BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 30, Number 2, June 2002

CONGRUENCE SUBGROUPS OF SOME HECKE GROUPS*

BY

İSMAİL NACİ CANGÜL AND OSMAN BİZİM

Abstract. Let Γ be a Fuchsian group generated by two elliptic generators whose product is parabolic. One of the most interesting classes of subgroups of Γ is known as the principal congruence subgroups and the level plays a very important role in their study. A subgroup containing a principal congruence subgroup is called a congruence subgroup. In the modular group case, there are two methods of obtaining principal congruence subgroups and Wohlfahrt proved that these two methods give the same normal subgroup by showing the equality of the kernel of the reduction homomorphism and the classical definition of the principal congruence subgroup.

Hecke groups can be thought as a generalisation of the modular group in some sense. In [1] and [2], many results concerning modular group had been generalised to Hecke groups. This suggests that one can also generalise the above result, i.e., the two methods in Hecke group case also coincide. But we give examples in which the above two methods give different subgroups. By showing this, we actually show that not all of the two generator Fuchsian groups act like modular group when the congruence subgroups are considered.

The principal congruence and congruence subgroups of the two important Hecke groups $H(\sqrt{m})$, for $m = 2$ or 3, are classified and the quotients of $H(\sqrt{m})$ with these normal subgroups are given. The method used to obtain these quotients depends on [4]. Also the indices of these two classes of subgroups are listed.

Received by the editors April 11, 2001.

*This work depends on the first authors PhD Thesis

1991 Mathematics subject classification number: 11F06, 20H05, 20H10.
Key words: congruence subgroup, principal congruence subgroup, level, Hecke groups.

1. Congruence Subgroups of Modular Group. Classical modular group Γ is a discrete subgroup of $PSL(2,\mathbf{R})$ with generators

$$R(z) = -\frac{1}{z} \qquad \text{and} \qquad T(z) = z + 1.$$

It is a Fuchsian group with signature $(0; 2, 3, \infty)$ and is isomorphic to the free product of two cyclic groups of orders 2 and 3.

Let Γ_1 be a subgroup of Γ. The level of Γ_1 is defined to be the least positive integer n so that $T^n \in \Gamma_1$. Perhaps the most interesting and difficult normal subgroups of modular group Γ are the principal congruence subgroups. A complete classification of these groups is given by Newman [6] and Mc Quillan [5]. The *principal congruence subgroup of level* n *of* Γ is defined by

$$\Gamma(n) = \Big\{T(z) = \frac{az+b}{cz+d} \in \Gamma : \quad ad - bc = 1,\ a \equiv d \equiv \mp 1,\ b \equiv c \equiv o(n)\Big\}.$$

A subgroup of Γ containing $\Gamma(n)$ is called a *congruence subgroup of level* n.

$\Gamma(n)$ is a normal subgroup of Γ, but in general, not all congruence subgroups are normal in Γ.

There is another way of obtaining $\Gamma(n)$: If we use the *reduction homomorphism mod* n which reduces everything in Γ modulo n, then $\Gamma(n)$ can be considered as the kernel of this homomorphism.

In [7], Wohlfahrt showed the equality of the two methods of obtaining $\Gamma(n)$.

2. Congruence Subgroups of Hecke Groups. Hecke groups $H(\sqrt{m})$, for $m = 2$ or 3, are discrete subgroups of the group $PSL(2,\mathbf{R})$ of isometries of the hyperbolic plane $\mathbf{U}$, generated by

$$R(z) = -\frac{1}{z} \quad \text{and} \quad T(z) = z + \sqrt{m}.$$

Here R is of order 2 and $S = RT$ is of order $2m$. Therefore $H(\sqrt{m})$, is a Fuchsian group with signature $(0; 2, 2m, \infty)$.

The principal congruence subgroups of level p of $H(\sqrt{m})$ are defined by Cangül, [1], as

$$\begin{aligned}\Gamma_p(\sqrt{m}) &= \{T \in H(\sqrt{m}) : \ T \equiv \mp I(p)\} \\ &= \left\{ \begin{pmatrix} a & \sqrt{m}b \\ \sqrt{m}c & d \end{pmatrix} : a \equiv d \equiv \mp 1, \ b \equiv c \equiv o(p), ad - mbc = 1 \right\}\end{aligned}$$

for prime p. (There are many algebraic problems in defining these subgroups for any level $n \in \mathbf{N}$). $\Gamma_p(\sqrt{m})$ is always normal in $H(\sqrt{m})$.

Congruence subgroups are possibly the most interesting ones amongst the infinitely many normal subgroups of $H(\sqrt{m})$. Interestingly, although most results for the modular group can easily be generalised to $H(\sqrt{m})$, we can not always get the equality of the two classes of above subgroups in the case of $H(\sqrt{m})$.

3. Some Results of Macbeath. Let $\boldsymbol{k} = GF(p^n)-$ a field with p^n elements and $\boldsymbol{k}_1$ be its unique quadratic extension. Let $G_0 = SL(2, \boldsymbol{k})$ and $G = PSL(2, \boldsymbol{k})$ so that $G \cong G_0/\{\pm I\}$. We shall also consider the subgroup G_1 of $SL(2, \boldsymbol{k}_1)$ consisting of the matrices of the form

$$\begin{pmatrix} a & b \\ b^q & a^q \end{pmatrix}$$

where $a, \ b \in \boldsymbol{k}_1$ and $a^{q+1} - b^{q+1} = 1$. Macbeath classifies the G_0-triples $(A, B, C), C = (AB)^{-1}$, of elements of G_0 finding out what kind of subgroup they generate. The ordered triple of the traces of the elements of the G_0-triple (A, B, C) will be a $\boldsymbol{k}$-triple (α, β, γ). Also to each G_0-triple (A, B, C), there is an associated $\mathbf{N}$-triple (l, m, n) where l, m, n are the orders of A, B and C in G.

Macbeath first considers the G_0-triples and then using the natural homomorphism

$$\phi : G_0 \to G,$$

passes to the G-triples in the following way: If H is the subgroup generated by $\phi(A)$, $\phi(B)$ and $\phi(C)$, we shall say, by slight abuse of language, that H is the subgroup generated by the G_0-triple (A, B, C).

In the $H(\sqrt{m})$ case, we have $A = r_p$, $B = s_p$ and $C = t_p$, where r_p, s_p and t_p denotes the image of R, S and T, respectively, under the homomorphism φ_p^* reducing all elements of $H(\sqrt{m})$ modulo p. Hence the corresponding $\boldsymbol{k}$-triple is $(0, u, 2)$ where u is a root of the minimal polynomial $P(\sqrt{m})$ *modulo* p in $GF(p)$ or in a suitable extension field. Also the corresponding **N**-triple is $(2, 2m, n)$ where n is the level (i.e., the least positive integer so that T^n belongs to the subgroup) of the normal subgroup.

Macbeath obtained three kinds of subgroups of G: affine, exceptional and projective groups. We now consider them in connection with $H(\sqrt{m})$.

Let $p > 2$. A $\boldsymbol{k}$-triple (α, β, γ) is called *singular* if the quadratic form

$$Q_{\alpha,\beta,\gamma}(\xi, \eta, \zeta) = \xi^2 + \eta^2 + \zeta^2 + \alpha\eta\zeta + \beta\xi\zeta + \gamma\xi\eta$$

is singular, i.e., if

$$\begin{vmatrix} 1 & \gamma/2 & \beta/2 \\ \gamma/2 & 1 & \alpha/2 \\ \beta/2 & \alpha/2 & 1 \end{vmatrix} = 0.$$

Now consider the set of matrices of the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$. They form a subgroup of G_0. By mapping it to G with the natural homomorphism ϕ we obtain a subgroup A_1 of G. Now consider the set of matrices $\begin{pmatrix} t & 0 \\ 0 & t^q \end{pmatrix}$, $t \in \boldsymbol{k}_1$, $t^{q+1} = 1$ in G_1, where $\boldsymbol{k}_1$ is the unique quadratic extension of $\boldsymbol{k}$. This is conjugate to a subgroup of $SL(2, \boldsymbol{k}_1)$. It is mapped, firstly by the

isomorphism from G_1 to G_0, and then by the natural homomorphism ϕ from G_0 to G, to a subgroup A_2 of G. Any subgroup of a group conjugate, in G, to either A_1 or A_2 will be called an *affine subgroup* of G.

A G_0-triple is called *singular* if the associated $\boldsymbol{k}$-triple (α, β, γ) is singular. Any group associated with a singular G_0-triple is an *affine group.*

We now restrict ourselves to the case $\boldsymbol{k} = GF(p)$, p prime.

For $H(\sqrt{m})$, the above determinant is equal to $-m/4$ and therefore vanishes only when $m \equiv 0$ *modulo* p. Therefore, it only vanishes when $p = m$.

The triples $(2, 2, n)$, $n \in \mathbf{N}$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$ and $(2, 5, 5)$- as $(2, 3, 5)$ is a homomorphic image of $(2, 5, 5)$ — which are the associated $\mathbf{N}$-triples of the finite triangle groups, are called the *exceptional triples.* The *exceptional groups* are those which are isomorphic images of the finite triangle groups. Therefore for $H(\sqrt{m})$, the only exceptional triples are obtained for $p = 2$ and 3.

The final class of the subgroups of G is the class of the projective subgroups. It is known that there are two kinds of them: $PSL(2, \boldsymbol{k}_s)$ and $PGL(2, \boldsymbol{k}_s)$ where $\boldsymbol{k}_s < \boldsymbol{k}$, the latter containing the former with index two, except for $p = 2$ where two groups are equal. The groups $PSL(2, \boldsymbol{k}_s)$ for all subfields of $\boldsymbol{k}$, and whenever possible, the groups $PGL(2, \boldsymbol{k}_2)$, together with their conjugates in $PGL(2, \boldsymbol{k})$ will be called *projective subgroups* of G.

Dickson, [3], proved that every subgroup of G is either affine, exceptional or projective. Therefore the remaining thing to do is to determine which one of these three kinds of subgroups is generated by the G_0-triple (r_p, s_p, t_p). We shall see that in most cases it is a projective group, and our problem will be to determine this subgroup. In doing this, we shall make use of the following results of Macbeath.

Theorem 3.1. *A G_0-triple which is neither singular nor exceptional generates a projective subgroup of G.*

Theorem 3.2. *If a G_0-triple generates a projective subgroup of G, then it generates either a subgroup isomorphic to $PSL(2,\kappa)$ or a subgroup isomorphic to $PGL(2,\kappa_0)$ where κ is the smallest subgield of $\boldsymbol{k}$ containing α, β and γ, and κ_0 is the subfield, if any, of which, κ is a quadratic extension.*

There are some $\boldsymbol{k}$-triples which are neither exceptional nor singular. These are called irregular by Macbeath, i.e., a $\boldsymbol{k}$-triples is called *irregular* if the subfield generated by its elements, say κ, is a quadratic extension of another subfield κ_0, and if one of the elements of the triple lies in κ_0 while the others are both square roots in κ of non-squares in κ_0, or zero. Then we have

Theorem 3.3. [4] *A G_0-triple which is neither singular, exceptional nor irregular generates in G a projective group isomorphic to $PSL(2,\kappa)$ where κ is the subfield generated by the traces of its matrices.*

4. On Klein's Level Concept. Let us once more consider the reduction homomorphism modulo p, for prime p. In the modular group case we mentioned that the kernel of this homomorphism is $\Gamma(p)$. Now we shall show that the situation for Hecke groups $H(\sqrt{m})$ is more complex as there is not usually a unique way of defining the reduction homomorphism.

Let $\wp$ be an ideal of $Z[\sqrt{m}]$. Then the natural map

$$Q_\wp : Z[\sqrt{m}] \to Z[\sqrt{m}]/\wp$$

induces a map

$$H(\sqrt{m}) \to PSL(2, Z[\sqrt{m}]/\wp)$$

whose kernel is going to be called *the principal congruence subgroup of level* $\wp$.

Let now s be an integer so that the minimal polynomial $P(\sqrt{m})$ of $\sqrt{m}$ has solutions in $GF(p^s)$. We know that such an s exists and satisfies $1 \leq s \leq d = \deg P(\sqrt{m})$. Let u be a root of $P(\sqrt{m})$ in $GF(p^s)$. Let us take $\wp$ to be the ideal generated by u in $Z[\sqrt{m}]$. As above we can define

$$\Theta_{p,u,m} : \ H(\sqrt{m}) \rightarrow \ PSL(2, p^s)$$

as the homomorphism induced by $\sqrt{m} \rightarrow \ u$. Let

$$K_{p,u}(\sqrt{m}) = Ker(\Theta_{p,u,m}).$$

$K_{p,u}(\sqrt{m})$ is then a normal subgroup of $H(\sqrt{m})$.

Let now p be a given prime. As $K_{p,u}(\sqrt{m})$ depends on p and u, we have a chance of having a different kernel for each root u. However sometimes they coincide:

Lemma 4.1. *If u and v correspond to the same irreducible factor f of $P(\sqrt{m})$ over $GF(p)$, then*

$$K_{p,u}(\sqrt{m}) = K_{p,v}(\sqrt{m}).$$

Proof. Note that $A \in K_{p,u}(\sqrt{m})$ if and only if

$$A = \pm \begin{pmatrix} 1 + g(\sqrt{m}) & h(\sqrt{m}) \\ k(\sqrt{m}) & 1 + l(\sqrt{m}) \end{pmatrix}$$

with $g(u) = h(u) = k(u) = l(u) = 0$ in $GF(p^s)$. Therefore as f is irreducible, $(g, f) = 1$ or $(g, f) = f$. If it is 1, then there are polynomials a and b such that $ag + bf = 1$. But $f(u) = g(u) = 0$. Therefore $(g, f) = f$, and g is a multiple of f. Similarly, h, k and l are all multiples of f. As v is another root of the same factor of $P(\sqrt{m})$, $g(v) = h(v) = k(v) = l(v) = 0$ in $GF(p^s)$; i.e., $A \in K_{p,v}(\sqrt{m})$.

Even when u, v give different factors of $P(\sqrt{m})$, we may have $K_{p,u}(\sqrt{m}) = K_{p,v}(\sqrt{m})$. For example

4.2. Example. For the two roots 3 and 4 of $P(\sqrt{2}) = x^2 - 2$ modulo 7, we have the odd elements

$$A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 2\sqrt{2} & 7 \\ 21 & 37\sqrt{2} \end{pmatrix}$$

in $K_{7,3}(\sqrt{2}) - \Gamma_7(\sqrt{2})$ and $K_{7,4}(\sqrt{2}) - \Gamma_7(\sqrt{2})$, respectively. But

$$A \cdot B^{-1} = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix} \begin{pmatrix} 37\sqrt{2} & -7 \\ -21 & 2\sqrt{2} \end{pmatrix} \equiv \text{-I mod } 7,$$

i.e., $A \cdot \Gamma_7(\sqrt{2}) = B \cdot \Gamma_7(\sqrt{2})$, so that $K_{7,3}(\sqrt{2}) = K_{7,4}(\sqrt{2})$.

To show that unlike modular group, the kernel $K_{p,u}(\sqrt{m})$ is actually not a principal congruence subgroup, but only a congruence subgroup, we first give the relation between $K_{p,u}(\sqrt{m})$ and $\Gamma_p(\sqrt{m})$ in the following result:

4.3. Theorem. *$K_{p,u}(\sqrt{m})$ is a normal congruence subgroup of level p of $H(\sqrt{m})$, i.e.,*

$$\Gamma_p(\sqrt{m}) \lhd K_{p,u}(\sqrt{m}).$$

Therefore

$$\Gamma_p(\sqrt{m}) \leq \bigcap_{\text{all } u} K_{p,u}(\sqrt{m}).$$

Proof. Let $T = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix} \in \Gamma_p(\sqrt{m})$ with each p_i is a polynomial of degree less than the degree of the minimal polynomial of $\sqrt{m}$. By the definition of $\Gamma_p(\sqrt{m})$, we have

$$p_1 \equiv p_4 \equiv \pm 1 \bmod p, \ p_2 \equiv p_3 \equiv 0 \bmod p.$$

Therefore T is an element of the kernel $K_{p,u}(\sqrt{m})$ defined above. Hence $\Gamma_p(\sqrt{m})$ is a subgroup of $K_{p,u}(\sqrt{m})$. Furthermore as $\Gamma_p(\sqrt{m})$ and $K_{p,u}(\sqrt{m})$ are both normal in $H(\sqrt{m})$,

$$\Gamma_p(\sqrt{m}) \lhd K_{p,u}(\sqrt{m}).$$

By this theorem, we can only say that $\Gamma_p(\sqrt{m})$ is a normal subgroup of $K_{p,u}(\sqrt{m})$. To say that they could be different, i.e., $\Gamma_p(\sqrt{m})$ is a proper subgroup of $K_{p,u}(\sqrt{m})$, we need a counter example:

4.4. Example. Let $q = 4$ and $p = 7$. Consider the element

$$A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & 5\sqrt{2} \end{pmatrix}.$$

The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$. In modulo 7, it could be considered as $x^2 - 9$ or $x^2 - 16$, and hence would have roots 3 and 4 in $GF(7)$. According to the definition of $\Gamma_7(\sqrt{2})$, $\sqrt{2}$ must be in the secondary diagonal (such elements are called *even* and form a normal subgroup of $H(\sqrt{2})$). Therefore A is not element of $\Gamma_7(\sqrt{2})$. Now consider the reduction homomorphism modulo 7. Under this homomorphism, one can consider $\sqrt{2}$ as an element of $GF(7)$, because $\sqrt{2} = 3$ or $\sqrt{2} = 4$ in $GF(7)$. Then $5\sqrt{2} = 5.3 = 15 \equiv 1 \mod 7$ and $5\sqrt{2} = 5.4 = 20 \equiv -1 \mod 7$. Also as $7 \equiv 0 \mod 7$, A belongs to $K_{7,3}(\sqrt{2}) = K_{7,4}(\sqrt{2})$. Using Theorem 2.3 one concludes that $\Gamma_7(\sqrt{2}) \lhd K_{7,3}(\sqrt{2}) = K_{7,4}(\sqrt{2})$.

4.5. Conclusion. Here we consider the principal congruence subgroups of Hecke groups. These subgroups were similarly defined as for modular group. We also consider another way of these subgroups. These two coincides in the modular group case. Here we give an example of that these two subgroups do not necessarily coincide. It would be interesting to know for which values of q and p, this happens.

5. Some Properties of Principal Congruence Subgroups of $H(\sqrt{m})$. In §4, it was shown that $K_{p,u}(\sqrt{m})$ is a normal subgroup of $H(\sqrt{m})$ and is therefore a congruence subgroup of level $\wp$. In the modular group case, this kernel coincides with the principal congruence subgroup. But in the case of $H(\sqrt{m})$, these two subgroups can be different for some values of p.

(i) **The case $m = 2$.** Here we have the following result.

5.1. Theorem. *The quotients of the Hecke group $H(\sqrt{2})$ by its congruence subgroups $K_{p,u}(\sqrt{2})$ and principal congruence subgroups $\Gamma_p(\sqrt{2})$ are as follows.*

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong \begin{cases} PSL(2,p) & \text{if } p \equiv \pm 1 \bmod 8 \\ PGL(2,p) & \text{if } p \equiv \pm 3 \bmod 8 \\ C_2 & \text{if } p = 2 \end{cases}$$

and

$$H(\sqrt{2})/\Gamma_p(\sqrt{2}) \cong \begin{cases} C_2 \times PSL(2,p) & \text{if } p \equiv \pm 1 \bmod 8 \\ PGL(2,p) & \text{if } p \equiv \pm 3 \bmod 8 \\ D_4 & \text{if } p = 2 \end{cases}.$$

Proof. Case 1. Let $p \neq 2$ be so that 2 is a square *modulo* p, that is, $p \equiv \pm 1 \bmod 8$. In that case there exists an element u in $GF(p)$ such that $u^2 = 2$. Therefore $\sqrt{2}$ can be considered as an element of $GF(p)$. Then r_p, s_p and t_p belong to $PSL(2,p)$. Now there is a homomorphism

$$\theta : H(\sqrt{2}) \to PSL(2,p)$$

induced by

$$\begin{pmatrix} a\sqrt{2} & b \\ c & d\sqrt{2} \end{pmatrix} \to \begin{pmatrix} au & b \\ c & du \end{pmatrix} \text{ and } \begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix} \to \begin{pmatrix} a & bu \\ cu & d \end{pmatrix}$$

where in $SL(2,p)$, we write, with slight abuse of language, a, b, c and d for their classes in $\mathbf{Z}_p$. Then our problem is to find the subgroup of G generated by r_p, s_p and t_p.

Following Macbeath's terminology let $\boldsymbol{k} = GF(p)$. Then κ, the smallest subfield of $\boldsymbol{k}$ containing traces of r_p, s_p and t_p, is also $GF(p)$ as $\sqrt{2} \in GF(p)$. In this case , for all p, the $H_p(\sqrt{2})$-triple (r_p, s_p, t_p) is not singular since the discriminant of the assoicated quadratic form, is not 0. It is also not exceptional since the associated **N**-triple (giving the orders of its elements) $(2,4,p)$ is not an exceptional triple for $p \equiv \pm \bmod 8$. Then by Theorem 3.1, (r_p, s_p, t_p) generates a projective subgroup of G, and by Theorem 3.2, as $\kappa = GF(p)$ is not a quadratic extension of any other field, this subgroup is the whole $PSL(2,p)$, i.e.,

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong PSL(2,p).$$

Let us now find the quotient of $H(\sqrt{2})$ by the principal congruence subgroup $\Gamma_p(\sqrt{2})$. In this case note that $\Gamma_p(\sqrt{2})$ is a subgroup of the even subgroup $H_e(\sqrt{2})$ consisting of all even elements in the form $\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}$ and of index 2 in $H(\sqrt{2})$. Therefore there are no odd elements in $\Gamma_p(\sqrt{2})$.

We now want to find the quotient group $K_{p,u}(\sqrt{2})/\Gamma_p(\sqrt{2})$. To show that it is not the trivial group, we show that $K_{p,u}(\sqrt{2})$ contains an odd element, as $\Gamma_p(\sqrt{2}) < H_e(\sqrt{2})$.

An odd element

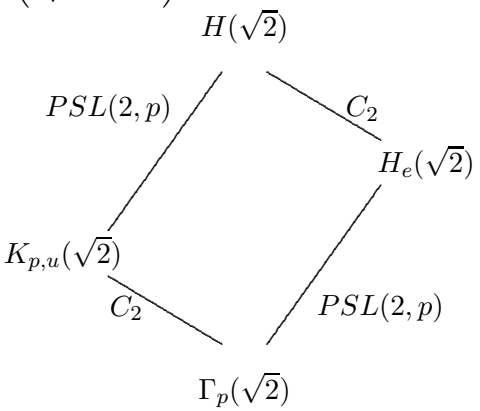
$$A = \begin{pmatrix} x\sqrt{2} & y \\ x & t\sqrt{2} \end{pmatrix}$$

with $\Delta = 2xt - yz = 1$, x, y, z, $t \in \mathbf{Z}$, is in $K_{p,u}(\sqrt{2}) - \Gamma_p(\sqrt{2})$. Now A is of exponent two mod $\Gamma_p(\sqrt{2})$. Then we can write

$$K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2}) \cup A.\Gamma_p(\sqrt{2})$$

As $A \notin \Gamma_p(\sqrt{2})$.

Any element $\begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}$ of $H_e(\sqrt{2})/\Gamma_p(\sqrt{2})$ commutes with A *mod* p.



Therefore

$$\begin{aligned} H(\sqrt{2})/\Gamma_p(\sqrt{2}) &\cong K_{p,u}(\sqrt{2})/\Gamma_p(\sqrt{2}) \times H_e(\sqrt{2})/\Gamma_p(\sqrt{2}) \\ &\cong C_2 \times PSL(2,p). \end{aligned}$$

To find the odd element mentioned above, we need to solve a Diophantine equation. Let us see this with an example.

5.2. Example.

(i) Let $p = 7$. Then $u = \sqrt{2} \equiv \pm 3 \mod 7$. We choose $u \equiv 3 \mod 7$. We are looking for an odd matrix $A = \begin{pmatrix} x\sqrt{2} & y \\ z & t\sqrt{2} \end{pmatrix}$ of $K_{7,3}(\sqrt{2})$ which is not in $\Gamma_7(\sqrt{2})$. Such an element must satisfy the following conditions:

$$\Delta = 2xt - yz = 1,\ xu \equiv tu \equiv 1,\ y \equiv z \equiv 0 \mod 7.$$

As $u \equiv 3 \mod 7$,

$$x \equiv t \equiv 5 \mod 7.$$

Then we have

$$2 \cdot (5 + 7a)(5 + 7b) - 7c \cdot 7d = 1,$$

where a, b, c, d are non-negative integers. Hence

$$7 + 10(a + b) + 14ab = 7cd$$

which has a solution whenever $a + b$ is an integer multiple of 7. A particular solution of this Diophantine equation is

$$a = b = 0,\ c = d = 1$$

giving

$$A = \begin{pmatrix} 5\sqrt{2} & 7 \\ 7 & b\sqrt{2} \end{pmatrix}.$$

If we choose the other value 4 of $u \in GF(7)$, then again we obtain an odd element

$$B = \begin{pmatrix} 2\sqrt{2} & 7 \\ 21 & 37\sqrt{2} \end{pmatrix}.$$

In fact, as 3 is the negative of 4 mod 7, generators of one of the two principal congruence subgroups corresponding to these two values of u are just the inverses of each other. Therefore these two subgroups of $H(\sqrt{2})$ are the same.

(ii) Let $p = 17$. Then in a similar way, solving the Diophantine equation

$$1 + 6(a + b) - 34ab = 17cd,$$

we obtain the required odd element

$$A = \begin{pmatrix} 24\sqrt{2} & 17 \\ 85 & 3\sqrt{2} \end{pmatrix}$$

Case 2. Now choose p so that 2 is not a squre *modulo* p, and let $p \neq 2$, i.e., let $p \equiv \pm 3 \bmod 8$. In this case $\sqrt{2}$ cannot be considered as an element of $GF(p)$. Therefore we shall extend this field to its quadratic extension $GF(p^2)$. Then $u = \sqrt{2}$ can be considered to be in $GF(p^2)$ and there exists

a homomorphism

$$\theta : \ H(\sqrt{2}) \rightarrow \ PSL(2, p^2)$$

induced in a similar way to case 1.

Let $\boldsymbol{k} = GF(p^2)$. Then κ, the smallest subfield of $\boldsymbol{k}$ containing traces α, β, γ of R_p, S_p, T_p, is also $GF(p^2)$.

Except for $p = 3$, the G_0-triple (r_p, s_p, t_p) is not an exceptional triple. If $p = 3$, then the corresponding **N**-triple is $(2, 4, 3)$ and therefore the generated subgroup is isomorphic to the symmetric group S_4.

Now suppose $p > 3$. Then as in case 1, (r_p, s_p, t_p) is not a singular triple. Since κ is the quadratic extension of $\kappa_0 = GF(p)$ and as $\beta = 2$ lies in κ_0 while $\alpha = 0$, and $\gamma = \sqrt{2}$ is the square root in κ of 2 which is a non-square in κ_0, by Theorem 2.2, (r_p, s_p, t_p) generates $PGL(2, p)$, i.e.,

$$H(\sqrt{2})/K_{p,u}(\sqrt{2}) \cong PGL(2, p).$$

Since 2 is not a square *modulo* p, there are no odd elements in the kernel $K_{p,u}(\sqrt{2})$. Hence $K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2})$

$$\begin{array}{c} H(\sqrt{2}) \\ | \\ | \ 2 \\ | \\ H_e(\sqrt{2}) \\ | \\ | \\ | \ \frac{p(p-1)(p+1)}{2} \\ | \\ | \\ | \\ K_{p,u}(\sqrt{2}) = \Gamma_p(\sqrt{2}) \end{array}$$

and hence

$$H(\sqrt{2})/\Gamma_p(\sqrt{2}) \cong PGL(2,p).$$

If $p = 3$, then again the two subgroups coincide and

$$H(\sqrt{2})/\Gamma_3(\sqrt{2}) \cong H(\sqrt{2})/K_{3,u}(\sqrt{2}) \cong PGL(2,3) \cong S_4.$$

Case 3. Let finally $p = 2$. Then $\sqrt{2}^2 = 2 \equiv 0 \bmod 2$. It is easy to find exactly 8 elements in $H(\sqrt{2})/\Gamma_2(\sqrt{2})$ and as

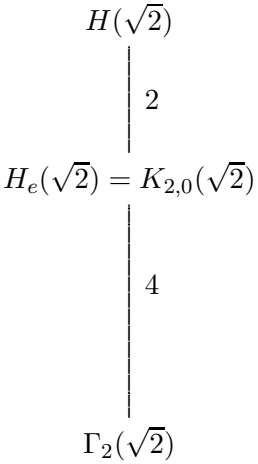
$$r_2^2 = s_2^4 = t_2^2 = I,$$

(r_2, s_2, t_2) is an exceptional triple generating the dihedral group D_4 of order 8, that is

$$H(\sqrt{2})/\Gamma_2(\sqrt{2}) \cong D_4.$$

Now $GF(2) = \{0, 1\}$ and $\sqrt{2} = 0$ in $GF(2)$. Therefore $t_2 \equiv I \bmod 2$. Hence $H(\sqrt{2})/K_{2,0}(\sqrt{2})$, generated by r_2, s_2 and t_2 is isomorphic to the cyclic group of order 2, i.e.,

$$H(\sqrt{2})/K_{2,0}(\sqrt{2}) \cong C_2.$$



(ii) The case $m = 3$**.** Here we have a very similar result to the case $m = 2$. The poof uses the same arguments with the proof of Theorem 5.1 and therefore is omitted.

5.3. Theorem. *The quotients of the Hecke group* $H(\sqrt{3})$ *by its congruence subgroups* $K_{p,u}(\sqrt{3})$ *and principal congruence subgroups* $\Gamma_p(\sqrt{3})$ *are as follows.*

$$H(\sqrt{3})/K_{p,u}(\sqrt{3}) \cong \begin{cases} PSL(2,p) & \text{if } p \equiv \pm 1 \ mod 12 \\ PGL(2,p) & \text{if } p \equiv \pm 3, \pm 5 \ mod 12 \\ C_2 & \text{if } p = 3 \\ D_3 & \text{if } p = 2 \end{cases}$$

and

$$H(\sqrt{3})/\Gamma_p(\sqrt{3}) \cong \begin{cases} C_2 \times PSL(2,p) & \text{if } p \equiv \pm 1 \ mod 12 \\ PGL(2,p) & \text{if } p \equiv \pm 3, \pm 5 \ mod 12 \\ (C_3 \times C_3) l C_2 & \text{if } p = 3 \\ D_6 & \text{if } p = 2 \end{cases}$$

where $(C_3 \times C_3)lC_2$ *denotes the Wreath product of the two groups.*

5.4. Corollary. *The indices of the congruence subgroups* $K_{p,u}(\sqrt{m})$ *and* $\Gamma_p(\sqrt{m})$ *in* $H(\sqrt{m})$ *are*

$$\left|\frac{H(\sqrt{m})}{K_{p,u}(\sqrt{m})}\right| = \begin{cases} p(p-1)(p+1)/2 & \text{if } m \text{ is a square mod } p \text{ and } p \neq m \\ p(p-1)(p+1) & \text{if } m \text{ is not a square mod } p \text{ and } p \neq 6/m \\ 2 & \text{if } p = m \\ 24 & \text{if } m = 2,\ p = 3 \\ 6 & \text{if } m = 3,\ p = 2 \end{cases}$$

and

$$|H(\sqrt{m})/\Gamma_p(\sqrt{m})| = \begin{cases} p(p-1)(p+1) & \text{if } p \neq m,\ 6/m \\ 2m^2 & \text{if } p = m \\ 24 & \text{if } m = 2,\ p = 3 \\ 12 & \text{if } m = 3,\ p = 2 \end{cases}$$

References

1. İ. N. Cangül, *Normal subgroups of Hecke groups*, PhD Thesis, Southampton, 1993.

2. İ. N. Cangül and D. Singerman, *Normal subgroups of Hecke groups and regular maps*, Math. Proc. Camb. Phil. Soc., **123** (1998), 59-74.

3. L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig, 1901, reprinted by Dover, 1960.

4. A. M. Macbeath, *Generators of the linear fractional groups*, Proc. Symp. Pure Math., **12** (1969), A.M.S., 14-32.

5. D. L. McQuillan, *Classification of normal subgroups of the modular group*, Amer. J. Math., **87** (1965), 285-296.

6. M. Newman, *Normal congruence subgroups of the modular group*, Amer. J. Math., **85** (1963), 419-427.

7. K. Wohlfahrt, *An extension of F. Klein's level concept*, Illionis J. Math., **8** (1964), 529-535.

University of Uludağ, Faculty of Science and Arts, Dept. of Mathematics, Görükle 16059 BURSA/TURKEY.

E-mail: cangul@uludag.edu.tr

E-mail: obizim@uludag.edu.tr