WOHLFAHRT’S THEOREM FOR THE HECKE GROUP $G_5$

CHENG LIEN LANG AND MONG LUNG LANG

ABSTRACT. Let $K$ be a subgroup of the inhomogeneous Hecke group $G_5$ of geometric level $r$. Then $K$ is congruence if and only if $K$ contains the principal congruence subgroup $G(2r)$. In the case $r \not\equiv 0 \pmod{4}$, $K$ is congruence if and only if $K$ contains the principal congruence subgroup $G(r)$.

1. Introduction

1.1. Let $H_5$ be the homogeneous Hecke group generated by $S$ and $T$ given as follows and let $H_5(\pi) = \{A \in H_5 : A \equiv I \pmod{\pi}\}$ be the principal congruence subgroup associated with $\pi \in \mathbb{Z}[\lambda]$.

$$T = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

(1.1)

where $\lambda = 2\cos \pi/5$. Let $Z = \langle \pm I \rangle$ be the centre of $H_5$. The inhomogeneous Hecke group $G_5$ and its principal congruence subgroup $G(\pi)$ in which a matrix and its negative are identified are defined as $G_5 = H_5/Z$ and $G(\pi) = H(\pi)Z/Z$. A subgroup $K$ of $G_5$ is called a congruence subgroup if $G(\pi) \subseteq K$ for some $\pi$. Let $K$ be a congruence subgroup of $G_5$. Since $\mathbb{Z}[\lambda]$ is a principal ideal domain, there exists a unique subgroup $G(\pi)$ of $G_5$ such that $G(\pi) \subseteq G(\pi)$ whenever $G(\pi) \subseteq K$. The ideal $(\pi)$ is called the algebraic level of $K$. The least common multiple $N$ of the cusp widths of $K$ is called the geometric level of $G$ (the width of a cusp $x$ is the smallest positive integer $m$ such that $\pm T_q^m$ is conjugate in $G_5$ to an element of $K$ fixing $x$).

The main purpose of the present article is to prove the following theorem which is an obvious generalisation of Wohlfahrt’s Theorem for the modular group $PSL(2, \mathbb{Z})$.

**Theorem 4.1.** Let $K \subseteq G_5$ be a congruence subgroup of geometric level $m$ and algebraic level $(\pi)$. Let $n$ be the rational integer below $(\pi)$. Then the following holds.

(i) Suppose that $m \equiv 0 \pmod{4}$. Then $G(m) \subseteq K$ and $n = m$.

(ii) Suppose that $4|m$. Then $G(2m) \subseteq K$ and $n$ is either $m$ or $2m$.

1.2. The Plan. Let $m$ be the geometric level of $K$ and $n$ the rational integer below the algebraic level $(\pi)$ of $K$. (i) Theorem 4.1 is equivalent to $N(G(mn), T^m) = G(m)$ and (ii) of Theorem 4.1 is equivalent to $G(2m) \subseteq N(G(mn), T^m)$, where $N(G(mn), T^m)$ is the smallest normal subgroup of $G_5$ that contains $G(mn)$ and $T^m$. Since $N(G(mn), T^m)$ is an intermediate subgroup of $G(mn)$, it is clear that (i) Theorem 4.1 can be proved if a small upper bound $U$ for $[G(m) : G(mn)]$ and a large lower bound $L$ for $[N(H(mn), T^m) : G(mn)]$ enjoys the fact that $U = L$. This is achieved in Section 2 (Lemmas 2.1 and 2.3 for the upper bound) and Appendices A-C (for the lower bound). As for (ii) of Theorem 4.1, one may obtain the fact $G(2m) \subseteq N(G(mn), T^m)$ by studying all the conjugates of $T^m$ modulo $G(mn)$ (Lemmas 3.7 and 3.8).

1.3. Geometry of $G_5$. An easy study of the group $PSL(2, \mathbb{Z}[\lambda])$ will provide us a good upper bound for $[G(m) : G(mn)]$ (Lemma 2.1) except for the case $[G(2\pi) : G(4\pi)]$, where $\gcd(2, \pi) = 1$. This is where the study of the geometry of $G_5$ comes in. The actual index of $[G(2\pi) : G(4\pi)]$ is obtained by studying a special polygon (fundamental domain) associated to $G(2)$ (subsection 2.2). As an application of Theorem 4.1, one can prove easily the following proposition.

2000 Mathematics Subject Classification. 11F06.

Key words and phrases. Hecke groups, Congruence subgroups, Wohlfahrt’s Theorem.
Proposition 5.1. Let $K$ be a subgroup of finite index of $G_5$ with geometric level $m$. Then

(i) Suppose that $m \not\equiv 0 \pmod{4}$. Then $K$ is congruence if and only if $G(m) \subseteq K$.

(ii) Suppose that $4|m$. Then $K$ is congruence if and only if $G(2m) \subseteq K$.

1.4. An Algorithm. Wohlfahrt’s Theorem has been recognised as one of the indispensable part of the study of the congruence subgroups for $SL(2, \mathbb{Z})$ and $PSL(2, \mathbb{Z})$ as the geometric level of a subgroup of $PSL(2, \mathbb{Z})$ or $SL(2, \mathbb{Z})$ can be determined geometrically (see (v) of subsection 2.2). Algorithms for the determination of whether a subgroup of $PSL(2, \mathbb{Z})$ is congruence can be found in [LLT2]. With the help of Proposition 5.1, the algorithm given in [LLT2] can be generalised easily to the Hecke group $G_q$ ($q$ prime). We will investigate subgroups of $G_5$ of index $\leq 5$ in Section 5.

1.5. The rest of the article is organised as follows. In Section 2, we give some technical lemmas which will be used to prove Theorem 4.1. Section 3 is devoted to the study of the normal closure of $G(mn)$ and $T^m$. Proof of Wohlfahrt’s Theorem for $G_5$ can be found in Section 4. Section 5 studies the congruence subgroups of small indices for $G_5$. A proof of Wohlfahrt’s Theorem for the modular group without Dirichlet’s Theorem can be found in Appendix D.

2. Technical Lemmas

Let $x, y \in \mathbb{Z}[\lambda]$. Denoted by $(x)$ the ideal generated by $x$. We say $x$ is a divisor of $y$ ($y$ is a multiple of $x$) if $(y) \subseteq (x)$. For our convenience, for any $x, y \in \mathbb{Z}[\lambda]$, we will use the notation $x|y$ if $x$ is a divisor of $y$. Recall that

(i) $5 = \lambda^2(2 + \lambda)^2$ ramifies totally in $\mathbb{Z}[\lambda]$,

(ii) 2 and rational primes of the form $10k \pm 3$ are primes in $\mathbb{Z}[\lambda]$,

(iii) rational primes of the form $10k \pm 1$ splits into $p = p_1p_2$, where $p_1 \in \mathbb{Z}[\lambda]$ are primes.

The smallest positive rational integer $m$ in $(\pi)$ is called the rational integer below $(\pi)$.

2.1. For $A$ an ideal of $\mathbb{Z}[\lambda]$, we may also define the principal congruence subgroup $L(A)$ of $L_5 = SL(2, \mathbb{Z}[\lambda])$ analogously. The formula for the index of the principal congruence subgroup $L(A)$ in $SL(2, \mathbb{Z}[\lambda])$ is easily calculated as the modular group case (see [Sh]); it is

$$[L_5 : L(A)] = N(A)^3 \prod_{P|A} (1 - N(P)^{-2}), \quad (2.1)$$

For any $u, v \in \mathbb{Z}[\lambda]$, it is clear that $[G(u) : G(uv)] = \epsilon[H(u) : H(uv)]$, where $\epsilon = 1/2$ or 1 and $\epsilon = 1/2$ if and only if $(2) = (u) \neq (uv)$. Applying (2.1), the following is clear.

Lemma 2.1. Let $n \in \mathbb{N}$ and let $\pi, \tau \in \mathbb{Z}[\lambda]$. Suppose that $\pi$ is a prime and that $\tau \notin (\pi)$. Then

$$[G(\pi \tau) : G(\pi^2 \tau)] \leq \epsilon[H(\pi) : H(\pi^2)] \leq \epsilon[L(\pi) : L(\pi^2)] = \epsilon N(\pi)^3. \quad (2.2)$$

where $\epsilon = 1/2$ or 1 and $\epsilon = 1/2$ if and only if $(\pi \tau) = (2)$.

Remark. $N(2) = 4, N(2 + \lambda) = 5$. If $p$ is a rational prime, then $N(p) = p^2$. In the case the rational prime below $(\pi)$ is of the form $p = 10k \pm 1$, $N(\pi) = p$.

Lemma 2.2. Let $m$ be a rational integer and let $p \in \mathbb{N}$ be a rational prime divisor of $m$. Suppose that $mp \neq 4$. Then the following matrices generate an elementary abelian group of order $p^6$ modulo $mp$.

$$\begin{pmatrix} 1 & m \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \lambda \\ -m \lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 - m^2 \lambda^2 & m \lambda^3 \\ 1 + m^2 \lambda^2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \lambda \\ -m & 1 + m \lambda \end{pmatrix}.$$

Proof. Put the above six matrices into the form $I + mU$. One sees easily the following identity.

$$(I + mU)(I + mV) \equiv I + m(U + V) \equiv (I + mU)(I + mV) \pmod{mp}. \quad (2.3)$$

Hence every non-identity element has order $p$ modulo $mp$ and the above matrices modulo $mp$ generate an abelian group. Note that (2.3) makes the unpleasant multiplication of $I + mU$ and
\[ I + mV \text{ into the very easy addition of } U \text{ and } V. \] In order to show the above matrices generate a group of order \( p^6 \) modulo \( mp \), we consider the following groups.

\[
M = \begin{pmatrix} 1 & m\lambda^i \\ 0 & 1 \end{pmatrix}, \quad Y_i = \begin{pmatrix} 1 & 0 \\ -m\lambda^i & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 - m\lambda^{i+1} & m\lambda^{i+2} \\ -m\lambda^i & 1 + m\lambda^{i+1} \end{pmatrix},
\]

where \( 0 \leq i \leq 1 \). It is easy to see that \( M \) and \( N \) are abelian groups of order \( p^4 \) and \( p^2 \) respectively. Applying (2.3) and the fact that \( N \) is abelian, elements in \( N \) take the following simple form

\[
Z_{c}^{c_1} \equiv \left( 1 - m\sum_{i=0}^{1} c_i\lambda^{i+1} - m\sum_{i=0}^{1} c_i\lambda^{i+1} \right).
\]

Note that we may assume that \( 0 \leq c_i \leq p - 1 \). Similar to (2.4), elements in \( M \) take the form

\[
X_{a}^{a_1}Y_{b}^{b_1} \equiv \left( -m\sum_{i=0}^{1} b_i\lambda^i m\sum_{i=0}^{1} a_i\lambda^i \right).
\]

Suppose that \( Z_{c}^{c_1} \equiv \pm X_{a}^{a_1}Y_{b}^{b_1} \) modulo \( mp \) (in \( G_p \), a matrix is identified with its negative). An easy study of (2.2)-entries of (2.4) and (2.5) implies that \( 1 + m\sum_{i=0}^{1} c_i\lambda^{i+1} \equiv \pm 1 \) (mod \( mp \)). Since \( mp \neq 1 \), one must have \( c_0 = c_1 = 0 \). As a consequence, \( M \cap N = \{1\} \). Hence \( |\Omega| = |M|/|N| = p^6 \).

\[
2.2. \text{ In [K], Kulkarni applied a combination of geometric and arithmetic methods to show that one can produce a set of independent generators in the sense of Rademacher for the congruence subgroups of the modular group, in fact for all subgroups of finite indices. His method can be generalised to all subgroups of finite indices of the inhomogeneous Hecke groups } G_p. \text{ where } q \text{ is a prime. See [LLT1] for detail (Propositions 8-10 and Section 3 of [LLT1]). In short, for each subgroup } K \text{ of finite index of } G_q, \text{ one can associate with } K \text{ a set of Hecke-Farey symbols } (HFS) \{-\infty, x_0, x_1, \cdots, x_n, \infty\}, \text{ a special polygon (fundamental domain) } \Phi, \text{ and an additional structure on each consecutive pair of } x_i \text{'s of the three types described below :}
\]

\[
x_i \overset{o}{\sim} x_{i+1}, \quad x_{i-1} \overset{\bullet}{\sim} x_{i+1}, \quad x_i \overset{a}{\sim} x_{i+1}.
\]

where \( a \) is a nature number. Each nature number \( a \) occurs exactly twice or not at all. Similar to the modular group, the actual values of the \( a \)'s is unimportant: it is the pairing induced on the pairs that matters.

(i) The side pairing \( o \) is an elliptic element of order 2 that pairs the even line \((a/b, c/d)\) with itself. The trace of such an element is 0.

(ii) The side pairing \( \bullet \) is an elliptic element of order \( q \) that pairs the odd line \((a/b, c/d)\). The absolute value of the trace of such an element is \( \lambda_q \).

(iii) The two sides \((a/b, c/d)\) and \((a/v, x/y)\) with the label \( a \) are paired together by an element of infinite order.

(iv) The special polygon associated with the HFS is a fundamental domain of \( K \) and the side pairings \( I_K = \{g_1, g_2, \cdots, g_m\} \) associated with the HFS is a set of independent generators of \( K \) (Theorem 7, Propositions 8-10 of [LLT1]).

(v) The width of a cusp \( x \), denoted by \( w(x) \), is the number of even lines in \( \Phi \) that comes into \( x \). Algebraically, it is the smallest positive integer \( m \) such that \( \pm T_q^m \) is conjugate in \( G_q \) to an element of \( K \) fixing \( x \) (keep in mind that a matrix is identified with its negative in \( G_q \)).

**Lemma 2.3.** \( G(2)/G(4) \) is an elementary abelian group of order \( 2^4 \). Suppose that \( \gcd(2, \pi) = 1 \) and \( (\pi) \neq (1) \). Then \( G(2\pi)/G(4\pi) \) is an elementary abelian group of order \( 2^5 \).

**Proof.** A set of independent generators of \( G(2) \) is given as follows (see [LLT1] for detail).

\[
\Omega_2 = \left\{ \begin{pmatrix} 1 & 2\lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2\lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2\lambda \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2\lambda \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2\lambda \\ 2 & 1 \end{pmatrix} \right\}.
\]
Denoted by $a_i$ the members in $\Omega_2$. It is easy to see that $a_i^2 \equiv 1$ and $a_i a_j \equiv a_i a_j$ modulo 4. Similar to Lemma 2.2, one can show that $[G(2) : G(4)] = 2^4$. By Lemma 2.1, $[G(2\pi) : G(2\pi)] \leq [H(2) : H(4)] = 2^5$. Let $m$ be the smallest rational integer in $[\pi]$. By our results in Appendix B, $G(2\pi)$ contains the following five matrices (modulo $4\pi$).

$$
t + 2m \begin{pmatrix} 0 & \lambda \\ -1 & 0 \end{pmatrix}, t + 2m \begin{pmatrix} 0 & 0 \\ -1 & \lambda \end{pmatrix}, t + 2m \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, t + 2m \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, t + 2m \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}.
$$

Since these matrices generate an elementary abelian group of order $2^5$ (see Appendix B), one has $[G(2\pi) : G(4\pi)] = 2^5$. $\square$

2.3. The homogeneous Hecke group $H_5$. In $G_5$, $G(ab) \neq G(a) \cap G(b)$. This creates some obstruction for our study of the normal closure (see Lemma 3.2) and we have to turn our study to the homogeneous group $H_5$ as follows.

**Lemma 2.4.** Let $K$ be a normal subgroup of $H_5$. Suppose that $T \in K$. Then $K = H_5$. Let $a, b \in \mathbb{N}$. Suppose that $gcd(a, b) = 1$. Then $H(a)H(b) = H_5$ and $H_5/H(ab) \cong H_5/H(a) \times H_5/H(b)$.

**Proof.** We note first that we are working on $H_5$, where $H(a) \cap H(b) = H(ab)$ and the order of $S$ is 4 ($S$ has order 2 in $G_5$). Every element $x$ in $H_5$ can be written as a word $w(S, T)$ in $S$ and $T$. Since $K$ is normal, $T \in K$, and $S$ is of order 4, we have $xK = K$, $SK$, $S^2K$ or $S^3K$. Hence $[G_5 : K] = 1, 2$ or 4. Note that $ST$ is of order 5. Hence $ST = (ST)^{16} \in K$. Since $T \in K$, we have $S \in K$. As a consequence, $K = H_5$. We shall now study the second part of the lemma. Since $gcd(a, b) = 1$, $T^a \in H(a)$, and $T^b \in H(b)$, one has $T \in H(a)H(b)$. This implies that $H_5 = H(a)H(b)$. Note that $H(a) \cap H(b) = H(ab)$. As a consequence, $H_5/H(ab) \cong H_5/H(a) \times H_5/H(b)$.

Lemma 2.4 can be generalised to all Hecke group $G_q$, where $q$ is a prime, as follows.

**Lemma 2.5.** Let $q$ be a prime and let $K$ be a normal subgroup of $G_q$. Suppose that $T \in K$. Then $K = G_q$. In particular, for any $a, b \in \mathbb{N}$, if $gcd(a, b) = 1$, then $G(a)G(b) = G_q$.

3. The Normal Closure $N(G(\pi), T^m)$

**Definition 3.1.** Let $m \in \mathbb{N}$ and $\pi \in \mathbb{Z}[\lambda]$. Denoted by $N(G(\pi), T^m)$ the smallest normal subgroup (normal closure) of $G_5$ that contains $G(\pi)$ and $T^m$.

3.1. The main purpose of this subsection is to study the group $N(G(mn), T^m)$ where $m$ or $n$ is odd, or $gcd(m, n) = 1$. We will show that $N(G(mn), T^m) = G(m)$ under such assumption.

**Lemma 3.2.** Let $a, b \in \mathbb{N}$. Suppose that $gcd(a, b) = 1$. Then $N(G(ab), T^b) = G(b)$.

**Proof.** To prove our lemma, we shall work on $H_5$, where $H(a) \cap H(b) = H(ab)$ and $H_5 \cong H(b)/H(ab) \times H(a)/H(ab)$ (Lemma 2.4). Set $X = N(H(ab), T^b)$. Then $H(ab) \subseteq X \subseteq H(b)$. Since $T^b \in X, T^a \in H(a)$ and $gcd(a, b) = 1$, one has $T \in XH(a)$. By Lemma 2.4, $XH(a) = H_5$. Hence

$$X/H(ab) \times H(a)/H(ab) \cong XH(a)/H(ab) = H_5/H(ab) \cong H(b)/H(ab) \times H(a)/H(ab).$$

Note that $X \subseteq H(b)$. It is now clear that (3.1) implies that $X = H(b)$. Equivalently, $H(b) = N(H(ab), T^b)$. As a consequence, one has $G(b) = N(G(ab), T^b)$.

**Remark** In Lemma 3.2, one has to work on $H_5$ rather than $G_5$ as $H(a) \cap H(b) = H(ab)$ but $G(a) \cap G(b) \neq G(ab)$.

**Lemma 3.3.** Suppose that $n \in \mathbb{N}$ is odd. Then $N(G(mn), T^m) = G(m)$.

**Proof.** We shall first assume that $n = p$ is an odd prime. Applying (A8) of Appendix A, $N(G(mp), T^m)$ contains the following six matrices (modulo $mp$).

$$\begin{pmatrix} 1 & m \lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \lambda^2 \\ -m \lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \lambda^3 \\ -m \lambda^2 + 1 + m \lambda^3 \end{pmatrix}, \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ -m & 1 \end{pmatrix}, \begin{pmatrix} 1 & \lambda^2 \\ -m & 1 + m \lambda \end{pmatrix}.$$

By Lemma 2.2, $|N(G(mp), T^m)/G(mp)| \geq p^6$. Since $N(G(mp), T^m)/G(mp) \subseteq G(m)/G(mp)$ and $|G(m)/G(mp)| \leq p^6$ (Lemma 2.1), we have $N(G(mp), T^m) = G(m)$. We shall now study
the general case. It is clear that \( N(G(nm), T^m) \subseteq G(m) \). Let \( n_0 \) be the smallest positive integer such that \( G(n_0 m) \subseteq G(m) \). Suppose that \( n_0 > 1 \). Let \( p \) be a prime divisor of \( n_0 \) Then
\[
G(n_0 m/p) = N(G(p(n_0 m/p)), T^{m_0 p}) \subseteq N(G(nm), T^m) \subseteq G(m). \tag{3.2}
\]
This contradicts the minimality of \( n_0 \). It follows that \( n_0 = 1 \) and that \( N(G(nm), T^m) = G(m) \). This completes the proof of the lemma.

**Lemma 3.4.** Let \( m, n \in \mathbb{N} \). Suppose that \( m \) is odd. Then \( N(G(nm), T^m) = G(m) \).

**Proof.** Decompose \( n \) into \( n = m'n_0 \), where \( m_0 = \gcd(m, n) \). It follows that \( \gcd(m', m_0 m) = 1 \).

It is clear that
\[
N(G(m'm_0 m), T^{m_0 m}) \subseteq N(G(nm), T^m). \tag{3.3}
\]
Since \( \gcd(m', m_0 m) = 1 \), we may apply Lemma 3.2 and conclude that the group to the right hand side of (3.3) is
\[
N(G(m'm_0 m), T^{m_0 m}) = G(m_0 m). \tag{3.4}
\]
Hence \( G(m_0 m) \subseteq N(G(nm), T^m) \). As a consequence, \( N(G(m_0 m), T^m) \subseteq N(G(nm), T^m) \).

Since \( m \) is odd and \( m_0 = \gcd(m, n) \), \( m_0 \) is odd as well. Applying Lemma 3.3, one has
\[
G(m) = N(G(m_0 m), T^m) \subseteq N(G(nm), T^m) \subseteq G(m). \tag{3.5}
\]
Hence \( N(G(nm), T^m) = G(m) \). This completes the proof of the lemma.

3.2. The main purpose of this subsection is to study the group \( N(G(mn), T^m) \) when \( n \) or \( m \) is even. It turns out that the group \( N(G(nm), T^m) \) does not behave very well as their counterparts in subsection 3.1.

**Lemma 3.5.** Let \( m \in \mathbb{N} \). Suppose that \( \gcd(m, 2) = 1 \). Then \( N(G(4m), T^{2m}) = G(2m) \).

**Proof.** By our results in Appendix B, \( N(G(4m), T^{2m}) \subseteq G(2m) \) possesses the following five matrices (modulo \( 4m \)).
\[
t + 2m \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix}, t + 2m \begin{pmatrix} 0 & 0 \\ -\lambda & 0 \end{pmatrix}, t + 2m \begin{pmatrix} -\lambda & 0 \\ -1 & \lambda \end{pmatrix}, t + 2m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, t + 2m \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.
\]
The above matrices modulo \( 4m \) generate an elementary abelian group of order \( 2^5 \) if \( m \geq 2 \), an elementary abelian group of order \( 2^4 \) if \( m = 1 \) (see Appendix B). Note that the orders meet the upper bound of \( [G(2m) : G(4m)] \) is both cases (Lemma 2.3). As a consequence, one has \( N(G(4m), T^{2m}) = G(2m) \).

**Lemma 3.6.** Let \( m \in \mathbb{N} \). Suppose that \( \gcd(m, 2) = 1 \). Then \( N(G(8m), T^{2m}) = G(2m) \).

**Proof.** It is clear that \( N(G(8m), T^{4m}) \subseteq N(G(4m), T^{2m}) \). Apply our results in Appendix B, the following are members of \( N(G(8m), T^{4m}) \subseteq G(4m) \cap N(G(8m), T^{2m}) \) modulo \( 8m \).
\[
t + 4m \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix}, t + 4m \begin{pmatrix} 0 & 0 \\ -\lambda & 0 \end{pmatrix}, t + 4m \begin{pmatrix} -\lambda & 0 \\ -1 & \lambda \end{pmatrix}, t + 4m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, t + 4m \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.
\]

Denote these five matrices by \( X_1, X_2, X_3, X_4, X_5 \). Then \( \{X_1, X_2, X_3, X_4, X_5\} \) generates an elementary abelian group \( E \) of order \( 2^5 \) modulo \( 8m \) (see Appendix B). Note that \( E \subseteq G(4m)/G(8m) \) and that
\[
I + 4m \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ is not an element of } E \subseteq G(4)/G(8m). \tag{3.6}
\]
We now consider the element \( (T^{2ST^{-2S^{-1}T^{-1}}})^2 \). Since \( 4m^2 \equiv 4m \pmod{8m} \), \( \lambda^2 = \lambda + 1 \), direct calculation shows that (modulo \( 8m \))
\[
X = (T^{2ST^{-2S^{-1}T^{-1}}})^2 \equiv I + 4m \begin{pmatrix} \lambda + 1 & \lambda \\ \lambda & \lambda + 1 \end{pmatrix} \in N(G(8m), T^{2m}) \cap G(4m). \tag{3.7}
\]
Applying the identity \( (I + 4mU)(I + 4mV) \equiv I + 4m(U + V) \) modulo \( 8m \), the following is clear.
\[
X_1 X_2 X_3 X_4 X_5 X \equiv I + 4m \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{3.8}
\]
By (3.6), \(X_1X_2X_3X_4X_5X \notin E\). Hence \((X_1, X_2, X_3, X_4, X_5, X)\) modulo 8m is an elementary abelian group of order 2^6. Note that
\[
F = \langle X_1, X_2, X_3, X_4, X_5, X \rangle \subseteq G(4m)/G(8m) \cap N(G(8m), T^{2m})/G(8m).
\] (3.9)
Since \(|F| = 2^6\) and \(|G(4m) : G(8m)| \leq 2^6\) (Lemma 2.1), we conclude that \(F = G(4m)/G(8m)\) and that \(G(4m) \subseteq N(G(8m), T^{2m})\). As a consequence, \(N(G(4m), T^{2m}) \subseteq N(G(8m), T^{2m}) \subseteq G(2m)\). By Lemma 3.5, \(N(G(4m), T^{2m}) = G(2m)\). Hence \(N(G(8m), T^{2m}) = G(2m)\). This completes the proof of the lemma.

\[\square\]

**Lemma 3.7.** Let \(m \in \mathbb{N}\). Suppose that \(m\) is a multiple of 4. Then \(G(2m) \subseteq N(G(4m), T^{2m})\).

**Proof.** By (C4) of Appendix C, \(N(G(4m), T^{2m})\) contains the following six matrices (modulo 4m).
\[
\left( \begin{array}{cc}
1 & 2m \lambda \\
0 & 1
\end{array} \right), \left( \begin{array}{cc}
1 & 0 \\
-2m \lambda & 1
\end{array} \right), \left( \begin{array}{cc}
1 - 2m \lambda^2 & 2m \lambda \\
-2m \lambda & 1 + 2m \lambda
\end{array} \right), \left( \begin{array}{cc}
1 & 0 \\
-2m \lambda & 1
\end{array} \right), \left( \begin{array}{cc}
1 - 2m \lambda & 2m \lambda^2 \\
-2m \lambda & 1 + 2m \lambda
\end{array} \right).
\]
Applying Lemma 2.2, the above matrices generate an abelian group of \(G(2m)/G(4m)\) of order \(2^6\). Since \(|G(2m)/G(4m)| \leq 2^6\) (Lemma 2.1), we have \(G(2m) \subseteq N(G(4m), T^{2m})\).

\[\square\]

**Lemma 3.8.** Let \(m \in \mathbb{N}\). Suppose that \(2|m\). Then \(N(G(4m), T^{2m}) : G(4m) = 2^5\). In particular, \(N(G(4m), T^{2m}) \neq G(2m)\).

**Proof.** We note first that although members in (C4) are not generated by the conjugates of \(T^{2m}\) but they are members of \(G(2m)\). As a consequence, one has \(|G(2m) : G(4m)| \geq 2^5\). This implies that \(|G(2m) : G(4m)| = 2^6\) (Lemma 2.1). Let \(S_1 = \langle T^{2m} \rangle\) and define \(S_{n+1}\) inductively to be \(S_{n+1} = S_n \cup \{Sx, S^{-1}, Tx, T^{-1} : x \in S_n\}\). It is clear that \(S_i \subseteq G(2m)\) for all \(i\). Each \(S_i\) generates an elementary abelian group modulo \(G(4m)\). Since \(|G(2m) : G(4m)| = 2^6\) is finite, there exists some \(r\) such that \(\langle S_r \rangle = \langle S_{r+1} \rangle\) modulo \(G(4m)\). It follows that \(N(G(4m), T^{2m}) = S_r G(4m)/G(4m)\). Direct calculation shows that \(\langle S_5 \rangle = \langle S_6 \rangle = \langle S_7 \rangle = \cdots\) is given as follows.
\[
\left( \begin{array}{cc}
1 & 2m \lambda \\
0 & 1
\end{array} \right), \left( \begin{array}{cc}
1 & 0 \\
2m \lambda & 1
\end{array} \right), I + 2m \left( \begin{array}{cc}
\lambda & 1 \\
0 & \lambda + 1
\end{array} \right), I + 2m \left( \begin{array}{cc}
0 & 1 \\
1 & 0
\end{array} \right).
\]
One can show by direct calculation that the above five matrices modulo 4m generate an elementary abelian group of order \(2^5\). Hence \(N(H(4m), T^{2m}) : G(4m) = 2^5\) and \(N(G(4m), T^{2m}) \neq G(2m)\).

\[\square\]

**Lemma 3.9.** Let \(m \in \mathbb{N}\). Suppose that \(m\) is a multiple of 4. Then \(G(2m) \subseteq N(G(4m), T^{2m})\).

**Proof.** By (C4) of Appendix C, \(N(G(4m), T^{2m})\) contains the following six matrices (modulo 4m).
\[
\left( \begin{array}{cc}
1 & 2m \lambda \\
0 & 1
\end{array} \right), \left( \begin{array}{cc}
1 & 0 \\
-2m \lambda & 1
\end{array} \right), \left( \begin{array}{cc}
1 - 2m \lambda^2 & 2m \lambda \\
-2m \lambda & 1 + 2m \lambda
\end{array} \right), \left( \begin{array}{cc}
1 & 0 \\
-2m \lambda & 1
\end{array} \right), \left( \begin{array}{cc}
1 - 2m \lambda & 2m \lambda^2 \\
-2m \lambda & 1 + 2m \lambda
\end{array} \right).
\]
Applying Lemma 2.2, the above matrices generate an abelian group of \(G(2m)/G(4m)\) of order \(2^6\). Since \(|G(2m)/G(4m)| \leq 2^6\) (Lemma 2.1), we have \(G(2m) \subseteq N(G(4m), T^{2m})\).
(ii) Since the geometric level is \( r, ±xT^r x^{-1} \in K \) for all \( x \in G_5 \). This implies that \( N(G(nr), T^r) \subseteq K \). Set \( nr = (2k + 1)2^s r \). By Lemma 3.3, one has

\[
G(2^r r) = N(G((2k + 1)2^s r), T^{2^s r}) \subseteq N(G(nr), T^r) \subseteq K.
\]

As a consequence,

\[
N(G(2^s r), T^r) \subseteq N(G(nr), T^r) \subseteq K.
\]

We now study the group \( N(G(2^s r), T^r) \) in (4.2). It is clear that if \( s \leq 2 \). Then one has the following,

\[
G(r) = N(G(2^s r), T^r) \subseteq K \quad \text{(Lemmas 3.5, 3.6)}.
\]

We shall now assume that \( s \geq 3 \). Let \( k \) be the smallest positive integer such that \( G(2^kr) \subseteq K \). Suppose that \( 2^k \geq 8 \). By Lemma 3.7,

\[
G(2^{k-1} r) = N(G(4(2^{k-2} r), T^{2^{k-2} r}) \subseteq N(G(2^k r), T^r) \subseteq K.
\]

This contradicts the minimality of \( k \). Hence \( s \leq 2 \) and \( G(r) \subseteq K \). This completes the proof of (ii). (iii) can be proved similarly. \( \square \)

Discussion 4.2. Unlike the modular group case, the algebraic level \((\pi)\) of \( K \) is not uniquely determined by the geometric level \( r \). For instance, while the algebraic level of \( G(5) \) and \( G(2 + \lambda) \) are \((5)\) and \((2 + \lambda)\) respectively, both \( G(5) \) and \( G(2 + \lambda) \) are congruence of geometric level 5.

Discussion 4.3. (iii) of Theorem 4.1 cannot be improved as \( K = N(G(8), T^4) \) has geometric level 4 and algebraic 8 (see Lemma 3.8).

5. Congruence Subgroup Problem

Let \( K \) be a subgroup of \( G_5 \) of finite index and let \( \Phi \) be a special polygon of \( K \) (see subsection 3.2). Applying (v) of subsection 3.2, the geometric level \( r \) of \( K \) can be determined geometrically. By Theorem 4.1, we have the following.

Proposition 5.1. Let \( K \) be a subgroup of finite index of \( G_5 \) with geometric level \( m \). Then

(i) Suppose that \( m \not\equiv 0 \pmod{4} \). Then \( K \) is congruence if and only if \( G(m) \subseteq K \).

(ii) Suppose that \( 4|m \). Then \( K \) is congruence if and only if \( G(2m) \subseteq K \).

An algorithm for the determination of whether a subgroup of \( PSL(2, Z) \) is congruence can be found in [LLT2]. With the help of Proposition 5.1, the algorithm given in [LLT2] can be generalised easily to the Hecke group \( G_q \ (q \text{ prime}) \). An easy observation of the special polygons implies that

(i) There is a unique subgroup of index 2 given as in subsection 5.1.

(ii) \( G_5 \) has subgroups of all possible indices except for 3 and 4.

(iii) A special polygon of a subgroup of index 5 consists of one special 5-gon. Its side pairings must have an element of order 2. There are altogether 26 subgroups of index 5 (see [LLT3]).

(iv) The only normal subgroup of index 5 is \( K = \langle x^5 : x \in G_5 \rangle \), a set of independent generators of \( K \) consists of 5 elements of order 2 (see subsection 5.7).

Note that since 5 is a prime, subgroups of index 5 are either normal or self-normalised. As a consequence, each non-normal subgroup of index 5 has 5 conjugates. Our study of subgroups of index \( \leq 5 \) is recorded as follows.

5.1. \( G_5 \) has a unique subgroup of index 2 with the following Hecke Farey symbol. It is congruence of geometric level 2. The algebraic level is also 2.

\[
-\infty \cdot 0 \cdot \infty
\]

(5.1)
5.2. Index 5, \( v_2 = 1 \) with geometric level 2. \( G_0(2) \) is one of them with the following Hecke Farey symbols. \( G_0(2) \) is self normalised. Consequently, \( G_0(2) \) has 5 conjugates. \( \mathbb{Z}_2 \cong G_0(2)/G(2) \subseteq G_5/G(2) \cong D_{10} \).

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.2)

5.3. Index 5, \( v_2 = 1 \) with geometric level 3. The following subgroup \( K \) is one of them. \( K \) has 5 conjugates. Since \( G_5/G(3) \cong A_5 \) has 5 subgroups of index 5, \( G_5 \) has 5 congruence subgroups of geometric level 3, index 5. It follows that \( K \) and its conjugates are congruence as they are the only subgroups (of geometric level 3) among the 26 subgroups of index 5. The algebraic level of these groups is also 3.

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.3)

5.4. Index 5, \( v_2 = 1 \) with geometric level 5. The following subgroup \( K \) is one of them. \( K \) has 5 conjugates. Since \( G_5/G(2+\lambda) \cong A_5 \) has 5 subgroups of index 5, \( G_5 \) has 5 congruence subgroups of geometric level 5, algebraic level 2 + \( \lambda \), index 5. It follows that \( K \) and its conjugates are congruence as they are the only non-normal subgroups (of geometric level 5) among the 26 subgroups of index 5. The algebraic level of these groups is 2 + \( \lambda \).

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.4)

5.5. Index 5, \( v_2 = 3 \) with geometric level 4. The following subgroup \( K \) is one of them. \( K \) has 5 conjugates. Suppose that \( K \) is congruence. By Proposition 5.1, \( G(8) \subseteq K \). Note that \( |G_5 : G(8)| = 2^{11}5 \), \( |G_5 : K| = 5 \). Hence \( K/G(8) \) is a Sylow 2-subgroup of \( G_5/G(8) \). Note that \( G_0(2)/G(8) \) is also a Sylow 2-subgroup of \( G_5/G(8) \). Hence \( K \) and \( G_0(2) \) are conjugate to each other. This is a contradiction as these two groups have different geometric invariants. Hence \( K \) is not congruence.

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.5)

5.6. Index 5, \( v_2 = 3 \) with geometric level 6. \( H_5/H(6) \cong H(2)/H(6) \times H(3)/H(6) \cong SL(2,5) \times D_{10} \). Let \( A \) be a subgroup of \( H(2)/H(6) \) of order 24 and let \( B \) be a subgroup of \( H(3)/H(6) \) of order 2. Set \( V = \langle A \times B, (a,b) \rangle \) where \( a \) is an element of \( H(2)/H(6) \) of order 5 and \( b \) is an element of \( H(3)/H(6) \) of order 5. It is clear that \( H(2)/H(6) \) and \( H(3)/H(6) \) are not subgroups of \( V \) and that \( V \) is of index 5 in \( H_5/H(6) \). Set \( K = V \mathbb{Z}/\mathbb{Z} \) (\( \mathbb{Z} \) is the centre of \( H_5 \)). Then \( K \) is a subgroup of \( G_5/G(6) \) of index 5. Note that \( G(3)/G(6) \) and \( G(2)/G(6) \) are not subgroups of \( K \). Hence \( K \) is of geometric level 6. By (ii) of Theorem 4.1, \( K \) has algebraic level 6 (2 and 3 are primes in \( \mathbb{Z} [\lambda] \)). \( K \) has 5 conjugates and one of them is given as follows. They are the only ones among the 26 groups with geometric level 6.

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.6)

5.7. Index 5, \( v_2 = 5 \) with geometric level 5. Such subgroup is unique. A set of independent generators is given as follows. We will investigate this group further in a separate article (see [LL]).

\[
\infty \ 0 \ \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty \\
1 \ 2 \ 1/\lambda \ \lambda \ \lambda \ \lambda \ \lambda \ \infty
\] (5.7)

Discussion. It is well known that subgroups of index \( \leq 6 \) of the modular group \( \text{PSL}(2,\mathbb{Z}) \) are congruence. This is not true for the Hecke group \( G_5 \) as the above examples indicate (subsection 5.5).
Let \( m \in \mathbb{N} \) be fixed. Set
\[
A = T^m = I + m \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix}, \quad B = ST^m S^{-1} = I + m \begin{pmatrix} \frac{1}{\lambda} & 0 \\ -\lambda & 0 \end{pmatrix}.
\] (A1)

Let \( S \) and \( T \) be given as in (1.1). Denoted by \( \Phi_m \) the smallest normal subgroup of \( G_5 \) that contains \( T^m \). Note that \( T^{-m} \in \Phi_m \). The main purpose of this appendix is to find members of \( \Phi_m \). It is clear that \( C = TST^m S^{-1}T^{-1} \) and \( D = T^{-1}ST^{-m}S^{-1}T \) are members of \( \Phi_m \). \( C \) and \( D \) are given as follows.
\[
C = \begin{pmatrix} 1 - m\lambda^2 & m\lambda^3 \\ -m\lambda & 1 + m\lambda^2 \end{pmatrix}, \quad D = \begin{pmatrix} 1 - m\lambda^2 & -m\lambda^3 \\ m\lambda & 1 + m\lambda^2 \end{pmatrix}.
\] (A2)

Note that \( \lambda^2 = \lambda + 1 \) and \( \lambda^3 = 2\lambda + 1 \). Hence the actual matrix form of \( C \) and \( D \) are given as follows as well.
\[
C = I + m \begin{pmatrix} -\lambda & 1 \\ -1 & \lambda + 1 \end{pmatrix}, \quad D = I + m \begin{pmatrix} -\lambda & 1 \\ -1 & \lambda + 1 \end{pmatrix}.
\] (A3)

Let \( p \) be an odd prime divisor of \( m \). Then \( (I + mU)(I + mV) \equiv I + m(U + V) \pmod{mp} \). This transforms matrix multiplication \( (I + mU)(I + mV) \) modulo \( mp \) into matrix addition \( I + m(U + V) \). As a consequence, we have the following.
\[
E = A^{-2}B^{-1}C \equiv I + m \begin{pmatrix} -\lambda & 1 \\ -1 & \lambda + 1 \end{pmatrix}, \quad F = A^2BD \equiv I + m \begin{pmatrix} -\lambda & 1 \\ -1 & \lambda + 1 \end{pmatrix} \pmod{mp}.
\] (A4)

Note that \( A, B, C, D, E, \) and \( F \) are members of \( \Phi_m \). We now conjugate \( E \) and \( F \) by \( S \). It follows easily that
\[
G = SES^{-1} \equiv I + m \begin{pmatrix} \lambda & 0 \\ -1 & \lambda - 1 \end{pmatrix}, \quad H = SFS^{-1} \equiv I + m \begin{pmatrix} \lambda & 0 \\ -1 & \lambda - 1 \end{pmatrix} \pmod{mp}.
\] (A5)

Note that \( G, H \in \Phi_m \). Applying the identity \( (I + mU)(I + mV) \equiv I + m(U + V) \pmod{mp} \), we have
\[
GE \equiv I + m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad GF \equiv I + m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \pmod{mp}.
\] (A6)

Recall that \( p \) is odd. Let \( r \in \mathbb{N} \) be chosen such that \( 2r \equiv 1 \pmod{p} \). It follows that \( \Phi_m \) contains the following element.
\[
X = (GEGF)^r = I + m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I + m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \pmod{mp}.
\] (A7)

**Lemma A.** Let \( m \in \mathbb{N} \) and let \( p \) be an odd prime divisor of \( m \). Denoted by \( \Phi_m \) the smallest normal subgroup of \( G_5 \) that contains \( T^m \). Then \( \Phi_m \) contains the set
\[
\Delta_m = \{ T^m, ST^m S^{-1}, TST^m S^{-1}T^{-1}, SXS^{-1}, X, TXS^{-1}T^{-1} \}.
\] (A8)

**Remark.** The matrix representatives of the members in the set \( \Delta_m \) modulo \( mp \) are given as follows.
\[
\begin{pmatrix} 1 & m\lambda \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -m\lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & m\lambda^2 \\ -m\lambda & 1 + m\lambda^2 \end{pmatrix}, \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & m\lambda^2 \\ -m\lambda & 1 + m\lambda^2 \end{pmatrix}.
\]

Note that \( \lambda^n = F_n \lambda + F_{n-1} \) where \( F_k \) is the \( k \)-th Fibonacci numbers \( (F_1 = 1, F_2 = 1, F_3 = 2, F_{k+1} = F_k + F_{k-1}) \).

**7. Appendix B**

Let \( m \) be an odd rational integer and let \( \Phi_{2m} \) be the smallest normal subgroup of \( G_5 \) that contains \( T^{2m} \). Following step by step of what we have done in Appendix A ((A1) to (A6)), \( \Phi_{2m} \) consists of the following elements, \( A, B, C, GE \) and \( T(GE)T^{-1} \). The matrix representatives of these five matrices modulo \( 4m \) are
\[
A_1 = I + 2m \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix}, \quad A_2 = I + 2m \begin{pmatrix} 0 & 0 \\ -\lambda & 0 \end{pmatrix}, \quad A_3 = I + 2m \begin{pmatrix} -\lambda & 1 \\ -\lambda & 1 + 1 \end{pmatrix}, \quad A_4 = I + 2m \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.
\]
and $A_5 = I + 2m \left( \begin{array}{cc} -\lambda & \lambda \\ -1 & 1 \end{array} \right)$. In order to determine the order of the group generated by these five matrices modulo $4m$, we consider $A_6 = A_1 A_5$ and $A_7 = A_1 A_2 A_3 A_5$. The matrix representatives of $A_1, A_2, A_6, A_4$ and $A_7$ (in this order) are given as follows.

$I + 2m \left( \begin{array}{cc} 0 & \lambda \\ 0 & 0 \end{array} \right), I + 2m \left( \begin{array}{cc} 0 & 0 \\ -\lambda & 0 \end{array} \right), I + 2m \left( \begin{array}{cc} -\lambda & 0 \\ -1 & 1 \end{array} \right), I + 2m \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right)$. 

Denoted by $E$ the group generated by the above five elements modulo $4m$. Applying the identity $(I + 2mU)(I + 2mV) \equiv I + 2m(U + V)$ modulo $4m$, one sees that the (1,1) and (2,2)-entries the matrix generated by the first three matrices is of the form $1 + 2m\lambda$ or 1 and the (1,1) and (2,2)-entries the matrix generated by the last two matrices is of the form 1 or 1. Consequently, one can show that $E$ is elementary abelian of order $2^4$ if $m \geq 2$. In the case $m = 1$, the last two matrices $A_4$ and $A_7$ satisfy $A_4 \equiv -A_7 \pmod{4}$. As we are working on $G_5$, where a matrix is identified with its negative, $E$ has order $2^4$.

8. Appendix C

Let $m$ be a rational integer. Suppose that $m$ is a multiple of 4. One sees easily that

$$(I + mU)(I + mV) \equiv I + m(U + V) \pmod{4m}.$$  \hspace{1cm} (C1) 

Let $S$ and $T$ be given as in (1.1) and construct matrices $A, B, C, D, E, F$ as what we have done in Appendix A. It follows that

$$GE \equiv I + m \left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right), \quad GF \equiv I + m \left( \begin{array}{cc} 0 & -1 \\ -1 & 0 \end{array} \right) \pmod{4m}. \hspace{1cm} (C2)$$

Hence

$$Y = GEGF \equiv I + m \left( \begin{array}{cc} 0 & 0 \\ -2 & 0 \end{array} \right) = I + 2m \left( \begin{array}{cc} 0 & 0 \\ -1 & 0 \end{array} \right) \pmod{4m}. \hspace{1cm} (C3)$$

Let $\Phi_{2m}$ be the smallest normal subgroup that contains $T^m$. Similar to Appendix A, $\Phi_{2m}$ contains

$$\Delta_{2m} = \{ T^{2m}, ST^{2m}S^{-1}, TST^{2m}S^{-1}T^{-1}, SY^{-1}S^{-1}, Y, TSY^{-1}T^{-1} \}. \hspace{1cm} (C4)$$

Similar to Appendix A, the actual matrix representatives of members in $\Phi_{2m}$ modulo $4m$ are given as follows.

$$\left( \begin{array}{cc} 1 & 2m\lambda \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} 1 & -2m\lambda \\ -2m\lambda & 1 \end{array} \right), \left( \begin{array}{cc} 1 & 2m\lambda^3 \\ 2m\lambda & 1 \end{array} \right), \left( \begin{array}{cc} 1 & 2m \\ 0 & 1 \end{array} \right), \left( \begin{array}{cc} 1 & -2m\lambda \\ -2m\lambda & 1 \end{array} \right), \left( \begin{array}{cc} 1 & 2m \lambda^3 \\ 2m\lambda & 1 \end{array} \right).$$

9. Appendix D. Wohlfarth’s Theorem for Modular Group

The main purpose of this appendix is to give an elementary proof of Wohlfarth’s Theorem where Dirichlet’s Theorem (see pp. 34 of [Wa]) is not used.

**Lemma D1.** Let $p$ be a prime and let $A$ be a subgroup of $SL(2,p)$ that contains at least two Sylow $p$-subgroups. Then $A = SL(2,p)$.

*Proof.* Recall first that $|SL(2,p)| = (p+1)p(p-1)$ and that $SL(2,p)$ has $p+1$ Sylow $p$-subgroups. Since $A$ has at least two Sylow $p$-subgroups, Sylow’s Theorem implies that $A$ contains all the Sylow $p$-subgroups of $SL(2,p)$. In particular, $A$ contains all the elements of the following forms.

$U(x) = \left( \begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right), L(y) = \left( \begin{array}{cc} 1 & 0 \\ y & 1 \end{array} \right), x, y \in \mathbb{Z}_p. \hspace{1cm} (D1)$

Since $\mathbb{Z}_p$ is a field, one sees easily by applying elementary row and column operation that every element in $SL(2,p)$ can be written as a word in $U(x)$ and $L(y)$. Hence $A = SL(2,p)$. \hspace{1cm} $\square$

**Lemma D2.** Let $p, m \in \mathbb{N}$, where $p$ is a be a prime. Then $N(\Gamma(m), T^m) = \Gamma(m)$, where $N(\Gamma(m), T^m)$ is the smallest normal subgroup of $SL(2,\mathbb{Z})$ that contains $\Gamma(m)$ and $T^m$.

*Proof.* We first assume that $p$ is a divisor of $m$. The index formula of $\Gamma(n)$ implies that $|\Gamma(m)/\Gamma(n)| = p^3$. Every element in $\Gamma(m)$ takes the form $I + m\sigma$, where $\sigma$ is a $2 \times 2$ matrix. Since $p$ is a prime divisor of $m$, one has $(I + m\sigma)(I + m\tau) \equiv I + m(\sigma + \tau) \pmod{
mp). Hence $\Gamma (m) / \Gamma (mp)$ is abelian and every non-identity element has order $p$. Equivalently, $\Gamma (m) / \Gamma (mp) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. The following is clear.

$$\Gamma (m) / \Gamma (mp) \cong \left\langle U = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, V = \begin{pmatrix} 1 & 0 \\ -m & 1 \end{pmatrix}, W = \begin{pmatrix} 1 - m & m \\ -m & 1 + m \end{pmatrix} \right\rangle. \quad (D2)$$

One sees easily that $U = T^m$, $V = ST^mS^{-1}$ and $W = TVT^{-1}$. Since these three elements are conjugates of $T^m$, we conclude that $\Gamma (m) / \Gamma (mp) \subseteq N(\Gamma (mp), T^m) / \Gamma (mp)$. Hence $\Gamma (m) = N(\Gamma (mp), T^m)$. We now assume that $\gcd (p, m) = 1$. The index formula of $\Gamma (n)$ implies that $\Gamma (m) / \Gamma (mp) \cong SL(2, \mathbb{Z}_p)$. It is clear that $\langle T^m \rangle$ and $\langle ST^mS^{-1} \rangle$ are two different Sylow $p$-subgroups of $N(\Gamma (mp), T^m) / \Gamma (mp)$. By Lemma D1, $N(\Gamma (mp), T^m) = \Gamma (m)$. \square

Wohlfahrt’s Lemma. Let $r, s \in \mathbb{N}$ be given. Then the smallest normal subgroup of $SL(2, \mathbb{Z})$ that contains $\Gamma (rs)$ and $T^s$ is $\Gamma (s)$.

Proof. Let $k$ be the smallest positive integer such that $\Gamma (k) \subseteq N(\Gamma (rs), T^s)$. Note that $N(\Gamma (rs), T^s) \subseteq \Gamma (s)$. Hence $s | k$. Suppose that $s < k$. We may write $k$ into $k = mp$, where $p$ is a prime and $s | m$. By Lemma D2, $\Gamma (m) = N(\Gamma (mp), T^m) = N(\Gamma (k), T^m) \subseteq N(\Gamma (rs), T^s)$. This contradicts the minimality of $k$. Hence $N(\Gamma (rs), T^s) = \Gamma (s)$. \square

Wohlfahrt’s Theorem. Let $K \subseteq PSL(2, \mathbb{Z})$ be a congruence subgroup of geometric level $r$ and algebraic level $s$. Then $r = s$.

Proof. Set $\overline{\Gamma} (r) = \Gamma (r) \langle \pm I \rangle / \langle \pm I \rangle$. Since the geometric level of $K$ is $r$, $xT^r x^{-1} \in K$ for all $x$. Let $N(\overline{\Gamma} (rs), T^r)$ be the smallest normal subgroup of $PSL(2, \mathbb{Z})$ that contains $\overline{\Gamma} (rs)$ and $T^r$. By Wohlfahrt’s Lemma, $\overline{\Gamma} (r) = N(\overline{\Gamma} (rs), T^r) \subseteq K$. It follows that $\overline{\Gamma} (r) \subseteq \overline{\Gamma} (s)$ as $s$ is the algebraic level. Hence $s$ is a divisor of $r$. On the other hand, since $\overline{\Gamma} (s) \subseteq \overline{\Gamma} (K)$, the geometric level $r$ is a divisor of $s$. In summary, $r = s$. \square

References

[K] R.S. Kulkarni, An arithmetic-Geometric method in the study of subgroups of the modular group, Amer. J Math. 113 (1991), 1053-1134.

[LL] C. L. Lang and M. L. Lang, The commutator subgroup of the Hecke group $G_5$ is not congruence, Preprint.

[LLT1] M. L. Lang, C. H. Lim, S. P. Tan, Independent generators for congruence subgroups of Hecke groups, Math. Z. 220 (1995), 569 – 594.

[LLT2] M. L. Lang, C. H. Lim, S. P. Tan, An algorithm for determining if a subgroup of the modular group is congruence, J. London Math. Soc. (2) 51 (1995), 491-502.

[LLT3] M. L. Lang, C. H. Lim, S. P. Tan, Subgroups of the Hecke groups with small index, Linear and multilinear algebra, 35 (1993), 75-77.

[Sh] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten, Publishers and Princeton University Press 1971.

[Wa] L. C. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

[Wo] K. Wohlfahrt, An extension of F. Klein’s level concept, Illinois J. of Math. 8 (1964), 529 – 535.

Department of Mathematics, I-Shou University, Kaohsiung, Taiwan, Republic of China. c1lang@isu.edu.tw

Singapore 669608, Republic of Singapore. lang2to46@gmail.com