ILLINOIS JOURNAL OF MATHEMATICS
Volume 38, Number 4, Winter 1994

THE INVARIANTS OF THE CONGRUENCE SUBGROUPS $G_0(\mathfrak{P})$ OF THE HECKE GROUP G_5

SHIH-PING CHAN, MONG-LUNG LANG, CHONG-HAI LIM AND SER-PEOW TAN

1. Introduction

The modular group Γ together with its congruence subgroups have been extensively studied; the formulae for the geometric invariants of the principal congruence subgroups are well-known (see [5]) for example). One can define in an analogous way the principal congruence subgroups of the Hecke groups G_q $(q = 3, 4, 5, \ldots)$ and ask for analogous formulae for the geometric invariants of these subgroups. Posed in this generality, this is not an easy question, for example, although it is easy to find upper bounds for the index of these subgroups, there are examples where these bounds are not attained and a general formula for the actual index is not known (see [2]). The purpose of this paper is to study the geometric invariants for the congruence subgroups of G_5 corresponding to the subgroups $\Gamma_0(N)$ of Γ.

Let

$$\lambda = 2\cos(\pi/5) = \frac{1+\sqrt{5}}{2},$$

and let G denote the Hecke group G_5, that is, the group of linear fractional transformations acting on the upper-half complex plane

$$\mathbf{H} = \{z \in \mathbf{C}: \operatorname{Im}(z) > 0\}$$

generated by the transformations

$$z \to -\frac{1}{z}, \quad \text{and} \quad z \to z + \lambda.$$

Thus, G may be identified with the subgroup

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \right\rangle \quad \text{of } \mathrm{PSL}_2(\mathbf{Z}[\lambda]).$$

Received August 12, 1992.
1991 Mathematics Subject Classification. Primary 11F06.

Table 1. p is the positive rational prime contained in $\mathfrak{P}$.

$\mathfrak{P}$	μ	t	ν_2	ν_5	g
(2)	5	3	1	0	0
$(2+\lambda)$	6	2	2	1	1
(p), $p \equiv \pm 2 \pmod 5$, $p \neq 2$	p^2+1	$p+1$	2	0	$(3p-1)(p-3)/20$
$N(\mathfrak{P}) \equiv 1 \pmod{20}$	$p+1$	2	2	2	$(3p-23)/20$
$N(\mathfrak{P}) \equiv 11 \pmod{20}$	$p+1$	2	0	2	$(3p-13)/20$
$N(\mathfrak{P}) \equiv 9 \pmod{20}$	$p+1$	2	2	0	$(3p-7)/20$
$N(\mathfrak{P}) \equiv 19 \pmod{20}$	$p+1$	2	0	0	$(3p+3)/20$

Fix a non-zero ideal $\mathfrak{P}$ of $\mathbf{Z}[\lambda]$, and define

$$G_0(\mathfrak{P}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : c \in \mathfrak{P} \right\}.$$

In this article, we give explicit formulas for

(i) $\mu = [G : G_0(\mathfrak{P})]$,
(ii) t: number of inequivalent cusps of $G_0(\mathfrak{P})$,
(iii) ν_2: number of inequivalent elliptics of order 2 of $G_0(\mathfrak{P})$,
(iv) ν_5: number of inequivalent elliptics of order 5 of $G_0(\mathfrak{P})$,
(v) g: genus of $G_0(\mathfrak{P}) \backslash \mathbf{H}$.

Of special interest is the case when $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$; we obtain the following theorem.

THEOREM. *If $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$, then μ, t, ν_2, ν_5 and g for $G_0(\mathfrak{P})$ is given in Table* 1.

We thank the referee for suggestions which have improved the exposition of the results in this paper.

2. The geometric invariants

The three main facts used in the derivation of the formulae are:

(i) $\mathbf{Z}[\lambda]$ is a principal ideal domain,
(ii) the set of cusps for G is $\mathbf{Q}[\lambda] \cup \{\infty\}$ (see [5]),
(iii) the Hurwitz formula: once we find expressions for μ, t, ν_2 and ν_5, the value of g then follows from the equation

$$3\mu = 5\nu_2 + 8\nu_5 + 20(g-1) + 10t. \tag{1}$$

2.1. Formula for μ. For a non-zero ideal $\mathfrak{P}$ of $\mathbf{Z}[\lambda]$, let $N(\mathfrak{P})$ denote the absolute norm of $\mathfrak{P}$.

LEMMA 1. *If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, then*

$$\mu = [G : G_0(\mathfrak{P})] = N(\mathfrak{P}) \prod_{\mathfrak{Q} \mid \mathfrak{P}} \left(1 + \frac{1}{N(\mathfrak{Q})}\right),$$

where the product is over the set of all prime ideals $\mathfrak{Q}$ which divide $\mathfrak{P}$.

Proof. We recall that

$$|\mathrm{PSL}_2(\mathbf{Z}[\lambda]/\mathfrak{P})| = N(\mathfrak{P}) \prod_{\mathfrak{Q} \mid \mathfrak{P}} \left(1 + \frac{1}{N(\mathfrak{Q})}\right),$$

where the product is over the set of all prime ideals $\mathfrak{Q}$ which divide $\mathfrak{P}$, and note that

$$G_0(\mathfrak{P}) = G \cap H, \quad H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z}[\lambda]) : c \in \mathfrak{P} \right\}.$$

In order to show that

$$[G : G_0(\mathfrak{P})] = N(\mathfrak{P}) \prod_{\mathfrak{Q} \mid \mathfrak{P}} \left(1 + \frac{1}{N(\mathfrak{Q})}\right),$$

it suffices to show that

$$\mathrm{PSL}_2(\mathbf{Z}[\lambda])/H$$

has coset representatives

$$\left\{ g_i : i = 1, \ldots, N(\mathfrak{P}) \prod_{\mathfrak{Q} \mid \mathfrak{P}} \left(1 + \frac{1}{N(\mathfrak{Q})}\right) \right\} \subseteq G.$$

Notice that for each $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbf{Z}[\lambda])$,

$$\frac{a}{c} \in \mathbf{Q}[\lambda] \cup \{\infty\}$$

is a cusp by Leutbecher's Theorem ([3]). Therefore, there exists a $\gamma \in G$ such that

$$\gamma^{-1}\left(\frac{a}{c}\right) = \infty.$$

Hence,

$$\gamma^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in H \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} H = \gamma H. \quad \square$$

2.2. Formula for t. In this subsection, we give a formula for t, first for non-zero prime ideals $\mathfrak{P}$ and then for arbitrary non-ideal ideals $\mathfrak{P}$ of $\mathbf{Z}[\lambda]$. We start with some definitions.

DEFINITION. If x is a cusp of $\Phi \leq G$, the width of x with respect to Φ, denoted by $w(x)$, is defined to be the smallest positive integer n such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{Stab}_{\Phi}(x)$$

for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ taking ∞ to x.

DEFINITION. If Φ has finite index in G, the geometric level of Φ, denoted by level(Φ), is defined to be the l.c.m. of the widths of its cusps.

DEFINITION. The principal congruence subgroup of G associated to the ideal $\mathfrak{P}$ is

$$G(\mathfrak{P}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} (\mathrm{mod}\ \mathfrak{P}) \right\}.$$

DEFINITION. If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, let $N'(\mathfrak{P})$ denote the smallest positive integer in $\mathfrak{P}$. If $\alpha \in \mathbf{Z}[\lambda] \setminus \{0\}$, we denote $N'(\alpha\mathbf{Z}[\lambda])$ by $N'(\alpha)$.

PROPOSITION 2. *$G(\mathfrak{P}) \triangleleft G$ and if x is a cusp of $G(\mathfrak{P})$, then $w(x) = N'(\mathfrak{P})$.*

Proof. Proof of normality is easy and will be omitted. It follows from normality that all the cusps have the same width and it is easy to see what $w(\infty) = N'(\mathfrak{P})$. $\square$

PROPOSITION 3. *If $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$, then any cusp of $G_0(\mathfrak{P})$ of width one is equivalent to ∞.*

Proof. If x is a cusp of $G_0(\mathfrak{P})$ and $w(x) = 1$, then there is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in G_0(\mathfrak{P}), \tag{1}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\infty = x. \tag{2}$$

It follows directly from (1) that

$$cd - c(c\lambda + d) \in \mathfrak{P},$$

that is, $c^2\lambda \in \mathfrak{P}$. As $\lambda \in (\mathbf{Z}[\lambda]^\times$, we have $c \in \mathfrak{P}$. This proves the proposition. □

LEMMA 4. *If $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$ and $p = N'(\mathfrak{P})$, then*

$$t = \begin{cases} 2 & \text{if } \mathfrak{P} = (\sqrt{5}) \text{ or } p \equiv \pm 1 \pmod 5, \\ p + 1 & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}.$$

Proof. Let $x_1, \ldots, x_t$ be the inequivalent cusps of $G_0(\mathfrak{P})$, and let $p = N'(\mathfrak{P})$ (note that p is a prime). Then we have that

$$G(\mathfrak{P}) \subseteq G_0(\mathfrak{P}) \quad \text{and} \quad \text{level}(G(\mathfrak{P})) = p \Rightarrow w(x_i) | p \quad \text{for all } x_i,$$

that is

$$w(x_i) \in \{1, p\} \quad \text{for all } x_i.$$

Hence, if we let $x_1 = \infty$, then

$$w(x_i) = p \quad \text{for } 2 \le i \le t.$$

Hence,

$$\sum_{i=1}^{t} w(x_i) = \mu \Rightarrow 1 + (t-1)p = \begin{cases} p + 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ p^2 + 1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Hence, from Lemma 1,

$$t = 2 \quad \text{when} \quad p \equiv \pm 1 \pmod 5,$$

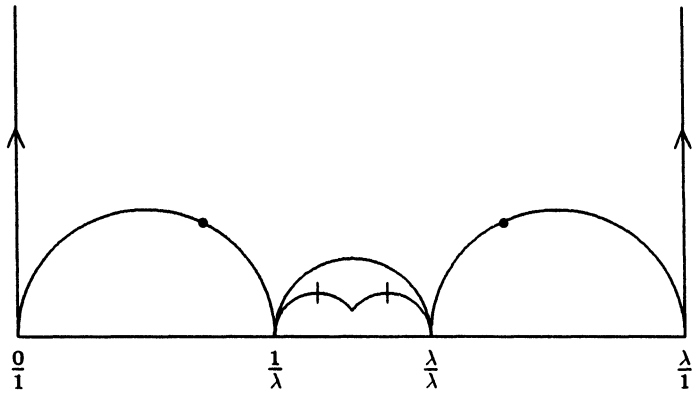

FIG. 1 Fundamental domain for $G_0(5,(\sqrt{5})\mathbf{Z}[\lambda_5])$

and

$$t = p + 1 \quad \text{when} \quad p \equiv \pm 2 \pmod 5.$$

If $\mathfrak{P} = (\sqrt{5})$, then we obtain $t = 2$ geometrically from the fact that a fundamental domain for $G_0((\sqrt{5}))$ is as given in Fig. 1 (see also [1]). □

DEFINITION. If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, we let π to be a positive generator of $\mathfrak{P}$.

DEFINITION. Let

$$T_\pi = \{(a,b,d) \in (\mathbf{Z}[\lambda])^3 : ad = \pi,\ d > 0 \quad \text{and} \quad (a,b,d) = 1\}/\sim,$$

where $(a,b,d) \sim (a',b',d')$ if there is a unit $u \in (\mathbf{Z}[\lambda])^\times$ such that $a = ua'$, and $b \equiv b' \pmod{d\mathbf{Z}[\lambda]}$.

PROPOSITION 5. *There is a set $S_\pi \subseteq (\mathbf{Z}[\lambda])^3$ of representatives for T_π such that*

$$\Omega\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\Omega = \bigsqcup_{(a,b,d)\in S_\pi} \Omega\begin{pmatrix}a & b\\ 0 & d\end{pmatrix},$$

where $\Omega := \mathrm{PSL}_2(\mathbf{Z}[\lambda])$.

Proof. Clearly,

$$\Omega\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\Omega = \bigcup_{\left(\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right)\in\Omega} \Omega\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}x & y\\ z & w\end{pmatrix} = \bigcup_{\left(\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right)\in\Omega} \Omega\begin{pmatrix}\pi x & \pi y\\ z & w\end{pmatrix}.$$

For $\left(\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right)\in\Omega$, let a be a g.c.d. of πx and z, and let $r, s \in \mathbf{Z}[\lambda]$ be such that

$$r\pi x + sz = a.$$

Then

$$\Omega\begin{pmatrix}\pi x & \pi y\\ z & w\end{pmatrix} = \Omega\begin{pmatrix} r & s\\ -z/a & \pi x/a\end{pmatrix}\begin{pmatrix}\pi x & \pi y\\ z & w\end{pmatrix} = \Omega\begin{pmatrix}a & \pi ry + sw\\ 0 & \pi/a\end{pmatrix}.$$

In particular,

$$\Omega\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\Omega \text{ is a union of } \Omega\begin{pmatrix}a' & b'\\ 0 & d'\end{pmatrix}.$$

We note three facts:

(i) If $b_1 \equiv b_2 \pmod{d}$, then

$$\Omega\begin{pmatrix}a & b_1\\ 0 & d\end{pmatrix} = \Omega\begin{pmatrix}a & b_2\\ 0 & d\end{pmatrix}.$$

(ii) The g.c.d. of a, $\pi ry + sw$ and π/a is 1.

For if α is a prime element in $\mathbf{Z}[\lambda]$ and α divides each of a, $\pi ry + sw$ and π/a, then α divides sw. So $\alpha|s$ or $\alpha|w$. In the first case, $\alpha|s$ and $\alpha|\pi/\alpha$, which contradicts the fact that $\pi x/a$ and s are relatively prime. In the second case, α divides w, then α divides a, and also z. This contradicts $xw - yz = 1$.

(iii) If $a_i, b_i, d_i \in \mathbf{Z}[\lambda]$ are such that $a_i d_i = \pi$ and g.c.d.$(a_i, b_i, d_i) = 1$ $(i = 1, 2)$, then

$$\Omega\begin{pmatrix}a_1 & b_1\\ 0 & d_1\end{pmatrix} = \Omega\begin{pmatrix}a_2 & b_2\\ 0 & d_2\end{pmatrix}$$

implies $d_1 = d_2\lambda^k$, $a_1 = a_2\lambda^{-k}$ for some integer k.

Fact (iii) follows from

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} d_2/\pi & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} d_2/\pi & -b_2/\pi \\ 0 & a_2/\pi \end{pmatrix} \in \Omega.$$

Facts (i), (ii) and (iii) together imply the proposition with S_π being any set of representatives for T_π. □

DEFINITION. (i) Let $\mathfrak{P}$ be any non-zero ideal of $\mathbf{Z}[\lambda]$ with a positive generator π, and let S_π be a subset of $(\mathbf{Z}[\lambda])^3$ as in Proposition 5. Define $\sigma : S_\pi \to \mathbf{Z}[\lambda]$ to be the mapping

$$(a, b, d) \to d.$$

(ii) Let

$$\Omega_0(\mathfrak{P}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Omega : c \in \mathfrak{P} \right\}.$$

If $x \in \mathbf{Q}[\lambda] \cup \{\infty\}$, we define the width of x with respect to $\Omega_0(\mathfrak{P})$, denoted by $W(x)$, to be the smallest positive integer n such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n\lambda \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \in \mathrm{Stab}_{\Omega_0(\mathfrak{P})}(x),$$

for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Omega$.

PROPOSITION 6. *If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, then the number of inequivalent classes of the action of $\Omega_0(\mathfrak{P})$ on $\mathbf{Q}[\lambda] \cup \{\infty\}$ is given by*

$$\sum_{d \in \sigma(S_\pi),\, \xi \in U,\, \xi \mid d} \frac{N(d/\xi)}{N'(d/\xi)} \prod_{(\xi) = \mathfrak{Q}_1^{\alpha_1} \cdots \mathfrak{Q}_m^{\alpha_m}} \left[N(\mathfrak{Q}_i^{\alpha_i}) - N(\mathfrak{Q}_i^{\alpha_i - 1}) \right],$$

where U is a set of representatives for $\mathbf{Z}[\lambda]/(\mathbf{Z}[\lambda])^\times$.

Proof. Let $x \in \mathbf{Q}[\lambda]$ and let $M \in \Omega$ be such that $x = M\infty$. Then $A \in \Omega_0(\mathfrak{P})$ fixes x if and only if

$$M^{-1}AM\infty = \infty. \qquad (*)$$

Clearly, $(*)$ is equivalent to the existence of $m \in \mathbf{Z}$ such that

$$M^{-1}AM = \begin{pmatrix} 1 & m\lambda \\ 0 & 1 \end{pmatrix}.$$

Let π be a positive generator of $\mathfrak{P}$ and we write

$$\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} M = B \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad ((a, b, d) \in S_\pi, B \in \Omega).$$

In particular, we have

$$\begin{pmatrix} 1 & m\lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} B^{-1} \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix} B \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

or

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & m\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} \in \Omega.$$

The latter is equivalent to

$$ma\lambda \equiv 0 \pmod{d}.$$

As λ is a unit in $\mathbf{Z}[\lambda]$, m is an integer in the ideal of $\mathbf{Z}[\lambda]$ generated by (d/ξ) $(\xi = \gcd(a, d))$. Thus $W(x)$ is the smallest positive integer in (d/ξ), i.e., $N'(d/\xi)$.

For each $d \in \sigma(S)$, we count the number of elements in the set $\sigma^{-1}(d)$. Let $a = d/\pi$ and let $\xi = \gcd(a, d)$. Then $\gcd(b, \xi) = 1$ and if we have the prime factorisation

$$(\xi) = \mathfrak{Q}_1^{\alpha_1} \dots \mathfrak{Q}_m^{\alpha_m},$$

then clearly

$$|\sigma^{-1}(d)| = N\left(\frac{d}{\xi}\right) \prod_{j=1}^{m} \left[N(\mathfrak{Q}_j^{\alpha_j}) - N(\mathfrak{Q}_j^{\alpha_j - 1})\right].$$

Since $W(x) = N'(d/\xi)$, the proposition follows. □

LEMMA 7. *If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, then*

$$t = \sum_{d \in \sigma(S_\pi),\, \xi \in U,\, \xi \mid d} \frac{N(d/\xi)}{N'(d/\xi)} \prod_{(\xi) = \mathfrak{Q}_1^{\alpha_1} \dots \mathfrak{Q}_m^{\alpha_m}} \left[N(\mathfrak{Q}_i^{\alpha_i}) - N(\mathfrak{Q}_i^{\alpha_i - 1})\right],$$

where U is a set of representatives for $\mathbf{Z}[\lambda]/(\mathbf{Z}[\lambda])^\times$.

Proof. We will show that there is a one-to-one correspondence between the set of cusps for $G_0(\mathfrak{P})$ and the set of classes for the action of $\Omega_0(\mathfrak{P})$ on $\mathbf{Q}[\lambda] \cup \{\infty\}$.

First let $M, N \in G$, and suppose that $M\infty$ and $N\infty$ are not equivalent by $G_0(\mathfrak{P})$. Thus, $N^{-1}M \notin G_0(\mathfrak{P})$ and hence, $N^{-1}M \notin \Omega_0(\mathfrak{P})$. So $M\infty$ and $N\infty$ are not in the same class under the action of $\Omega_0(\mathfrak{P})$.

Now let

$$P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \in \Omega.$$

There exists $m \in \mathbf{Z}$ such that

$$P_0 = \begin{pmatrix} p_{11}\lambda^m & * \\ p_{21}\lambda^m & * \end{pmatrix} \in G.$$

Clearly, $P\infty = P_0\infty$. Suppose that $Q \in \Omega$ and $P\infty$ and $Q\infty$ are inequivalent with respect to $\Omega_0(\mathfrak{P})$. Then $Q_0^{-1}P_0 \notin \Omega_0(\mathfrak{P})$ and $Q_0^{-1}P_0 \notin G_0(\mathfrak{P})$. This proves Lemma 7. □

Remarks. Lemma 4 also follows from Lemma 7 by a detailed case by case study but the proof we give for Lemma 4 is shorter and offers more geometric insight.

2.3. Formula for ν_2. We maintain the notation of the previous section.

DEFINITION. If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, we define

$$\left(\frac{-1}{\mathfrak{P}}\right) := \text{number of solutions } u \text{ in } \mathbf{Z}[\lambda]/\mathfrak{P} \text{ of } u^2 + 1 \equiv 0 \pmod{\mathfrak{P}}.$$

PROPOSITION 8. (i) *If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$ with prime factorisation $\mathfrak{P} = \mathfrak{Q}_1^{\alpha_1} \ldots \mathfrak{Q}_m^{\alpha_m}$, then*

$$\left(\frac{-1}{\mathfrak{P}}\right) = \prod_{j=1}^{m} \left(\frac{-1}{\mathfrak{Q}_j^{\alpha_j}}\right).$$

(ii) *With the notation as in* (i),

$$\left(\frac{-1}{\mathfrak{Q}_j^{\alpha_j}}\right) = \begin{cases} \left(\dfrac{-1}{\mathfrak{Q}_j}\right)^{\alpha_j} & \text{if } \mathfrak{Q}_j \text{ lies over an odd prime} \\ 1 & \text{if } \alpha_j = 1 \text{ and } \mathfrak{Q}_j = 2\mathbf{Z}[\lambda], \\ 0 & \text{if } 4 | \mathfrak{Q}_j^{\alpha_j}. \end{cases}$$

(iii) *If* $\mathfrak{P}$ *is a non-zero ideal of* $\mathbf{Z}[\lambda]$,

$$\nu_2 = \left(\frac{-1}{\mathfrak{P}}\right).$$

Proof. Assertion (i) is an easy consequence of the Chinese Remainder Theorem, and the proof of assertion (ii) is straightforward.

To prove (iii), we first note that the double coset $G\left(\begin{smallmatrix}\pi & 0\\ 0 & 1\end{smallmatrix}\right) G$ is a finite disjoint union of some $G\left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$, where $a, b, d \in \mathbf{Z}[\lambda]$ and $ad = \pi$ (the proof is similar to that of Proposition 5 but we need Leutbecher's Theorem [5]). Furthermore, $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ generates the subgroup of G consisting of elements which fix i. Let $x = Mi (M \in G)$ be an elliptic point for $G_0(\mathfrak{P})$. Writing

$$\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix} M = B \begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \quad (B \in G, a, b, d \in \mathbf{Z}[\lambda], ad = \pi),$$

we have that

$$\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}^{-1} B \begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1} B^{-1} \begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix} \in G_0(\mathfrak{P}),$$

or

$$\begin{pmatrix}a & b\\ 0 & d\end{pmatrix} \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \begin{pmatrix}a & b\\ 0 & d\end{pmatrix}^{-1} = \begin{pmatrix}b/a & -(b^2 + a^2)/\pi\\ d/a & -b/a\end{pmatrix} \in \Omega. \quad (**)$$

$(**)$ is clearly equivalent to

$$a \in (\mathbf{Z}[\lambda])^{\times} \quad \text{and} \quad b^2 + a^2 \equiv 0 \pmod{\pi}.$$

In this way we obtain a well-defined map f from the set of elliptic points of order 2 for $G_0(\mathfrak{P})$ to the set of solutions $u \pmod{\mathfrak{P}}$ of

$$u^2 + 1 \equiv 0 \pmod{\mathfrak{P}}.$$

First, we check that f is injective. Let $x = Mi$ and $y = Ni$ be two inequivalent elliptic points of order 2 for $G_0(\mathfrak{P})$, that is, $MN^{-1} \notin G_0(\mathfrak{P})$. Write

$$\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} M = B_M \begin{pmatrix} \lambda^m & b_M \\ 0 & \pi/\lambda^m \end{pmatrix}$$

and

$$\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} N = B_N \begin{pmatrix} \lambda^n & b_N \\ 0 & \pi/\lambda^n \end{pmatrix},$$

where $b_M^2 + 1 \equiv b_N^2 + 1 \equiv 0 \pmod{\mathfrak{P}}$ and $B_m, B_N \in G$. $MN^{-1} \notin G_0(\mathfrak{P})$ implies that

$$B_M \begin{pmatrix} \lambda^m & b_M \\ 0 & \pi/\lambda^m \end{pmatrix} \begin{pmatrix} \lambda^n & b_N \\ 0 & \pi/\lambda^n \end{pmatrix}^{-1} B_N^{-1}$$

does not have integral coefficients. Thus

$$\begin{pmatrix} \lambda^m & b_M \\ 0 & \pi/\lambda^m \end{pmatrix} \begin{pmatrix} \lambda^n & b_N \\ 0 & \pi/\lambda^n \end{pmatrix}^{-1}$$

is not integral, whence

$$\lambda^m b_N - \lambda^n b_M \not\equiv 0 \pmod{\mathfrak{P}}.$$

So $b_M/\lambda^m \neq b_N/\lambda^n$, and f is injective. Thus ν_2 is at most $(-1/\mathfrak{P})$.

Conversely, let c be a given solution of $u^2 + 1 \equiv 0 \pmod{\mathfrak{P}}$. Then for suitable $k \in \mathbf{Z}$ and $a, b \in \mathbf{Z}[\lambda]$, $\left(\begin{smallmatrix} a & b \\ c\lambda^k & \lambda^k \end{smallmatrix}\right) i$ is an elliptic point for $G_0(\mathfrak{P})$ since

$$\begin{pmatrix} a & b \\ c\lambda^k & \lambda^k \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c\lambda^k & \lambda^k \end{pmatrix}^{-1} \in G_0(\mathfrak{P}).$$

Let c_1, c_2 be two distinct solutions modulo $\mathfrak{P}$ of $u^2 + 1 \equiv 0 \pmod{\mathfrak{P}}$. Then

$$\begin{pmatrix} a_1 & b_1 \\ c_1\lambda^{k_1} & \lambda^{k_1} \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2\lambda^{k_2} & \lambda^{k_2} \end{pmatrix}^{-1} \notin G_0(\mathfrak{P})$$

for all appropriate choices of k_i, a_i, b_i. Thus c_i and c_2 give rise to two

distinct elliptic points

$$\begin{pmatrix} a_1 & b_1 \\ c_1\lambda^{k_1} & \lambda^{k_1} \end{pmatrix} i, \begin{pmatrix} a_2 & b_2 \\ c_2\lambda^{k_2} & \lambda^{k_2} \end{pmatrix}^{-1} i$$

of $G_0(\mathfrak{P})$. In particular, ν_2 is at least $(-1/\mathfrak{P})$. □

Although a case by case calculation using Proposition 8 yields the following lemma, we give an alternate short proof.

LEMMA 9. *If $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$,*

$$\nu_2 = \begin{cases} 0 & \text{if } \mathfrak{P} \text{ lies over a prime } p \equiv 11, 19 \pmod{20}, \\ 1 & \text{if } \mathfrak{P} = 2\mathbf{Z}[\lambda], \\ 2 & \text{otherwise.} \end{cases}$$

Proof. From equation (1), we have

$$3\mu \equiv 5\nu_2 + 10t \pmod 4.$$

From Lemmas 1 and 4, we have

$$\nu_2 \equiv \begin{cases} 0 \pmod 4 & \text{if } \mathfrak{P} \text{ lies over a prime} \equiv 11, 19 \pmod{20}, \\ 1 \pmod 4 & \text{if } \mathfrak{P} = 2\mathbf{Z}[\lambda], \\ 2 \pmod 4 & \text{otherwise.} \end{cases}$$

It therefore suffices to prove that $\nu_2 \leq 2$ for all non-zero prime ideals $\mathfrak{P}$.

Suppose that $A \in G_0(\mathfrak{P})$ is an elliptic elements of order 2. Then

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ and

$$B = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}^{-1}$$

is also an elliptic element of order 2 in $G_0(\mathfrak{P})$.

We claim that if X is an elliptic element of order 2 in $G_0(\mathfrak{P})$, then X is conjugate to A or B in $G_0(\mathfrak{P})$, so that $\nu_2 \leq 2$. Suppose

$$X = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix}^{-1}$$

is an elliptic element of order 2 in $G_0(\mathfrak{P})$, for some $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in G$. We observe that

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} A \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix}^{-1} = X$$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}^{-1} B \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix}^{-1} = X,$$

with

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} * & * \\ zd - wc & * \end{pmatrix},$$

$$\begin{pmatrix} x & z \\ y & w \end{pmatrix} \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}^{-1} = \begin{pmatrix} * & * \\ zd + wc & * \end{pmatrix}.$$

Note that

$$-z^2 \equiv w^2 \pmod{\mathfrak{P}}, \quad -d^2 \equiv c^2 \pmod{\mathfrak{P}}.$$

Because $\mathfrak{P}$ is a prime ideal, we have

$$\mathfrak{P} | (zd + wc) \quad \text{or} \quad \mathfrak{P} | (zd - wc).$$

This proves that X is conjugate to A or B in $G_0(\mathfrak{P})$. □

In view of Proposition 8 and Lemma 9, we have the following lemma:

LEMMA 10. *If* $\mathfrak{P} = \mathfrak{Q}_1^{\alpha_1} \ldots \mathfrak{Q}_m^{\alpha_m}$ *is the prime factorisation of the non-zero ideal* $\mathfrak{P}$ *in* $\mathbf{Z}[\lambda]$, *then*

$$\nu_2 = 2^{\delta(\mathfrak{P})} \varepsilon(\mathfrak{P}),$$

where

$$\varepsilon(\mathfrak{P}) = \begin{cases} 0 & \text{if } 4 \mid \mathfrak{P} \text{ or some } \mathfrak{Q}_j \text{ lies over a prime } \equiv 11, 19 \pmod{20}, \\ 1 & \text{otherwise} \end{cases}$$

and

$\delta(\mathfrak{P}) =$ *number of* j *for which* $\mathfrak{Q}_j$ *lies over a prime* $\equiv 1, 9 \pmod{20}$ *or* $\mathfrak{Q}_j = (\sqrt{5})$.

2.4. Formula for ν_5. First, we introduce the following notation.

DEFINITION. If $\mathfrak{P}$ is a non-zero prime ideal of $\mathbf{Z}[\lambda]$,

$$\left(\frac{\lambda}{\mathfrak{P}}\right) := \text{number of solutions } u \text{ in } \mathbf{Z}[\lambda]/\mathfrak{P} \text{ of } u^2 + \lambda u + 1 \equiv 0 \pmod{\mathfrak{P}}.$$

The proof of the following proposition is omitted since it is similar to that of Proposition 8.

PROPOSITION 11. *If* $\mathfrak{P} = \mathfrak{Q}_1^{\alpha_1} \ldots \mathfrak{Q}_m^{\alpha_m}$ *is the prime factorisation of the non-zero prime ideal of* $\mathbf{Z}[\lambda]$, *then*

$$\nu_5 = \left(\frac{\lambda}{\mathfrak{P}}\right) = \prod_{j=1}^{m} \left(\frac{\lambda}{\mathfrak{Q}_j^{\alpha_j}}\right).$$

LEMMA 12. *Let* $\mathfrak{P}$ *be a non-zero prime ideal of* $\mathbf{Z}[\lambda]$.

(i) *If* $\mathfrak{P} = (\sqrt{5})$, *then*

$$\left(\frac{\lambda}{\mathfrak{P}}\right) = 1 \quad \text{and} \quad \left(\frac{\lambda}{\mathfrak{P}^\alpha}\right) = 0 \text{ if } \alpha > 1.$$

(ii) *If* $\mathfrak{P} \neq (\sqrt{5})$, *then*

$$\left(\frac{\lambda}{\mathfrak{P}}\right) = \begin{cases} 2 & \text{if } \mathfrak{P} \text{ lies over a prime } p \equiv 1 \pmod{5}, \\ 0 & \text{if } \mathfrak{P} \text{ lies over a prime } p \equiv -1, \pm 2 \pmod{5} \end{cases}$$

and

$$\left(\frac{\lambda}{\mathfrak{P}^\alpha}\right) = \left(\frac{\lambda}{\mathfrak{P}}\right)^\alpha.$$

Proof. (i) follows directly by considering the congruences

$$x^2 + \lambda x + 1 \equiv 0 \,(\mathrm{mod}\,\sqrt{5}) \quad \text{and} \quad x^2 + \lambda x + 1 \equiv 0 \,(\mathrm{mod}\,5).$$

It remains to prove (ii), which follows by a case by case application of Proposition 11. It is easier to determine ν_5 for the case when $\mathfrak{P}$ is a non-zero prime ideal if we follow the proof for the number of inequivalent elliptic points of order 3 for the congruence subgroup $\Gamma_0(N)$ of the modular group $\mathrm{PSL}_2(\mathbf{Z})$ found in §1.6 of [9].

Put $\zeta = e^{2\pi i/5}$, $A = \mathbf{Z}[\lambda][\zeta] = \mathbf{Z}[\zeta]$, and

$$L = (\mathbf{Z}[\lambda])^2 := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbf{Z}[\lambda] \right\},$$

$$L_\pi := \left\{ \begin{pmatrix} x \\ \pi y \end{pmatrix} \in L : x, y \in \mathbf{Z}[\lambda] \right\},$$

where $\mathfrak{P} = (\pi)$. Denote by S_j the set of all elliptic elements of G of order 5 conjugate to $\begin{pmatrix} \lambda & -1 \\ 1 & 0 \end{pmatrix}^j$ $(j = 1, 2, 3, 4)$ under G.

For every $\sigma \in S_1 \cup S_2 \cup S_3 \cup S_4$, we consider L as a $(\mathbf{Z}[\lambda])[\sigma]$-module. Since $(\mathbf{Z}[\lambda])[\sigma]$ is isomorphic to A, and A is a principal ideal domain, there is a $\mathbf{Z}[\lambda]$-linear isomorphism f of A to L such that $f(\zeta x) = \sigma f(x)$ for all $x \in A$. Now let T be the set of all $\mathbf{Z}[\lambda]$-linear isomorphisms of A to L. Then T is a disjoint union of the subsets

$$T_j = \{ f \in T : f(\zeta x) = \sigma f(x) \text{ with } \sigma \in S_j \} \qquad (j = 1, 2, 3, 4).$$

If $\alpha \in M_2(\mathbf{Z}[\lambda])$ has determinant λ^j, then

$$f \in T_1 \Leftrightarrow \alpha f \in T_j.$$

For $f \in T_1$, we put $J = f^{-1}(L_\pi)$. Since

$$G_0(\mathfrak{P}) = \{ \gamma \in G : \gamma L_\pi = L_\pi \},$$

we see that the element σ satisfying $f(\zeta x) = \sigma f(x)$ belongs to $G_0(\mathfrak{P})$ if and only if J is an ideal of A. Note that

$$\mathbf{Z}[\zeta]/J \cong \mathbf{Z}[\lambda]/(\pi).$$

As in [5], there is a one-to-one correspondence between J and the conjugacy class of σ in $G_0(\mathfrak{P})$. □

Remark. In the modular case, the above calculation also works for ν_2. However for G_5, it does not work for ν_2 because the ring of integers of $\mathbf{Q}(\sqrt{-1}, \lambda)$ is not a principal ideal domain.

By Proposition 11 and Lemma 12, we obtain the following.

LEMMA 13. *Let $\mathfrak{P}$ be a non-zero ideal of $\mathbf{Z}[\lambda]$ and let $\mathfrak{P} = \mathfrak{Q}_1^{\alpha_1} \dots \mathfrak{Q}_m^{\alpha_m}$ be its prime factorisation. Then*

$$\nu_5 = 2^{\Delta(\mathfrak{P})} E(\mathfrak{P}),$$

where

$$E(\mathfrak{P}) = \begin{cases} 0 & \text{if } 5 \mid \mathfrak{P} \text{ or if some } \mathfrak{Q}_j \text{ lies over a prime } \not\equiv 0, 1 \pmod 5, \\ 1 & \text{otherwise} \end{cases}$$

and

$$\Delta(\mathfrak{P}) = \text{number of } j \text{ such that } \mathfrak{Q}_j \text{ lies over a prime } \equiv 1 \pmod 5.$$

The main result of this paper is the following theorem.

THEOREM 14. *If $\mathfrak{P}$ is a non-zero ideal of $\mathbf{Z}[\lambda]$, then μ, t, ν_2 and ν_5 for $G_0(\mathfrak{P})$ is given by the expressions in Lemmas* 1, 7, 10 *and* 13 *respectively.*

REFERENCES

1. M.L. LANG, C.H. LIM and S.P. TAN, *Independent generators for congruence subgroups of Hecke groups*, Math. Z., to appear.
2. _____, *The arithmetic and geometry of Hecke groups*, in preparation, 1992.
3. A. LEUTBECHER, *Über die Heckeschen Gruppen $G(\lambda)$*, Abh. Math. Sem. Hambg. **31** (1967), 199–205.
4. _____, *Über die Heckeschen Gruppen $G(\lambda)$, II*, Math. Ann. **211** (1974), 63–68.
5. G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Publishers and Princeton University Press, Princeton, N.J., 1971.

NATIONAL UNIVERSITY OF SINGAPORE
SINGAPORE, REPUBLIC OF SINGAPORE