PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 11, Pages 3131–3140
S 0002-9939(99)05154-0
Article electronically published on May 4, 1999

NORMALIZERS OF THE CONGRUENCE SUBGROUPS OF THE HECKE GROUP G_5

MONG-LUNG LANG AND SER-PEOW TAN

(Communicated by Ronald M. Solomon)

Abstract. Let $\lambda = 2\cos(\pi/5)$ and let G be the Hecke group associated to λ. In this article, we show that for τ a prime ideal in $\mathbb{Z}[\lambda]$, the congruence subgroups $G_0(\tau)$ of G are self-normalized in $PSL_2(\mathbb{R})$.

1. Introduction

In this paper, we continue our study into the extent to which properties of the modular group hold for the Hecke groups; see [CLLT], [LLT1], [LLT2] for some previous results. We are, in particular, interested in the Hecke group G_5 which we denote by G and its congruence subgroups $G_0(\tau)$ of prime level τ. Our main result is that the groups $G_0(\tau)$ are self-normalized in $PSL_2(\mathbb{R})$. This contrasts with the case of the congruence subgroups $\Gamma_0(p)$ of the modular group Γ which admit Atkin-Lehner involutions, so have strictly larger normalizers; see for example [AL].

We recall the following definitions, notation and results. For $q \geq 4$, the Hecke groups G_q are the (discrete) subgroups $\langle w, u_q \rangle$ of $PSL_2(\mathbb{Z}[\lambda_q])$ where $\lambda_q = 2\cos(\pi/q)$ and

$$w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ u_q = \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix}.$$

When $q = 3$, we recover the modular group Γ so the above can be thought of as a natural generalization of Γ. Alternatively, we can interpret the generalization as G_q being maximal discrete subgroups whose entries are in some extension of $\mathbb{Z}$. Finally, we have the geometric interpretation: Γ is a $(2, 3, \infty)$ triangle group and the Hecke group G_q is a $(2, q, \infty)$ triangle group.

Let $\mathcal{A}$ be an ideal of $\mathbb{Z}[\lambda_q]$. We define

$$G_0(\mathcal{A}) = \{\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_q \mid c \in \mathcal{A}\}.$$

Again, this is a natural generalization of the congruence subgroups $\Gamma_0(n)$ of Γ. It works because the elements of G_q sit naturally in the ring $\mathbb{Z}[\lambda_q]$.

Recall that G_q is commensurable with $PSL_2(\mathbb{Z})$ if and only if $q = 4$ or 6. The elements of such groups are completely known; see [P], for example. The normalizer of $G_0(\mathcal{A})$ in $PSL_2(\mathbb{R})$ can be determined [LT].

Received by the editors January 10, 1998.
1991 *Mathematics Subject Classification.* Primary 11F06.
Key words and phrases. Congruence subgroups, Hecke groups.

Suppose G_q is not commensurable with $PSL_2(\mathbb{Z})$. By the results of Leutbecher, [L1], [L2], $\mathbb{Q}[\lambda] \cup \{\infty\}$ is the set of cusps of G_q if and only if $q = 5$. Also, 5 is the only q other than 4, 6 for which $\mathbb{Q}[\lambda]$ is a quadratic field. For all other q's, the degree is > 2. As a consequence, $q = 5$ is the next most workable and interesting q. Some of the classical results on the modular group can be generalized to $G = G_5$ ([CLLT], [LLT2]). The main result in this paper is the following:

Main Theorem. *If (τ) is a prime ideal of $\mathbb{Z}[\lambda] = \mathbb{Z}[\lambda_5]$, then $G_0(\tau) \leq G_5 = G$ is self-normalized in $PSL_2(\mathbb{R})$.*

The main facts used in the proof are:

(a) $\mathbb{Z}[\lambda]$ is a principal ideal domain.

(b) The set of cusps of G is $\mathbb{Q}[\lambda] \cup \{\infty\}$ ([L1], [L2]). Furthermore, if $x \in \mathbb{Q}[\lambda]$ is a cusp, x has a unique reduced form $x = \frac{a}{b}$ [LLT1]. By definition, this means that $a, b \in \mathbb{Z}[\lambda]$ with $b > 0$ and there exists $c, d \in \mathbb{Z}[\lambda]$ such that $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in G$. Clearly, $(a, b) = 1$ so that if $x = \frac{a'}{b'}$ with $(a', b') = 1$, then $a = \mu a'$, $b = \mu b'$ where μ is a unit in $\mathbb{Z}[\lambda]$.

(c) (Proposition 6 of [LLT1]) Suppose x_i, x_j are G-rationals with reduced form a_i/b_i and a_j/b_j, respectively, and suppose that $x_i < x_j$. Then the following statements are equivalent:

(i) $\begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix} \in G$;

(ii) (x_i, x_j) is an even line, that is, it is the image of the complete hyperbolic geodesic with ends at 0 and ∞ under the action of some $A \in G$;

(iii) $a_j b_i - a_i b_j = 1$.

(d) (Corollary 5 of [LLT1]) $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G$ if and only if $b = m\lambda$, $m \in \mathbb{Z}$. Similarly, $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in G$ if and only if $c = n\lambda$, $n \in \mathbb{Z}$.

The rest of this paper is organized as follows. In the next section, we give the possible forms which an element A of $N(G_0(\tau))$ can take, breaking it into different cases. In section 3, we complete the proof of the main theorem in the case where the group $G_0(\tau)$ has 2 inequivalent cusps. By [CLLT], this occurs when the rational prime p lying under τ is 5 or is congruent to $\pm 1 \pmod{10}$. Finally, in section 4, we complete the proof of the main theorem in the case where the group $G_0(\tau)$ has $p + 1$ cusps. By [CLLT], this occurs when the rational prime p lying under τ is congruent to $\pm 3 \pmod{10}$ or $p = 2$.

2. Upper bound for $N(G_0(\tau))$

Let I be a prime in $\mathbb{Z}[\lambda] = \mathbb{Z}[\lambda_5]$. Since $\mathbb{Z}[\lambda]$ is a principal ideal domain, $I = (\tau)$ for some τ. Note that we may assume that τ is positive. Let p be the positive rational prime which lies below τ. It is an easy matter to check that p is square free in $\mathbb{Z}[\lambda]$ if and only of $p \neq 5$.

Denote by $N(G_0(\tau))$ the normalizer of $G_0(\tau)$ in $PSL_2(\mathbb{R})$. For any

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N(G_0(\tau)),$$

we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - ac\lambda & a^2\lambda \\ -c^2\lambda & 1 + ac\lambda \end{pmatrix} \in G_0(\tau), \tag{2.1}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 + dc\lambda & d^2\lambda \\ -c^2\lambda & 1 - dc\lambda \end{pmatrix} \in G_0(\tau), \tag{2.2}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p\lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 + bdp\lambda & -b^2p\lambda \\ d^2p\lambda & 1 - bdp\lambda \end{pmatrix} \in G_0(\tau), \tag{2.3}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ p\lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 - abp\lambda & -b^2p\lambda \\ a^2p\lambda & 1 + abp\lambda \end{pmatrix} \in G_0(\tau). \tag{2.4}$$

In the rest of this section, we determine the possible forms that A can take (Lemmas 1–5).

Lemma 1. $N(G_0(\tau)) \cap PSL_2(\mathbb{Z}[\lambda]) = G_0(\tau)$.

Proof. For any $A \in N(G_0(\tau)) \cap PSL_2(\mathbb{Z}[\lambda])$, by (2.1), the $(2,1)$-entry of A is a multiple of τ. Hence

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

where a, b, c, $d \in \mathbb{Z}[\lambda]$. Suppose $c \neq 0$. Recall that $x = a/c\tau \in \mathbb{Q}(\lambda)$ is a cusp of G [L1], [L2]. Let $x = a'/c'$ be the reduced form for x. G contains an element of the form

$$B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Since $(a, c\tau) = 1$, $c' = \mu c\tau$ where μ is a unit of $\mathbb{Z}[\lambda]$. Hence c' is a multiple of τ. This implies that $B \in G_0(\tau) \leq N(G_0(\tau))$. Since $A\infty = B\infty$, it follows that

$$B^{-1}A = \begin{pmatrix} u & v \\ 0 & u^{-1} \end{pmatrix} \in N(G_0(\tau)),$$

where u, $v \in \mathbb{Z}[\lambda]$. Applying (2.1) and (2.2) to $B^{-1}A$, one has that

$$\begin{pmatrix} 1 & u^2\lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & u^{-2}\lambda \\ 0 & 1 \end{pmatrix}$$

are elements of $G_0(\tau)$. By Corollary 5 of [LLT1], $u = \pm 1$. Multiplying $B^{-1}A$ by $-I$ if necessary, we may assume that $u = 1$ and

$$B^{-1}A = \begin{pmatrix} 1 & x + y\lambda \\ 0 & 1 \end{pmatrix},$$

where $x, y \in \mathbb{Z}$. Note that

$$\begin{pmatrix} 1 & y\lambda \\ 0 & 1 \end{pmatrix} \in N(G_0(\tau)).$$

As a consequence,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N(G_0(\tau)).$$

Suppose that $x \neq 0$. Since $\lambda \in \mathbb{R} \setminus \mathbb{Q}$, for any $\epsilon > 0$, there exist k and l such that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}^l = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix} = \sigma \in N(G_0(\tau)),$$

where $0 < |\delta| < \epsilon$. As a consequence,

$$\sigma \begin{pmatrix} 1 & 0 \\ p\lambda & 1 \end{pmatrix} \sigma^{-1} = \begin{pmatrix} 1 + \delta p\lambda & \delta^2 p\lambda \\ p\lambda & 1 - \delta p\lambda \end{pmatrix} \in G_0(\tau)\,.$$

This implies that $G_0(\tau)$ is not discrete, giving a contradiction. Hence $x = 0$ and $B^{-1}A \in G_0(\tau)$. Since $B \in G_0(\tau)$, $A \in G_0(\tau)$.

Suppose $c = 0$. From the above argument, we have $A \in G_0(\tau)$. □

Lemma 2. *Suppose $p \neq 5$, $A \in N(G_0(\tau))$. If $c = 0$, then $A \in G_0(\tau)$.*

Proof. Applying (2.1), (2.2), (2.3), and (2.4) to A, we have

$$\begin{pmatrix} 1 & a^2\lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d^2\lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 + bdp\lambda & -b^2p\lambda \\ d^2p\lambda & 1 - bdp\lambda \end{pmatrix}, \begin{pmatrix} 1 - abp\lambda & -b^2p\lambda \\ a^2p\lambda & 1 + abp\lambda \end{pmatrix}$$

are elements of $G_0(\tau)$. By Corollary 5 of [LLT1], a^2 and d^2 are elements in $\mathbb{Z}$. Since $ad = 1$, $a = d = \pm 1$. Multiplying by $-I$ if necessary, we may assume that $a = d = 1$. Since $bdp = bp \in \mathbb{Z}[\lambda]$, $b = k/p$ for some $k \in \mathbb{Z}[\lambda]$. Since $b^2p \in \mathbb{Z}[\lambda]$, $k^2/p \in \mathbb{Z}[\lambda]$. It follows that k is a multiple of p (p is square free). Consequently, $b = k/p = x + y\lambda \in \mathbb{Z}[\lambda]$ and A is of the form

$$A = \begin{pmatrix} 1 & x + y\lambda \\ 0 & 1 \end{pmatrix}.$$

Applying the proof of Lemma 1, we conclude that $A \in G_0(\tau)$. □

Remark. If $p = 5$, $\tau = 2 + \lambda$ and by direct calculation, we can show that if $c = 0$, then A is of the form $A = \begin{pmatrix} 1 & k/\sqrt{5} \\ 0 & 1 \end{pmatrix}$, where $k \in \mathbb{Z}[\lambda]$.

Lemma 3. *Suppose $A \in N(G_0(\tau))$. If $b = 0$, then $A \in G_0(\tau)$.*

Proof. Applying (2.1), (2.2), (2.3) and (2.4) to A, we have

$$\begin{pmatrix} 1 - ac\lambda & a^2\lambda \\ -c^2\lambda & 1 + ac\lambda \end{pmatrix}, \begin{pmatrix} 1 + dc\lambda & d^2\lambda \\ -c^2\lambda & 1 - dc\lambda \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ d^2p\lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a^2p\lambda & 1 \end{pmatrix}$$

are elements of $G_0(\tau)$. By Corollary 5 of [LLT1], a^2 and d^2 are elements in $\mathbb{Z}$. Since $ad = 1$, $a = d = \pm 1$. As a consequence, $c \in \mathbb{Z}[\lambda]$. This implies that $A \in PSL_2(\mathbb{Z}[\lambda])$. By Lemma 1, $A \in G_0(\tau)$. □

Lemma 4. *Suppose $p \neq 5$. Let $A \in N(G_0(\tau))$. Then A is of the form*

$$\begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix} \text{ if } a = 0\,, \begin{pmatrix} h\sqrt{p} & 1/\sqrt{p} \\ -\sqrt{p} & 0 \end{pmatrix} \text{ if } d = 0\,,$$

where $h \in \mathbb{Z}[\lambda]$.

Proof. Suppose $a = 0$. Applying (2.1), (2.2), (2.3) and (2.4) to A, we have,

$$\begin{pmatrix} 1 & 0 \\ -c^2\lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 + dc\lambda & d^2\lambda \\ -c^2\lambda & 1 - dc\lambda \end{pmatrix}, \begin{pmatrix} 1 + bdp\lambda & -b^2p\lambda \\ d^2p\lambda & 1 - bdp\lambda \end{pmatrix}, \begin{pmatrix} 1 & -b^2p\lambda \\ 0 & 1 \end{pmatrix}$$

are elements of $G_0(\tau)$. By Corollary 5 of [LLT1], $c^2 = kp$ for some $k \in \mathbb{Z}$, $b^2p = l \in \mathbb{Z}$. Hence $c^2b^2p = lkp$, $k \in \mathbb{Z}$. Since $bc = -1$, one has $k = 1$, $l = 1$. It follows that

$c = \pm\sqrt{p}$, $b = \mp 1/\sqrt{p}$. Multiplying by $-I$ if necessary, we may assume that $c = \sqrt{p}$. Since $dc \in \mathbb{Z}[\lambda]$, $d = s/\sqrt{p}$ for some $s \in \mathbb{Z}[\lambda]$. Since $d^2 \in \mathbb{Z}[\lambda]$, $d^2 = s^2/p \in \mathbb{Z}[\lambda]$. Since p is square free ($p \neq 5$), $s = hp$ for some $h \in \mathbb{Z}[\lambda]$. Hence $d = h\sqrt{p}$ and

$$A = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix}.$$

Suppose $d = 0$. Applying (2.1), (2.2), (2.3) and (2.4) to A^{-1}, we have,

$$A^{-1} = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix}.$$

This completes the proof of the lemma. □

Remark. If $p = 5$, by direct calculation, we can show that A is of the form

$$\begin{pmatrix} 0 & -1/\sqrt{5} \\ \sqrt{5} & h \end{pmatrix} \text{ if } a = 0\,, \begin{pmatrix} h & 1/\sqrt{5} \\ -\sqrt{5} & 0 \end{pmatrix} \text{ if } d = 0\,.$$

Lemma 5. *Let $A \in N(G_0(\tau))$. Suppose $p \neq 5$ and $abcd \neq 0$. Then either $A \in G_0(\tau)$ or $b/a \in \mathbb{Q}(\lambda)$ and the denominator of the reduced form of b/a is a multiple of τ.*

Proof. By (2.1), (2.2), (2.3) and (2.4),

$$\begin{pmatrix} 1 - ac\lambda & a^2\lambda \\ -c^2\lambda & 1 + ac\lambda \end{pmatrix}, \begin{pmatrix} 1 + dc\lambda & d^2\lambda \\ -c^2\lambda & 1 - dc\lambda \end{pmatrix},$$

$$\begin{pmatrix} 1 + bdp\lambda & -b^2p\lambda \\ d^2p\lambda & 1 - bdp\lambda \end{pmatrix}, \begin{pmatrix} 1 - abp\lambda & -b^2p\lambda \\ a^2p\lambda & 1 + abp\lambda \end{pmatrix}$$

are elements of $G_0(\tau)$. By (2.1), $c^2 \in \mathbb{Z}[\lambda]$ is a multiple of τ. It follows easily that one of the following holds:

(a) $c = s\tau$ where $s \in \mathbb{Z}[\lambda]$,
(b) $c = s\sqrt{\tau}$ where $s \in \mathbb{Z}[\lambda]$,
(c) $c = s\tau\sqrt{w}$ where $s, w \in \mathbb{Z}[\lambda]$ ($(w, \tau) = 1$), w is square free,
(d) $c = s\sqrt{w\tau}$ where $(w, \tau) = 1$ and $s, w \in \mathbb{Z}[\lambda]$, w is square free.

(a) By (2.1) $ac \in \mathbb{Z}[\lambda]$. This implies that $a = r/s\tau$, where $r \in \mathbb{Z}[\lambda]$. By (2.1) $a^2 = (r/s\tau)^2 \in \mathbb{Z}[\lambda]$. It follows that r is a multiple of $s\tau$. Hence $a = r/s\tau \in \mathbb{Z}[\lambda]$. By (2.2) $dc, d^2 \in \mathbb{Z}[\lambda]$, similar to the above, $d \in \mathbb{Z}[\lambda]$. By (2.3) $bdp \in \mathbb{Z}[\lambda]$. Hence $b = t/dp$ for some $t \in \mathbb{Z}[\lambda]$. Since $b^2p \in \mathbb{Z}[\lambda]$, $t^2/d^2p \in \mathbb{Z}[\lambda]$. Since p is square free, pd is a divisor of t. This implies that $b \in \mathbb{Z}[\lambda]$. Summing up the above, we have $A \in N(G_0(p)) \cap PSL_2(\mathbb{Z}[\lambda]) = G_0(p)$ (Lemma 1).

(b) By (2.1) $ac \in \mathbb{Z}[\lambda]$. This implies that $a = r'/s\sqrt{\tau}$, where $r' \in \mathbb{Z}[\lambda]$. By (2.1) $a^2 = (r'/s\sqrt{\tau})^2 = r'^2/s^2\tau \in \mathbb{Z}[\lambda]$. Since τ is a prime, It follows that $s\tau | r'$. Hence $a = r\sqrt{\tau}$ where $r \in \mathbb{Z}[\lambda]$. By (2.2) dc, $d^2 \in \mathbb{Z}[\lambda]$. Using a similar argument to the above, we have $d = u\sqrt{\tau}$ where $u \in \mathbb{Z}[\lambda]$. By (2.3) $bdp \in \mathbb{Z}[\lambda]$. Hence $b = t'/dp = t'/up\sqrt{\tau}$ for some $t' \in \mathbb{Z}[\lambda]$. Since $b^2p \in \mathbb{Z}[\lambda]$, $b^2p = t'^2/u^2p\tau \in \mathbb{Z}[\lambda]$. Hence $pu | t'$. This implies that $b = t/\sqrt{\tau}$ where $t \in \mathbb{Z}[\lambda]$. Summing up the above, we conclude that $b/a = t/\tau r \in \mathbb{Q}(\lambda)$. Since $ru\tau - st = 1$, $(t, \tau) = 1$. It follows that the denominator of the reduced form of b/a is a multiple of τ.

(c) Let $p = \tau\tau'$. As in **(b)**, we may show

$$a = r\sqrt{w},\ b = t\sqrt{w},\ d = u\sqrt{w}, \qquad \text{if} \qquad (\tau', w) = 1$$

and

$$a = r\sqrt{w_1\tau'},\ b = t\sqrt{w_1}/\sqrt{\tau'},\ d = u\sqrt{w_1\tau'}, \qquad \text{if} \qquad (\tau', w) = \tau' \neq 1,\ w = w_1\tau',$$

where $r, t, u, w_1 \in \mathbb{Z}[\lambda]$.

Suppose $(\tau', w) = 1$. Since the determinant of A is 1, w is a unit. We have $a/c = r/s\tau$. Let X/Y be the reduced form of a/c. Since $ruw - swt\tau = 1$, $(r, s\tau) = 1$. Hence $Y = \mu s\tau$ where μ is a unit of $\mathbb{Z}[\lambda]$. Since X/Y is the reduced form of a cusp, G admits an element of the form

$$B = \begin{pmatrix} X & Z \\ Y & W \end{pmatrix}.$$

Since Y is a multiple of τ, $B \in G_0(\tau)$. Since $A\infty = B\infty$, $B^{-1}A$ fixes ∞ and takes the following form:

$$B^{-1}A = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in N(G_0(\tau)).$$

By Lemma 2, $B^{-1}A \in G_0(\tau)$. Hence $A \in G_0(\tau)$.

Suppose $w = w_1\tau'$. Similar to the case $(w, \tau') = 1$, w_1 is a unit in $\mathbb{Z}[\lambda]$. The denominator of the reduced form of $a/c = r/s\tau$ is again a multiple of τ and we have $A \in G_0(\tau)$. This gives a contradiction as $\sqrt{\tau'} \notin \mathbb{Z}[\lambda]$.

(d) As in **(c)**, we may show

$$a = r\sqrt{w\tau},\ b = t\sqrt{w}/\sqrt{\tau},\ d = u\sqrt{w\tau}, \qquad \text{if} \qquad (w, \tau) = 1,$$

$$a = r\sqrt{w_1 p},\ b = t\sqrt{w_1}/\sqrt{p},\ d = u\sqrt{w_1 p}, \qquad \text{if} \qquad (\tau', w) = \tau' \neq 1, w = w_1\tau'.$$

Using a similar argument to that in case (b), we can show that the denominator of the reduced form of b/a is a multiple of τ. □

3. Two cusps

In this section, we deal with the case when $G_0(\tau)$ has exactly 2 inequivalent cusps. By [CLLT], the prime p lying below τ is 5 or $p \equiv \pm 1 \pmod{10}$ and $(p) \neq (\tau)$.

Theorem 6. *Let τ be a prime such that $G_0(\tau)$ has exactly 2 inequivalent cusps. Then $N(G_0(\tau)) = G_0(\tau)$.*

Proof. We first consider the case $p \neq 5$. Suppose $N(G_0(\tau)) \neq G_0(\tau)$. Let $A \in N(G_0(\tau)) \setminus G_0(\tau)$. Suppose $A\infty$ is equivalent to ∞ in $G_0(\tau)$. Without loss of generality, we may assume $A\infty = \infty$. This implies that $c = 0$ and $A \in G_0(\tau)$ (Lemma 2), a contradiction. Hence we may assume that $A\infty$ is not equivalent to ∞ in $G_0(\tau)$. Since $G_0(\tau)$ has exactly 2 inequivalent cusps, $A\infty$ is equivalent to 0. Without loss of generality, we may assume that $A\infty = 0$. It follows by Lemma 4 that A is of the form

$$A = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix}.$$

Let $x = 1/\tau \in \mathbb{Q}(\lambda)$. By Leutbecher's theorem ([L1], [L2]), x is a cusp of G. By [LLT1], the reduced form for x is of the form $c/c\tau$, where c is a unit in $\mathbb{Z}[\lambda]$. Consequently (Proposition 6(ii) of [LLT1]), $G_0(\tau)$ contains an element of the form

$$B = \begin{pmatrix} c & b \\ c\tau & d \end{pmatrix}.$$

Since $A \in N(G_0(\tau))$,

$$ABA^{-1} = \begin{pmatrix} * & -c\tau/p \\ ** & * \end{pmatrix} \in G_0(\tau)\,.$$

In particular, $-c\tau/p \in \mathbb{Z}[\lambda]$. This is a contradiction (c and p have no common divisors in $\mathbb{Z}[\lambda]$ and $(\tau) \neq (p)$). It follows that $N(G_0(\tau)) = G_0(\tau)$.

Now, suppose $p = 5$ and $N(G_0(\tau)) \neq G_0(\tau)$. In this case, $\tau = \lambda + 2$. Let $A \in N(G_0(\tau)) \setminus G_0(\tau)$. $A\infty$ is equivalent to either ∞ or 0. Without loss of generality, we may assume that either $A\infty = \infty$ or $A\infty = 0$. By the remarks following Lemma 2 and Lemma 4, A takes the form

$$A_1 = \begin{pmatrix} 1 & k/\sqrt{5} \\ 0 & 1 \end{pmatrix} \qquad \text{if} \qquad A\infty = \infty,$$

$$A_2 = \begin{pmatrix} 0 & -1/\sqrt{5} \\ \sqrt{5} & h \end{pmatrix} \qquad \text{if} \qquad A\infty = 0,$$

where $h, k \in \mathbb{Z}[\lambda]$. By [LLT1],

$$\sigma = \begin{pmatrix} \lambda & -1 \\ \lambda + 2 & -\lambda \end{pmatrix} \in G_0(\lambda + 2)\,.$$

In the first case, since $A_1 \sigma A_1^{-1} \in G_0(\lambda + 2)$, $k = \sqrt{5}u$ where $u \in \mathbb{Z}[\lambda]$. By Lemma 1, $A_1 \in G_0(\lambda + 2)$, a contradiction. In the second case, an easy calculation shows that $A_2 \sigma A_2^{-1} \notin G_0(\lambda + 2)$, again giving a contradiction. It follows that $N(G_0(\lambda + 2)) = G_0(\lambda + 2)$. □

4. $p + 1$ CUSPS

In this section, we assume that $p \equiv \pm 3 \pmod{10}$ or $p = 2$. Then p is prime in $\mathbb{Z}[\lambda]$ so $\tau = p$. By [CLLT], $G_0(\tau)$ has $p + 1$ inequivalent cusps.

Lemma 7. *Suppose $p \equiv \pm 3$ (mod 10). Then $-\lambda/(1 + hp\lambda) \in \mathbb{Q}(\lambda)$ is in reduced form if and only if $h = k\lambda$ for some $k \in \mathbb{Z}$. If $p = 2$, $-\lambda/(1 + 2h\lambda) \in \mathbb{Q}(\lambda)$ is in reduced form if and only if $h = k\lambda$ or $1 + k\lambda$ for some $k \in \mathbb{Z}$.*

Proof. $-\lambda/(1 + hm\lambda) \in \mathbb{Q}(\lambda)$ is in reduced form if and only if $(1 + hm\lambda)/\lambda$ is in reduced form. The only cusps between 0 and λ whose reduced form has denominator λ are $1/\lambda$ and λ/λ. Hence any cusp whose reduced form has denominator λ is of the form $(u\lambda^2 + 1)/\lambda$ or $(u\lambda^2 + \lambda)/\lambda$ where $u \in \mathbb{Z}$ [LLT1]. The result follows easily from this. □

Lemma 8. *Let p be a prime in $\mathbb{Z}[\lambda]$ such that $G_0(p)$ has $p + 1$ inequivalent cusps. Then $N(G_0(p))/G_0(p)$ is a subgroup of $\mathbb{Z}_2$.*

Proof. Suppose $N(G_0(p)) \neq G_0(p)$. For any $A \in N(G_0(p)) \setminus G_0(p)$, by Lemmas 1, 2, 3, 4, and 5, A is of the form

$$\text{(i)} \quad A_1 = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix} \text{ or } \quad \text{(ii)} \quad A_2 = \begin{pmatrix} h\sqrt{p} & 1/\sqrt{p} \\ -\sqrt{p} & 0 \end{pmatrix}$$

or (iii) $\quad abcd \neq 0$.

(i) Suppose A takes the form

$$A = A_1 = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix}\,.$$

A simple calculation shows that

$$A\begin{pmatrix}1 & 0\\ p\lambda & 1\end{pmatrix}A^{-1}=\begin{pmatrix}1-hp\lambda & -\lambda\\ h^2p^2\lambda & 1+hp\lambda\end{pmatrix}\in G_0(p)\,.$$

This implies that

$$\frac{-\lambda}{1+hp\lambda}$$

is a reduced form. In the case $p\neq 2$, by Lemma 7, $h=k\lambda$ for some k in $\mathbb{Z}$. Hence

$$\begin{pmatrix}1 & 0\\ kp\lambda & 1\end{pmatrix}A=\begin{pmatrix}0 & -1/\sqrt{p}\\ \sqrt{p} & 0\end{pmatrix}\in N(G_0(p))\,.$$

It follows that

$$AG_0(p)=\begin{pmatrix}0 & -1/\sqrt{p}\\ \sqrt{p} & 0\end{pmatrix}G_0(p)\,.$$

In the case $p=2$, by Lemma 7, $h=k\lambda$ or $1+k\lambda$. It follows easily that

$$\begin{pmatrix}1 & 0\\ 2k\lambda & 1\end{pmatrix}A=\begin{pmatrix}0 & -1/\sqrt{2}\\ \sqrt{2} & 0\end{pmatrix}\text{ or }\begin{pmatrix}0 & -1/\sqrt{2}\\ \sqrt{2} & \sqrt{2}\end{pmatrix}\,.$$

We show that the second case is not possible. By [LLT1],

$$\sigma=\begin{pmatrix}2\lambda+1 & -\lambda\\ 2\lambda & -1\end{pmatrix}\in G_0(2)\,.$$

$$\begin{pmatrix}0 & -1/\sqrt{2}\\ \sqrt{2} & \sqrt{2}\end{pmatrix}\sigma\begin{pmatrix}0 & -1/\sqrt{2}\\ \sqrt{2} & \sqrt{2}\end{pmatrix}^{-1}=\begin{pmatrix}* & \lambda\\ ** & 4\lambda+1\end{pmatrix}\notin G_0(2)$$

($\lambda/(4\lambda+1)$ is not a reduced form). Hence, the second case is not possible.

It follows that

$$AG_0(2)=\begin{pmatrix}0 & -1/\sqrt{2}\\ \sqrt{2} & 0\end{pmatrix}G_0(2)\,.$$

(ii) Suppose A takes the form

$$A=A_2=\begin{pmatrix}h\sqrt{p} & 1/\sqrt{p}\\ -\sqrt{p} & 0\end{pmatrix}\,.$$

Since A_2 is the inverse of A_1 and $A_1G_0(p)$ has order 2 in $N(G_0(p))/G_0(p)$,

$$A_2G_0(p)=A_1G_0(p)=\begin{pmatrix}0 & -1/\sqrt{p}\\ \sqrt{p} & 0\end{pmatrix}G_0(p)\,.$$

(iii) Suppose $abcd\neq 0$. By Lemma 5, b/a is an element of $\mathbb{Q}(\lambda)$. Furthermore, if x/y is the reduced form of $-b/a$, then y is a multiple of p ($\tau=p$). By Leutbecher's Theorem ([L1], [L2]) $-b/a=x/y$ is a cusp of G. By Proposition 6(ii) of [LLT1], G contains an element of the form

$$B=\begin{pmatrix}x & z\\ y & w\end{pmatrix}\,.$$

Since y is a multiple of p, $B\in G_0(p)$. A direct calculation shows that

$$\sigma=AB=\begin{pmatrix}0 & -u^{-1}\\ u & v\end{pmatrix}\in N(G_0(p))$$

and $\sigma\infty = 0$. By Lemma 4,

$$AB = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & h\sqrt{p} \end{pmatrix}.$$

As above, one has

$$AG_0(p) = ABG_0(p) = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix} G_0(p).$$

Summing up the above, we have

$$AG_0(p) = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix} G_0(p),$$

for all $A \in N(G_0(p)) \setminus G_0(p)$. This implies that $N(G_0(p))/G_0(p)$ is a subgroup of $\mathbb{Z}_2$. □

Lemma 9. *$r/s \in \mathbb{Q}[\lambda]^\times$ such that $(r,s) = 1$ is equivalent to ∞ in $G_0(p)$ if and only if s is a multiple of p in $\mathbb{Z}[\lambda]$.*

Proof. It is clear that if r/s is equivalent to ∞ in $G_0(p)$, then s is a multiple of p. Conversely, for any $c = x/py \in \mathbb{Q}[\lambda]$ such that $x \neq 0$ and $(x,p) = 1$, let x'/y' be the reduced form of c. By Leutbecher's Theorem ([L1], [L2]) and Proposition 6(ii) of [LLT1], G contains an element of the form

$$A = \begin{pmatrix} x' & z \\ y' & w \end{pmatrix}.$$

Since $(x,p) = 1$, y' is a multiple of p. This implies that $A \in G_0(p)$. Consequently, c is a cusp of $G_0(p)$ equivalent to ∞. □

Theorem 10. *Let p be a prime in $\mathbb{Z}[\lambda]$ such that $G_0(p)$ has $p+1$ inequivalent cusps. Then $N(G_0(p)) = G_0(p)$.*

Proof. Suppose not. By Lemma 8, $N(G_0(p))/G_0(p) \simeq \mathbb{Z}_2$ and

$$N(G_0(p)) = \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix} G_0(p) \cup G_0(p).$$

This implies that $N(G_0(G(p))$ has at least 2 cusps.

Let d be a cusp of $G_0(p)$ such that d is not equivalent to ∞ in $N(G_0(p))$. $d \neq 0$ since 0 is equivalent to ∞ in $N(G_0(p))$ by

$$\begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}.$$

Write $d = r/s \in \mathbb{Q}[\lambda]^\times$ ($(r,s) = 1$). Since d is not equivalent to ∞ in $G_0(p)$, s is not a multiple of p (Lemma 9). However,

$$\begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix} \frac{r}{s} = -\frac{s}{pr}$$

and $(s,p) = 1$; hence d is equivalent to ∞ in $N(G_0(p))$, a contradiction. This completes the proof of Theorem 10 and hence the main theorem. □

References

[AL] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_o(m)$, Math. Ann. 185, (1970), $134-160$. MR **42:**3022

[C] J. H. Conway, *Understanding Groups like* $\Gamma_o(N)$, Groups, difference sets and the monster (Columbus, Ohio, 1993), Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996, 327-343. MR **98b:**11041

[CLLT] S. P. Chan, M. L. Lang, C. H. Lim, S. P. Tan, *The invariants of the congruence subgroups* $G_0(P)$ *of the Hecke group*, Illinois J. of Math. 38 (1994), $636-652$.

[L1] A. Leutbecher, *Uber die Heckeschen Gruppen* $G(\lambda)$, Abh. Math. Sem. Hambg. 31 (1967), $199-205$. MR **37:**4018

[L2] A. Leutbecher, *Uber die Heckeschen Gruppen* $G(\lambda)$*, II*, Math. Ann. 211 (1974), $63-68$. MR **50:**238

[LT] M. L. Lang, S. P. Tan, *Normalizer of the congruence subgroups of the Hecke groups* G_4 *and* G_6., (in preparation).

[LLT1] M. L. Lang, C. H. Lim, S. P. Tan, *Independent generators for congruence subgroups of Hecke groups*, Math. Z. 220 (1995), $569-594$. MR **96k:**11049

[LLT2] M. L. Lang, C. H. Lim, S. P. Tan, *Principal congruence subgroups of the Hecke groups*, (submitted for publication).

[LN] J. Lehner, M. Newman, *Weierstrass Point of* $\Gamma_o(N)$, Annals of Math. 79 (1964), $360-368$. MR **28:**5045

[P] L.A. Parson, *generalized Kloosterman sums and the Fourier coefficients of cusp forms*, Trans. Amer. Math. Soc. 217 (1976), $329-350$. MR **54:**241

[R] D. Rosen, *The substitutions of the Hecke group* $\Gamma(2cos\pi/5)$, Arch. Math., 46 (1986), $533-538$. MR **87k:**11048

Department of Mathematics, National University of Singapore, Singapore 119260, Republic of Singapore

E-mail address: matlml@math.nus.edu.sg