On Larcher Subgroups and Fourier Coefficients of Modular Forms

Noushin SabetghadamHaghighi

A Thesis

In the Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements

For the Degree of Doctor of Philosophy at

Concordia University

Montréal, Québec, Canada

April 2010

Your file Votre référence
ISBN: 978-0-494-67366-9
Our file Notre référence
ISBN: 978-0-494-67366-9

Abstract

On Larcher Subgroups and Fourier Coefficients of Modular Forms

Noushin SabetghadamHaghighi, Ph.D.

Concordia University, 2010.

The Theory of Moonshine was initiated more than three decades ago to explore the interaction between the sporadic simple groups and the Fourier coefficients of modular functions on Moonshine-type groups. Even though this theory now involves a larger variety of diverse concepts and structures, the interplay between these two subjects remains the central theme of this theory. The purpose of this thesis was motivated by Moonshine, but it is within the second domain. This work is two-fold, covering the structure of a class of congruence subgroups and the computation of the Fourier coefficients of modular forms defined on genus-zero moonshine-type subgroups.

The purpose of the first part of this thesis is to compute some invariants of a family of congruence subgroups containing Larcher subgroups. These subgroups initially were defined by Larcher to prove his result on the cusp widths of congruence subgroups. However it later turned out that these subgroups have an interesting role in the classification of genus-zero and genus-one torsion-free congruence subgroups.

The second part of this thesis is a generalization of the recurrence formulae which were first established by Bruinier. Kohnen and Ono for the Forurier coefficients of the modular forms of the full modular group. Shortly after, similar recurrences were found by some other authors for some genus-zero congruence subgroups of the full modular group. Using a different technique, this work finds the universal recursive formulae satisfied by the Fourier coefficients of any meromorphic modular form on any genus-zero subgroup of $\mathrm{SL}(2,\mathbb{R})$ commensurable with $\mathrm{SL}(2,\mathbb{Z})$.

Acknowledgement

It is a pleasure to express my deepest gratitude to those who made this thesis possible. I am deeply indebted to my supervisor, Professor Cummins for his encouragement, advice and persistent guidance from the very early stage to the final level of my whole program. I am heartily grateful to him not only for his supervision and direction but also for his caring and kindness. With no doubt this thesis would not have come about without his help and constant support.

Besides my advisor, my sincere thanks are due to the other members of my defense committee for their comments, feedback and input to my thesis.

I would also acknowledge my teachers both in the Department of Mathematics and Computer Science of the University of Tehran and the Department of Mathematics and Statistics of Concordia University for getting me interested in mathematics, helping me develop my mathematical knowledge and encouraging me to pursue and accomplish my Ph.D.

I wish to thank Prof. Cummins as well as the Department of Mathematics and Statistics of Concordia University and ISM, the Institut des sciences mathématiques, for the financial support that I have received during my program.

Most importantly, I owe my deepest gratitude to my extended family, in particular my parents in Iran for their love, prayers and supports. I am heartily grateful to my daughters, Samar and Saba, whose love encouraged me whenever I felt disappointed. I am also indebted to my husband, Shahab, who planned such a long way for me from my bachelor in mathematics around eighteen years ago at the University of Tehran to this point. Thank you my dear!

And at last , I am deeply grateful to GOD for granting me the opportunities, talent and encouragement to reach this achievement.

Contents

Chapter 1

Introduction

"Moonshine is NOT a well-defined term, but everyone in the area recognizes it when they see it. Roughly speaking it means weird connections between modular forms and sporadic simple groups."

Richard E. Borcherds [B.R01].

1.1 Big Picture

The classification of finite simple groups states that every finite simple group either belongs to one of the infinite families: Cyclic groups of prime orders; Alternating groups of degree at least five; Lie type groups including 16 infinite families; or it is one of the 26 sporadic finite simple groups. The smallest sporadic simple group, the Mathieu Group M_{11}, is of order 7920 and the largest one, Fischer-Griess, denoted by $\mathbb{M}$ is of order

$$|\mathbb{M}| = 2^{46} \cdot 3^{20} \cdot 5^{9} \cdot 7^{6} \cdot 11^{2} \cdot 13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71,$$

known as the "Monster". Although the existence of $\mathbb{M}$ had been independently proved by Fischer and Griess in 1973, it was in 1980 that Griess [G81] constructed $\mathbb{M}$ as the automorphism group of the Griess algebra, a 196883-dimensional commutative non-associative algebra. The theory of "Monstrous Moonshine" unofficially began in 1974 when Ogg [Og74] noticed that the prime numbers appearing in the factorization of $|\mathbb{M}|$ coincide with those p's for which the Riemann surface resulting from taking the quotient of the extended upper half plane $\mathfrak{H}^*$ by the group

$$\Gamma_0(p)^+ := \left\langle \Gamma_0(p), \frac{1}{\sqrt{p}}\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \right\rangle$$

is of genus zero. Shortly after, Mckay observed that $196884 = 196883 + 1$, where 196884 is the first non-trivial coefficient of the normalized Hauptmodul $J = j - 744 = q^{-1} + 196884q + 21493760q^2 + \cdots$ of the full modular group $\mathrm{SL}(2, \mathbb{Z})$ and 196883 is the smallest dimension of a non-trivial complex representation of $\mathbb{M}$. Although it first seemed to be a coincidence, Mackay's observation was generalized by Thompson [Th79] who found that the first five coefficients of J are simple linear combinations of the character degrees of $\mathbb{M}$. Indeed, Thompson asked if there exists a graded $\mathbb{M}$-module $V = \oplus_{n\geq 1} V_n$ such that $\dim(V_n) = c_n$, where

$$J = q^{-1} + \sum_{n=1}^{\infty} c_n q^n$$

is the normalized Hauptmodul of $\mathrm{SL}(2, \mathbb{Z})$. Moreover, he suggested studying the Thompson-Mckay series

$$T_g := q^{-1} + \sum_{n=1}^{\infty} \mathrm{Tr}(g|V_n) q^n$$

for all $g \in \mathbb{M}$. Since the conjugate elements in $\mathbb{M}$ have identical Thompson-Mckay series, g (in T_g) could be considered as a representative of one of 194 conjugacy classes of the Monster.

The term "Monstrous Moonshine" was coined by Conway as a name for unexpected relationships between sporadic simple groups and modular functions. Conway and Norton [CN79] in their article under the title of "Monstrous Moonshine" conjectured that for any $g \in \mathbb{M}$, the Thompson-Mckay series T_g associated to g gives rise to a normalized Hauptmodul of a genus-zero modular group G_g of moonshine-type. A modular group G is called of moonshine-type if it contains $\Gamma_0(N)$ for some N and also if G has the transformation $z \mapsto z + k$ then $k \in \mathbb{Z}$. The group G_g is a genus-zero modular group which lies between $\Gamma_0(N)$ and its normalizer in $\mathrm{PSL}(2, \mathbb{R})$, for some $N = hn$ where n is the order of g in $\mathbb{M}$ and h is the largest divisor of 24 whose square divides N. These groups are genus-zero subgroups of $\mathrm{SL}(2, \mathbb{R})$ which are commensurable with $\mathrm{SL}(2, \mathbb{Z})$.

Conway and Norton also conjectured that there must be "three or four hundred cases" of such subgroups whose Hauptmoduls have algebraic integer coefficients, 171 of which correspond to the elements of $\mathbb{M}$. It turns out that the Hauptmoduls of interest have rational coefficients. So we are dealing with "rational conjugacy classes" rather than conjugacy classes. Therefore for any $g \in \mathbb{M}$, T_g and T_{g^m} turn out to be the same if m is coprime to n where n is the order of g in $\mathbb{M}$. Then, having the same Thompson-Mckay series for the classes $27A$ and $27B$ "accidently" reduces the number of distinct T_g's by 1. So the number of the distinct Thompson-Mckay Series is less than the number of the conjugacy classes of $\mathbb{M}$. Although the correspondence between the Monster conjugacy classes and the genus-zero moonshine-type subgroups is quite remarkable, it is not one to one.

Cummins [Cu04] found all genus-zero and genus-one moonshine-type subgroups of $\mathrm{SL}(2, \mathbb{R})$ to answer the question of Conway and Norton regarding a complete list of such subgroups. He showed there are precisely 6486 genus-zero moonshine-type groups of which 616 have rational coefficients. However there is an action of $\mathbb{Z}/24\mathbb{Z}$ on such subgroups and also Galois conjugations which reduce these groups to 371 equivalence classes, 310 of them have rational coefficients.

1.2 Chapter 2: Overview

Due to the significant role played by genus-zero modular groups in Monstrous Moonshine, Sebbar [Seb01] classified the torsion free genus-zero congruence subgroups of $\mathrm{SL}(2,\mathbb{R})$. Sebbar exploits a family of congruence subgroups

$$\Gamma_\tau(m; m/d, \varepsilon, \chi) =$$
$$\left\{ A \in \mathrm{SL}(2,\mathbb{Z}) \middle| \, A = \pm \begin{pmatrix} 1 + k_1(m/\varepsilon\chi) & k_2 d \\ k_3(m/\chi) & 1 + k_4(m/\varepsilon\chi) \end{pmatrix}, \ k_3 \equiv \tau k_1 \pmod{\chi} \right\},$$

where $d \mid m$, $m/d = h^2 n$, with n square-free, $\varepsilon \mid h$ and $\chi \mid \gcd(d\varepsilon, m/d\varepsilon^2)$, first introduced by Larcher [L84]. Larcher defined these subgroups to prove that the set of cusp widths of any congruence subgroup is closed under taking greatest common divisor and least common multiple. First he verified this property for the set of cusp widths of any $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ and then he remarked that for any congruence subgroup H of $\mathrm{SL}(2,\mathbb{Z})$ of level m and least cusp width d, there exists a $\Gamma_\tau(m; m/d, \varepsilon, \chi)$ for suitable χ and τ such that they have the same set of cusp widths.

Besides the application of Larcher subgroups in Sebbar's work, Larcher's results have been used as a criterion to distinguish between congruence and non-congruence subgroups of the full modular groups (see for instance [Hs96]). These applications together with the possibility of extending Sebbar's work to higher genus groups motivated us to study a class of congruence subgroups of the full modular group which contains Larcher subgroups and to compute their signature. The signature of a congruence subgroup H is the 5-tuple $(\mu, \nu_2, \nu_3, \nu_\infty, \nu'_\infty)$ where μ stands for the index of $\overline{H}$ in $\mathrm{PSL}(2,\mathbb{Z})$, ν_2 and ν_3 are the number of its inequivalent elliptic fixed points of order 2 and 3 respectively, ν_∞ gives the number of regular cusps of H and ν'_∞ is the number of irregular cusps of H. What follows is a summary of the results of this joint project with Cummins ([CS09] and [CS1]) which will be presented in Chapter 2 with the details. To begin with, we define:

$$H(p,q,r;\chi,\tau) =$$

$$\left\{ \begin{pmatrix} 1+ap & bq \\ cr & 1+dp \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \middle| \, a,b,c,d \in \mathbb{Z}, \quad c \equiv \tau a \pmod{\chi} \right\},$$

where $p \mid qr$ and $\chi \mid \gcd(p, qr/p)$, and note that this class contains the family of Larcher subgroups projectively and more specifically

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

The following technical lemma will allow us to reduce the computations to special cases.

Lemma 1.2.1. *Suppose p, q, r, χ and τ are positive integers such that $p \mid qr$ and $\chi \mid \gcd(p, qr/p)$. Let $g = \gcd(\chi, \tau)$. Then the groups $H(p,q,r;\chi,\tau)$ and $H(p, gqr; \chi/g)$ have the same signature, where $H(p,N;\chi) = H(p,N,1;\chi,1)$.*

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

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

where $d\,d' = k/\chi$ and where ϕ is the Euler function. It is proved in Chapter 2 that $c(p,N;\chi)$ is the number of orbits of $H(p,N;\chi)$ acting on a set related to the cusps of

$\Gamma(N)$. This number is closely related to the number of regular and irregular cusps of $H(p, N; \chi)$. Our main result is as follows:

Theorem 1.2.2. *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 $\psi(N) = N \prod_{\substack{p \mid N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right)$. The signature $(\mu, \nu_2, \nu_3, \nu_\infty, \nu'_\infty)$ of $H(p, N; \chi)$ is given by:*

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

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

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

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

where $a \mid\mid b$ means $a \mid b$ and $\gcd(a, b/a) = 1$, and where $\nu_2(N)$ and $\nu_3(N)$ stand for *the number of inequivalent elliptic fixed points of order* 2 *and* 3 *respectively of* $\Gamma_0(N)$. *Furthermore, the signature of* $\pm H$ *is* $(\mu, \nu_2, \nu_3, \nu_\infty + \nu'_\infty, 0)$.

As an interesting application, Cummins has used these formulae to classify the torsion free genus one congruence subgroups into eight classes which correspond to the eight weight two multiplicative η products, first investigated in [DKM82]. Larcher's results have recently been generalized to Drinfeld modules by Mason and Schweizer [MS09].

1.3 Chapter 3: Overview

As for the second part of my thesis we come back to the main conjecture of Monstrous Moonshine regarding the relations between two seemingly incomparable objects, namely the Monster and the Hauptmoduls of genus-zero discrete subgroups of $\mathrm{PSL}(2,\mathbb{R})$ via the graded $\mathbb{M}$-module V. Shortly after Conway and Norton's seminal paper, Atkin, Fong and Smith [Sm85] gave a computational proof of the main conjecture. They did not, however, give any reason for the existence of V or for the mysterious relations in which it involves. The conceptual proof was the result of the works of several people and was finalized by Borcherds [B.R92], who received a Fields Medal in 1998 for his spectacular proof. Borcherds [B.R98] outlined the proof of Conway and Norton's main conjecture in his ICM talk as follows:

- Frenkel, Lepowsky and Meurman [FLM88] found an explicit construction of the $\mathbb{M}$-module V with some extra algebraic structure making it into a "vertex algebra".

- The action of the Monster on the $\mathbb{M}$-module V equipped with the structure of a vertex algebra gives rise to a Lie algebra, called the "Monster Lie algebra".
- The monster Lie algebra is a "generalized Kac-Moody algebra" [B.R88]; the twisted Weyl-Kac character formula is then used to show that T_g's are "completely replicable functions".
- Martin [Ma96], Cummins and Gannon [CG97] proved that completely replicable functions are Hauptmoduls of genus-zero discrete modular groups.

Here we emphasize the last step regarding replicability of Hauptmoduls of moonshine-type groups which says that for any Thompson-Mckay series T_g and for any $n \geq 1$, the sum

$$\sum_{\substack{ad=n \\ 0\leq b<d}} T_{g^a}\left(\frac{az+b}{d}\right),$$

is in fact a polynomial in T_g. These polynomials are called Faber polynomials (see Section 3.1.2 for the definition). Intriguingly, Faber polynomials also occur in the work of several authors on "universal" recurrence relations satisfied by the Fourier coefficients of modular forms on certain moonshine-type groups. This program was originally initiated by Bruninier, Kohnen and Ono [BKO04] for the full modular group, and was subsequently extended to the groups $\Gamma_0(4)$ (by Atkinson [At05]), $\Gamma_0(p)$, $p \in \{2, 3, 5, 7, 11, 13\}$ (by Ahlgren [Ah02]), and $\Gamma_0(p)^+$ (by Choi [C.S.06]). In the latter case, p is any prime divisor of the order of the Monster.

Using a different technique, Cummins and SabetghadamHaghighi have generalized these works in [CS2] establishing universal recursive formulae satisfied by the Fourier coefficients of *any meromorphic modular form on any genus-zero subgroup* Γ *of* $\mathrm{SL}(2, \mathbb{R})$

commensurable with SL(2, $\mathbb{Z}$). By a theorem of Helling [He66], any such subgroup is conjugate to a subgroup of $\Gamma_0(N)^+$

$$\Gamma_0(N)^+ = \left\{ e^{\frac{-1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R}) \middle| \; a, b, c, d, e \in \mathbb{Z},\; e|N, e|a, e|d, N|c,\; ad - bc = e \right\},$$

for some square-free N. So we may restrict our attention to the case where Γ is contained in $\Gamma_0(N)^+$.

Now suppose that Γ is a genus-zero subgroup of $\Gamma_0(N)^+$ for some square-free N and h_0 is the cusp width of ∞ in Γ. Let

$$\phi(q) = \frac{1}{q} + \sum_{n\geq 0} c_n q^n, \qquad \text{where } q = e^{\frac{2\pi i z}{h_0}},$$

be its Hauptmodul. A main theorem of [CS2] is the following.

Theorem 1.3.1. *Let* $f = q^r + \sum_{n=1}^{\infty} a_n q^{r+n}$ *be a weight* k *meromorphic modular form for the genus-zero subgroup* Γ *of* $\Gamma_0(N)^+$. *Let* $s_0 = \infty, s_1, s_2, ..., s_t$ *be representatives of the inequivalent cusps of* Γ, *of widths* $h_0, h_1, h_2, ..., h_t$ *respectively. Then*

$$a_n = \sum_{\substack{m_1,\dots,m_{n-1}\geq 0 \\ m_1+\cdots+(n-1)m_{n-1}=n}} (-1)^{m_1+\cdots+m_{n-1}} \frac{(m_1+\cdots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} a_1^{m_1}\cdots a_{n-1}^{m_{n-1}}$$

$$-\frac{1}{n}\left(\frac{2kh_0}{\tau(N)}\sum_{\delta|N}\delta\sigma(\frac{n}{\delta h_0}) + \sum_{i=1}^{t}\left(\mathrm{ord}_{s_i} f - \frac{kh_i\sigma(N)}{12\tau(N)}\right)F_n(\phi(s_i)) + \sum_{\tau\in\Gamma\backslash\mathcal{H}} \mathrm{ord}_\tau f F_n(\phi(\tau))\right),$$

where F_n *is the nth Faber polynomial associated to the Hauptmodul* ϕ *of* Γ *and the functions* $\tau(N)$ *and* $\sigma(N)$ *are the number and the sum of positive divisors of* N *respectively.*

This theorem gives recursive formulae for the coefficients of f in terms of the divisor of f and the Faber polynomials attached to the Hauptmodul ϕ evaluated at the points of fundamental domain of Γ. By applying the above theorem to the derivative of the

Hauptmodul ϕ one can retrieve the coefficients c_n's recursively. This combined with the fact that the Faber polynomials associated to ϕ can also be calculated recursively yields the following refinement.

Theorem 1.3.2. *Let the hypotheses be as above. Then*

$$a_n = \frac{1}{n}\Bigg\{ S(n; a_1, ..., a_{n-1}) - \frac{2kh_0}{\tau(N)} \sum_{\delta | N} \delta\sigma(\frac{n}{\delta h_0})$$
$$- \sum_{i=1}^{t} \Big(\mathrm{ord}_{s_i} f - \frac{kh_i\sigma(N)}{12\tau(N)}\Big) S\Big(n; c_0 - \phi(s_i), c_1, ..., c_{n-1}\Big)$$
$$- \sum_{\tau \in \Gamma\backslash\mathcal{H}} \mathrm{ord}_\tau f S\Big(n; c_0 - \phi(\tau), c_1, ..., c_{n-1}\Big)\Bigg\}.$$

where

$$S(l; \alpha_1, ..., \alpha_n) = l \sum_{\substack{m_1, ..., m_n \geq 0 \\ m_1 + 2m_2 + \cdots + nm_n = l}} (-1)^{m_1 + ... + m_n} \frac{(m_1 + \cdots + m_n - 1)!}{m_1! \cdots m_n!} \alpha_1^{m_1} \cdots \alpha_n^{m_n}.$$

The details and the full proofs of these results will be presented in Chapter 3. In that chapter, first we find recurrences for the Fourier coefficients of any meromorphic modular form on any genus-zero subgroup of the full modular group, and then with the same method, we will establish the general case. Comparing with the other works cited above, some of the advantages of this work are highlighted as:

- The recurrences work for expansions at irregular cusps as well as regular ones (see Section 3.5),
- They work for non-congruence subgroups therefore it covers a big family of the subgroups; Cummins [Cu04] and [Cu09] showed that there are 506 SL$(2, \mathbb{R})$ conjugacy classes of genus-zero, congruence subgroups of PSL$(2, \mathbb{R})$. It is also known there are infinitely many non-congruence, genus-zero groups (see [J86] for instance).

- The form of the recurrences is well adapted to using the data which has been computed for studying moonshine. For example, Norton has computed the ramification data for all the (rational) genus-zero groups of moonshine type. So the recurrences are of particular use for the study of functions and forms associated with moonshine.

Remark 1.3.3. Though the two works presented in Chapters 2 and 3 are both related to and motivated by the Theory of Monstrous Moonshine, they are concerned with two independent problems. Therefore in writing these chapters it has been attempted to make each chapter as self-contained as possible. Thus the reader will notice that some of the definitions are repeated. It should also be emphasized that some notation used in both chapters will have two entirely different meanings; for instance, in chapter 2 the letter Γ represents the full modular group where throughout Chapter 3 the same letter is used for a genus-zero subgroup of $\mathrm{SL}(2, \mathbb{R})$ commensurable with $\mathrm{SL}(2, \mathbb{Z})$.

Chapter 2

Signature of a Class of Congruence Subgroups

2.1 Generalized Larcher Subgroups

Let Γ be the full modular group $\mathrm{SL}(2,\mathbb{Z})$ and define a subgroup H of Γ to be a congruence subgroup if it contains one of the principal congruence subgroups:

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

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

Let $\mathfrak{H}$ be the upper half plane and $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q}^*$ where $\mathbb{Q}^* = \mathbb{Q} \cup \{\infty\}$ and define the action of Γ on $\mathfrak{H}^*$ by fractional linear transformation

$$\sigma z = \frac{az+b}{cz+d} \qquad \text{where } \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \text{ and } z \in \mathfrak{H}^*.$$

An element σ of Γ is classified as:

$$\begin{aligned} \sigma \text{ is } \textit{parabolic} &\iff \operatorname{tr}(\sigma) = \pm 2, \\ \sigma \text{ is } \textit{elliptic} &\iff |\operatorname{tr}(\sigma)| < 2, \\ \sigma \text{ is } \textit{hyperbolic} &\iff \text{otherwise,} \end{aligned}$$

where $\operatorname{tr}(\sigma) = a+d$. If H is a subgroup of Γ then H also acts on $\mathfrak{H}^*$ by fractional linear transformations and its elements are classified as parabolic, elliptic and hyperbolic as above. Any fixed point of a parabolic element of H is called a *cusp* of H and it is easy to see that $\mathbb{Q}^*$ is the set of cusps of Γ. By Proposition 1.30 of [Sh71], if G and G' are *commensurable* discrete subgroups of $\mathrm{SL}(2,\mathbb{R})$, that is to say, if

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

then they have the same set of cusps. In particular the set of cusps of any finite index subgroup of Γ is $\mathbb{Q}^*$. If H is a finite index subgroup of Γ then the number of orbits of H acting on $\mathbb{Q}^*$ is called the cusp number of H. One can see that Γ acts transitively on $\mathbb{Q}^*$ and so its cusp number is one. For each $\alpha \in \mathbb{Q}^*$ let H_α be the stabilizer of α in H and let σ be an element of Γ such that $\sigma\alpha = \infty$. If $-1_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \notin H$ then $\sigma H_\alpha \sigma^{-1}$ is generated by either $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$ for some positive integer n (see Proposition 1.17 of [Sh71]), and the cusp α of H is called *regular* or *irregular* respectively. If H contains -1_2 then by definition all of its cusps are regular. The set of cusp widths of H is defined to be

$$C(H) = \left\{ \operatorname{Index}(\overline{\Gamma_\alpha} : \overline{H_\alpha}) \mid \alpha \in \mathbb{Q}^* \right\}$$

where $\overline{\Gamma_\alpha}$ and $\overline{H_\alpha}$ are the images of Γ_α and H_α in $\overline{\Gamma} := \mathrm{PSL}(2,\mathbb{Z})$ respectively.

It is a remarkable fact that for any congruence subgroup H the set of cusp widths $C(H)$ is closed under taking greatest common divisors and least common multiples. To establish this result Larcher in [L84] defined the following congruence subgroups of level m:

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

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

Larcher shows that the set of cusp widths of this class of congruence subgroups is closed under taking gcd and lcm. He then proves that for any congruence subgroup H of level m the set of its cusp widths, $C(H)$, coincide 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 desired property. In fact, his result is somewhat stronger, since he shows that up to a conjugation, every congruence subgroup H where $-1_2 \in H$ contains at least one Larcher subgroup L with the property that if h is an element of H which stabilizes some α in $\mathbb{Q}^*$, then h is also an element of L so that L is a "large" subgroup of H.

Although Larcher's results indicate the importance of his subgroups, there had been little study of their properties except for Sebbar [Seb01] who used Larcher's results to classify the torsion-free genus-zero congruence subgroups. His results were also applied by some authors to decide whether a subgroup of Γ is congruence or not (see for instance [Hs96]).

The significance of Larcher subgroups in proving Larcher's result and also the role which these subgroups played in Sebbar's work motivated us to investigate a class of congruence subgroups which contains Larcher subgroups. More precisely, we found explicit formulae for the indices, the number of elliptic fixed points and the cusp numbers of these groups. This data together with Riemann-Hurwitz formula gives the genus of such subgroups. Subsequently, Cummins applied these formulae to classify the torsion-free genus one congruence subgroups into eight classes which correspond to the eight weight two multiplicative η products, first investigated in [DKM82].

So, let us consider the following class of congruence subgroups:

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

where $p \mid qr$ and $\chi \mid \gcd(p, qr/p)$. We note that this family of groups include $\Gamma(N) = H(N,N,N,1,1)$, $\Gamma_0(N) = H(1,1,N,1,1)$ and $\Gamma_1(N) = H(N,1,N,1,1)$. More interestingly, Larcher subgroups are also 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 2.2.8). We call these groups "*Generalized Larcher Subgroups*".

The goal of this chapter is to compute the *signature* $(\mu, \nu_2, \nu_3, \nu_\infty, \nu'_\infty)$ of $H = H(p,q,r;\chi,\tau)$ 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.

Remark 2.1.1. The definition of signature given above is slightly different from one usually found in the literature. (see for instance [JS87]) The signature of H where H is a subgroup of $\mathrm{SL}(2,\mathbb{R})$ of genus g and cusp number t, having r inequivalent elliptic elements of orders $m_1,\cdots,m_r$, is usually defined as $(g;m_1,\cdots,m_r;t)$. In fact the algebraic structure of H can be determined by its signature. More precisely H has a presentation of the form

$$\langle A_1, B_1, \cdots, A_g, B_g, E_1, \cdots, E_r, P_1, \cdots, P_t \Big| \\ E_1^{m_1} = \cdots = E_r^{m_r} = \prod_{i=1}^r E_i \prod_{i=1}^t P_i \prod_{i=1}^g [A_i, B_i] = I \rangle,$$

where the generators E_i's are elliptic, P_i's are parabolic and A_i, B_i's are hyperbolic. One easily sees that the data $(g; m_1, \cdots, m_r; t)$ of H can be obtained from μ, ν_2, ν_3, ν_∞ and ν'_∞ by using Riemann-Hurwitz formula.

In Section 2.2 [1] the index formula will be derived. The number of inequivalent elliptic fixed points is found in Section 2.3. In Section 2.4 we will compute ν_∞ and ν'_∞; this computation is the main part of this chapter.

Our strategy will be to reduce the computation of ν_∞ and ν'_∞ to the case $H(p, N; \chi) := H(p, N, 1; \chi, 1)$. One important step toward this goal will be to find the number $c(p, N; \chi)$ of orbits of (a conjugate of) $H(p, N; \chi)$ acting on the subset of $(\mathbb{Z}/N\mathbb{Z})^2$ consisting of elements of additive order N. The virtue of working with $c(p, N; \chi)$ is that they are "multiplicative" in the generalized sense of Selberg [Sel77] as shown in Section 2.4.3. This reduces the calculation to the case that the level is a prime power. The task of computing regular and irregular cusps where $-1_2 \notin H$, which is required to compute the cusp number of such groups, involves a detailed analysis of the action of -1_2 and it is done in Section 2.4.4. We should remark that our approach is simply a long case by case verification, but it is possible that a simpler method exists; this could be a topic for future investigations. For the convenience of the reader, Section 2.5 will give a summary of the results of this chapter.

[1]This subsection is based on some notes of my supervisor Professor Cummins. I would like to thank him for giving me permission to add this section to my thesis.

2.2 The Index Formula

The goal here is to compute the index of $\overline{H}$ in $\overline{\Gamma}$ where $H = H(p,q,r;\chi,\tau)$. To achieve this, we will first compute the index of H in Γ. In order to pass from H to $\overline{H}$ we are forced then to separate the two cases whether -1_2 is in H or not. The final result will be stated in Theorem 2.2.10.

We first recall the following proposition (see for example [Cu04]). For positive integers p, q and r such that $p \mid qr$, it is straightforward to verify that

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

is a subgroup of Γ, and then:

Proposition 2.2.1. *We have*

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

where ϕ, known as the Euler function, and ψ are as follow:

$$\phi(N) = N \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} (1 - \frac{1}{\ell}) \quad \text{and} \quad \psi(N) = N \prod_{\substack{\ell \mid N \\ \ell \text{ prime}}} (1 + \frac{1}{\ell}).$$

Now define

$$\rho : H(p,q,r) \to \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$
$$\rho(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}) = ((\alpha - 1)/p, \beta/q, \gamma/r).$$

where $e = \gcd(p, qr/p)$. It is not difficult to verify that ρ is a group homomorphism.

Lemma 2.2.2. *The homomorphism ρ is surjective.*

Proof. First note that $\rho(\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}) = (0,1,0)$ and $\rho(\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}) = (0,0,1)$, so to show that ρ is surjective it is sufficient to find $h = \begin{pmatrix} 1+ap & bq \\ cr & 1+dp \end{pmatrix} \in H(p,q,r)$ such that a is coprime to e. 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 e. We must now show that we can choose b, c and d such that h is in $H(p,q,r)$. First set $c = 1$, and then choose b to be any solution to the congruence $bs \equiv a \pmod{1 + ap}$. 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 h has determinant 1 and so is in $H(p,q,r)$ as required. □

Proposition 2.2.3. *The kernel of* ρ *is* $H(ep, pq, pr)$.

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

Definition 2.2.4. Let S be a subgroup of $\mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, then we define $H(p,q,r;S)$ to be the preimage of S under ρ.

Proposition 2.2.5.

$$\mathrm{Index}(\Gamma : H(p,q,r;S)) = |S|^{-1} ep^3 qr \prod_{\substack{\ell | qr \\ \ell \text{ prime}}} (1 + \frac{1}{\ell}) \prod_{\substack{\ell | p \\ \ell \text{ prime}}} (1 - \frac{1}{\ell}) = |S|^{-1} ep^2 \phi(p) \psi(qr).$$

Proof. From Proposition 2.2.3 we have:

$$\mathrm{Index}(\Gamma : H(p,q,r;S)) = \mathrm{Index}(\Gamma : \Gamma(ep,pq,pr))/|S|.$$

The formula now follows from Proposition 2.2.1 by noting that a prime divides ep if and only if it divides p, since e divides p and similarly a prime divides p^2qr if and only if it divides qr. $\square$

Let χ be a divisor of e and τ be any integer and let T be the subgroup of $(\mathbb{Z}/\chi\mathbb{Z})^2$ generated by $(1,\tau)$, so $|T| = \chi$. Now define $\mu : \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/\chi\mathbb{Z})^2$ by $\mu(a,b,c) = (a,c)$ and also define $H(p,q,r;\chi,\tau) = H(p,q,r;\mu^{-1}(T))$. Since $|\mu^{-1}(T)| = ep^2/\chi$, we have from 2.2.5:

Proposition 2.2.6. *Let p, q, r and χ be in $\mathbb{Z}$ such that $p \mid qr$ and $\chi \mid \gcd(p, qr/p)$. Then for any integer τ we have:*

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

Proposition 2.2.7. *The congruence subgroups $H(p,q,r;\chi,\tau)$ can also be defined as*

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

Proof. If $h = \begin{pmatrix} 1+ap & qb \\ rc & 1+dp \end{pmatrix} \in \Gamma$ with $a,b,c,d \in \mathbb{Z}$ then $h \in H(p,q,r)$. Moreover we have $\mu(\rho(h)) = (a,c) = (a,\tau a)$ since $c \equiv \tau a \pmod{\chi}$, so $h \in H(p,q,r;\chi,\tau)$. Conversely, if $h \in H(p,q,r)$ then $h = \begin{pmatrix} 1+ap & qb \\ rc & 1+dp \end{pmatrix}$, with $a,b,c,d \in \mathbb{Z}$. If also $h \in H(p,q,r;\chi,\tau)$, then since $\mu(\rho(h)) = (a,c) \in T$ we must have $c \equiv \tau a \pmod{\chi}$. $\square$

Lemma 2.2.8. *Larcher 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 $\chi \mid \gcd(d\varepsilon, m/d\varepsilon^2)$ implies $\chi \mid e$, where $e = \gcd(m/\varepsilon\chi, d(m/\chi)(\varepsilon\chi/m)) = \gcd(m/\varepsilon\chi, d\varepsilon)$. However, if $\chi \mid \gcd(d\varepsilon, m/d\varepsilon^2)$, 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 $\chi \mid e$ as required. $\square$

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 2.2.9. *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 2.2.7 an element of $H(p,q,r;\chi,\tau)$ must have the form $\begin{pmatrix} 1+ap & qb \\ rc & 1+dp \end{pmatrix}$ 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 is trivial and so $\mu(\rho(-1_2)) \in T$ and so $-1_2 \in H(p,q,r;\chi,\tau)$ in cases **(2)** and **(3)**. 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)**. $\square$

The following corollary is the straightforward result of Propositions 2.2.6 and 2.2.9.

Corollary 2.2.10. *Let $H = H(p,q,r;\chi,\tau)$ then the index μ of $\overline{H}$ in $\overline{\Gamma}$, is given by*

$$\mu = \begin{cases} \chi\phi(p)\psi(qr) & \text{if } p=2,\ \chi=2 \text{ and } \tau \text{ even,} \\ & \text{or } p=2,\ \chi=1, \\ & \text{or } p=1; \\ \frac{1}{2}\chi\phi(p)\psi(qr) & \text{otherwise.} \end{cases}$$

2.3 The Inequivalent 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 of $H(p,q,r;\chi,\tau)$ respectively. To do so we use the fact that the signature remains invariant under conjugation. This reduces the number of cases which we have to consider. The following proposition will also help later when we compute the cusp numbers of the generalized Larcher subgroups.

Proposition 2.3.1. *Let p,q,r,χ and τ be positive integers such that $p \mid qr$ and $\chi \mid \gcd(p, qr/p)$. 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 $\mathrm{GL}^+(2,\mathbb{Q})$ 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

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

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 $\mathrm{GL}^+(2,\mathbb{Q})$.

Next we have that $H(p,N,1;\chi,\tau)$ is conjugate to $H(p,Ng,1;\chi/g,\tau/g)$, where $g=\gcd(\chi,\tau)$. To see this suppose $\begin{pmatrix} 1+ap & bN \\ c & 1+dp \end{pmatrix} \in H(p,N,1;\chi,\tau)$, 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 2.3.1 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 Theorem 2.3.2. To state our results we first give some notation.

For integers a and b, we say 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, [Sh71], Prop 1.43):

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

and

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

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

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

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

Now we have enough ingredients to state and compute ν_2 and ν_3 of generalized Larcher subgroups.

Theorem 2.3.2. *Let p, N, χ and τ be positive integers such that $p \mid N$, $\chi \mid \gcd(p, N/p)$ and $\gcd(\chi, \tau) = 1$. The values of ν_2 and ν_3, the number of inequivalent elliptic fixed* *points of order two and three of $H(p,N,1;\chi,\tau)$ are given by:*

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

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

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

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

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

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 earlier.

For $p=2$, we deduce that there exist no elliptic element if $2 \mid \frac{N}{2}$. To see this, suppose that $\begin{pmatrix} 1+2a & bN \\ c & 1+2d \end{pmatrix}$ 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 $2 \mid \frac{N}{2}$, 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 $3 \mid \frac{N}{3}$.

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

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

since both have the same index in Γ by Proposition 2.2.1. Thus if $p = 2$ and $2 \parallel N$ the number of inequivalent fixed points are given by $\nu_2(N)$ and $\nu_3(N)$. However, since $2 \mid N$ in this case we have $\nu_3(N) = 0$ from the formula given for $\nu_3(N)$ earlier. 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 Corollary 2.2.10. So in the case $p = 3$ and $3 \parallel N$ the number of inequivalent elliptic fixed points are given by $\nu_2(N)$ and $\nu_3(N)$. However, since $3 \mid N$ in this case we have $\nu_2(N) = 0$ as mentioned before. This accounts for all the cases listed in the Theorem. □

The statement of Theorem 2.3.2 shows that the generalized Larcher subgroups are mostly torsion free and for those with torsion points, ν_2 and ν_3 are independent of τ. Having found μ, ν_2 and ν_3 for generalized Larcher subgroups it remains to compute the numbers of their inequivalent regular and irregular cusps. As mentioned in Section 2.1, this is the most technical part of our result. We start in the next section by developing the necessary machinery. The computation of the cusp numbers is contained in the final subsection.

2.4 The Cusp Numbers of the Generalized Larcher Subgroups

2.4.1 Double Cosets and Regular and Irregular Cusps

We first recall some standard facts about group actions and the relation of double cosets and cusp number of finite index subgroups of Γ. The treatment in this section is based on that of Miyake [Mi89] in particular §4.2 in which Miyake computes the signature of $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$.

Lemma 2.4.1. *Let a group G act transitively on a set S, and 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 2.4.2. *Under the assumptions of Lemma 2.4.1, we have*

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

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

Since Γ acts transitively on $\mathbb{Q}^*$, it follows from Lemma 2.4.1 that

Theorem 2.4.3. *Suppose that H is a finite index subgroup of Γ, then there exists a bijective map $\phi : H\backslash\Gamma/\Gamma_\infty \to H\backslash\mathbb{Q}^*$ defined by $H\alpha\Gamma_\infty \mapsto H\alpha(\infty)$ and therefore $|H\backslash\mathbb{Q}^*| = |H\backslash\Gamma/\Gamma_\infty|$.*

Now we need to recall the definition of regular and irregular cusps of Section 2.1 with more details. Note that the stabilizer subgroup of ∞ in Γ is

$$\Gamma_\infty = \left\{ \pm\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}.$$

Definition 2.4.4. Let x be a cusp of a subgroup H of Γ and σ be an element of Γ such that $\sigma x = \infty$. Then there exists $n > 0$ so that

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

If $-1_2 \notin H$, the cusp x is regular or irregular depending on whether $\sigma H_x \sigma^{-1}$ contains $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$. It is clear that $\sigma H_x \sigma^{-1}$ can not have both matrices since H does not contain -1_2.

The (ir)regularity of a cusp x of H is independent of the choice of σ. See, for example, [Mi89] Lemma 1.5.6.

To distinguish regular and irregular cusps of H, we put

$$\Gamma_\infty^+ = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$

and define a map $\eta : H\backslash\Gamma/\Gamma_\infty^+ \to H\backslash\Gamma/\Gamma_\infty$ by $H\alpha\Gamma_\infty^+ \mapsto H\alpha\Gamma_\infty$. This map is well defined since $\Gamma_\infty^+ \subset \Gamma_\infty$. We also remark that $\mathrm{Index}(\Gamma_\infty : \Gamma_\infty^+) = 2$.

Lemma 2.4.5. *If $-1_2 \in H$ 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 $-h \in H$, in the second case also $\beta \in H\alpha\Gamma_\infty^+$ and so η is injective. □

Lemma 2.4.6. *If H does not contain -1_2 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 $\eta(H\beta\Gamma_\infty^+) = \eta(H\alpha\Gamma_\infty^+)$ and suppose $H\beta\Gamma_\infty^+ \neq H\alpha\Gamma_\infty^+$. Then since $H\beta\Gamma_\infty = H\alpha\Gamma_\infty$ we must have $\beta = h\alpha \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$, for some $n \in \mathbb{Z}$ and therefore $\beta = h(-\alpha)\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$. This implies that $H\beta\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+$. □

Theorem 2.4.7. *For a subgroup H of Γ where $-1_2 \notin H$ 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) $\mathrm{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 2$,

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

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

$$\begin{aligned} H\alpha\Gamma_\infty^+ = H(-\alpha)\Gamma_\infty^+ &\iff -\alpha \in H\alpha\Gamma_\infty^+ \\ &\iff -1_2 \in \alpha^{-1}H\alpha\Gamma_\infty^+ \\ &\iff \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} \in \alpha^{-1}H\alpha \text{ for some } n \in \mathbb{Z} \\ &\iff \alpha(\infty) \text{ is an irregular cusp.} \end{aligned}$$

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

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

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

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

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

Finally we show that **(1)** and **(4)** are equivalent. Since $-1_2 \notin H$ we must have $H\alpha(-1_2) \neq H\alpha$ and so $-1_2 \notin \Gamma_{\infty(H\alpha)}$. It follows that $\Gamma_{\infty(H\alpha)}$ is a cyclic subgroup generated either by $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ or by $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$ for some $n > 0$. In the former case $\text{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) = 2n$, $\text{Index}(\Gamma_\infty^+ : \Gamma^+_{\infty(H\alpha)}) = n$ and $\text{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 1$. While in the latter $\text{Index}(\Gamma_\infty : \Gamma_{\infty(H\alpha)}) = 2n$. $\text{Index}(\Gamma_\infty^+ : \Gamma^+_{\infty(H\alpha)}) = 2n$ and $\text{Index}(\Gamma_{\infty(H\alpha)} : \Gamma^+_{\infty(H\alpha)}) = 2$. This shows that **(4)** is equivalent to the statement that $\Gamma_{\infty(H\alpha)}$ contains $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$ 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 $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for some $n > 0$. $\Gamma_{\infty(H\alpha)}$ contains an element of the form $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix}$ for some $n > 0$ if and only if $\begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} \in \alpha^{-1}H\alpha$ which means **(1)** is equivalent to **(4)** and this completes the proof. □

An analogous theorem also can be stated for regular cusps.

Theorem 2.4.8. *For $\alpha \in \Gamma$ and a subgroup H of Γ where $-1_2 \notin H$, the following statements are equivalent:*

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

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

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

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

Corollary 2.4.9. *Suppose $-1_2 \notin H$ and let ν_∞ and ν'_∞ be the number of 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 2.4.10. *If H is a subgroup of Γ containing -1_2 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 a congruence subgroup in terms of double cosets. However, we will need a more concrete description which will be derived in the next section.

2.4.2 The Action of Congruence Subgroups on M_N

We set

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

Consider the faithful action of $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ 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 $\varphi_N : \Gamma \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. Moreover the image $\varphi_N(H)$ is isomorphic to $H/\Gamma(N)$.

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

Theorem 2.4.11. *Suppose H is a subgroup of Γ which contains $\Gamma(N)$. Define*

$$\begin{aligned} \psi : H\backslash\Gamma/\Gamma_\infty^+ &\to H\backslash M_N \\ H \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_\infty^+ &\mapsto \mathcal{O}_{\binom{a}{c}} \end{aligned}$$

where $\mathcal{O}_{\binom{a}{c}}$ is the orbit of the action of H on M_N containing $\begin{pmatrix} a \\ c \end{pmatrix}$. 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 $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in H \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Gamma_\infty^+$, then $\begin{pmatrix} a' \\ c' \end{pmatrix} = h \begin{pmatrix} a \\ c \end{pmatrix}$ for some $h \in H$ and so $\begin{pmatrix} a' \\ c' \end{pmatrix} \in \mathcal{O}_{\binom{a}{c}}$.

ψ is surjective. One way to see this is that if we have two integers a and c such that $0 \leq a, c < N$ 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, c'

with $\gcd(a, c') = 1$ and $c' \equiv c \pmod N$. We can then find b and d such that $m = \begin{pmatrix} a & b \\ c' & d \end{pmatrix}$ is in Γ and by construction satisfies $\psi(Hm\Gamma_\infty^+) = \mathcal{O}_{\binom{a}{c}}$. To prove its injectivity, suppose $\psi(H\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma_\infty^+) = \psi(H\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\Gamma_\infty^+)$. So we have $\begin{pmatrix} a' \\ c' \end{pmatrix} \in \mathcal{O}_{\binom{a}{c}}$ and therefore $\begin{pmatrix} a' \\ c' \end{pmatrix} \equiv h\begin{pmatrix} a \\ c \end{pmatrix} \pmod N$ for some $h \in H$. By [Sh71] Lemma 1.41, there exists $g \in \Gamma(N)$ such that $\begin{pmatrix} a' \\ c' \end{pmatrix} = gh\begin{pmatrix} a \\ c \end{pmatrix}$. We also know that for any matrix $\begin{pmatrix} a & * \\ c & * \end{pmatrix} \in \Gamma$ there exists $\gamma \in \Gamma_\infty^+$ such that $\begin{pmatrix} a & * \\ c & * \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\gamma$. These imply that $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = gh\begin{pmatrix} a & b \\ c & d \end{pmatrix}\gamma$, and this completes the proof. □

Next observe that the image of -1_2 under the map φ_N is a central element of $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. Thus there is an action of -1_2 on $H\backslash M_N$ given by $-1_2 \cdot H\begin{pmatrix} a \\ c \end{pmatrix} = H\begin{pmatrix} -a \\ -c \end{pmatrix}$. 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 2.4.12. Let H be a congruence subgroup of Γ and suppose that the level of H divides N. If $-1_2 \in H$ we say that all the orbits of H on M_N are regular. If $-1_2 \notin H$ then an orbit $\mathcal{O}$ of H on M_N is called 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 provided by the following result:

Theorem 2.4.13. *The mapping*

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

maps regular orbits to regular cusps and irregular orbits to irregular cusps. If $-1_2 \in H$ then w is a bijection. When $-1_2 \notin H$, if a/c represents a regular cusp and $\gcd(a, c) = 1$ then $w^{-1}(a/c) = \{\mathcal{O}_{\binom{a}{c}}, \mathcal{O}_{\binom{-a}{-c}}\}$ and these two elements are distinct, and if a/c represents an irregular cusp then $w^{-1}(a/c) = \{\mathcal{O}_{\binom{a}{c}}\}$.

Proof. If H contains -1_2 then by Theorem 2.4.11, Theorem 2.4.3 and Lemma 2.4.5 the map w is a bijection. Since $-1_2 \in H$, all cusps are regular and by Definition 2.4.12 all orbits of H on M_N are regular and are fixed by -1_2.

Suppose next that -1_2 doesn't belong to H. 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 2.4.7 and 2.4.8, the orbit of -1_2 acting on $H\backslash\Gamma/\Gamma_\infty^+$ maps to an irregular cusp under the composition $\phi\circ\eta$ if and only if it has length 1. Similarly it maps to a regular cusp 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 2.4.13 gives an explicit construction which allows us to determine the regularity or irregularity of a cusp of a given congruence subgroup. The next lemma will reduce the number of cases we shall need to consider.

Lemma 2.4.14. *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 from the definitions of these groups. Let $h = \begin{pmatrix} 1+ap & 0 \\ c & 1+dp \end{pmatrix} \in \varphi_N(H(p,N,1;\chi,\tau))$. Since $\gcd(\chi,\tau) = 1$ there exists $k \in \mathbb{N}$ 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 h is in $\varphi_N(H(p,N,1;\chi,1)$. Conversely suppose that $\begin{pmatrix} 1+ap & 0 \\ c & 1+dp \end{pmatrix} \in \varphi_N(H(p,N,1;\chi,1))$.

then applying the inverse of the conjugation given above we have $\begin{pmatrix} 1+ap & 0 \\ c(\tau+k\chi) & 1+dp \end{pmatrix} \in \varphi_N(H(p,N,1;\chi,\tau))$, because $c(\tau + k\chi) \equiv a\tau \pmod{\chi}$. Thus the two images are conjugate.

Finally note that since -1 commutes with the conjugation, 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. $\square$

Thanks to this lemma and Proposition 2.3.1, we may ignore the two parameters r and τ in generalized Larcher subgroups. So we define

$$H(p,N;\chi) := H(p,N,1;\chi,1),$$

where $p|N$ and $\chi|\gcd(p,N/p)$ and let

$$c(p,N;\chi) := |H(p,N;\chi)\setminus M_N|$$

be the number of orbits of $H(p,N;\chi)$ acting on M_N. In Section 2.4.4 we shall prove that

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

where $k = \operatorname{lcm}[\gcd(p^2,N)\chi, N]$, $d\,d' = k/\chi$ and ϕ is the Euler function. To do so we will need some "multiplicative decomposition" results which will be obtained in the next subsection.

2.4.3 Multiplicativity and the Action of -1_2

In [Sel77] 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's 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 $n_1,\ n_2, ..., n_r$ and writes

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

to denote that

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

Then a function $f(n_1, ..., n_r) = f(\{n\}_r)$ 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, $f_\ell(a_1, ..., a_r)$ is defined on r-tuples of non-negative integers and is such that $f_\ell(0, ..., 0) = 1$ 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 regular and irregular cusps of $H(p, N; \chi)$. We start with a technical Lemma:

Lemma 2.4.15. *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*

$p_1 \mid N_1$ and $p_2 \mid N_2$. Suppose also that $\chi \mid \gcd(N, N/p)$ with $\chi = \chi_1\chi_2$ with $\chi_1 \mid N_1$ and $\chi_2 \mid N_2$. 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 $h \in H(p_2N_1, N, N_1; \chi_2, p_1')$ then $h = \begin{pmatrix} 1+ap_2N_1 & bN \\ cN_1 & 1+dp_2N_1 \end{pmatrix}$ with $c \equiv p_1'a \pmod{\chi_2}$ and $\det(h) = 1$. As $N_1 \mid N$ we have $h \in \Gamma(N_1)$. 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 $h \in H(p, N, 1; \chi, 1)$ 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 $h \in H(p, N, 1; \chi, 1) \cap \Gamma(N_1)$ then $h \in H(p, N, 1) \cap H(N_1, N_1, N_1) = H(p_2N_1, N, N_1)$. So $h = \begin{pmatrix} 1+ap_2N_1 & bN \\ cN_1 & 1+dp_2N_1 \end{pmatrix}$. Moreover since $h \in H(p, N, 1; \chi, 1)$ 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. □

Now suppose G is a subgroup of Γ containing $\Gamma(N)$ and as above $N = N_1N_2$ with $\gcd(N_1, N_2) = 1$. 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

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

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 $G = H(p, N; \chi)$ 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 2.4.16. *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 $\mathrm{GL}(2, \mathbb{Z}/N_i\mathbb{Z})$ 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 $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \varphi_{N_1}(G_1)$ then

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

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 2.4.15

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

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 2.2.6

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

which, again by Proposition 2.2.6, is the same as $|\frac{H(p_1,N_1;\chi_1)}{\Gamma(N_1)}|$ as required.

The conjugation above induces a bijection between the orbits of the two groups acting on M_{N_1}. Moreover the conjugation commutes with the action of -1_2 and so by Theorem 2.4.13 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 2.4.17. *With notation as above, if $G = H(p, N; \chi)$ then the map $\psi_1 \times \psi_2$ is a surjection. In particular $G/\Gamma(N)$ is isomorphic to $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$.*

Proof. By Proposition 2.2.6 the order of $G/\Gamma(N)$ is $N\phi(N)/\chi\phi(p)$. But by Lemma 2.4.16 this is the order of $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$ and so $\psi_2 \times \psi_2$ is an isomorphism between $G/\Gamma(N)$ and $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$. □

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

Lemma 2.4.18. *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. $\square$

Applying this general result for the case of $A = \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ and $B = \mathrm{SL}(2, \mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/N_2\mathbb{Z})$ yields:

Corollary 2.4.19. *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 $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ and $\mathrm{SL}(2, \mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/N_2\mathbb{Z})$ 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 $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ and $\mathrm{SL}(2, \mathbb{Z}/N_1\mathbb{Z}) \times \mathrm{SL}(2, \mathbb{Z}/N_2\mathbb{Z})$. By 2.4.17 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 $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ and for convenience we use the same notation for the image of -1_2 in $\mathrm{SL}(2, \mathbb{Z}/N_1\mathbb{Z})$ and $\mathrm{SL}(2, \mathbb{Z}/N_2\mathbb{Z})$. 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 2.4.16 the actions of G_i on M_{N_i} are conjugate in $\mathrm{GL}(2, \mathbb{Z}/N_i\mathbb{Z})$ 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 actions of -1. Thus applying Lemma 2.4.18 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 2.2.9 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 2.4.19 are both trivial.

If -1_2 belongs to $H(p_1, N_1; \chi_1)$ and $H(p_1, N_1; \chi_2)$ then by Lemma 2.4.16, $G_1/\Gamma(N_1) \times G_2/\Gamma(N_2)$ contains $(-1,-1)$. So by Proposition 2.4.17 it follows that $-1_2 \in H(p, N; \chi)$. This leads to the four cases described in the following corollary:

Corollary 2.4.20. *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 cases:*

$-1_2 \in G$	$-1_2 \in H_1$	$-1_2 \in H_2$	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = 0$
$-1_2 \notin G$	$-1_2 \notin H_1$	$-1_2 \in H_2$	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = \nu'_1\nu_2$
$-1_2 \notin G$	$-1_2 \in H_1$	$-1_2 \notin H_2$	$\nu_\infty = \nu_1\nu_2$	$\nu'_\infty = \nu_1\nu'_2$
$-1_2 \notin G$	$-1_2 \notin H_1$	$-1_2 \notin H_2$	$\nu_\infty = 2\nu_1\nu_2 + \nu_1\nu'_2 + \nu'_1\nu_2$	$\nu'_\infty = \nu'_1\nu'_2$

Proof. By Corollary 2.4.19 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 2.4.2 that for a group containing -1_2 and $\Gamma(N)$ 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 all contain -1_2 we have $\nu_\infty = \nu_1\nu_2$ and

$\nu'_\infty = 0$.

Next suppose that $-1_2 \notin G$ and one of H_1 and H_2 contains -1_2; as discussed above, the other can not have -1_2. So let $-1_2 \in H_2$. Recall, again from Section 2.4.2, 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 2.4.19, $\mathcal{O}$ 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 H_1 on M_{N_1} and $\mathcal{O}_2$ is an orbit of H_2 on M_{N_2}. Therefore $\nu'_\infty = \nu'_1\nu_2$. 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 -1_2 is in G and G_1 but not in G_2 just exchanges the roles of G_1 and G_2.

Finally if none of groups contain -1_2, we have $-1_2 \cdot \mathcal{O} = \mathcal{O}$ 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. □

We will show in Proposition 2.4.28 that in the last case of Corollary 2.4.20 in practice at least one of ν'_1 or ν'_2 is zero and consequently $\nu' = 0$ in this case.

2.4.4 The Cusp Number of $H(p, N; \chi)$

The goal of this subsection is to complete the calculation of the number of inequivalent regular and irregular cusps of generalized Larcher subgroups. Based on Proposition 2.3.1 and Lemma 2.4.14 we observe that it suffices to do our computation for $H(p, N; \chi)$ where $p \mid N$ and $\chi \mid \gcd(N, N/p))$. We start by computing $c(p, N; \chi)$ which is the number of orbits of $H(p, N; \chi)$ acting on M_N. If ν_∞ and ν'_∞ are the number of inequivalent regular and irregular cusps of $H(p, N; \chi)$ then

$$c(p, N; \chi) = \begin{cases} 2\nu_\infty + \nu'_\infty & -1_2 \notin H(p, N; \chi), \\ \nu_\infty & -1_2 \in H(p, N; \chi). \end{cases}$$

Computing $c(p, N; \chi)$

A key theorem here is the Cauchy-Frobenius Formula so we recall its statement.

Theorem 2.4.21. *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 $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in M_N$ in $\varphi_N(H(p, N; \chi))$ is denoted by $H_{\binom{\alpha}{\beta}}$ then the Cauchy-Frobenius Formula implies that

$$c(p, N; \chi) = \frac{\chi\phi(p)}{N\phi(N)} \sum_{\binom{\alpha}{\beta} \in M_N} |H_{\binom{\alpha}{\beta}}|. \tag{2.1}$$

In order to compute $|H_{\binom{\alpha}{\beta}}|$ we also need the following form of the Chinese Remainder Theorem:

Lemma 2.4.22. *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 $\frac{\mathbb{Z}}{N\mathbb{Z}}$ *if and only if* $a \equiv b \pmod{(A,B)}$. *If this condition is satisfied, then the number of solutions is* $\frac{N}{[A,B]}$.[2]

Computing $|\mathbf{H}_{\binom{\alpha}{\beta}}|$

Now let $\begin{pmatrix} x^{-1} & 0 \\ y & x \end{pmatrix} \in H_{\binom{\alpha}{\beta}}$. It follows from the definition of $H(p,N;\chi)$ that

$$\begin{aligned} x &\equiv 1 \pmod{p}, && (2.2)\\ y &\equiv \frac{1-x}{p} \pmod{\chi}. && (2.3) \end{aligned}$$

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

$$\begin{aligned} x^{-1}\alpha &\equiv \alpha \pmod{N} && (2.4)\\ y\alpha + x\beta &\equiv \beta \pmod{N}. && (2.5) \end{aligned}$$

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 (2.2), (2.3), (2.4) and (2.5). We shall do this by finding an equivalent "triangular" system of congruences.

Observe first that

$$\begin{aligned} &(2.4) \iff x^{-1} \equiv 1 \pmod{\frac{N}{(N,\alpha)}} \iff x \equiv 1 \pmod{\frac{N}{(N,\alpha)}},\\ &(2.5) \iff -\beta(x-1) \equiv y\alpha \pmod{N}, \end{aligned}$$

and since $((N,\alpha),\beta) = 1$, we infer $x \equiv 1 \pmod{(N,\alpha)}$. The latter condition on x together with the congruence Equation (2.5) imply that

$$y \equiv \left(\frac{\alpha}{(N,\alpha)}\right)^{-1}(-\beta)\,\frac{x-1}{(N,\alpha)} \pmod{\frac{N}{(N,\alpha)}}. \qquad (2.6)$$

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

Now we apply Lemma 2.4.22 to the following system of equations in order to find condition(s) on x which guarantees the existence of a solution for y.

$$\begin{cases} y \equiv \frac{1-x}{p} \pmod{\chi} \\ y \equiv (\frac{\alpha}{(N,\alpha)})^{-1} (-\beta) \frac{x-1}{(N,\alpha)} \pmod{\frac{N}{(N,\alpha)}}. \end{cases} \tag{2.7}$$

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

$$(x-1)(\alpha - p\beta) \equiv 0 \pmod{(p(N,\alpha)(\frac{N}{(N,\alpha)}, \chi))}.$$

The last condition is satisfied if and only if

$$x \equiv 1 \pmod{\frac{p(N,\alpha)(\frac{N}{(N,\alpha)}, \chi)}{(\alpha - p\beta, p(N,\alpha)(\frac{N}{(N,\alpha)}, \chi))}}.$$

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

$$\begin{cases} x \equiv 1 \pmod{p}, \\ x \equiv 1 \pmod{(N,\alpha)}, \\ x \equiv 1 \pmod{\frac{N}{(N,\alpha)}}, \\ x \equiv 1 \pmod{\frac{p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)}{(\alpha-p\beta, p(N,\alpha)(\frac{N}{(N,\alpha)},\chi))}}. \end{cases} \tag{2.8}$$

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

As we have just seen, any solution for x and y to the congruences (2.2), (2.3), (2.4) and (2.5) gives rise to a solution to the congruences (2.7) and (2.8). Conversely, it is clear that any solution to (2.7) and (2.8) will satisfy (2.2),(2.3) and (2.4) and a solution to (2.7) and hence (2.6) gives a solution to (2.5). Thus the two sets of congruences are equivalent.

By applying Lemma 2.4.22, we find that the number of solutions for x of the congruences (2.8) is

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

For each given x satisfying (2.8) 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 (2.7). Thus we can count the number of solutions (2.7) using Lemma 2.4.22, which gives $\frac{N}{[\frac{N}{(N,\alpha)},\chi]}$. Therefore

$$|H_{\binom{\alpha}{\beta}}| = \frac{N}{[p,(N,\alpha),\frac{N}{(N,\alpha)},\frac{p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)}{(\alpha-p\beta,p(N,\alpha)(\frac{N}{(N,\alpha)},\chi))}]}\frac{N}{[\frac{N}{(N,\alpha)},\chi]} \tag{2.9}$$

and by substituting $|H_{\binom{\alpha}{\beta}}|$ in Formula (2.1), we get

$$\begin{aligned} c(p,N;\chi) &= \frac{\chi\phi(p)}{N\phi(N)}\sum_{\binom{\alpha}{\beta}\in M_N}\frac{N}{[p,(N,\alpha),\frac{N}{(N,\alpha)},\frac{p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)}{(\alpha-p\beta,p(N,\alpha)(\frac{N}{(N,\alpha)},\chi))}]}\frac{N}{[\frac{N}{(N,\alpha)},\chi]} \\ &= \frac{\chi\phi(p)N}{\phi(N)}\sum_{\binom{\alpha}{\beta}\in M_N}\frac{1}{[p,(N,\alpha),\frac{N}{(N,\alpha)},\frac{p(N,\alpha)(\frac{N}{(N,\alpha)},\chi)}{(\alpha-p\beta,p(N,\alpha)(\frac{N}{(N,\alpha)},\chi))}]\,[\frac{N}{(N,\alpha)},\chi]}. \end{aligned} \tag{2.10}$$

Although (2.10) is somewhat unwieldy, we shall show that it reduces to the following remarkably simple expression:

Theorem 2.4.23.

$$c(p,N;\chi) = \frac{N\chi\phi(p)}{\phi(N)}\sum_{d\mid\frac{k}{\chi}}\frac{\phi(d)\phi(d')}{[d,d',\frac{pk}{N}]}, \tag{2.11}$$

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 (2.10) and (2.11) are equal. We start with the following special case:

Lemma 2.4.24.
$$c(p,N;1) = \frac{N\phi(p)}{\phi(N)} \sum_{d|N} \frac{\phi(d)\phi(\frac{N}{d})}{[d,\frac{N}{d},p]}$$

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:

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

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

$$a \equiv 1 \pmod p,$$
$$a \equiv 1 \pmod{(N,\alpha)},$$
$$a \equiv 1 \pmod{\frac{N}{(N,\alpha)}},$$

and

$$b \equiv \left(\frac{\alpha}{(N,\alpha)}\right)^{-1}(-\beta)\,\frac{a-1}{(N,\alpha)} \pmod{\frac{N}{(N,\alpha)}}.$$

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 formula (2.10) becomes

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

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

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

which completes the proof. $\square$

Since $c(p, N; \chi)$ is a multiplicative function in the sense of Selberg [Sel77], as shown in Section 2.4.3, it will suffice to prove (2.11) 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

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

Lemma 2.4.25. *Let l be a prime number. Then*

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

Proof. Note that if $c = 0$, then the result is trivial. So we can assume below that $c \geq 1$. Since $c \leq min(a-b, b)$, we can also assume that $b \geq 1$ and $a \neq b$.

(**Case** $a \leq 2b$)

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 2.2.6 $H(l^b, l^a; l^c)$ and $H(l^{b+c}, l^a; 1)$ have the same index in Γ which implies that they are conjugate.

(**Cases** $2b + c \le a$ **and** $2b \le a \le 2b + c$)

Before proceeding we first show that

$$(\alpha - p\beta, p(N,\alpha)(\frac{N}{(N,\alpha)}, \chi)) = (p, (N,\alpha)), \tag{2.12}$$

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 (2.12) to simplify the formula of $c(l^b, l^a; l^c)$ 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:

$$c(l^b, l^a; l^c) = \frac{l^{a+c}\phi(l^b)}{\phi(l^a)} \sum_{\binom{\alpha}{\beta} \in M_{l^a}} \frac{1}{\left[l^b, (l^a,\alpha), \frac{l^a}{(l^a,\alpha)}, \frac{l^b(l^a,\alpha)(\frac{l^a}{(l^a,\alpha)}, l^c)}{(\alpha - l^b\beta, l^b(l^a,\alpha)(\frac{l^a}{(l^a,\alpha)}, l^c))}\right] \left[\frac{l^a}{(l^a,\alpha)}, l^c\right]}$$

$$= \frac{l^{a+c}\phi(l^b)}{\phi(l^a)} \left\{ \sum_{\substack{m=0 \\ m \neq b}}^{a} \frac{\phi(l^m)\phi(l^{a-m}) l^{a-m}}{\left[l^b, l^m, l^{a-m}, \frac{l^{b+m}(l^{a-m}, l^c)}{(l^b, l^m)}\right] \left[l^{a-m}, l^c\right]} \right.$$

$$\left. + \sum_{\substack{(u,l)=(\beta,l)=1 \\ 0 < u \le l^{a-b}}} \frac{1}{\left[l^b, l^{a-m}, \frac{l^{2b}(l^{a-b}, l^c)}{l^b(u - \beta, l^b(l^{a-b}, l^c))}\right] \left[l^{a-b}, l^c\right]} \right\}$$

It is convenient to split these two sums further 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

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

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

and S_2 can be written as

$$S_2 = \sum_{\substack{(u,l)=(\beta,l)=1 \\ 0<u\leq l^{a-b}}} \frac{1}{[l^{a-b}, l^b, \frac{l^{2b}(l^{a-b},l^c)}{l^b(u-\beta,l^b(l^{a-b},l^c))}][l^{a-b}, l^c]}$$
$$= \frac{(\phi(l^a) - l^{a-1})\phi(l^{a-b})}{[l^{a-b}, l^b(l^{a-b}, l^c)][l^{a-b}, l^c]} + \sum_{m=1}^{b+c} \frac{\phi(l^{a-m})\phi(l^{a-b})}{[l^{a-b}, l^b, \frac{l^{b+c}}{l^m}][l^{a-b}, l^c]} + \frac{l^{a-b-c-1}\phi(l^{a-b})}{[l^{a-b}, l^b][l^{a-b}, l^c]}.$$

If $(u-\beta, l^a) = l^k$, then these three terms correspond to $k=0$, $1 \leq k \leq b+c$ and $b+c < k \leq a$, 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

$$S_1 + S_2 + S_3 = \sum_{m=0}^{a-c} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}. \tag{2.13}$$

It is not difficult to see

$$S_1 = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{a-m})}{l^{a-m}} = \sum_{m=0}^{b-1} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}, \tag{2.14}$$

and also

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

The first sum can be rewritten as

$$\sum_{m=b+1}^{a-c-1} \frac{\phi(l^m)\phi(l^{a-c-m})}{[l^m, l^{a-c-m}, l^b]}, \tag{2.15}$$

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

$$\frac{1}{l^c}(1-\frac{1}{l}) \sum_{m=a-c}^{a-1} (\phi(l^{a-m})) + \frac{1}{l^c}(1-\frac{1}{l}) = 1 - \frac{1}{l}. \tag{2.16}$$

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

$$\begin{aligned} S_2 &= \frac{\phi(l^{a-b})}{l^{a-b}} \left\{ \frac{l^a - 2l^{a-1}}{l^{a-b}} + \frac{1}{l^{a-b}} \sum_{m=1}^{b+c} \phi(l^{a-m}) + \frac{1}{l^{c+1}} \right\} \\ &= (1 - \frac{1}{l})(l^b - l^{b-1}). \end{aligned} \tag{2.17}$$

The statement (2.13) follows from (2.14), (2.15), (2.16) and (2.17).

(**Case** $2b < a < 2b+c$)

In this case we want to show

$$S_1 + S_2 + S_3 = \sum_{m=0}^{2b} \frac{\phi(l^m)\phi(l^{2b-m})}{[l^m, l^{2b-m}, l^{3b+c-a}]}. \tag{2.18}$$

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

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

We can split S_3 into the following sums

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

which 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:

$$\begin{aligned} S_2 &= \frac{\phi(l^{a-b})}{l^{a-b}} \left\{ \frac{l^a - 2l^{a-1}}{l^{b+c}} + \sum_{m=1}^{2b+c-a} \frac{\phi(l^{a-m})}{l^{b+c-m}} + \sum_{2b+c-a+1}^{b+c} \frac{\phi(l^{a-m})}{l^{a-b}} + \frac{1}{l^{c=1}} \right\} \\ &= (1 - \frac{1}{l}) \left\{ l^{a-b-c} - 2l^{a-b-c-1} + (2b+c-a)(1 - \frac{1}{l})l^{a-b-c} + l^{a-b-c-1} \right\} \\ &= (1 - \frac{1}{l}) \left\{ (2b+c-a+1)\phi(l^{a-b-c}) \right\} \end{aligned} \tag{2.19}$$

It is easy to verify that the right hand side of (2.18) is

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

This completes the proof. □

Lemma 2.4.24 and Lemma 2.4.25 show that Theorem 2.4.23 holds for the prime power case and so the general case of Theorem 2.4.23 now follows from the multiplicativity of $c(p, N; \chi)$.

2.4.5 The Number of Inequivalent Regular and Irregular Cusps

By Theorem 2.4.13, if $-1_2 \in H(p, N; \chi)$ then $\nu_\infty = c(p, N; \chi)$ and $\nu'_\infty = 0$ and so by Theorem 2.4.23 and Proposition 2.2.9, the first case of the formula for $(\nu_\infty, \nu'_\infty)$ in Theorem 2.5.1 is proven. In this section we give the proof of the remaining cases of Theorem 2.5.1 giving the number of inequivalent regular and irregular cusps where $H(p, N; \chi)$ doesn't contain -1_2. We start with the following lemma

Lemma 2.4.26. *If p has an odd divisor greater or equal to 3 and $-1_2 \notin H(p, N; \chi)$ 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 2.4.13 the action of $H(p, N; \chi)$ on M_N has an irregular orbit. Let $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in M_N$ be an element of this irregular orbit. Since the action of -1_2 maps this orbit to itself it follows that there is an element $\begin{pmatrix} 1+px & Nz \\ y & 1+pt \end{pmatrix} \in H(p,N;\chi)$ 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 congruence equations:

$$\begin{cases} (1+px)\alpha \equiv -\alpha & \pmod{N} \\ y\alpha + (1+pt)\beta \equiv -\beta & \pmod{N}. \end{cases} \tag{2.20}$$

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

$$2 \equiv 0 \pmod{(\frac{N}{(N,\alpha)}, p)}. \tag{2.21}$$

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 number. The second part of the Lemma now follows from Theorem 2.4.13 since the preimage of a regular cusp consists of a pair of (distinct) regular orbits on M_N. □

Note that the previous lemma proves the final case of Theorem 2.5.1 except the case when p is a power of 2 greater than or equal to 4.

Lemma 2.4.27. *Suppose $N = 2^a$ for some $a \geq 1$ and $-1_2 \notin H(p,N;\chi)$. Let $c = c(p,N;\chi)$ then:*

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

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

And 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 $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in M_{2^a}$ 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 $\begin{pmatrix} 1+2^b x & 2^a z \\ y & 1+2^b t \end{pmatrix} \in H(2^b, 2^a; \chi)$. So

$$\begin{cases} (1+2^b x)\alpha \equiv -\alpha \pmod{2^a} \\ y\alpha + (1+2^b t)\beta \equiv -\beta \pmod{2^a}. \end{cases} \tag{2.22}$$

An argument similar to the one we used to conclude (2.21) implies that

$$2 \equiv 0 \pmod{(\frac{2^a}{(2^a, \alpha)}, 2^b)}. \tag{2.23}$$

We now consider the following cases:

Case I: $b \geq 2$. Congruence (2.23) 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

$$2^b t\beta \equiv -2\beta \pmod{2^{a-1}}. \tag{2.24}$$

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 irregular and two regular cusps. As $c(4, 4, 1) = 5$ the result follows in this case.

Subcase: $b > 2$. In this case (2.24) contradicts $(2, \beta) = 1$, thus there is no irregular cusp in this case and the number of 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 2.4.25. and so it has the same 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 $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ is an element of an irregular orbit of $H(2, 2^a; 2)$ if and only if there exist x, y and t satisfying

$$(1+2x)\alpha \equiv -\alpha \pmod{2^a} \tag{2.25}$$

$$y\alpha + (1+2t)\beta \equiv -\beta \pmod{2^a} \tag{2.26}$$

$$x \equiv y \pmod{2} \tag{2.27}$$

$$(1+2x)(1+2t) \equiv 1 \pmod{2^a}. \tag{2.28}$$

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 $a \geq m \geq \frac{a-1}{2}$, and β is odd. First we prove that α must be even. If not, by Congruence (2.25), $x\alpha \equiv -\alpha \pmod{2^{a-1}}$ and hence x is odd and so is y. But Congruence (2.26) 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 there exist no solution for the system of congruence equations above if $m \leq \frac{a-1}{2}$. By substituting $\alpha = u2^m$ where $a \geq m$ in (2.25) we have $2x \equiv -2 \pmod{2^{a-m}}$. Then (2.28) gives $2t \equiv -2 \pmod{2^{a-m}}$. These combined with (2.26) 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 both u and y are odd, the congruence $yu2^m \equiv 0 \pmod{2^{a-m}}$ then yields a contradiction and so $m > (a-1)/2$.

Any $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in M_{2^a}$, 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

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

is a solution to Congruences (2.25), (2.26), (2.27) and (2.28).

By the Cauchy-Frobenius Formula and Theorem 2.4.13 the number of irregular orbits and the number of inequivalent irregular cusps is given by

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

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 (2.9) gives

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

These simplify to

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

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

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 2.4.23 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 2.4.9 and Theorem 2.4.11 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 2.4.20 give the following proposition to obtain the number of inequivalent regular and irregular cusps for $H(p, N; \chi)$ in the case $-1_2 \notin H(p, N; \chi)$.

Proposition 2.4.28. *Let $N = 2^a N_1$, $p = 2^b$ and $\chi = 2^c$ where N_1 is an odd number. Suppose $-1_2 \notin H(p, N; \chi)$. Then there are no irregular cusps for $H(p, N; \chi)$, and therefore $\nu_\infty = \dfrac{c(p, N; \chi)}{2}$, except in the following cases.*
If $p = 2$ then $\chi = 2$ and

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

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

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

Proof. If $H(p, N; \chi)$ does not contain -1_2 then by Proposition 2.2.9 $b > 0$ and if $b = 1$ then $c > 0$. So again by Proposition 2.2.9, -1_2 is in $H(1, N_1; \chi)$ but not in $H(2^b, 2^a, 2^c)$. Thus by Corollary 2.4.20 the numbers of 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 of $H(1, N_1; 1)$ and ν_2 and ν'_2 are the numbers of regular and irregular cusps of $H(2^b, 2^a, 2^c)$. Except for the four cases listed in Lemma 2.4.27, $H(2^b, 2^a; 2^c)$ 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 2.4.27 and multiplicativity of $c(p, N; \chi)$. □

By Lemma 2.4.26 the cases in Proposition 2.4.28 are the only cases for which $-1_2 \notin H(p, N; \chi)$ and $H(p, N; \chi)$ has irregular cusps. This accounts for all the cases of Theorem 2.5.1 and so completes the proof of this Theorem.

2.5 The Signature Formulae

In this short section we summarize the results of previous sections. But first we recall some notations which will be needed in the statement of Theorem 2.5.1.

– For integers a and b we write $a \,||\, b$ if $a|b$ and $\gcd(a, b/a) = 1$.

– 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 $\Gamma_0(N)$.

– For a positive integer N set

$$\phi(N) = N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

and

$$\psi(N) = N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 + \frac{1}{p}\right).$$

Let p, N and χ be positive integers such that $p \mid N$ and $\chi \mid \gcd(p, N/p)$ and let

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

where $k = \operatorname{lcm}[\gcd(p^2, N)\chi, N]$, $d\,d' = k/\chi$.

We can put our results namely Corollary 2.2.10, Theorem 2.3.2 and Proposition 2.4.28 in one theorem as follows:

Theorem 2.5.1. *Suppose p, N and χ are positive integers such that $p \mid N$, $\chi \mid \gcd(p, N/p)$ and $c = c(p, N; \chi)$. Then the signature $(\mu, \nu_2, \nu_3, \nu_\infty, \nu'_\infty)$ of $H(p, N; \chi)$ is given by:*

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

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

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

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

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

Chapter 3

Fourier Coefficients of Modular Forms

3.1 Prologue

Suppose Γ is a genus-zero subgroup of $\mathrm{SL}(2,\mathbb{R})$ commensurable with $\mathrm{SL}(2,\mathbb{Z})$. Let

$$f = q^r + \sum_{n=1}^{\infty} a_n q^{r+n},$$

be a meromorphic modular form of integer weight k on Γ, where q is a suitable local parameter at the cusp ∞.

When Γ is the full modular group $\mathrm{SL}(2,\mathbb{Z})$, the problem of finding universal recursive relation satisfied by the Fourier coefficients of f was investigated by Bruinier, Kohnen and Ono in [BKO04]. Shortly after this work, Ahlgren in [Ah02] and Atkinson in [At05] obtained similar results for the cases $\Gamma_0(p)$ ($p = 2, 3, 5, 7, 13$) and $\Gamma_0(4)$ respectively. S. Y. Choi in [C.S.06] considered the case $\Gamma_0(p)^+$, which is the group $\Gamma_0(p)$ extended by the Fricke involution. These groups are genus-zero for $p \in \{2,3,5,7,11,13,17,19,23,29,31,41,47,59,71\}$. She also gave recursive relations expressing the coefficients of a Hauptmodul j_1 of Γ_1 by using those of the normalized Hauptmodul j_2 of Γ_2, where Γ_1 is a Fuchsian group of the first kind of genus-zero and Γ_2 is a finite index genus-zero subgroup of Γ_1. In related work, D. Choi [C.D.06] considered the case of forms on $\Gamma_0(N)$ for which N is square-free, but not necessarily genus zero, in terms of certain "(ℓ, N)-type" sequences of modular functions.

The strategy of these papers, following that of [BKO04], has been to express $\frac{\theta f}{f}$ in terms of a modular form f_θ of weight 2 and terms involving the Eisenstein series E_2, where θ is the Ramanujan θ operator. Then to compute $\frac{1}{2\pi i}\int f_\theta(z)F_n(z)dz$, along the boundary of a fundamental domain of the group in question, where F_n, $n = 1, 2, 3, \ldots$ are a certain polynomials in the Hauptmodul of Γ known as the Faber polynomials.

The motivation for the present chapter is to generalize this work, using a somewhat different method, so as to find universal recursive formulae satisfied by the Fourier coefficients of any meromorphic modular form on any genus-zero subgroup Γ of $\mathrm{SL}(2, \mathbb{R})$ commensurable with $\mathrm{SL}(2, \mathbb{Z})$. Our results hold for both even and odd level forms. The case where the cusp at ∞ is regular and the case where it is irregular are both treated. The results can also be applied to congruence and non-congruence subgroups. In Section 3.2 first we find the recurrences for genus-zero subgroups of $\mathrm{SL}(2, \mathbb{Z})$ of finite index and then by applying the same method, the general case will be studied.

Let N be a square-free integer and let $\Gamma_0(N)^+$ denote the group $\Gamma_0(N)$ extended by all of its Atkin-Lehner elements. To be more specific

$$\Gamma_0(N)^+ = \left\{ e^{\frac{-1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R}) \Big| a, b, c, d, e \in \mathbb{Z},\ e|N, e|a, e|d, N|c,\ ad - bc = e \right\}.$$

We will call these groups *Helling groups*. By a theorem of Helling [He66], any subgroup of $\mathrm{SL}(2, \mathbb{R})$ which is commensurable with $\mathrm{SL}(2, \mathbb{Z})$ is conjugate to a subgroup of a

Helling group. Since the Helling groups act transitively on cusps, we can also assume that the cusp at which we are computing coefficients is ∞.

The recurrence relations we find have as input a square-free integer N, specifying the Helling group of which Γ is a subgroup. Also the ramification locus and ramification orders of a normalized Hauptmodul ϕ_Γ of Γ are required. Finally, the weight and divisor of f and the values of ϕ_Γ at the points at which the divisor of f is supported are needed. Given these data, the recurrence relations, as found below in Theorems 3.3.6 and 3.3.7, have the same form for all Γ and f, and in this sense are universal.

Our method of proof is somewhat different in that we start with a suitable power of f divided by a certain power of a known cusp form on Γ, such that we obtain a weight zero meromorphic Γ-invariant function. Then we express this quotient as a rational function of a normalized Hauptmodul ϕ_Γ of Γ. Taking the logarithmic derivative of the resulting identity then allows us to derive the desired recursive formulae. As a corollary to our main theorem, we give an explicit formula for the Fourier coefficients of ϕ_Γ. We proceed by some preliminary considerations.

3.1.1 Preliminaries

Let Γ be a finite index subgroup of $\Gamma_0(N)^+$, for some square-free N. $\Gamma_0(N)^+$ as well as Γ act on $\mathfrak{H}^*$ by fractional linear transformations, where $\mathfrak{H}^*$ is the union of the upper half plane $\mathfrak{H}$ with the projective rational line $\mathbb{Q}^*$. Assume that $s_0 = \infty, s_1, \cdots, s_t \in \mathbb{Q}^*$ are a set of representatives of $\Gamma \setminus \mathbb{Q}^*$.

Since $\Gamma_0(N)^+$ acts transitively on $\mathbb{Q}^*$ (see [He70]), there is only one equivalence class of cusps and this class contains ∞. The stabilizer subgroup of ∞ in $\Gamma_0(N)^+$ is

$$\left\{\pm\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}.$$

Now we fix a cusp s of Γ and then take an element $\gamma \in \Gamma_0(N)^+$ such that $\gamma(s) = \infty$. We have

$$\pm\gamma\Gamma_s\gamma^{-1} = \left\{\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z}\right\}, \tag{3.1}$$

where h is a positive integer and $\Gamma_s := \{\alpha \in \Gamma : \alpha(s) = s\}$ is the stabilizer subgroup of s in Γ. If $-\mathbf{1}_2 \notin \Gamma$, then $\gamma\Gamma_s\gamma^{-1}$ is generated either by $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ or by $\begin{pmatrix} -1 & h \\ 0 & -1 \end{pmatrix}$. The cusp s is called *regular* or *irregular* of width h accordingly. By the definition, if $-\mathbf{1}_2 \in \Gamma$, then all the cusps of Γ are regular.

For a subgroup Γ of $\mathrm{SL}(2,\mathbb{R})$, we define $\overline{\Gamma}$ to be the image of Γ in $\mathrm{PSL}(2,\mathbb{R}) = \mathrm{SL}(2,\mathbb{R})/\{\pm 1\}$. If $h_0, h_1, \cdots, h_t$ are the cusp widths of the cusps $\infty, s_1, \cdots, s_t$ of Γ, then the following relation holds (cf. [J86]),

$$\sum_{i=0}^{t} h_i = [\overline{\Gamma_0(N)^+} : \overline{\Gamma}]. \tag{3.2}$$

This is called the *cusp-split equation* of Γ.

A complex valued function f on the upper half plane $\mathfrak{H}$ is said to be a meromorphic (resp. holomorphic) modular form of weight k with respect to Γ if

- f is meromorphic (resp. holomorphic) on $\mathfrak{H}$;
- $f|[\rho]_k = f$, for all $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

  where $f|[\rho]_k(z) := (cz+d)^{-k} f(\rho(z))$;
- f is meromorphic (resp. holomorphic) at every cusp s of Γ.

This last condition means that

$$f|[\gamma^{-1}]_k(z) = \begin{cases} \Psi(e^{\pi i z/h}) & \text{if } k \text{ is odd and } s \text{ is irregular,} \\ \Phi(e^{2\pi i z/h}) & \text{otherwise,} \end{cases} \tag{3.3}$$

where Φ and Ψ are meromorphic (resp. holomorphic) functions at zero, Ψ is an odd function, and h and γ are as in Equation (3.1). For more details, see Definition 2.1 of [Sh71].

We shall denote by $A_k(\Gamma)$ (resp. $G_k(\Gamma)$) the space of meromorphic modular forms (resp. holomorphic modular forms) of weight k for Γ. Moreover, if for each cusp of Γ, the functions Φ (or Ψ) in (3.3) vanishes at zero, then f is called a cusp form on Γ, and the set of all such cusp forms will be denoted by $S_k(\Gamma)$.

Let us recall the definition of the order of a meromorphic function f at a point $\tau \in \Gamma \setminus \mathfrak{H}^*$. First, for τ corresponding to a point $z_0 \in \mathfrak{H}$, we set $e_\tau = |\overline{\Gamma}_\tau|$, where $\overline{\Gamma}_\tau$ is the stabilizer subgroup of τ. One knows that $|e_\tau| < \infty$. Then $\mathrm{ord}_\tau f$ is defined (see 2.4 of [Sh71]) as

$$\mathrm{ord}_\tau f := e_\tau^{-1}\mathrm{ord}_{(z-z_0)} f.$$

If τ corresponds to a cusp s of Γ, with cusp width h, then

$$\mathrm{ord}_\tau f := \begin{cases} (\mathrm{ord}_{e^{\pi i z/h}}\Psi)/2 & \text{if } k \text{ is odd and s is irregular,} \\ \mathrm{ord}_{e^{2\pi i z/h}}\Phi & \text{otherwise,} \end{cases}$$

where Φ and Ψ are as in (3.3). We can associate with each $f \in A_k(\Gamma)$ the *divisor* of f defined as

$$\mathrm{div}(f) := \sum_{\tau \in \Gamma\setminus\mathfrak{H}^*} \mathrm{ord}_\tau f[\tau]. \tag{3.4}$$

From now on, we suppose that Γ is of *genus-zero* by which we mean that the compact Riemann surface $\Gamma \setminus \mathfrak{H}^*$ is of genus zero. Any generator ϕ_Γ of the function field of this Riemann surface is called a *Hauptmodul* of Γ. When no confusion will arise, we write ϕ rather than ϕ_Γ. If we require ϕ to have a simple pole at the cusp infinity, then after normalization, ϕ has a q-expansion of the form

$$\phi(q) = \frac{1}{q} + \sum_{n\geq 0} c_n q^n, \tag{3.5}$$

where $q = e^{\frac{2\pi i z}{h_0}}$.

Remark 3.1.1. In light of (3.3), any modular form $f(z)$ of weight k may also be viewed as a function of q, namely $f(z) = \Phi(q)$ (or $f(z) = \Psi(q^{1/2})$). Therefore, by abuse of notation, we allow ourselves to write $f(q)$ viewing f as a function of q. The same remark also applies to any reference to derivatives. In other words, $f'(q) = \frac{df}{dq}$ should be understood as $\frac{h_0}{2\pi i q}\frac{df}{dz}$. So, from now on we suppress Φ and Ψ from the notation.

Remark 3.1.2. Note that the derivative of ϕ is a meromorphic modular form of divisor

$$D = \sum_{\tau\in\Gamma\backslash\mathfrak{H}} (1 - e_\tau^{-1})[\tau] + \sum_{i=1}^{t} [s_i] - [\infty].$$

The divisor of a meromorphic modular form of weight k, when k is even, differs from $(k/2)D$ by an integral divisor of degree zero and thus all such divisors are known explicitly.

3.1.2 Faber Polynomials

Let

$$\varphi(q) = \frac{1}{q} + \sum_{n\geq 0} a_n(\varphi) q^n$$

be a formal power series in q. For $n \geq 1$, define the nth *Faber polynomial* to be the unique monic polynomial F_n of degree n which satisfies the following relation

$$F_n(\varphi) = \frac{1}{q^n} + \sum_{m\geq 1}^{\infty} F_{n,m} q^m.$$

The coefficients $F_{n,m}$ depend on the coefficients $a_n(\varphi)$. For later computations, it is also convenient to set $F_0 = 1$. Following this convention (cf. relation 14 on page 35 of [Su98]), one may verify that the Faber polynomials are given by the formal generating series

$$\frac{q\varphi'(q)}{w - \varphi(q)} = \sum_{n=0}^{\infty} F_n(w) q^n, \tag{3.6}$$

where $\varphi'(q)$ is the derivative of φ with respect to q. In fact, Equality (3.6) turns out to be an equality between holomorphic functions if φ is a holomorphic function on a bounded simply connected domain. (For the details, see Theorem 1, on page 51 of [Su98]). Using (3.6) one can show that the Faber polynomials F_n, for $n \geq 0$, also satisfy the following recurrence relation

$$F_{n+1}(w) = wF_n(w) - \sum_{k=0}^{n} a_{n-k}(\varphi) F_k(w) - n a_n(\varphi). \tag{3.7}$$

It is also possible to give an explicit formula for F_n in terms of the coefficients $a_0(\varphi), a_1(\varphi), \ldots, a_{n-1}(\varphi)$, $n \geq 1$. This can be done by invoking the following lemma whose proof has been inspired by Relation (2.11) on page 23 and Example 20 on page 33 of [Md95].

Lemma 3.1.3. *Let* $\Lambda = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3, \ldots]$, *and set* $\alpha_0 = 1$. *Now suppose* $S_i \in \Lambda$ *(*$i = 1, 2, 3, \ldots$*) are such that*

$$n\alpha_n + \sum_{j=1}^{n} S_j \alpha_{n-j} = 0 \quad (\text{for all } n \geq 1). \tag{3.8}$$

Then

$$S_n = S(n; \alpha_1, \ldots, \alpha_n).$$

where

$$S(l;\alpha_1,\ldots,\alpha_n) := \\ l \sum_{\substack{m_1,\ldots,m_n\geq 0\\ m_1+2m_2+\cdots+nm_n=l}} (-1)^{m_1+\cdots+m_n}\frac{(m_1+\cdots+m_n-1)!}{m_1!\cdots m_n!}\alpha_1^{m_1}\cdots\alpha_n^{m_n}.$$

Proof. In $\Lambda[[t]]$, let $H(t)=\sum_{n\geq 0}\alpha_n t^n$ and $P(t)=\sum_{n\geq 1} S_n t^{n-1}$. Then

$$-H(t)P(t)=H'(t).$$

This is true since

$$\begin{aligned} H'(t) &= \sum_{n\geq 1} n\alpha_n t^{n-1} \\ &= \sum_{n\geq 1}\left(\sum_{j=1}^{n} -S_j\alpha_{n-j}\right)t^{n-1} \\ &= -\sum_{n\geq 1} S_n t^{n-1}\sum_{n\geq 0}\alpha_n t^n \\ &= -P(t)H(t). \end{aligned}$$

For any element $z\in t\Lambda[[t]]$, define $L(z)=z+\frac{z^2}{2}+\frac{z^3}{3}+\cdots$. One has the identity $(1+z)L'(-z)=-z'$. Taking $z=H^+(t)=\sum_{n\geq 1}\alpha_n t^n$ yields $H(t)(H^+(t)-\frac{1}{2}H^+(t)^2+\frac{1}{3}H^+(t)^3-\cdots)'=-P(t)H(t)$. Thus, since $H(t)$ is not a zero divisor in $\Lambda[[t]]$,

$$-P(t)=(H^+(t)-\frac{1}{2}H^+(t)^2+\frac{1}{3}H^+(t)^3-\cdots)'. \tag{3.9}$$

To compute the coefficient of nt^{n-1} in (3.9) we argue as follows. For any choice of $m_1,\ldots,m_n\geq 0$ satisfying $m_1+\cdots+nm_n=n$, write $k=m_1+m_2+\cdots+m_n$ and note that $1\leq k\leq n$. Such choice uniquely gives rise to the term

$$\frac{(-1)^{k-1}k!}{km_1!\cdots m_n!}(\alpha_1 t)^{m_1}(\alpha_2 t^2)^{m_2}\cdots(\alpha_n t^n)^{m_n} = \\ (-1)^{k-1}\frac{(m_1+\cdots+m_n-1)!}{m_1!\cdots m_n!}\alpha_1^{m_1}\cdots\alpha_n^{m_n}t^n.$$

obtained by the generalized binomial theorem applied to the k-th term appearing in $H^+(t) - \frac{1}{2}H^+(t)^2 + \frac{1}{3}H^+(t)^3 - \cdots$. Now taking the sum over all possible choices gives the desired result. □

Combining Lemma 3.1.3 with (3.7) yields

Corollary 3.1.4. *Let F_n be the nth Faber polynomial corresponding to*

$$\varphi(q) = \frac{1}{q} + \sum_{n\geq 0} a_n(\varphi)q^n,$$

then

$$\begin{aligned} F_n(w) &= S(n; a_0(\varphi) - w, a_1(\varphi), \cdots, a_{n-1}(\varphi)) \\ &= n \sum_{m_1+2m_2+\cdots+nm_n=n} (-1)^{m_1+m_2+\cdots+m_n} \frac{(m_1 + \cdots + m_n - 1)!}{m_1! \cdots m_n!} \times \\ &\times (a_0(\varphi) - w)^{m_1} a_1(\varphi)^{m_2} \cdots a_{n-1}(\varphi)^{m_n}. \end{aligned} \tag{3.10}$$

Using a different method Bouali obtains the same recurrences for the Faber polynomials in [B.A06].

3.2 The Case of Genus-Zero Subgroups of $\mathrm{SL}(2,\mathbb{Z})$

3.2.1 Initial Lemmas

In this section, we assume that Γ is a finite index genus-zero subgroup of $\Gamma_0(1)^+ = \mathrm{SL}(2,\mathbb{Z})$ and retain the notation from the previous section. For any meromorphic modular form

$$f(z) = q^r + \sum_{n=1}^{\infty} a_n q^{r+n} \in A_k(\Gamma) \tag{3.11}$$

of weight k for Γ, where $q = e^{\frac{2\pi i z}{h_0}}$, we wish to find a recursive formula satisfied by the Fourier coefficients a_j, $j = 1, 2, \cdots$ of f. Let us remark that if k is odd and the cusp

∞ is irregular, then by the definition as in (3.3), r is equal to $r'/2$ for some odd integer r'. Otherwise r is an integer.

Since the discriminant function

$$\Delta := q^{h_0} \prod_{n=1}^{\infty} (1 - q^{h_0 n})^{24} \in S_{12}(\mathrm{SL}(2, \mathbb{Z}))$$

may be viewed as a cusp form on the subgroup Γ, it follows that

$$\Omega := \frac{f^{\frac{12}{(k,12)}}}{\Delta^{\frac{k}{(k,12)}}}$$

is a meromorphic modular form of weight zero for Γ or equivalently a meromorphic function on $\Gamma \setminus \mathfrak{H}^*$. In particular, Ω can be written as a rational function of ϕ. More precisely we have the following lemma:

Lemma 3.2.1. *Let Γ be a finite index genus-zero subgroup of* SL(2, $\mathbb{Z}$), *and let $s_0 = \infty, s_1, \dots, s_t$ be a set of representatives of inequivalent cusps of Γ with the cusp widths $h_0, h_1, \dots, h_t$ respectively. With f and Ω as above and for some non-zero constant λ, we have*

$$\Omega(z) = \lambda \prod_{i=1}^{t} (\phi(z) - \phi(s_i))^{\frac{12}{(k,12)} \mathrm{ord}_{s_i} f - \frac{h_i k}{(k,12)}} \prod_{\tau \in \Gamma \setminus \mathfrak{H}} (\phi(z) - \phi(\tau))^{\frac{12}{(k,12)} e_\tau \mathrm{ord}_\tau f}. \qquad (3.12)$$

Proof. To verify this equality, it suffices to show that for every point τ in $\Gamma \setminus \mathfrak{H}^*$, both sides have the same order at τ, since every meromorphic function on a compact Riemann surface is uniquely determined, up to a constant, by its divisor. If $\tau \in \Gamma \setminus \mathfrak{H}$, this is immediate since the everywhere holomorphic function Δ never vanishes on $\mathfrak{H}$. Next, suppose $\tau = s$ is a cusp of Γ with the cusp width h. The order of Ω at s is

$$\mathrm{ord}_s \Omega = \frac{12}{(k, 12)} \mathrm{ord}_s f - \frac{hk}{(k, 12)}.$$

That this is equal to the order of the right hand side of (3.12) is immediate if $s \neq \infty$, since ϕ is bijective. In order to prove the equality of orders at $s = \infty$, we shall use the *Valence Formula*

$$\sum_{\tau\in\Gamma\backslash\mathfrak{H}^*} e_\tau \mathrm{ord}_\tau f = \frac{k}{12}[\mathrm{PSL}(2,\mathbb{Z}):\bar{\Gamma}]. \tag{3.13}$$

This formula follows from Proposition 2.16 and Theorem 2.20 of [Sh71]. The Valence Formula together with Identity (3.2) now imply that

$$\frac{12}{(k,12)}\sum_{\tau\in\Gamma\backslash\mathfrak{H}^*} e_\tau \mathrm{ord}_\tau f = \sum_{i=0}^{t}\frac{kh_i}{(k,12)}.$$

Therefore,

$$\begin{aligned}\mathrm{ord}_\infty\Omega &= \frac{12}{(k,12)}\mathrm{ord}_\infty f - \frac{kh_0}{(k,12)}\\ &= -\frac{12}{(k,12)}\sum_{\tau\in\Gamma\backslash\mathfrak{H}\cup\{s_1,\cdots,s_t\}} e_\tau \mathrm{ord}_\tau f + \sum_{i=1}^{t}\frac{kh_i}{(k,12)},\end{aligned}$$

which gives the desired result. □

Lemma 3.2.2. *Let the hypotheses be as in the previous lemma. Then, the coefficients of f satisfy the following recursive relation*

$$a_n = \frac{-\beta_1 a_{n-1} - \beta_2 a_{n-2} - \cdots - \beta_n}{n}, \tag{3.14}$$

where, for $n \geq 1$, β_n is defined by the formula

$$\beta_n := 2kh_0\sigma(\frac{n}{h_0}) + \sum_{i=1}^{t}\left(\mathrm{ord}_{s_i} f - \frac{kh_i}{12}\right)F_n(\phi(s_i)) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\phi(\tau)). \tag{3.15}$$

where $\sigma(n) = \sum_{\delta|n}\delta$ and $\sigma(\frac{n}{h_0}) = 0$, if $h_0 \nmid n$.

Proof. First we take the logarithmic derivative (with respect to z) of both sides of (3.12) and obtain

$$\begin{aligned}\frac{12}{(k,12)}\frac{f'(z)}{f(z)} &= \frac{k}{(k,12)}\frac{\Delta'(z)}{\Delta(z)} + \sum_{i=1}^{t}(\frac{12}{(k,12)}\mathrm{ord}_{s_i} f - \frac{kh_i}{(k,12)})\frac{\phi'(z)}{\phi(z)-\phi(s_i)}\\ &+ \frac{12}{(k,12)}\sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f\frac{\phi'(z)}{\phi(z)-\phi(\tau)},\end{aligned}$$

or, equivalently,

$$\begin{aligned}\frac{f'(z)}{f(z)} &= \frac{k}{12}2\pi i E_2(z) + \sum_{i=1}^{t}(\mathrm{ord}_{s_i} f - \frac{kh_i}{12})\frac{\phi'(z)}{\phi(z)-\phi(s_i)} \\ &+ \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f \frac{\phi'(z)}{\phi(z)-\phi(\tau)},\end{aligned} \tag{3.16}$$

where $E_2(z) = 1 - 24\sum_{n=1}^{\infty}\sigma(n)e^{2\pi i z n}$ is the non-modular Eisenstein series of weight two on SL(2, $\mathbb{Z}$). For a proof of the identity $\frac{\Delta'(z)}{\Delta(z)} = 2\pi i E_2(z)$, see Proposition 14 on page 121 of [K97].

Using the convention adopted in Remark 3.1.1, we may rewrite Identity (3.16) as

$$\begin{aligned}\frac{2\pi i}{h_0}\frac{qf'(q)}{f(q)} &= \frac{2\pi i k}{12}E_2(q^{h_0}) + \sum_{i=1}^{t}(\mathrm{ord}_{s_i} f - \frac{kh_i}{12})\frac{2\pi i}{h_0}\frac{q\phi'(q)}{\phi(q)-\phi(s_i)} \\ &+ \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f \frac{2\pi i}{h_0}\frac{q\phi'(q)}{\phi(q)-\phi(\tau)}.\end{aligned}$$

Now applying (3.6) yields

$$\begin{aligned}\frac{qf'(q)}{f(q)} &= \frac{kh_0}{12}E_2(q^{h_0}) - \sum_{i=1}^{t}\left((\mathrm{ord}_{s_i} f - \frac{kh_i}{12})\sum_{n=0}^{\infty}F_n(\phi(s_i))q^n\right) \\ &- \sum_{\tau\in\Gamma\backslash\mathfrak{H}}\left(e_\tau \mathrm{ord}_\tau f \sum_{n=0}^{\infty}F_n(\phi(\tau))q^n\right) \\ &= \frac{kh_0}{12} - \frac{kh_0}{12} + r - \sum_{n=1}^{\infty}\beta_n q^n \\ &= r - \sum_{n=1}^{\infty}\beta_n q^n,\end{aligned} \tag{3.17}$$

where β_n is defined as in (3.15).

We are now in a position to prove the recursive relation (3.14) satisfied by the Fourier coefficients of f. Substituting the q-expansion of f given in (3.11) in Equation (3.17) yields

$$r + \sum_{n=1}^{\infty}(r+n)a_n q^n = (1 + \sum_{n=1}^{\infty}a_n q^n)(r - \sum_{n=1}^{\infty}\beta_n q^n).$$

By equating the coefficients of q^n on both sides of this last equality, we have

$$(r+n)a_n = ra_n - \beta_1 a_{n-1} - \beta_2 a_{n-2} - \cdots - \beta_n, \tag{3.18}$$

and this last equality is equivalent to the desired Identity (3.14). □

The goal in the following lemma is to provide an explicit formula in which β_n is expressed as a polynomial in $a_1, \cdots, a_n$.

Lemma 3.2.3. *Keeping the assumptions as before, we have*

$$\beta_n = S(n, a_1, \cdots, a_n), \tag{3.19}$$

for $n \geq 1$ where $S(n, a_1, \cdots, a_n)$ is defined as in Lemma 3.1.3.

Proof. By comparing (3.14) and (3.8), we see that the β_n's satisfy the same relations as the S_n's, where the S_n's, $n = 1, 2, 3, \cdots$, are as in Lemma 3.1.3, whence our result. □

3.2.2 The Main Recursive Formula

Now we are ready to state and prove the main theorem of this section concerning a recursive relation in which the nth coefficient a_n of the form f is given in terms of the coefficients $a_1, ..., a_{n-1}$, the divisor of f and the Faber polynomials evaluated at $\phi(\tau)$, for $\tau \in \Gamma \setminus \mathfrak{H}^*$, $\tau \neq \infty$.

Theorem 3.2.4. *Let $f = q^r + \sum_{n=1}^{\infty} a_n q^{r+n}$ be a weight k meromorphic modular form for the genus-zero subgroup Γ of the full modular group and let $s_0 = \infty, s_1, s_2, ..., s_t$ be a set of representatives of inequivalent cusps of Γ, respectively of widths $h_0, h_1, h_2, ..., h_t$. Then*

$$a_n = \sum_{\substack{m_1,\cdots,m_{n-1}\geq 0 \\ m_1+2m_2+\cdots+(n-1)m_{n-1}=n}} (-1)^{m_1+\cdots+m_{n-1}} \frac{(m_1+\cdots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} a_1^{m_1}\cdots a_{n-1}^{m_{n-1}}$$

$$-\frac{1}{n}\left(2kh_0\sigma(\frac{n}{h_0}) + \sum_{i=1}^{t}\left(\mathrm{ord}_{s_i}f - \frac{kh_i}{12}\right)F_n(\phi(s_i)) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\phi(\tau))\right), \quad (3.20)$$

where F_n is the nth Faber polynomial associated to the Hauptmodul ϕ of Γ.

Proof. First of all, we rewrite Equation (3.14) as

$$na_n + \beta_n = -\beta_1 a_{n-1} - \cdots - \beta_{n-1}a_1.$$

On the other hand, Lemma 3.2.3 implies that

$$\beta_n = -na_n + S(n, a_1, \cdots, a_{n-1}),$$

where $S(n, a_1, \cdots, a_{n-1})$ is defined as in Lemma 3.1.3. Therefore, we have

$$-\beta_1 a_{n-1} - \cdots - \beta_{n-1}a_1 = S(n, a_1, \cdots, a_{n-1}).$$

This last equality together with the Equations (3.14) and (3.15) yield the statement of the theorem. □

3.3 Recurrence Relations of the General Case

In this section we find recurrence relations for the forms on any genus-zero subgroup Γ of $\mathrm{SL}(2,\mathbb{R})$ which is commensurable with $\mathrm{SL}(2,\mathbb{Z})$. As mentioned in the Introduction, Helling in [He66] proved:

Theorem 3.3.1. *There exists a $\rho \in \mathrm{GL}^+(2,\mathbb{Q})$ and a square-free integer N such that*

$$\rho^{-1}\Gamma\rho \subseteq \Gamma_0(N)^+.$$

We remark that, as the map $f \mapsto f|[\rho]_k$ provides an isomorphism of complex vector spaces between $A_k(\Gamma)$ and $A_k(\rho^{-1}\Gamma\rho)$ (see for example [Sh71], Proposition 2.4), we may restrict ourselves to the case where Γ is contained in $\Gamma_0(N)^+$. So, from now on, we assume that $\Gamma \subseteq \Gamma_0(N)^+$ for the same square-free N. Also, since $\Gamma_0(N)^+$ acts transitively on cusps, without loss of generality, we only need to consider the cusp ∞.

Now let

$$f(z) = q^r + \sum_{n=1}^{\infty} a_n q^{r+n} \in A_k(\Gamma) \tag{3.21}$$

be a meromorphic modular form of weight k for Γ, where $q = e^{\frac{2\pi i z}{h_0}}$. As discussed in Section 3.1.1, if k is even or k is odd and the cusp ∞ is regular, then r is an integer. While if k is odd and the cusp ∞ is irregular, then r is equal to $r'/2$ for some odd integer r'.

3.3.1 The Weight Zero Quotient

For a square-free integer N, let $\nu(\Gamma_0(N)^+)$ be the volume of the compact Riemann surface $\Gamma_0(N)^+ \setminus \mathfrak{H}^*$, which is given by

$$\nu(\Gamma_0(N)^+) = \frac{\pi}{3}\prod_{p|N}\frac{p+1}{2}.$$

See, for example §3 of [He70]. This formula together with Proposition 2.16 and Theorem 2.20 of [Sh71] and the cusp-split Formula (3.2) imply that

$$\sum_{\tau\in\Gamma\setminus\mathfrak{H}^*} \mathrm{ord}_\tau f = \frac{k}{12}\prod_{p|N}\frac{p+1}{2}\sum_{i=0}^{t} h_i. \tag{3.22}$$

To continue, we seek a cusp form for $\Gamma_0(N)^+$ which plays the same role as Δ does for $\mathrm{SL}(2,\mathbb{Z})$. Let $\eta(z) = q^{h_0/24}\prod_{n=1}^{\infty}(1-q^{h_0 n})$ be the Dedekind eta function. Then for some suitable ℓ, the function

$$h(z) = \prod_{\delta | N} \eta(\delta z)^{\ell}$$

is a cusp form of weight $\varepsilon = \dfrac{\ell}{2}\tau(N)$ on $\Gamma_0(N)^+$, where $\tau(N)$ is the number of positive divisors of N (cf.[Cu09]). As we shall see, the results below are independent of the choice of ℓ.

The form $h(z)$ is holomorphic and non-vanishing on $\mathfrak{H}$ and has a zero of order $\dfrac{\ell}{24}\sigma(N)$ at ∞, where $\sigma(N) = \sum_{\delta | N} \delta$. One can easily see that

$$\Theta := \frac{f^{\frac{\varepsilon}{(\varepsilon,k)}}}{h^{\frac{k}{(\varepsilon,k)}}}$$

is a meromorphic modular form of weight zero on Γ, and therefore it can be expressed as a rational function of ϕ, the generator of the function field of $\Gamma\backslash\mathfrak{H}^*$. The first lemma of the next section gives the precise relation between Θ and ϕ.

3.3.2 The Recursive Formulae

We first state and prove two preliminary results which provide us with enough ingredients for the proof of the main theorem of this section.

Lemma 3.3.2. *Let the notation be as above. Then, for some non-zero constant λ, we have*

$$\Theta(z) = \lambda \prod_{i=1}^{t} (\phi(z) - \phi(s_i))^{\frac{\varepsilon}{(\varepsilon,k)}\mathrm{ord}_{s_i} f - \frac{\ell h_i k \sigma(N)}{24(\varepsilon,k)}} \prod_{\tau \in \Gamma\backslash\mathfrak{H}} (\phi(z) - \phi(\tau))^{\frac{\varepsilon}{(\varepsilon,k)}\mathrm{ord}_{\tau} f}. \tag{3.23}$$

Proof. To prove this equality it is enough to verify that both sides have the same order for the points of $\Gamma\backslash\mathfrak{H}^*$. Since $h(z)$ is holomorphic and non-vanishing on the upper half plane, for any $\tau \in \Gamma\backslash\mathfrak{H}$ the order of both sides of (3.23) are the same. For any cusp s_i, $1 \le i \le t$ we also have the equality of the orders because $\mathrm{ord}_{s_i} h = \frac{\ell h_i \sigma(N)}{24}$. At the cusp ∞ we start with equation (3.22) and immediately we have

$$\frac{\ell}{2}\tau(N) \sum_{\tau\in\Gamma\backslash\mathfrak{H}^*} \mathrm{ord}_\tau f = \frac{\ell k}{24}\prod_{p|N}(p+1)\sum_{i=0}^{t} h_i.$$

This relation combined with the identity $\prod_{p|N}(p+1) = \sigma(N)$ imply that

$$\frac{\varepsilon}{(\varepsilon,k)}\mathrm{ord}_\infty f - \frac{\ell h_0 k\sigma(N)}{24(\varepsilon,k)} = \sum_{i=1}^{t}\frac{\ell h_i k\sigma(N)}{24(\varepsilon,k)} - \sum_{\tau\in\Gamma\backslash\mathfrak{H}^*}\frac{\varepsilon}{(\varepsilon,k)}\mathrm{ord}_\tau f.$$

The last relation shows the equality of the orders at ∞ and this completes the proof. □

Lemma 3.3.3. *With the notation as above, the coefficients of f satisfy the following recursive relation*

$$a_n = \frac{-\beta_1 a_{n-1} - \beta_2 a_{n-2} - \cdots - \beta_{n-1}a_1 - \beta_n}{n}, \tag{3.24}$$

where, for $n \geq 1$, β_n is defined by the formula

$$\begin{aligned}\beta_n := \frac{2kh_0}{\tau(N)}\sum_{\delta|N}\delta\sigma\Big(\frac{n}{\delta h_0}\Big) + \sum_{i=1}^{t}\left(\mathrm{ord}_{s_i} f - \frac{kh_i\sigma(N)}{12\tau(N)}\right)F_n(\phi(s_i))\\ + \sum_{\tau\in\Gamma\backslash\mathfrak{H}}\mathrm{ord}_\tau f F_n(\phi(\tau)).\end{aligned} \tag{3.25}$$

Here $\sigma(\frac{n}{\delta h_0}) = 0$, if $\delta h_0 \nmid n$.

Proof. Taking the logarithmic derivative of (3.23) and using equation (3.6), we find

$$\begin{aligned}\frac{qf'(q)}{f(q)} = \frac{\ell k h_0}{\varepsilon}\sum_{\delta|N}\frac{\delta}{24}E_2(q^{\delta h_0})\\ - \sum_{i=1}^{t}\left(\left(\mathrm{ord}_{s_i} f - \frac{kh_i\sigma(N)}{12\tau(N)}\right)\sum_{n=0}^{\infty}F_n(\phi(s_i))q^n\right)\\ - \sum_{\tau\in\Gamma\backslash\mathfrak{H}}\left(\mathrm{ord}_\tau f\sum_{n=0}^{\infty}F_n(\phi(\tau))q^n\right).\end{aligned} \tag{3.26}$$

where F_n is the nth Faber polynomial associated to ϕ and $E_2(q)$ is the non-modular Eisenstein series of weight 2. The last equality can be written as

$$\begin{aligned}\frac{qf'(q)}{f(q)} &= \frac{\ell k h_0 \sigma(N)}{24\varepsilon} - \frac{k h_0 \sigma(N)}{12\tau(N)} + r - \sum_{n=1}^{\infty} \beta_n q^n \\ &= r - \sum_{n=1}^{\infty} \beta_n q^n,\end{aligned} \tag{3.27}$$

where β_n is defined as in (3.25). Substituting the q-expansion of f given in (3.21) in Equation (3.27) yields

$$r + \sum_{n=1}^{\infty}(r+n)a_n q^n = (1 + \sum_{n=1}^{\infty} a_n q^n)(r - \sum_{n=1}^{\infty} \beta_n q^n).$$

By equating the coefficients of q^n on both sides of this last equality, we have the desired Identity (3.24). □

Now, in a manner similar to Lemma 3.2.3 we can write β_n in terms of the a_j for $1 \leq j \leq n-1$.

Lemma 3.3.4. *By the assumptions as above, for $n \geq 1$, β_n can be given as*

$$\beta_n = S(n; a_1, \cdots, a_n), \tag{3.28}$$

where $S(n; a_1, \cdots, a_n)$ is defined as in Lemma 3.1.3.

Proof. Similar to the proof of Lemma 3.2.3. □

Theorem 3.3.5. *Let $f = q^r + \sum_{n=1}^{\infty} a_n q^{r+n}$ be a weight k meromorphic modular form for the genus-zero subgroup Γ of $\Gamma_0(N)^+$. Let $s_0 = \infty, s_1, s_2, \ldots, s_t$ be representatives of* *the inequivalent cusps of* Γ, *of widths* $h_0, h_1, h_2, ..., h_t$ *respectively. Then*

$$a_n = \sum_{\substack{m_1,\dots,m_{n-1}\geq 0 \\ m_1+\cdots+(n-1)m_{n-1}=n}} (-1)^{m_1+\cdots+m_{n-1}} \frac{(m_1+\cdots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} a_1^{m_1}\cdots a_{n-1}^{m_{n-1}}$$

$$-\frac{1}{n}\left(\frac{2kh_0}{\tau(N)}\sum_{\delta|N}\delta\sigma(\frac{n}{\delta h_0}) + \sum_{i=1}^{t}\left(\mathrm{ord}_{s_i}f - \frac{kh_i\sigma(N)}{12\tau(N)}\right)F_n(\phi(s_i)) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} \mathrm{ord}_\tau f F_n(\phi(\tau))\right),$$

where F_n *is the* n*th Faber polynomial associated to the Hauptmodul* ϕ *of* Γ.

Proof. The result follows from Lemmas 3.3.3 and 3.3.4. □

Theorem 3.3.5 gives recursive formulae for the coefficients of the modular form f. These formulae involve the Faber polynomials evaluated at points of $\mathfrak{H}$. These polynomials can also be calculated recursively. To clarify the situation, and to make clear the required input to the recursion relations, we start by giving a recursive formula for the Fourier coefficients of normalized Hauptmodul ϕ of Γ.

3.3.3 Retrieving Fourier Coefficients of Hauptmoduls: The Main Result

Let ϕ

$$\phi(q) = \frac{1}{q} + \sum_{n\geq 0} c_n q^n, \tag{3.29}$$

be a Hauptmodul of Γ. Applying Theorem 3.3.5 to the (normalized) derivative of the Hauptmodul ϕ gives the following equation

$$-nc_n = \frac{1}{n+1}\Big\{ S(n+1; 0, -c_1, -2c_2, \cdots, -(n-1)c_{n-1})$$
$$-\frac{4h_0}{\tau(N)}\sum_{\delta|N}\delta\sigma(\frac{n+1}{\delta h_0}) - \sum_{i=1}^{t}\Big(1-\frac{h_i\sigma(N)}{6\tau(N)}\Big)F_{n+1}(\phi(s_i)) \tag{3.30}$$
$$-\sum_{\tau\in\Gamma\backslash\mathfrak{H}}(1-e_\tau^{-1})F_{n+1}(\phi(\tau))\Big\}.$$

As c_n occurs linear on each side of this equation, we can solve for c_n. The result, after simplification and applying Corollary 3.1.4, is as follows.

Theorem 3.3.6. *If $n = -1$, then $c_{-1} = 1$.*

If $n = 0$, then

$$c_0 = \frac{24h_0}{\sigma(N)h_0 + 6\tau(N)}\delta_{1,h_0} + \frac{6\tau(N)}{\sigma(N)h_0 + 6\tau(N)}\times$$
$$\Big\{\sum_{i=1}^{t}(1-\frac{h_i\sigma(N)}{6\tau(N)})\phi(s_i) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}}(1-e_\tau^{-1})\phi(\tau)\Big\}.$$

If $n > 0$, then

$$c_n = \frac{1}{(n+1)(1+\frac{h_0\sigma(N)}{6\tau(N)}+n)}\times$$
$$\Big\{\frac{4h_0}{\tau(N)}\sum_{\delta|N}\delta\sigma(\frac{n+1}{\delta h_0}) - S(n+1; 0, -c_1, \cdots, -(n-1)c_{n-1})$$
$$+\sum_{i=1}^{t}(1-\frac{h_i\sigma(N)}{6\tau(N)})S(n+1; c_0-\phi(s_i), c_1, \ldots, c_{n-1})$$
$$+\sum_{\tau\in\Gamma\backslash\mathfrak{H}}(1-e_\tau^{-1})S(n+1; c_0-\phi(\tau), c_1, \ldots, c_{n-1})\Big\}.$$

Using Corollary 3.1.4, Theorem 3.3.5 can be rewritten to make the dependence on the coefficients of ϕ explicit.

Theorem 3.3.7. *Let the hypotheses be as in Theorem 3.3.5 and let c_i, $i = -1, 0, 1, \ldots$ be the coefficients of Hauptmodul ϕ of Γ, then*

$$a_n = \frac{1}{n}\Bigg\{S(n;a_1,...,a_{n-1}) - \frac{2kh_0}{\tau(N)}\sum_{\delta|N}\delta\sigma(\frac{n}{\delta h_0})$$

$$-\sum_{i=1}^{t}\Big(\mathrm{ord}_{s_i}f - \frac{kh_i\sigma(N)}{12\tau(N)}\Big)S\Big(n;c_0-\phi(s_i),c_1,...,c_{n-1}\Big)$$

$$-\sum_{\tau\in\Gamma\backslash\mathfrak{H}}\mathrm{ord}_\tau f S\Big(n;c_0-\phi(\tau),c_1,...,c_{n-1}\Big)\Bigg\}.$$

Remark 3.3.8. By Theorems 3.3.6 and 3.3.7, the recurrence relations established require as input:

- a square-free integer N such that Γ is a subgroup of $\Gamma_0(N)^+$;
- the weight and divisor of f;
- the ramification locus and the ramification orders of the Hauptmodul ϕ_Γ and the values $\phi_\Gamma(\tau)$, where $\mathrm{ord}_\tau f \neq 0$.

Given this input, the relations have the same form for all Γ and f and are, in this sense, universal.

3.4 The Product Expansion of f

In this section we see that the exponents $c(n)$ appear in the infinite product expansion of a modular form f can be expressed in terms of β_n's as defined in (3.27). First we recall the following proposition from [EN96].

Proposition 3.4.1. *Let $f = q^r + \sum_{n=1}^{\infty} a_n q^{r+n}$ be holomorphic on $\mathfrak{H}$ and assume that $f(z+h) = f(z)$, for all $z \in \mathfrak{H}$, where $h > 0$. Then there exists a unique sequence $c(n)$ of complex numbers such that*

$$f(z) = q^r\prod_{n=1}^{\infty}(1-q^n)^{c(n)}.$$

for sufficiently small $|q|$. Moreover,

$$\frac{qf'(q)}{f(q)} = r - \sum_{n=1} \left(\sum_{d|n} c(d)d \right) q^n.$$

This shows, in particular, that the modular form f of the preceding section admits a similar infinite product representation. This combined with (3.27) gives:

Corollary 3.4.2. *With the notation as above,*

$$c(n) = \frac{1}{n} \sum_{d|n} \mu(n/d)\beta_d,$$

where β_n is given as in (3.27) and μ is the Möbius function.

Proof. This is a consequence of the Möbius Inversion Formula since

$$\beta_n = \sum_{d|n} c(d)d.$$

□

3.5 Some Examples

In this subsection we shall re-derive, in the following two examples, the main formulae of the earlier works [BKO04] and [Ah02] as immediate corollaries of Theorem 3.2.4. In the third example below we study the recursive formulae for $\Gamma_0(p)$ for $p = 2, 3, 5, 7, 13$, first as a genus-zero subgroup of the full modular group and then as a subgroup of $\Gamma_0(p)^+$. The last example is concerned with a non-congruence lift of $\overline{\Gamma(3)}$ which has two classes of regular cusps and two classes of irregular ones. By a lift of $\overline{\Gamma(3)}$ here we mean a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ that projects to $\overline{\Gamma(3)}$ (see [KSV]). We will then determine the space of weight k holomorphic modular forms of this subgroup by computing a set of generators for this space.

Example 3.5.1. If $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, then β_n defined in (3.15) takes the following simplified form

$$\beta_n = 2k\sigma(n) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\tau).$$

Hence

$$a_{r+n} = \frac{1}{n}\left\{ S(n, a_{r+1}, \ldots, a_{r+n-1}) - \left(2k\sigma(n) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\tau)\right)\right\},$$

which is the same as theorem 1 in [BKO04].

Example 3.5.2. In the second example, we consider the case $\Gamma = \Gamma_0(p)$, where $p \in \{2, 3, 5, 7, 13\}$. According to [Ah02], one may take

$$\phi_p(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}, \qquad \text{where } \eta(z)^{24} = \Delta(z),$$

as a Hauptmodul of $\Gamma_0(p)$. First, we replace the $F_n(z)$ by the $j_n(z) + F_n(0)$, where j_n is $j_n^{(p)}$ defined as in [Ah02], as the unique modular function on $\Gamma_0(p)$ which vanishes at the cusp 0 and whose Fourier expansion at ∞ has the form

$$j_n(q) = \frac{1}{q^n} + \sum_{m=1}^{\infty} j_{n,m} q^m,$$

for all $n \geq 1$. Since $\Gamma_0(p)$ has two classes of inequivalent cusps represented by $s_0 = \infty$ and $s_1 = 0$ whose corresponding cusp widths are respectively $h_0 = 1$ and $h_1 = p$, the Equation (3.15) becomes

$$\begin{aligned}
\beta_n &= 2k\sigma(n) + \left(\mathrm{ord}_0 f - \frac{pk}{12}\right)(j_n(0) + F_n(0)) + \sum_{\tau\in\Gamma\backslash\mathcal{H}} e_\tau \mathrm{ord}_\tau f (j_n(\tau) + F_n(0)) \\
&= 2k\sigma(n) + \left(\sum_{\tau\in\Gamma\backslash\mathfrak{H}\cup\{0\}} e_\tau \mathrm{ord}_\tau f - \frac{pk}{12}\right) F_n(0) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f j_n(\tau) \\
&= 2k\sigma(n) + (\frac{k}{12} - r)F_n(0) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f j_n(\tau),
\end{aligned}$$

where the last equality follows from Valence Formula (3.13), Identity (3.2) and the fact that $[\Gamma : \Gamma_0(p)] = p+1$. It is not difficult to show that

$$F_n(0) = \frac{24}{p-1}\left(\sigma(n) - p\sigma(n/p)\right), \qquad \sigma(n/p) = 0 \ \ if\ p \nmid n. \tag{3.31}$$

To see this, we take the logarithmic derivative of $\phi_p(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}$ to get

$$\frac{\phi_p'(z)}{\phi_p(z)} = \frac{24}{p-1}\frac{\eta'(z)}{\eta(z)} - \frac{24p}{p-1}\frac{\eta'(pz)}{\eta(pz)}.$$

So,

$$\frac{q\phi_p'(q)}{\phi_p(q)} = \frac{1}{p-1}\left(1 - 24\sum_{n=1}^{\infty}\sigma(n)q^n\right) - \frac{p}{p-1}\left(1 - 24\sum_{n=1}^{\infty}\sigma(n)q^{pn}\right).$$

Replacing the left hand side by $-\sum_{n=0}^{\infty} F_n(0)q^n$ (see (3.6)) then yields

$$\sum_{n=0}^{\infty} F_n(0)q^n = 1 + \frac{24}{p-1}\sum_{n=1}^{\infty}\sigma(n)q^n - \frac{24}{p-1}\sum_{n=1}^{\infty}\sigma(n)q^{pn}.$$

Now comparing the coefficients of q^n on both sides gives Equation (3.31). Using this information and following a straightforward calculation, we deduce that

$$\begin{aligned}\beta_n &= 2k\sigma(n) + (\frac{k}{12} - r))\frac{24}{p-1}\left(\sigma(n) - p\sigma(n/p)\right) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f j_n(\tau) \\ &= \frac{2kp-24r}{p-1}\sigma(n) + \frac{24r-2k}{p-1}p\sigma(n/p) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f j_n(\tau).\end{aligned}$$

These coefficients are the same as those of Theorem 4 in [Ah02].

Example 3.5.3. Here we reconsider the case of $\Gamma = \Gamma_0(p)$, where $p \in \{2,3,5,7,13\}$, first as a subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and then as a subgroup of $\Gamma_0(p)^+$.

Case I. We recall that $\Gamma_0(p) \leq \mathrm{SL}(2,\mathbb{Z})$ has two inequivalent class of cusps represented by $s_0 = \infty$ and $s_1 = 0$ of widths $h_0 = 1$ and $h_1 = p$ respectively. One also knows that

$$\phi_p(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}$$

is a Hauptmodul of $\Gamma_0(p)$. The function $\phi_p(z)$ has a simple pole at ∞ and a simple zero at the cusp 0. By applying (3.20), we have

$$\begin{aligned} a_n &= \sum_{\substack{m_1,\dots,m_{n-1}\geq 0 \\ m_1+\dots+(n-1)m_{n-1}=n}} (-1)^{m_1+\dots+m_{n-1}} \frac{(m_1+\dots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} a_1^{m_1}\cdots a_{n-1}^{m_{n-1}} \\ &- \frac{1}{n}\left(2k\sigma(n) + \left(\mathrm{ord}_0 f - \frac{kp}{12}\right)F_n(0) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\tau)\right). \end{aligned} \tag{3.32}$$

Case II. We shall now regard $\Gamma_0(p)$ as a subgroup of $\Gamma_0(p)^+$. One knows that ∞ and 0 of widths $h_0 = h_1 = 1$ represent the two inequivalent class of cusps of $\Gamma_0(p)$. By using Theorem 3.3.5, one has

$$a_n = \sum_{\substack{m_1,\dots,m_{n-1}\geq 0 \\ m_1+\dots+(n-1)m_{n-1}=n}} (-1)^{m_1+\dots+m_{n-1}} \frac{(m_1+\dots+m_{n-1}-1)!}{m_1!\cdots m_{n-1}!} a_1^{m_1}\cdots a_{n-1}^{m_{n-1}}$$

$$-\frac{1}{n}\left(k\left(\sigma(n)+p\sigma(\frac{n}{p})\right) + \left(\mathrm{ord}_0 f - \frac{k(p+1)}{24}\right)F_n(0) + \sum_{\tau\in\Gamma\backslash\mathfrak{H}} e_\tau \mathrm{ord}_\tau f F_n(\tau)\right). \tag{3.33}$$

In order to see that the two Formulae (3.32) and (3.33) are the same, we need only to verify that the following

$$2k\sigma(n) - \frac{kp}{12}F_n(0) = k(\sigma(n) + p\sigma(\frac{n}{p})) - \frac{k(p+1)}{24}F_n(0)$$

holds. This last equality is equivalent to the identity

$$F_n(0) = \frac{24}{p-1}\left(\sigma(n) - p\sigma(\frac{n}{p})\right),$$

which was proved in the second example (see (3.31)).

Example 3.5.4. In this last example we work with a non-congruence subgroup Γ of $\mathrm{SL}(2,\mathbb{Z})$ and study the space of its modular forms. First we start with torsion-free genus-zero subgroup $\Gamma(3)$. This group has four class of inequivalent cusps represented by 0, 1, 2 and ∞. Let

$$P_0 = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}, \quad P_1 = \begin{pmatrix} -2 & 3 \\ -3 & 4 \end{pmatrix}, \quad P_2 = \begin{pmatrix} -5 & 12 \\ -3 & 7 \end{pmatrix}, \quad P_\infty = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix};$$

be the parabolic elements of $\Gamma(3)$ corresponding to 0, 1, 2 and ∞ respectively. To continue we need the following proposition.

Proposition 3.5.5. (cf. [JS87]) *Let H be a Fuchsian group of genus g and cusp number t, having r inequivalent elliptic elements of orders $m_1, \cdots, m_r$. Then H has a presentation of the form*

$$\langle A_1, B_1, \cdots, A_g, B_g, E_1, \cdots, E_r, P_1, \cdots, P_t \Big| \; E_1^{m_1} = \cdots = E_r^{m_r} = \prod_{i=1}^r E_i \prod_{i=1}^t P_i \prod_{i=1}^g [A_i, B_i] = I \rangle,$$

where the generators E_i's are elliptic, P_i's are parabolic and A_i, B_i's are hyperbolic.

Using this proposition, $\Gamma(3)$ can be generated by P_0, P_1, P_2 and P_∞. Now define Γ as

$$\Gamma := \langle -P_0, P_1, P_2, -P_\infty \rangle.$$

It is clear that the cusps 0 and ∞ are irregular. By using Corollary 2.3 of [KSV] one can see that Γ is a non-congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$. Since $\overline{\Gamma} = \overline{\Gamma(3)}$, the spaces of even weight holomorphic modular forms of Γ and $\Gamma(3)$ are the same. Now we recall that the graded ring of integer weight modular forms of $\Gamma(3)$,

$$G(\Gamma(3)) := \bigoplus_{n=0}^{\infty} G_n(\Gamma(3),$$

can be regarded as the ring of complex polynomials in two variables. That is to say, $G(\Gamma(3)) = \mathbb{C}[f_1, f_2]$, where f_1 and f_2 are algebraically independent modular forms of weight one for $\Gamma(3)$ (see [BKMS1]). These generators may be chosen so that the quotient $\frac{f_1}{f_2}$ is ϕ, a normalized Hauptmodul of $\Gamma(3)$. Knowing the values of ϕ at the cusps 0, 1 and 2 and the divisors of f_1 and f_2 as

$$\phi(0) = 0, \quad \phi(1) = \frac{-9 + 3\sqrt{3}i}{2}, \quad \phi(2) = \frac{-9 - 3\sqrt{3}i}{2},$$

$$\operatorname{div}(f_1) = [0], \quad \operatorname{div}(f_2) = [\infty]$$

(see [Seb02]), we can apply the formulae in Theorem 3.3.6 and Theorem 3.3.7 to find the q-expansions of ϕ, f_1 and f_2. The results are as follows

$$\begin{aligned}
\phi &= q^{-1} + 5q^2 - 7q^5 + 3q^8 + 15q^{11} + \cdots, \\
f_1 &= 1 - 3q + 6q^3 - 3q^4 - 6q^7 + 6q^9 + 6q^{12} + \cdots, \\
f_2 &= q + q^4 + 2q^7 + 2q^{12} + \cdots,
\end{aligned}$$

where $q = \frac{2\pi i}{3}$. As we mentioned earlier f_1 and f_2 generate the space of holomorphic modular forms of even weights for Γ as well. Since the space of holomorphic modular forms of Γ of weight one is one dimensional (see Theorem 2.25 [Sh71]), it is enough to compute the expansion of f, a generator of this space, by the values of ϕ at the cusps, the divisor $\operatorname{div}(f) = \frac{1}{2}[0] + \frac{1}{2}[\infty]$ of f and the formula given in (3.3.7). Having this data, the q-expansion of f is computed as

$$f = q^{\frac{1}{2}}\Big(1 + (3/4 - 3/4i\sqrt{3})q + (9/16 + 9/16i\sqrt{3})q^2 + (29/16)q^3 + \ldots\Big).$$

Since the space of holomorphic modular forms on Γ of weigh $2k$ and $2k+1$ for any $k \geq 1$ have the same dimension (see [Sh71]), it follows that a basis for $G_{2k+1}(\Gamma)$ can be obtained by a basis of $G_{2k}(\Gamma)$ and f.

3.6 Epilogue

The formulae obtained in the previous sections of this chapter are obviously of recursive nature making one wonder if there is any closed formula expressing the Fourier coefficients of modular forms in a non-recursive manner.

Such identities for the Fourier coefficients of the j-function have been proved by Kaneko in [K96] in terms of the singular moduli, i.e. the values of j at the imaginary quadratic points of the upper half plane. Using similar techniques, Ohta in [Oh09] has established analogues formulae for the Fourier coefficients of certain higher level modular functions on the groups $\Gamma_0(N)$ for $N = 2,\ 3,\ 4$ and $\Gamma_0^+(N)$ for $N = 2,\ 3$. They give some explicit formulae for the coefficients of the Hauptmoduls of these genus zero subgroups of $\mathrm{SL}(2, \mathbb{R})$.

The basis of their proofs is a fundamental result of Zagier [Z02] concerning the trace of singular moduli. To prove his theorem, Zagier in [Z02] begins with a certain modular function of weight $3/2$ on $\Gamma_0(4)$ and expresses it in terms of well known arithmetic functions and finally he finds the traces of singular moduli for the j-function. In the same paper he also briefly sketches the generalization of his result for the groups $\Gamma_0^+(N)$ where $N = 2,\ 3,\ 4,\ 5$ and 6. He then remarks that such a result may hold for other genus zero subgroups of $\mathrm{SL}(2, \mathbb{R})$ with some conditions.

It appears that one can generalize the works of Kaneko and Ohta to other genus zero Moonshine type subgroups. In order to do so, however, one might need to first carry out computations similar to those done by Zagier himself for $\Gamma_0^+(N)$. Once this is done, the extension of the works of Kaneko and Ohta to such other genus zero Moonshine type subgroups does not appear to present serious difficulties. In any case, it would be very interesting to compare the recursive formulae already found in [CS2] for the Fourier coefficients of Hauptmoduls of the groups under consideration with such sought for closed formulae: such comparison definitely leads to very interesting and genuinely new arithmetic identities!

Bibliography

[Ah02] S. Ahlgren, 'The theta-operator and the divisors of modular forms on genus-zero subgroups', *Mathematical Research Letters*, 10 (2002)787-798.

[At05] J. Atkinson, 'Divisors of modular forms on $\Gamma_0(4)$', *Journal of Number Theory*, 112 (2005)189-204.

[BKMS1] E. Bannai, M. Koike, A. Munemasa,J Sekiguchi, 'Some results on modular forms—subgroups of the modular group whose ring of modular forms is a polynomial ring.' *Groups and combinatorics—in memory of Michio Suzuki*, 245–254, *Adv. Stud. Pure Math., 32, Math. Soc. Japan, Tokyo,* 2001.

[B.R01] R. E. Borcherds, 'Problems in Moonshine', *First International Congress of Chinese Mathematicians (Beijing*, 1998), 3–10, *AMS/IP Stud. Adv. Math.*, 20, *Amer. Math. Soc., Providence, RI*, 2001.

[B.R98] R. E. Borcherds, 'What is Moonshine?', *Proceedings of the International Congress of Mathematicians, Vol. I (Berlin*, 1998). *Doc. Math.* 1998, *Extra Vol. I*, 607–615 (electronic).

[B.R92] R. E. Borcherds, 'Monstrous moonshine and monstrous Lie superalgebras', *Invent. Math.* 109 (1992), no. 2, 405–444.

[B.R88] R. E. Borcherds, 'Generalized Kac-Moody algebras', *J. Algebra* 115 (1988), no. 2, 501–512.

[B.A06] Ablilah Bouali, 'Faber polynomials, Cayley-Hamilton equation and Newton symmetric functions' *Bull. Sci. Math.* 130 (2006), no. 1, 49–70.

[BKO04] J. Bruinier, W. Kohnen and K. Ono, 'The arithmetic of the values of modular functions and the divisors of modular forms', *Compositio Math.* 140 (2004)552-566.

[C.D.06] D. Choi, 'On values of a modular form on $\Gamma_0(N)$', *Acta Arith.* 121 (2006), no. 4, 299–311.

[C.S.06] S. Y. Choi, 'The Values of Modular Functions and Modular Forms', *Canada Math. Bull.*Vol. 49(4), 2006 pp. 526-535.

[CN79] J. H. Conway and S. P. Norton, 'Monstrous Moonshine', *Bull. London Math. Soc.* 11, 1979, no 3,308-339.

[Cu09] C. J. Cummins, 'On conjugasy classes of comgruence subgroups of SL(2, $\mathbb{R}$)', *LMS J. Comput. Math.* To appear.

[Cu04] C. J. Cummins, 'Congruence subgroups of groups commensurable with PSL(2, $\mathbb{Z}$) of genus 0 and 1', *Experiment. Math.*, 13(3):361–382, 2004.

[Cu09] C. J. Cummins, 'Cusp forms like Δ', *Canad. Math. Bull.* 52 (2009), no. 1, 53-62.

[CG97] C. J. Cummins and T. Gannon, 'Modular equations and the genus-zero property of moonshine functions', *Invent. Math.* 129 (1997), no. 3, 413–443.

[CS09] C. J. Cummins and N. S. Haghighi, 'On a Class of Congruence Subgroups', *Groups and Symmetries*, 105-110, *CRM Proc. Lecture Notes,* 47. *Amer. Math. Soc. Providence RI,* 2009.

[CS1] C. J. Cummins and N. S. Haghighi, 'On the Signature of a Class of Congruence Subgroups', *To appear.*

[CS2] C. J. Cummins and N. S. Haghighi, 'Fourier Coefficients of Modular Forms', *Submitted.*

[DKM82] D. Dummit, H. Kisilevsky and J. McKay, 'Multiplicative product of η–functions', *finite groups-coming of age (Montreal, Quebec,* 1982), *volume* 45*of Contem. Math.,*pages 89-98 *Amer. Math. Soc., Providence, RI,* 1985.

[EN96] Wolfgang Eholzer, Nils-Peter Skoruppa, 'Product expansions of conformal characters', *Phys. Lett. B* 388 (1996), no. 1, 82–89.

[FLM88] I. Frenkel, J. Lepowsky and A. Meurman, 'Vertex operator algebras and the Monster', *Pure and Applied Mathematics,* 134. *Academic Press, Inc., Boston, MA,* 1988.

[Gao6] T. Gannon, ' Monstrous moonshine: the first twenty-five years', *Bull. London Math. Soc.* 38 (2006), no. 1, 1–33.

[G81] R. L. Jr. Griess, 'A construction of F_1 as automorphisms of a $196,883$-dimensional algebra', *Proc. Nat. Acad. Sci. U.S.A.* 78 (1981), no. 2, part 1, 686–691.

[He66] H. Helling, 'Bestimmung der Kommensurabilittsklasse der Hilbertschen Modulgruppe', *Math. Z.*, 92 (1966), 269-280.

[He70] H. Helling, 'On the Commensurability of the Rational Modular Group', *J. London Math. Soc.* (2), 2 (1970), 67-72.

[Hs96] T. Hsu, 'Identifying congruence subgroups of the modular group', *Proc. Amer. Math. Soc.* 124 (1996), no. 5, 1351–1359.

[J86] G. A. Jones, 'Congruence and Non-Congruence Subgroups of the Modular Group: a survey', *Proceedings of groups. St. Andrew* 1985, 223-234. *London Math. Soc. Lecture Note Ser.* 121 *Cambridge Univ. Press, Cambridge*, 1986.

[JS87] Gareth A. Jones and David Singerman, *Complex functions; An algebraic and geometric viewpoint*, Cambridge University Press, Cambridge, 1987.

[K96] Masanobu Kaneko, 'The Fourier coefficients and the singular moduli of the elliptic modular function $j(\tau)$', *Automorphic forms on algebraic groups (Japanese) (Kyoto, 1995). Surikaisekikenkyusho Kokyuroku No.* 965 (1996), 172–177.

[KSV] I. Kimming, M. Schtt and H. A. Verrill, 'Lifts of Projective Congruence Groups', *Submitted.* arXiv:0905.4798v2

[K97] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Text in Math. 97, Springer-Verlag, 1984.

[L84] H. Larcher, 'The cusp amplitudes of the congruence subgroups of the classical modular group' II, *Illinois J. Math.*, 28(2):312–338, 1984.

[MS09] A. W. Mason, A. Schweizer, 'The cusp amplitudes and quasi-level of a congruence subgroup of SL2 over any Dedekind domain', *Submitted on* 4 *Sep* 2009, arXiv:0909.0799

[Md95] I. G. Macdonald, *Symmetric Functions and Hall Polynomials, 2nd edition,* Oxford Science Publications, 1995.

[Ma96] Y. Martin, 'On modular invariance of completely replicable functions', *Moonshine, the Monster, and related topics*(South Hadley, MA, 1994), 263–286, *Contemp. Math.*, 193,*Amer. Math. Soc., Providence, RI,* 1996.

[Mi89] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989. Translated from the Japanese by Yoshitaka Maeda.

[Og74] A. P. Ogg, 'Automorphismes de courbes modulaires', (French) *Séminaire Delange-PisotPoitou* (16e anne: 1974/75),*Thorie des nombres, Fasc.* 1, Exp. No. 7, 8 pp. *Secrétariat Mathématique, Paris,* 1975

[Oh09] Kaori Ohta, 'Formulas for the Fourier coefficients of some genus zero modular functions', *Kyushu J. Math.* 63 (2009), no. 1, 1–15.

[On04] K. Ono, 'Hecke operators and the q-expansion of modular forms', *Number Theory,* 229-235 *CRM Proc. Lecture Notes,* 36.*Amer. Math. Soc. Providence, RI* 2004.

[Seb01] A. Sebbar, 'Classification of torsion-free genus-zero congruence groups', *Proc. Amer. Math. Soc.*, 129(9):2517–2527 (electronic), 2001.

[Seb02] A. Sebbar, 'Modular Subgroups, Forms, Curves and Surfaces', *Canada Math. Bull.*, 45(2):294–308, 2002.

[Sel77] A. Selberg, 'Remarks on multiplicative functions', Number theory day *(Proc. Conf., Rockefeller Univ., New York,* 1976), pages 232–241. *Lecture Notes in Math., Vol.* 626. *Springer, Berlin,* 1977.

[Sh71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Sm85] S. D. Smith, 'On the head characters of the Monster simple group', *Finite groups-coming of age* (Montreal, Que., 1982), 303–313, *Contemp. Math.,* 45,*Amer. Math. Soc., Providence, RI,* 1985.

[Su98] P. K. Suetin, *Series of Faber Polynomials.* An International Series of Monographs in Mathematics, Vol. 1, Gordon and Breach Science Publishers.

[Th79] J. G. Thompson, 'Some numerology between the Fischer-Griess Monster and the elliptic modular function',. *Bull. London Math. Soc.* 11 (1979), no. 3, 352–353.

[Z02] Don Zagier, 'Traces of singular moduli. Motives, polylogarithms and Hodge theory', *Part I (Irvine, CA,* 1998), 211 – –244, *Int. Press Lect. Ser.,* 3, *I, Int. Press, Somerville, MA,* 2002.