SUBGROUPS OF SOME FUCHSIAN GROUPS DEFINED BY TWO LINEAR CONGRUENCES

OMER YAYENIE

ABSTRACT. In this article we define a new family of subgroups of Fuchsian groups $\mathcal{H}(\sqrt{m})$, for a squarefree positive integer m , and calculate their index in $\mathcal{H}(\sqrt{m})$ and their parabolic class number. Moreover, we will show that the index of these subgroups is closely related to the solvability of a quadratic congruence $x^2 \equiv m \pmod{n}$ and the number of inequivalent solutions of a quadratic congruence $x^2 \equiv 1 \pmod{n}$. Finally, we will show that the results obtained by Yilmaz and Keskin [Acta Math. Sin **25** (2005), 215–222] are immediate corollaries of one of the main theorems of this article.

1. INTRODUCTION

A Fuchsian group $\mathcal{G}$ is a finitely generated non-elementary discrete group of conformal homeomorphisms of the hyperbolic plane $\mathbb{H}$. By the classical results of Fricke and Klein, Fuchsian groups of the first kind have the following presentation:

Generators:

$$(1) \quad \begin{aligned} &A_1, B_1, \dots, A_g, B_g \text{ (hyperbolic)} \\ &E_1, \dots, E_d \text{ (elliptic)} \\ &P_1, \dots, P_t \text{ (parabolic)} \end{aligned}$$

Relations:

$$E_1^{m_1} = \dots = E_d^{m_d} = \prod_{i=1}^g [A_i, B_i] \prod_{l=1}^d E_l \prod_{j=1}^t P_j = 1$$

We then say $\mathcal{G}$ has signature (see [1])

$$(g; m_1, m_2, \dots, m_d; t),$$

where g is the genus of its underlying Riemann surface, $m_1, \dots, m_d$ are the periods of the non-conjugate elliptic elements and t is the parabolic class number of the group. The signature tells us there are exactly d nonconjugate (in $\mathcal{G}$) maximal cyclic subgroups of $\mathcal{G}$ generated by elliptic elements of order m_j ($j = 1, \dots, d$) and t non-conjugate (in $\mathcal{G}$) maximal cyclic subgroups of $\mathcal{G}$ generated by parabolic elements.

Received by the editors March 26, 2007.

2000 *Mathematics Subject Classification*. Primary 11F06, 19B37; Secondary 20H05, 20H10.

Key words and phrases. Fuchsian groups, Hecke groups, modular group, congruence subgroups, and modular forms.

Let m be a squarefree natural number and let $\mathcal{H}(\sqrt{m})$ denote the discrete subgroup of $PSL(2, \mathbb{R})$, which contains all mappings of the form

- (i) $M(\tau) = \frac{a\tau + b\sqrt{m}}{c\sqrt{m}\tau + d}$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bcm = 1$.
- (ii) $M(\tau) = \frac{a\sqrt{m}\tau + b}{c\tau + d\sqrt{m}}$, where $a, b, c, d \in \mathbb{Z}$ and $adm - bc = 1$.

When $m = 1$, the resulting group is the modular group $\Gamma(1)$ and when $m = 2$ or $m = 3$, the resulting groups are the Hecke groups whose elements are completely described in [4] and [19]. Even though there is no complete classification of the elements of all Hecke groups, there have been attempts by various authors towards it (see [2], [13], [14], [15], [16], [17], and [20]). A family of subgroups of $\mathcal{H}(\sqrt{m})$ defined by one congruence relation are given by

$$\mathcal{H}_0^m(N) = \{M \in \mathcal{H}(\sqrt{m}) : c \equiv 0 \pmod{N}\} \quad (N \in \mathbb{N}).$$

For $m = 1$, $\mathcal{H}_0^m(N)$ is the usual Hecke congruence subgroups $\Gamma_0(N)$ and their index and parabolic class number can be found in [10]. For the general case $m \neq 1$, Keskin [6] showed that $\mathcal{H}_0^m(N)$ is a subgroup of finite index in $\mathcal{H}(\sqrt{m})$ and he gave their parabolic class numbers. It is our interest to introduce a subgroup of the above Fuchsian groups defined using two linear congruences. These subgroups (for $m = 1$) were first introduced by Ludwig ([9]) in his study of congruence restricted modular forms. He showed that if $f(z)$ is a modular form on a congruence subgroup $\Gamma_0(N)$, then the function $f(z; r, t)$ obtained by summing over the terms of the Fourier series expansion of $f(z)$ with index congruent to r modulo t is itself a modular form on a (smaller) congruence subgroup defined below. However, very little is known about them.

A family of subgroups of the modular group, denoted by $\Gamma_{0,n}(N)$, are defined using two linear congruences by

$$\Gamma_{0,n}(N) = \{M \in \Gamma(1) : c \equiv 0 \pmod{N} \text{ and } a \equiv d \pmod{n}\}.$$

The set $\Gamma_{0,n}(N)$ is a subgroup of $\Gamma(1)$ if and only if $n|N$. It is easy to see that if $n|N$, then $\Gamma_{0,n}(N)$ is a subgroup of $\Gamma(1)$. Conversely, if $\Gamma_{0,n}(N)$ is a subgroup of $\Gamma(1)$, then

$$\begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ N & 1+N \end{pmatrix} \in \Gamma_{0,n}(N).$$

This implies that $N \equiv 0 \pmod{n}$.

We will analogously define subgroups of the Fuchsian groups $\mathcal{H}(\sqrt{m})$ using two linear congruences as follows. For any two positive integers n and N with the property that $n|N$, define

$$\mathcal{H}_{0,n}^m(N) = \{M \in \mathcal{H}(\sqrt{m}) : c \equiv 0 \pmod{N} \text{ and } a \equiv d \pmod{n}\}.$$

One can easily show that $\mathcal{H}_{0,n}^m(N)$ is a subgroup of $\mathcal{H}(\sqrt{m})$ for any $m \in \mathbb{N}$.

It is the object of this article to determine the index of $\mathcal{H}_{0,n}^m(N)$ in $\mathcal{H}(\sqrt{m})$ and the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ for any squarefree integer m .

2. INDEX OF $\mathcal{H}_{0,n}^m(N)$ IN $\mathcal{H}(\sqrt{m})$

From now on, m will stand for a squarefree natural number and $\mathcal{H}_e^m$ stands for the subgroup of $\mathcal{H}(\sqrt{m})$ defined by

$$\mathcal{H}_e^m = \left\{ M = \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} : M \in \mathcal{H}(\sqrt{m}) \right\}.$$

We call $\mathcal{H}_e^m$ the even subgroup of $\mathcal{H}(\sqrt{m})$ (see [2, p. 61]). We will often make use of the following basic lemmas whose proofs are omitted as they are straightforward consequences of the above definitions.

Lemma 2.1. $\mathcal{H}_{0,n}^m(N)$ is a normal subgroup of $\mathcal{H}_0^m(N)$.

Lemma 2.2. For $m > 1$, the even subgroup $\mathcal{H}_e^m$ is a normal subgroup of $\mathcal{H}(\sqrt{m})$ of index 2 and

$$\mathcal{H}(\sqrt{m}) = \mathcal{H}_e^m \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{m} & m-1 \\ 1 & \sqrt{m} \end{pmatrix} \right\}.$$

We want to determine the index of the subgroups $\mathcal{H}_{0,n}^m(N)$ in $\mathcal{H}(\sqrt{m})$.

Lemma 2.3. If $\gcd(m, N) > 1$, then

$$[\mathcal{H}(\sqrt{m}) : \mathcal{H}_{0,n}^m(N)] = 2[\Gamma_0(m) : \Gamma_{0,n}(mN)],$$

where $[\Gamma_0(m) : \Gamma_{0,n}(mN)]$ will be determined later in Lemma 2.6.

Proof. We want to show that $\mathcal{H}_{0,n}^m(N) \subset \mathcal{H}_e^m$. If $M = \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix} \in \mathcal{H}_{0,n}^m(N)$, then $adm - bc = 1$, $N|c$, and $ad \neq 0$. This implies that $\gcd(m, N) = 1$, which is a contradiction. Therefore

$$\mathcal{H}_{0,n}^m(N) \subset \mathcal{H}_e^m.$$

Next we will define a group isomorphism to complete the proof of the lemma. Define a mapping

$$\Phi : \mathcal{H}_e^m \longrightarrow \Gamma_0(m)$$

by

$$\Phi \left(\begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} \right) = \begin{pmatrix} a & b \\ cm & d \end{pmatrix}.$$

It can be easily shown that Φ is a group isomorphism and

$$\Phi(\mathcal{H}_{0,n}^m(N)) = \Gamma_{0,n}(mN).$$

By the Lattice Isomorphism Theorem (see [3]) we get

$$[\mathcal{H}_e^m : \mathcal{H}_{0,n}^m(N)] = [\Gamma_0(m) : \Gamma_{0,n}(mN)]$$

and hence by Lemma 2.2 we get

$$[\mathcal{H}(\sqrt{m}) : \mathcal{H}_{0,n}^m(N)] = 2[\Gamma_0(m) : \Gamma_{0,n}(mN)].$$

Lemma 2.4. Let $\gcd(m, N) = 1$. Then

$$\mathcal{H}_{0,n}^m(N) \subseteq \mathcal{H}_e^m$$

if and only if the quadratic congruence

$$x^2 \equiv m \pmod{n}$$

has no solution.

Proof.

($\Leftarrow$) Suppose that the quadratic congruence

$$x^2 \equiv m \pmod{n}$$

has no solution. Then the congruence

$$x^2 \equiv \overline{m} \pmod{n},$$

where $m\overline{m} \equiv 1 \pmod{n}$, has no solution. If

$$\begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix} \in \mathcal{H}_{0,n}^m(N),$$

then $a^2 \equiv \overline{m} \pmod{n}$, which is a contradiction. Thus,

$$\mathcal{H}_{0,n}^m(N) \subseteq \mathcal{H}_e^m.$$

($\Rightarrow$) Suppose that the quadratic congruence

$$x^2 \equiv m \pmod{n}$$

has a solution. If $\overline{m}$ is a positive integer such that $m\overline{m} \equiv 1 \pmod{n}$, then the congruence

$$x^2 \equiv \overline{m} \pmod{n}$$

has a solution. Let a_0 be a solution to the above quadratic congruence. Since $n|N$, we can express N as $N = n \cdot n_1 \cdot N_1$, where $\gcd(n, N_1) = 1$ and every prime factor of n_1 is a prime factor of n . For all $k \in \mathbb{Z}$, we have $\gcd(a_0 + knn_1, nn_1) = 1$. Moreover, there exists a nonnegative integer l such that

$$\gcd(a_0 + lnn_1, N_1) = 1$$

and hence

$$\gcd(a_0 + lnn_1, N) = 1.$$

From the above arguments one can easily show that $\gcd((a_0 + lnn_1)^2m, N) = 1$. There exist two integers u and v in $\mathbb{Z}$ such that $(a_0 + lnn_1)^2mu - Nv = 1$. If

$$M = \begin{pmatrix} (a_0 + lnn_1)u\sqrt{m} & v \\ N & (a_0 + lnn_1)\sqrt{m} \end{pmatrix},$$

then $M \in \mathcal{H}_0^m(N)$. Since $(a_0 + lnn_1)^2mu - Nv = 1$, we have

$$(a_0 + lnn_1)^2mu \equiv 1 \pmod{n}.$$

Since $a_0^2 \equiv \overline{m} \pmod{n}$, we have

$$(a_0 + lnn_1)^2m \equiv 1 \pmod{n}.$$

Combining the above two congruences we get

$$u \equiv 1 \pmod{n}$$

and hence

$$(a_0 + lnn_1)u \equiv (a_0 + lnn_1) \pmod{n}.$$

Therefore $M \in \mathcal{H}_{0,n}^m(N)$. This completes the proof of the lemma.

Lemma 2.5. *If $\gcd(m, N) = 1$, then*

$$\left[\mathcal{H}(\sqrt{M}) : \mathcal{H}_{0,n}^m(N) \right] = \delta(m, n, N) [\Gamma_0(m) : \Gamma_{0,n}(mN)],$$

where

$$\delta(m, n, N) = \begin{cases} 1 & \text{if } x^2 \equiv m \pmod{n} \text{ has a solution,} \\ 2 & \text{if } x^2 \equiv m \pmod{n} \text{ has no solution.} \end{cases}$$

Proof. In this case the subgroup $\mathcal{H}_{0,n}^m(N)$ may not be contained in $\mathcal{H}_e^m$. Let Φ be the isomorphism defined in the proof of Lemma 2.3. If

$$\mathcal{H}_1 = \mathcal{H}_e^m \cap \mathcal{H}_0^m(N)$$

and

$$\mathcal{H}_2 = \mathcal{H}_e^m \cap \mathcal{H}_{0,n}^m(N),$$

then it can be easily shown that

$$\Phi(\mathcal{H}_1) = \Gamma_0(mN),$$

$$\Phi(\mathcal{H}_2) = \Gamma_{0,n}(mN).$$

By the Lattice Isomorphism Theorem (see [3]) we get

$$[\mathcal{H}_e^m : \mathcal{H}_1] = [\Gamma_0(m) : \Gamma_0(mN)],$$

$$[\mathcal{H}_1 : \mathcal{H}_2] = [\Gamma_0(mN) : \Gamma_{0,n}(mN)]$$

and

$$\begin{aligned} (2) \quad [\mathcal{H}(\sqrt{m}) : \mathcal{H}_{0,n}^m(N)] &= \frac{[\mathcal{H}(\sqrt{m}) : \mathcal{H}_2]}{[\mathcal{H}_{0,n}^m(N) : \mathcal{H}_2]} \\ &= \frac{[\mathcal{H}(\sqrt{m}) : \mathcal{H}_e^m] [\mathcal{H}_e^m : \mathcal{H}_1] [\mathcal{H}_1 : \mathcal{H}_2]}{[\mathcal{H}_{0,n}^m(N) : \mathcal{H}_2]} \\ &= \frac{2 [\Gamma_0(m) : \Gamma_0(mN)] [\Gamma_0(mN) : \Gamma_{0,n}(mN)]}{[\mathcal{H}_{0,n}^m(N) : \mathcal{H}_2]} \\ &= \frac{2 [\Gamma_0(m) : \Gamma_{0,n}(mN)]}{[\mathcal{H}_{0,n}^m(N) : \mathcal{H}_2]}. \end{aligned}$$

Hence, by using Lemma 2.4 we obtain

$$\begin{aligned} &[\mathcal{H}(\sqrt{m}) : \mathcal{H}_{0,n}^m(N)] \\ &= \begin{cases} [\Gamma_0(m) : \Gamma_{0,n}(mN)] & \text{if } x^2 \equiv m \pmod{n} \text{ has a solution,} \\ 2 [\Gamma_0(m) : \Gamma_{0,n}(mN)] & \text{if } x^2 \equiv m \pmod{n} \text{ has no solution.} \end{cases} \end{aligned}$$

Lemma 2.6. *If*

$$\begin{aligned} n &= 2^s p_1^{v_1} p_2^{v_2} \cdots p_t^{v_t}, \\ N &= 2^{s+\theta} p_1^{v_1+\theta_1} p_2^{v_2+\theta_2} \cdots p_t^{v_t+\theta_t} \underbrace{p_{t+1}^{\beta_{t+1}} \cdots p_r^{\beta_r}}_{N_1}, \end{aligned}$$

then

$$[\Gamma(1) : \Gamma_{0,n}(N)] = \frac{\phi(n)\Psi(N)}{\mathcal{K}(n)},$$

where $\phi(n)$ is the Euler's totient function, $\Psi(q) = q \prod_{p|q} \left(1 + \frac{1}{p}\right)$, and $\mathcal{K}(n)$ is the number of inequivalent solutions of the quadratic congruence $x^2 \equiv 1 \pmod{n}$; $\mathcal{K}(n)^1$ is given by

$$(3) \quad \mathcal{K}(n) = \begin{cases} 2^t & \text{if } s = 0, 1, \\ 2^{t+1} & \text{if } s = 2, \\ 2^{t+2} & \text{if } s \geq 3. \end{cases}$$

Proof. Suppose that N and n are as given in the hypothesis and let $N_0 = 2^{s+\theta} p_1^{v_1+\theta_1} p_2^{v_2+\theta_2} \dots p_t^{v_t+\theta_t}$. Clearly $n|N_0$, n and N_0 have the same set of prime factors, and $\gcd(N_0, N_1) = 1$.

Since

$$\frac{\phi(n)\Psi(N)}{\mathcal{K}(n)} = \frac{\frac{1}{2}N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)}{\frac{1}{2}N\mathcal{K}(n)\phi(N_1)\frac{N}{nN_1}},$$

and the principal congruence subgroup of level N ,

$$\Gamma(N) = \{M \in \Gamma(1) : a \equiv d \equiv 1 \pmod{N}, \quad c \equiv b \equiv 0 \pmod{N}\},$$

is a subgroup of $\Gamma_{0,n}(N)$ such that (see [5] and [12])

$$[\Gamma(1) : \Gamma(N)] = \frac{1}{2}N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right); \text{ for } N \geq 3,$$

it is enough to show that

$$[\Gamma_{0,n}(N) : \Gamma(N)] = \frac{1}{2}N\mathcal{K}(n)\phi(N_1)\frac{N}{nN_1}.$$

Following the approach taken by Rankin [12] the index of $\Gamma(N)$ in $\Gamma_{0,n}(N)$ is the same as half (since the latter group viewed as a group of matrices over integers contains $-I$) of the number of incongruent solutions, modulo N , to the system of congruences

$$(4) \quad \begin{aligned} c &\equiv 0 \pmod{N}, \\ ad - bc &\equiv 1 \pmod{N}, \\ a &\equiv d \pmod{n}. \end{aligned}$$

Since there are N distinct choices for b , it is enough to show that the number of incongruent solutions, modulo N , to the system of congruences

$$(5) \quad \begin{aligned} ad &\equiv 1 \pmod{N}, \\ a &\equiv d \pmod{n} \end{aligned}$$

$$\text{is } \left(\frac{N}{nN_1}\right) \cdot \mathcal{K}(n) \cdot \phi(N_1).$$

Note that the system of congruences

$$(6) \quad \begin{aligned} ad &\equiv 1 \pmod{N_0}, \\ a &\equiv d \pmod{n} \end{aligned}$$

¹Convention: $\phi(1) = \mathcal{K}(1) = 1$

has $\left(\frac{N_0}{n}\right) \mathcal{K}(n)$ incongruent solutions modulo N_0 . Suppose that (a_0, d_0) is a solution to the system (6). Then there are $\phi(N_1)$ incongruent solutions (a, d) to the system of congruences (5) such that $a \equiv a_0 \pmod{N_0}$ and $d \equiv d_0 \pmod{N_0}$. To prove this claim first note that the set

$$\{a_0, a_0 + N_0, a_0 + 2N_0, \dots, a_0 + (N_1 - 1)N_0\}$$

forms a complete residue system modulo N_1 . Therefore there exist $\phi(N_1)$ nonnegative integers, say $l_1, l_2, \dots, l_{\phi(N_1)}$, less than N_1 such that the set

$$\{a_0 + l_1 N_0, a_0 + l_2 N_0, \dots, a_0 + l_{\phi(N_1)} N_0\}$$

forms a reduced residue system modulo N_1 .

Since $\gcd(N_1, N_0) = 1$, $\gcd(a_0 + l_j N_0, N_0) = 1$, and $\gcd(a_0 + l_j N_0, N_1) = 1$, we have $\gcd(a_0 + l_j N_0, N) = 1$ for all $1 \leq j \leq \phi(N_1)$. For each $1 \leq j \leq \phi(N_1)$ there exists a positive integer D_j , $1 \leq D_j \leq N - 1$, such that

$$(a_0 + l_j N_0) D_j \equiv 1 \pmod{N}.$$

We want to show that $D_j = d_0 + s_j N_0$ for some $0 \leq s_j \leq N_1 - 1$. Using the Euclidean division algorithm, one can write

$$D_j = d_j + s_j N_0,$$

where $0 \leq d_j \leq N_0 - 1$ and $0 \leq s_j \leq N_1 - 1$. Since

$$(a_0 + l_j N_0) D_j \equiv 1 \pmod{N}$$

we get

$$(a_0 + l_j N_0)(d_j + s_j N_0) \equiv 1 \pmod{N}$$

which implies

$$a_0 d_j \equiv 1 \pmod{N_0}.$$

Since

$$a_0 d_0 \equiv 1 \pmod{N_0},$$

we get $d_j = d_0$. This completes the proof of the claim. Therefore, each solution to the system of congruences (6) gives rise to $\phi(N_1)$ incongruent solutions to the system of congruences (5). Thus, the system of congruences

$$(7) \quad ad \equiv 1 \pmod{N},$$

$$(8) \quad a \equiv d \pmod{n},$$

has $\mathcal{K}(n) \cdot \phi(N_1) \cdot \left(\frac{N}{nN_1}\right)$ incongruent solutions modulo N and hence the system

$$(9) \quad c \equiv 0 \pmod{N},$$

$$(10) \quad ad - bc \equiv 1 \pmod{N},$$

$$(11) \quad a \equiv d \pmod{n},$$

has $N \cdot \mathcal{K}(n) \cdot \phi(N_1) \cdot \left(\frac{N}{nN_1}\right)$ incongruent solutions modulo N . So for any n and N satisfying the given description we showed that

$$[\Gamma(1) : \Gamma_{0,n}(N)] = \frac{\frac{1}{2} N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)}{\frac{N^2 \mathcal{K}(n) \phi(N_1)}{2nN_1}} = \frac{\phi(n) \Psi(N)}{\mathcal{K}(n)}.$$

The following corollary is an immediate consequence of the above lemma.

Corollary 1. *If $n|N$, then $\Gamma_{0,n}(N)$ is a normal subgroup of $\Gamma_0(N)$ with*

$$[\Gamma_0(N) : \Gamma_{0,n}(N)] = \frac{\phi(n)}{\mathcal{K}(n)}.$$

Moreover,

$$\Gamma_{0,n}(N) = \Gamma_0(N) \Leftrightarrow \phi(n) = \mathcal{K}(n) \Leftrightarrow n|24.$$

The following corollary is an immediate consequence of the above lemma and Theorem 4.2.5 [10].

Corollary 2. *Let N be any positive integer and let*

$$\Gamma_1(N) = \{M \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N}\}.$$

Then the following are true:

- (a) $\Gamma_1(N) \subseteq \Gamma_0(N)$ and $[\Gamma_0(N) : \Gamma_1(N)] = \frac{\phi(N)}{2}$ ($N > 2$).
- (b) $\Gamma_1(N) \subseteq \Gamma_{0,N}(N) \subseteq \Gamma_{0,n}(N)$ for any $n|N$ and

$$[\Gamma_{0,n}(N) : \Gamma_1(N)] = \frac{N\mathcal{K}(n)\phi(N_1)}{2nN_1},$$

where N_1 is the largest positive divisor of N that is relatively prime to n ($N > 2$).

- (c) $\Gamma_1(N) = \Gamma_{0,N}(N) \Leftrightarrow \mathcal{K}(N) = 2 \Leftrightarrow N = 4$ or $N = p^k$ or $N = 2p^k$ for some odd prime p and $k \in \mathbb{N}$.

Theorem 2.1. *For any two positive integers n and N such that $n|N$, we have*

$$\left[\mathcal{H}(\sqrt{M}) : \mathcal{H}_{0,n}^m(N) \right] = \delta(m, n, N) \frac{\phi(n)\Psi\left(\frac{N}{\gcd(m, N)}\right) \gcd(m, N)}{\mathcal{K}(n)},$$

where

$$\delta(m, n, N) = \begin{cases} 2 & \text{if } \gcd(m, N) > 1, \\ 1 & \text{if } \gcd(m, N) = 1 \text{ \& } x^2 \equiv m \pmod{n} \text{ has a solution,} \\ 2 & \text{if } \gcd(m, N) = 1 \text{ \& } x^2 \equiv m \pmod{n} \text{ has no solution.} \end{cases}$$

Proof. The proof follows from Lemmas 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, and Corollary 1.

$$\begin{aligned} \left[\mathcal{H}(\sqrt{M}) : \mathcal{H}_{0,n}^m(N) \right] &= \delta(m, n, N) [\Gamma_0(m) : \Gamma_{0,n}(mN)] \\ &= \delta(m, n, N) [\Gamma_0(m) : \Gamma_0(mN)] [\Gamma_0(mN) : \Gamma_{0,n}(mN)] \\ &= \delta(m, n, N) \frac{\Psi(mN)}{\Psi(m)} \frac{\phi(n)}{\mathcal{K}(n)} \\ &= \delta(m, n, N) \frac{\phi(n)}{\mathcal{K}(n)} \Psi\left(\frac{N}{\gcd(m, N)}\right) \gcd(m, N). \end{aligned}$$

The result obtained by Keskin [6] is a corollary of the above theorem.

Corollary 3. *For any positive integer N , the set $\mathcal{H}_0^m(N)$ is a subgroup of $\mathcal{H}(\sqrt{m})$ and its index in $\mathcal{H}(\sqrt{m})$ is given by*

$$[\mathcal{H}(\sqrt{m}) : \mathcal{H}_0^m(N)] = \begin{cases} N \prod_{p|N} (1 + \frac{1}{p}) & \text{if } \gcd(m, N) = 1, \\ 2N \prod_{\substack{p|N \\ p \nmid m}} (1 + \frac{1}{p}) & \text{if } \gcd(m, N) > 1. \end{cases}$$

Proof. It is easy to show that $\mathcal{H}_0^m(N) = \mathcal{H}_{0,n}^m(N)$ for $n = 1$. By Theorem 2.1, we obtain

$$[\mathcal{H}(\sqrt{m}) : \mathcal{H}_0^m(N)] = \begin{cases} \Psi(N) & \text{if } \gcd(m, N) = 1, \\ 2\Psi\left(\frac{N}{\gcd(m, N)}\right) \gcd(m, N) & \text{if } \gcd(m, N) > 1. \end{cases}$$

This completes the proof of the corollary.

Corollary 4. *For any positive integers n and N with $n|N$, $\mathcal{H}_{0,n}^m(N)$ is a normal subgroup of $\mathcal{H}_0^m(N)$ and*

$$[\mathcal{H}_0^m(N) : \mathcal{H}_{0,n}^m(N)] = \begin{cases} \delta(m, n, N) \frac{\phi(n)}{\mathcal{K}(n)} & \text{if } \gcd(m, N) = 1, \\ \frac{\phi(n)}{\mathcal{K}(n)} & \text{if } \gcd(m, N) > 1. \end{cases}$$

3. THE PARABOLIC CLASS NUMBER

Let Γ be a Fuchsian group. If $r \in \mathbb{R} \cup \{\infty\}$ is fixed by a parabolic element of Γ , then we say that r is a parabolic point or a cusp of Γ . For any point $\tau \in \overline{\mathbb{H}}$, the sets

$$\Gamma_\tau = \{g \in \Gamma : g(\tau) = \tau\} \quad \text{and} \quad \Gamma\tau = \{g(\tau) : g \in \Gamma\}$$

are called the stabilizer of τ and the Γ -orbit of τ , respectively. It is not terribly difficult to show that if r is a parabolic point of Γ , then its stabilizer contains only parabolic elements of Γ . Also, if $\mathcal{D} \subset \overline{\mathbb{H}}$ and $\mathcal{D}$ is itself a Γ -orbit, then we say that Γ acts transitively on $\mathcal{D}$. If Γ acts transitively on $\mathcal{D}$, then all the stabilizers of elements of $\mathcal{D}$ are conjugates, since

$$\Gamma_{g(d)} = g\Gamma_d g^{-1}$$

for any $g \in \Gamma$ and any $d \in \mathcal{D}$.

We now give a theorem from [10], which is related to the parabolic points of Γ and all its finite index subgroups.

Theorem 3.1. (a) *If $x \in \mathbb{R} \cup \{\infty\}$ is a cusp of Γ , then there exist $L \in PSL(2, \mathbb{R})$ and $h > 0$ such that $L(\infty) = x$ and*

$$\Gamma_x = L \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle L^{-1}.$$

(b) *If Γ' is a subgroup of Γ of finite index, then the set of cusps of Γ' is the same as that of Γ .*

Let

$$\sqrt{m}\hat{\mathbb{Q}} = \left\{ \frac{u}{v}\sqrt{m} : \frac{u}{v} \in \mathbb{Q}, \gcd(u, v) = 1 \right\} \cup \{\infty\}.$$

Then the set of parabolic points of $\mathcal{H}(\sqrt{m})$ is $\sqrt{m}\hat{\mathbb{Q}}$. For any subgroup Γ of finite index in $\mathcal{H}(\sqrt{m})$, there exist a finite number of pairwise disjoint Γ -orbits, say,

$$\Gamma\mathfrak{a}_1, \dots, \Gamma\mathfrak{a}_\lambda$$

such that

$$\sqrt{m}\hat{\mathbb{Q}} = \bigcup_{k=1}^{\lambda} \Gamma\mathfrak{a}_k.$$

The natural number λ is called the parabolic class number of Γ .

First we will calculate the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ when $m = 1$. For $m = 1$, we have

$$\mathcal{H}(\sqrt{m}) = \Gamma(1) \quad \text{and} \quad \mathcal{H}_{0,n}^m(N) = \Gamma_{0,n}(N).$$

To calculate the parabolic class number of $\Gamma_{0,n}(N)$, we will use the set of inequivalent parabolic points of a larger subgroup, namely the Hecke congruence subgroup $\Gamma_0(N)$. Note that $\Gamma_{0,n}(N)$ is a normal subgroup of $\Gamma_0(N)$. The set of inequivalent cusps of $\Gamma_0(N)$, denoted by $\mathcal{P}_0(N)$, is given by (see [5, §2.4]),

$$(12) \quad \mathcal{P}_0(N) = \left\{ \frac{u}{v} : \gcd(u, v) = 1, \ v|N, \ u \left(\bmod \gcd\left(v, \frac{N}{v}\right) \right) \right\}.$$

The period (cusp width) of the parabolic point $\frac{u}{v}$ is $\frac{N}{\gcd(v^2, N)}$. The parabolic class number of $\Gamma_0(N)$ is given by

$$\sigma_\infty(N) = \sum_{d|N} \phi\left(\gcd(d, \frac{N}{d})\right).$$

The following lemma, which can be found in [8] and also in [10] in a more general setting, which is also true for any Fuchsian group G , will be useful in this article.

Lemma 3.1. *Let G and H be subgroups of finite index in the modular group $\Gamma(1)$ and H is a normal subgroup of G . For a cusp q of G , the number of H -inequivalent cusps which are G -equivalent to q is equal to*

$$(13) \quad \frac{[G : H]}{[G_q : H_q]}.$$

Proof. Suppose that λ is the smallest natural number such that $M = LS^\lambda L^{-1} \in G$ and $G_q = \langle M \rangle$ and let $\mu = [G : H]$. Let $n = \min \{k \in \mathbb{N} : M^k \in H\} = [G_q : H_q]$. Then there exist a finite number of elements of G , say $L_1, L_2, \dots, L_r$, such that

$$G = \bigcup_{k=1}^r H \{L_k, L_k M, \dots, L_k M^{n-1}\}$$

and

$$\mu = nr.$$

Therefore the number of H -inequivalent cusps that are G -equivalent to q is given by

$$r = \frac{\mu}{n} = \frac{[G : H]}{[G_q : H_q]}.$$

This completes the proof of the lemma.

Taking $\Gamma_0(N)$ as G , $\Gamma_{0,n}(N)$ as H and $\frac{u}{v}$ as q we get:

Lemma 3.2. *Let N be a natural number and n be a positive divisor of N . If $\frac{u}{v} \in \mathcal{P}_0(N)$, then the number of $\Gamma_{0,n}(N)$ -inequivalent cusps which are $\Gamma_0(N)$ -equivalent to $\frac{u}{v}$ is equal to*

$$(14) \quad \frac{\phi(n)}{n\mathcal{K}(n)} \cdot \gcd\left(n, \frac{2Nu}{\gcd\left(v, \frac{N}{v}\right)}\right).$$

Proof. For convenience let $\Gamma = \Gamma_0(N)$ and $\Gamma' = \Gamma_{0,n}(N)$. For $\mathfrak{a} = \frac{u}{v} \in \mathcal{P}_0(N)$, the set of elements of Γ fixing $\mathfrak{a}$ is a cyclic group given by

$$\Gamma_{\mathfrak{a}} = \left\langle \begin{pmatrix} 1 - muv & mu^2 \\ -mv^2 & 1 + muv \end{pmatrix} \right\rangle,$$

where $m = \frac{N}{\gcd(N, v^2)}$. Since Γ' is a subgroup of Γ of finite index, there exists a smallest natural number h such that

$$\Gamma'_{\mathfrak{a}} = \left\langle \begin{pmatrix} 1 - muv & mu^2 \\ -mv^2 & 1 + muv \end{pmatrix}^h \right\rangle = \left\langle \begin{pmatrix} 1 - hmuv & hmu^2 \\ -hmv^2 & 1 + hmuv \end{pmatrix} \right\rangle.$$

That means h is the smallest natural number such that

$$1 - hmuv \equiv 1 + hmuv \pmod{n}.$$

Thus,

$$h = \frac{n}{\gcd(n, 2muv)} = \frac{n}{\gcd\left(n, \frac{2Nu}{\gcd(v, N/v)}\right)}.$$

The number of Γ' -inequivalent cusps that are Γ -equivalent to $\mathfrak{a}$, by Lemma 3.1, is given by

$$\frac{[\Gamma : \Gamma']}{h} = \frac{\phi(n)}{\mathcal{K}(n)} \cdot \frac{\gcd\left(n, \frac{2Nu}{\gcd(v, N/v)}\right)}{n}.$$

This completes the proof of the lemma.

To simplify some of the calculation we are about to see, let us introduce a set, denoted by $\mathcal{M}(v, N)$, of reduced residue system modulo $\gcd\left(v, \frac{N}{v}\right)$ containing only nonnegative integers that are relatively prime to v , where $v|N$. One can easily verify that if

- (a) $v = p^\theta v_1$ and $N = p^\beta N_1$, where $(p, v_1) = (p, N_1) = 1$, $0 \leq \theta \leq \beta$, and $v_1|N_1$;
- (b) $\mathcal{M}(p^\theta, p^\beta) = \{b_1, b_2, \dots, b_{\phi(p^\delta)}\}$ and $\mathcal{M}(v_1, N_1) = \{u_1, u_2, \dots, u_{\phi(g)}\}$,
where $\delta = \min\{\theta, \beta - \theta\}$ and $g = \gcd\left(v_1, \frac{N_1}{v_1}\right)$.

Then, the set

$$\{u_k p^\theta + b_j v_1 : 1 \leq k \leq \phi(g), 1 \leq j \leq \phi(p^\delta)\}$$

can be taken as $\mathcal{M}(v, N)$. Thus, we can rewrite the set of inequivalent cusps of $\Gamma_0(N)$ as

$$(15) \quad \mathcal{P}_0(N) = \left\{ \frac{u}{v} : v|N, u \in \mathcal{M}(v, N) \right\}.$$

Lemma 3.3. *The parabolic class number of the congruence subgroup $\Gamma_{0,n}(N)$, denoted by $\sigma_\infty(n, N)$, is given by*

$$(16) \quad \sigma_\infty(n, N) = \frac{\phi(n)}{n\mathcal{K}(n)} \cdot \sum_{v|N} \sum_{u \in \mathcal{M}(v, N)} \gcd \left(n, \frac{2Nu}{\gcd \left(v, \frac{N}{v} \right)} \right),$$

where $\mathcal{M}(v, N)$ is as defined above.

Proof. Use Lemma 3.2 and (15).

Lemma 3.4. *Let $n = p^\alpha n_1$ and $N = p^\beta N_1$, where $(n_1, p) = (N_1, p) = 1$ and $n|N$. If $v = p^\theta v_1$, with $\gcd(p, v_1) = 1$, is a divisor of N , then*

$$(17) \quad \sum_{u \in \mathcal{M}(v, N)} \gcd \left(n, \frac{2Nu}{\gcd \left(v, \frac{N}{v} \right)} \right) = \phi(p^{\delta_1}) p^{\delta_2} \cdot \sum_{u \in \mathcal{M}(v_1, N_1)} \gcd \left(n_1, \frac{2N_1 u}{\gcd \left(v, \frac{N_1}{v} \right)} \right),$$

where

$$(18) \quad \begin{aligned} \delta_1 &= \min \{ \theta, \beta - \theta \}, \\ \delta_2 &= \begin{cases} \min \{ \alpha, \beta + 1 - \delta_1 \} & \text{if } p = 2, \\ \min \{ \alpha, \beta - \delta_1 \} & \text{otherwise.} \end{cases} \end{aligned}$$

Proof. Suppose that p is an odd prime and δ_1 and δ_2 are as defined in the lemma. Let

$$\mathcal{M}(p^\theta, p^\beta) = \{b_1, b_2, \dots, b_{\phi(p^{\delta_1})}\}$$

and

$$\mathcal{M}(v_1, N_1) = \{u_1, u_2, \dots, u_{\phi(g)}\},$$

where $g = \gcd(v_1, N_1/v_1)$. Then the set

$$\{u_k p^\theta + b_j v_1 : 1 \leq k \leq \phi(g), 1 \leq j \leq \phi(p^{\delta_1})\}$$

can be taken as $\mathcal{M}(v, N)$. First note that $\gcd \left(v, \frac{N}{v} \right) = p^{\delta_1} g$ and

$$\begin{aligned} \gcd \left(n, \frac{2Nu}{\gcd \left(v, \frac{N}{v} \right)} \right) &= \gcd \left(p^\alpha n_1, \frac{2p^\beta N_1 u}{p^{\delta_1} g} \right) \\ &= \gcd(p^\alpha, p^{\beta - \delta_1}) \gcd \left(n_1, \frac{2N_1 u}{g} \right) \\ &= p^{\delta_2} \gcd \left(n_1, \frac{2N_1 u}{g} \right). \end{aligned}$$

If $u = u_k p^\theta + b_j v_1$, then

$$\gcd\left(n_1, \frac{2N_1 u}{g}\right) = \gcd\left(n_1, \frac{2N_1 u_k p^\theta}{g} + 2N_1 b_j m\right) = \gcd\left(n_1, \frac{2N_1 u_k}{g}\right),$$

where $m = \frac{v_1}{g}$. Therefore

$$\begin{aligned} \sum_{u \in \mathcal{M}(v, N)} \gcd\left(n, \frac{2Nu}{\gcd\left(v, \frac{N}{v}\right)}\right) &= \sum_{k=1}^{\phi(g)} \sum_{j=1}^{\phi(p^{\delta_1})} p^{\delta_2} \gcd\left(n_1, \frac{2N_1 u_k}{g}\right) \\ &= \phi(p^{\delta_1}) p^{\delta_2} \sum_{k=1}^{\phi(g)} \gcd\left(n_1, \frac{2N_1 u_k}{g}\right) \\ &= \phi(p^{\delta_1}) p^{\delta_2} \sum_{u \in \mathcal{M}(v_1, N_1)} \gcd\left(n_1, \frac{2N_1 u}{g}\right). \end{aligned}$$

The proof is similar for the case $p = 2$.

Lemma 3.5. *If p is a prime and $\alpha, \beta \in \mathbb{N}$ such that $\alpha \leq \beta$, then*

$$\begin{aligned} \Delta_p(\alpha, \beta) &:= \sum_{\substack{\theta=0 \\ \delta_1 = \min\{\theta, \beta-\theta\} \\ \delta_2 = \min\{\alpha, \beta^* - \delta_1\}}}^{\beta} \phi(p^{\delta_1}) p^{\delta_2} \\ &= \begin{cases} (p+1)p^{\alpha+l-1} & \text{if } 2\alpha \leq \beta = 2l, \\ 2p^{\alpha+l} & \text{if } 2\alpha \leq \beta = 2l+1, \\ [(2\alpha - \beta^* + 1)(p-1) + 2 - (\beta^* - \beta)]p^{\beta^*-1} & \text{if } 2\alpha > \beta, \end{cases} \end{aligned}$$

$$\text{where } \beta^* = \begin{cases} \beta + 1 & \text{if } p = 2, \\ \beta & \text{otherwise.} \end{cases}$$

Proof. One can easily prove the above result by direct computation of the sum.

Theorem 3.2. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} N_1$, where $\gcd(N_1, n) = 1$ and $n|N$. The parabolic class number of the congruence subgroup $\Gamma_{0,n}(N)$ is given by*

$$(19) \quad \sigma_\infty(n, N) = \left(\frac{\phi(n)}{n\mathcal{K}(n)} \cdot \prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \right) \sigma_\infty(N_1).$$

Proof. Rewrite n and N as follows:

$$n = p_1^{\alpha_1} n_1, \quad N = p_1^{\beta_1} N_1^*.$$

Using (12) and Lemmas 3.2, 3.3, and 3.4, we get

$$\begin{aligned} \sigma_\infty(n, N) &= \frac{\phi(n)}{n\mathcal{K}(n)} \cdot \sum_{v|N} \sum_{u \in \mathcal{M}(v, N)} \gcd \left(n, \frac{2Nu}{\gcd \left(v, \frac{N}{v} \right)} \right) \\ &= \frac{\phi(n)}{n\mathcal{K}(n)} \sum_{\theta=0}^{\beta_1} \phi(p_1^{\delta_1}) p_1^{\delta_2} \cdot \sum_{v_1|N_1^*} \sum_{u \in \mathcal{M}(v_1, N_1^*)} \gcd \left(n_1, \frac{2N_1^* u}{\gcd \left(v, \frac{N_1^*}{v} \right)} \right) \\ &= \frac{\phi(n)}{n\mathcal{K}(n)} \left(\sum_{\theta=0}^{\beta_1} \phi(p_1^{\delta_1}) p_1^{\delta_2} \right) \cdot \sum_{v_1|N_1^*} \sum_{u \in \mathcal{M}(v_1, N_1^*)} \gcd \left(n_1, \frac{2N_1^* u}{\gcd \left(v, \frac{N_1^*}{v} \right)} \right) \\ &= \frac{\phi(n)}{n\mathcal{K}(n)} \Delta_{p_1}(\alpha_1, \beta_1) \cdot \sum_{v_1|N_1^*} \sum_{u \in \mathcal{M}(v_1, N_1^*)} \gcd \left(n_1, \frac{2N_1^* u}{\gcd \left(v, \frac{N_1^*}{v} \right)} \right). \end{aligned}$$

Applying the above steps repeatedly, we get

$$\begin{aligned} \sigma_\infty(n, N) &= \frac{\phi(n)}{n\mathcal{K}(n)} \prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \cdot \sum_{v_1|N_1} \sum_{u \in \mathcal{M}(v_1, N_1)} \gcd \left(1, \frac{2N_1 u}{\gcd \left(v, \frac{N_1}{v} \right)} \right) \\ &= \frac{\phi(n)}{n\mathcal{K}(n)} \left(\prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \right) \cdot \sigma_\infty(N_1). \end{aligned}$$

Next we will calculate the parabolic class number $\sigma_\infty^m(n, N)$ of $\mathcal{H}_{0,n}^m(N)$ when m is a product of finite number of distinct primes. It is not difficult to see that all the parabolic elements of $\mathcal{H}(\sqrt{m})$ are contained in a maximal normal subgroup $\mathcal{H}_e^m$. Thus, the parabolic class number of $\mathcal{H}_e^m$ is $2\sigma_\infty^m(1, 1)$, where $\sigma_\infty^m(1, 1)$ is the parabolic class number of $\mathcal{H}(\sqrt{m})$. Consider the group isomorphism

$$\Phi : \mathcal{H}_e^m \longrightarrow \Gamma_0(m)$$

defined in the proof of Lemma 2.3 by

$$\Phi \left(\begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} \right) = \begin{pmatrix} a & b \\ cm & d \end{pmatrix}.$$

There are two cases to consider depending on whether m and N are relatively prime.

If $\gcd(m, N) > 1$, then $\mathcal{H}_{0,n}^m(N) \subset \mathcal{H}_e^m$ and hence

$$\Phi(\mathcal{H}_{0,n}^m(N)) = \Gamma_{0,n}(mN).$$

Therefore the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ is the same as the parabolic class number of $\Gamma_{0,n}(mN)$. Therefore we get the following theorem.

Theorem 3.3. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ with $n|N$. If $\gcd(m, N) > 1$ and $mN = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} N_1$ such that $\gcd(N_1, n) = 1$, then the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ is given by

$$(20) \quad \sigma_{\infty}^m(n, N) = \left(\frac{\phi(n)}{n\mathcal{K}(n)} \cdot \prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \right) \sigma_{\infty}(N_1).$$

Let $\gcd(m, N) = 1$. We have seen in Lemma 2.4 that

$$[\mathcal{H}_{0,n}^m(N) : \mathcal{H}_1] = \begin{cases} 1 & \text{if } x^2 \equiv m \pmod{n} \text{ has no solution,} \\ 2 & \text{if } x^2 \equiv m \pmod{n} \text{ has a solution,} \end{cases}$$

and

$$\Phi(\mathcal{H}_1) = \Gamma_{0,n}(mN)$$

where

$$\mathcal{H}_1 = \mathcal{H}_e^m \cap \mathcal{H}_{0,n}^m(N).$$

Therefore the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ is either equal to or one half of the parabolic class number of $\mathcal{H}_1$. Thus,

Theorem 3.4. Let m be a product of k distinct primes and $\gcd(m, N) = 1$. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ with $n|N$ and $N = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} N_1$ such that $\gcd(N_1, n) = 1$, then the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ is given by

$$(21) \quad \sigma_{\infty}^m(n, N) = 2^{k-1} \sigma_{\infty}(n, N) \cdot \begin{cases} 2 & \text{if } x^2 \equiv m \pmod{n} \text{ has no solution,} \\ 1 & \text{if } x^2 \equiv m \pmod{n} \text{ has a solution.} \end{cases}$$

Proof. Since $\Phi(\mathcal{H}_1) = \Gamma_{0,n}(mN)$, the parabolic class number of $\mathcal{H}_1$ is given by

$$\begin{aligned} \sigma_{\infty}(n, mN) &= \left(\frac{\phi(n)}{n\mathcal{K}(n)} \cdot \prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \right) \sigma_{\infty}(mN_1) \\ &= \left(\frac{\phi(n)}{n\mathcal{K}(n)} \cdot \prod_{k=1}^r \Delta_{p_k}(\alpha_k, \beta_k) \right) \sigma_{\infty}(m) \sigma_{\infty}(N_1) \\ &= \sigma_{\infty}(n, N) \sigma_{\infty}(m) \\ &= 2^k \sigma_{\infty}(n, N). \end{aligned}$$

Therefore the parabolic class number of $\mathcal{H}_{0,n}^m(N)$ is given by

$$(22) \quad \sigma_{\infty}^m(n, N) = 2^{k-1} \sigma_{\infty}(n, N) \cdot \begin{cases} 2 & \text{if } x^2 \equiv m \pmod{n} \text{ has no solution,} \\ 1 & \text{if } x^2 \equiv m \pmod{n} \text{ has a solution.} \end{cases}$$

The results obtained by Yilmaz and Keskin [18] are given below as immediate corollaries of the above theorem.

Corollary 5. Let m be a product of k distinct primes. The parabolic class number of the Fuchsian group $\mathcal{H}(\sqrt{m})$ is 2^{k-1} and the set of inequivalent parabolic points of $\mathcal{H}(\sqrt{m})$ is given by

$$\left\{ \frac{1}{m^*} \sqrt{m} : m^* | m, m^* < \sqrt{m} \right\}.$$

Proof. Note that $\mathcal{H}(\sqrt{m}) = \mathcal{H}_{0,1}^m(1)$ and hence the parabolic class number of $\mathcal{H}(\sqrt{m})$ is given by

$$\sigma_{\infty}^m(1, 1) = 2^{k-1} \sigma_{\infty}(1, 1) = 2^{k-1}.$$

Since the set of inequivalent parabolic points of $\Gamma_0(m)$ is given by (see Equation (12))

$$\left\{ \frac{1}{m^*} : 1 \leq m^* \leq m, \quad m^* | m \right\}$$

and $\mathcal{H}_e^m = L^{-1} \cdot \Gamma_0(m) \cdot L$, where $L = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{m} \end{pmatrix}$, the set of inequivalent parabolic points of $\mathcal{H}_e^m$ is given by

$$\left\{ L^{-1} \left(\frac{1}{m^*} \right) : m^* | m \right\}$$

or

$$\left\{ \frac{1}{m^*} \sqrt{m} : m^* | m \right\}.$$

Next we want to show that if $m^* m^{**} = m$, then the parabolic point $\frac{1}{m^*} \sqrt{m}$ is equivalent to $\frac{1}{m^{**}} \sqrt{m}$ under the group $\mathcal{H}(\sqrt{m})$. If $m^* m^{**} = m$, then $\gcd(m^*, m^{**}) = 1$, because m is squarefree, and as a result there exist two integers a and b such that

$$m^{**}b - m^*a = 2.$$

Let $M = \begin{pmatrix} b\sqrt{m} & -1 - m^*a \\ 1 + m^*a & -a\sqrt{m} \end{pmatrix}$. Clearly $M \in \mathcal{H}(\sqrt{m})$ and

$$M \left(\frac{1}{m^*} \sqrt{m} \right) = \frac{1}{m^{**}} \sqrt{m}.$$

This completes the proof of the corollary.

Remark 3.1. The Fuchsian group $\mathcal{H}(\sqrt{m})$ acts transitively on the set of parabolic points $\sqrt{m}\mathbb{Q}$ if and only if m is either 1 or a prime.

Corollary 6. *Let m be a product of k distinct primes, $N \in \mathbb{N}$, and $\gcd(m, N) = 1$. The parabolic class number of the subgroup $\mathcal{H}_0^m(N)$ of $\mathcal{H}(\sqrt{m})$ is*

$$2^{k-1} \sigma_{\infty}(N)$$

and the set of inequivalent parabolic points is given by

$$\left\{ \frac{a}{bm^*} \sqrt{m} : m^* | m, m^* < \sqrt{m}, \gcd(a, b) = 1, a \left(\bmod \gcd \left(b, \frac{N}{b} \right) \right) \right\}.$$

REFERENCES

- [1] A. F. Beardon, The Geometry of Discrete Groups, *GTM, Springer* (1983). MR698777 (85d:22026)
- [2] N. Cangül and D. Singerman, Normal Subgroups of Hecke Groups and Regular Maps, *Math. Proc. Camb. Phil. Soc.*, **123** (1998), 59-74. MR1474865 (98j:20071)
- [3] D. S. Dummitt and R. M. Foote, Abstract Algebra, *Prentice Hall, Upper Saddle River, NJ* (1999). MR1138725 (92k:00007)
- [4] J. J. Hutchinson, On A Class Of Automorphic Functions, *Trans. Amer. Math. Soc.* **3** (1902), 1-11. MR1500582
- [5] H. Iwaniec, Topics in Classical Automorphic Forms, *American Mathematical Society, Providence, RI, 1997*. MR1474964 (98e:11051)

- [6] R. Keskin, On the Parabolic Class Number Of Some Subgroups Of Fuchsian Groups, *Note di Matematica*, **Vol. 19** (1999), no.2, 275-283. MR1816881 (2002a:20053)
- [7] R. Keskin, On the Parabolic Class Number Of Some Subgroups Of Hecke Groups, *Tr. J. of Maths.* **22** (1998), 199-205. MR1651026 (99j:11041)
- [8] M. I. Knopp and M. Newman, Congruence subgroups of positive genus of the modular group, *Illinois J. Math.* **9** (1965), 577-583. MR0181675 (31:5902)
- [9] K. Ludwick, Congruence Restricted Modular Forms, *Ramanujan J.* **9** (2005), no. 3, 341-355. MR2173493 (2006e:11049)
- [10] T. Miyake, Modular Forms, *Springer Verlag*, 1989. MR1021004 (90m:11062)
- [11] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction To The Theory Of Numbers, *John Wiley & Sons, New York* (1991).
- [12] R. A. Rankin, The Modular Group and its Subgroups, *Ramanujan Institute, Madras* (1969). MR0265289 (42:200)
- [13] D. Rosen, A class of continued fractions associated with certain properly discontinuous groups, *Duke Math. J.* **21** (1954), 549-563. MR0065632 (16:458d)
- [14] D. Rosen, Continued Fractions in Algebraic Number Fields, *Amer. Math. Monthly*, **Vol. 84** (1977), no. 1, 37-39. MR1538246
- [15] D. Rosen, The substitutions of Hecke group $\Gamma(2\cos(\pi/5))$, *Arch. Math.*, **46** (1986), no. 6, 533-538. MR849858 (87k:11048)
- [16] D. Rosen and T. Schmidt, Hecke group and continued fractions, *Bull. Austral. Math. Soc.*, **46** (1992), no. 3, 459-474. MR1190349 (93i:11050)
- [17] N. Yilmaz and N. Cangül, On the group structure and parabolic points of the Hecke group $H(\lambda)$, *Proc. Estonian Acad. Sci. Phys. Math.*, **51** (2002), no. 1, 35-46. MR1906718 (2003k:20082)
- [18] N. Yilmaz and R. Keskin, Proof of a conjecture related to the parabolic class numbers of some Fuchsian groups, *Acta mathematica Scientia*, **Vol. 25** (2005), no. 2, 215-222. MR2133061 (2005m:20125)
- [19] J. W. Young, On The Group Of Sign $(0, 3; 2, 4, \infty)$ And The Functions Belonging To It, *Trans. Amer. Math. Soc.* **5** (1904), 81-104. MR1500662
- [20] J. Wolfart, Eine Bemerkung über Heckes Modulgruppen, *Arch. Math.*, **29** (1977), 72-77. MR0453643 (56:11903)

DEPARTMENT OF MATHEMATICS AND STATISTICS, MURRAY STATE UNIVERSITY, MURRAY, KENTUCKY 42071

E-mail address: omer.yayenie@murraystate.edu