irregular, then by Proposition 2.9, $b > 0$, and if $b = 1$ then $c > 0$. Then, again by Proposition 2.9, $H(1, N_1; \chi)$ is regular and $H(2^b, 2^a, 2^c)$ is irregular. Thus, by Corollary 6.6, the numbers of inequivalent regular and irregular cusps of $H(p, N; \chi)$ is given by $\nu_\infty = \nu_1\nu_2$ and $\nu'_\infty = \nu_1\nu'_2$ where ν_1 is the cusp number of $H(1, N_1; 1)$ and ν_2 and ν'_2 are, respectively, the numbers of inequivalent regular and irregular cusps of $H(2^b, 2^a, 2^c)$. Except for the four cases listed in Lemma 7.8, $H(2^b, 2^a; 2^c)$ has no irregular cusps, and so, by the multiplicativity of $c(p, N; \chi)$, $\nu_\infty = (c(1, N_1; 1)) \times (c(2^b, 2^a; 2^c)/2) = c(p, N; \chi)/2$. The four exceptions follow similarly using the expressions for ν_2 and ν'_2 from Lemma 7.8 and multiplicativity of $c(p, N; \chi)$. □

By Lemma 7.8 the cases in Proposition 7.9 are the only cases for which $H(p, N; \chi)$ is irregular and has irregular cusps. This accounts for all the cases of Theorem 1.2 and so completes the proof of this theorem.

REFERENCES

1. C.J. Cummins, *Congruence subgroups of groups commensurable with* $\mathrm{PSL}(2, \mathbf{Z})$ *of genus* 0 *and* 1, Exper. Math. **13** (2004), 361–382.

2. ———, *Torsion-free, genus-one congruence subgroups of* $\mathrm{PSL}(2, \mathbf{R})$ *and multiplicative* η*-products*, accepted.

3. H. Larcher, *The cusp amplitudes of the congruence subgroups of the classical modular group*, II, Illinois J. Math. **28** (1984), 312–338.

4. A.W. Mason and Andreas Schweizer, *The cusp amplitudes and quasi-level of a congruence subgroup of SL2 over any Dedekind domain*, arXiv:0909.0799 2009

5. Toshitsune Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989.

6. Abdellah Sebbar, *Classification of torsion-free genus zero congruence groups*, Proc. Amer. Math. Soc. **129** (2001), 2517–2527 (electronic).

7. Atle Selberg, *Remarks on multiplicative functions*, in *Number theory day*, 1976, pages 232–241; Lect. Notes Math. **626**, Springer, Berlin, 1977.

8. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan **11**, Iwanami Shoten, Publishers, Tokyo, 1971.

Department of Mathematics and Statistics, Concordia University, Montreal, Quebec, Canada H3G 1M8
Email address: chris.cummins@concordia.ca

Mathematics Department, Dawson College, Montreal, Quebec, Canada H3Z 1A4
Email address: nsabetghadam@dawsoncollege.qc.ca