Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 45 (2004), No. 1, 75-85.

On the Principal Congruence Subgroups of the Hecke-Group $H(\sqrt{5})$

Nihal Yılmaz Özgür **İ. Naci Cangül**

Balikesir Universitesi, Fen-Edebiyat Fakultesi, Matematik Bolumu
10100 Balikesir, Turkey
e-mail: nihal@balikesir.edu.tr

Uludag Universitesi, Fen-Edebiyat Fakultesi, Matematik Bolumu
16059 Bursa, Turkey
e-mail: cangul@uludag.edu.tr

Abstract. Using the notion of quadratic reciprocity, we discuss the principal congruence subgroups of the Hecke group $H(\sqrt{5})$.
MSC 2000: 11F06(primary); 20H05 (secondary)
Keywords: Hecke groups, principal congruence subgroup

1. Introduction

The Hecke groups $H(\lambda)$ are the discrete subgroups of $PSL(2,\mathbb{R})$ (the group of the orientation preserving isometries of the upper half plane U) generated by two linear fractional transformations

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

where $\lambda \in \mathbb{R}$, $\lambda \geq 2$ or $\lambda = \lambda_q = 2\cos(\frac{\pi}{q})$, $q \in \mathbb{N}$, $q \geq 3$. These values of λ are the only ones that give discrete groups, by a theorem of Hecke, [2].

The Hecke groups $H(\lambda_q)$ have been studied for many aspects in literature (see for instance [17], [1], [3], [8], [13] or [14]). The most important and studied Hecke group is the modular group $H(\lambda_3) = PSL(2,\mathbb{Z})$. The next two interesting Hecke groups are obtained for $q = 4$

and 6. These two groups are of particular interest since they are the only Hecke groups $H(\lambda_q)$, aside from the modular group, whose elements are completely known. The principal congruence subgroups of these Hecke groups have been investigated extensively (see [1], [3], [8], [13] or [14]).

In this paper, we are interested in the case $\lambda \geq 2$. When $\lambda > 2$, these Hecke groups are Fuchsian groups of the second kind. When $\lambda = 2$, the element $S = RT$ is parabolic and when $\lambda > 2$, the element $S = RT$ is hyperbolic. It is known that $H(\lambda)$ is a free product of a cyclic group of order 2 and of an infinite cyclic group where $\lambda \geq 2$ (see [4] and [12]). In other words

$$H(\lambda) \cong C_2 * \mathbb{Z}.$$

Here, we only consider the case $\lambda = \sqrt{5}$. We determine the quotient groups of the Hecke group $H(\sqrt{5})$ by its principal congruence subgroups using a classical method, defined by Macbeath ([5]). Then we compute signatures of these normal subgroups using the permutation method and Riemann-Hurwitz formula (see [18] and [6]). We make use of the notion of the quadratic reciprocity and the Fibonacci and Lucas numbers. Note that in [10], these results have been extended to all the Hecke groups $H(\sqrt{q})$ ($q \geq 5$ prime number) by using two new number sequences related to Fibonacci and Lucas numbers.

In the case $\lambda = \sqrt{5}$, the underlying field is a quadratic extension of $\mathbb{Q}$ by $\sqrt{5}$, i.e. $\mathbb{Q}(\sqrt{5})$. A presentation of $H(\sqrt{5})$ is

$$H(\sqrt{5}) = \left\langle R, S;\ R^2 = S^\infty = (RS)^\infty = 1 \right\rangle$$

where $S = RT$ and the signature of $H(\sqrt{5})$ is $(0; 2, \infty; 1)$. By identifying the transformation $w = \frac{az+b}{cz+d}$ with the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $H(\sqrt{5})$ may be regarded as a multiplicative group of 2×2 matrices in which a matrix is identified with its negative. R and S have matrix representations

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{5} \end{pmatrix},$$

respectively. All elements of $H(\sqrt{5})$ are one of the following two forms:

(i) $$\begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix}; a, b, c, d \in \mathbb{Z}, ad - 5bc = 1,$$

(ii) $$\begin{pmatrix} a\sqrt{5} & b \\ c & d\sqrt{5} \end{pmatrix}; a, b, c, d \in \mathbb{Z}, 5ad - bc = 1.$$

Those of type (i) are called even while those of type (ii) are called odd. But the converse statement is not true. That is, all elements of type (i) or (ii) need not be in $H(\sqrt{5})$. In [16], Rosen proved that $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in H(\lambda)$ if and only if $\frac{A}{C}$ is a finite λ -fraction (see [16] for more details).

The set of all even elements form a subgroup of index 2 called the even subgroup. It is denoted by $H_e(\sqrt{5})$. In [11], it was proved that $H_e(\sqrt{5})$ is isomorphic to the free product of two infinite cyclic groups generated by the parabolic generators $T = RS$ and $U = SR$, that is,

$$H_e(\sqrt{5}) \cong \mathbb{Z} * \mathbb{Z} \cong F_2.$$

Also the signature of $H_e(\sqrt{5})$ is $(0; \infty^{(2)}; 1)$.

The even subgroup $H_e(\sqrt{5})$ is the most important amongst the normal subgroups of $H(\sqrt{5})$. It contains infinitely many normal subgroups of $H(\sqrt{5})$.

Being a free product of a cyclic group of order 2 and of an infinite cyclic group, by the Kurosh subgroup theorem, $H(\sqrt{5})$ has two kinds of subgroups those which are free and those with torsion (being free product of $\mathbb{Z}_2$'s and $\mathbb{Z}$'s).

2. Principal congruence subgroups

An important class of normal subgroups in $H(\sqrt{5})$ are the principal congruence subgroups. Let p be a rational prime. The principal congruence subgroup $H_p(\sqrt{5})$ of level p is defined by

$$H_p(\sqrt{5}) = \left\{ A = \begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix} \in H(\sqrt{5}) : \ A \equiv \pm I \ (mod\ p) \right\}.$$

In general, this is equivalent to

$$H_p(\sqrt{5}) = \left\{ \begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix} : \ a \equiv d \equiv 1, \ b \equiv c \equiv 0 \ (mod\ p), \ ad - 5bc = 1 \right\}.$$

$H_p(\sqrt{5})$ is always a normal subgroup of $H(\sqrt{5})$. Note that by the definition

$$H_p(\sqrt{5}) \lhd H_e(\sqrt{5}). \tag{1}$$

A subgroup of $H(\sqrt{5})$ containing a principal congruence subgroup of level p is called a congruence subgroup of level p. In general, not all congruence subgroups are normal in $H(\sqrt{5})$.

Another way of obtaining $H_p(\sqrt{5})$ is to consider the reduction homomorphism which is induced by reducing entries modulo p.

Let $\wp$ be an ideal of $\mathbb{Z}[\sqrt{5}]$ which is an extension of the ring of integers by the algebraic number $\sqrt{5}$. Then the natural map

$$\Theta_\wp : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]/\wp$$

induces a map

$$H(\sqrt{5}) \to PSL(2, \mathbb{Z}[\sqrt{5}]/\wp)$$

whose kernel is called the principal congruence subgroup of level $\wp$.

Let now s be an integer such that the polynomial x^2-5 has solutions in $GF(p^s)$. We know that such an s exists and satisfies $1 \le s \le 2 = \deg(x^2-5)$. Let u be a solution of x^2-5 in $GF(p^s)$. Let us take $\wp$ to be the ideal generated by u in $\mathbb{Z}[\sqrt{5}]$. As above we can define

$$\Theta_{p,u} : H(\sqrt{5}) \to PSL(2,\ p^s)$$

as the homomorphism induced by $\sqrt{5} \to u$. Let

$$K_{p,u}(\sqrt{5}) = Ker(\Theta_{p,u}).$$

As the kernel of a homomorphism of $H(\sqrt{5})$, $K_{p,u}(\sqrt{5})$ is normal in $H(\sqrt{5})$.

Given p, as $K_{p,u}(\sqrt{5})$ depends on p and u, we have a chance of having a different kernel for each root u. However sometimes they do coincide. Indeed, it trivially follows from the Kummer's theorem that if u, v correspond to the same irreducible factor f of x^2-5 over $GF(p^s)$, then $K_{p,u}(\sqrt{5}) = K_{p,v}(\sqrt{5})$. Even when $u,\ v$ give different factors of x^2-5, we may have $K_{p,u}(\sqrt{5}) = K_{p,v}(\sqrt{5})$. In Lemma 2.4, we show that $K_{p,u}(\sqrt{5}) = K_{p,-u}(\sqrt{5})$ when 5 is a quadratic residue mod p.

It is easy to see that $K_{p,u}(\sqrt{5})$ is a normal congruence subgroup of level p of $H(\sqrt{5})$, i.e.

$$H_p(\sqrt{5}) \trianglelefteq K_{p,u}(\sqrt{5}).$$

Therefore $H_p(\sqrt{5}) \le \bigcap\limits_{\text{all } u} K_{p,u}(\sqrt{5})$. When the index of $H_p(\sqrt{5})$ in $K_{p,u}(\sqrt{5})$ is not 1, i.e. when they are different, we shall use $K_{p,u}(\sqrt{5})$ to calculate $H_p(\sqrt{5})$. We first try to find the quotient of $H(\sqrt{5})$ with $K_{p,u}(\sqrt{5})$. It is then easy to determine $H(\sqrt{5})/H_p(\sqrt{5})$. To determine both quotients we use some results of Macbeath, [5]. After finding the quotients of $H(\sqrt{5})$ by the principal congruence subgroups, we find the group theoretical structure of them. For notions and terminology see [5] and [18]. Also for the notion of quadratic reciprocity see [15].

Before stating our main results we need the following lemmas. Firstly, the following lemma can be found as an exercise in [15].

Lemma 2.1. *Let p be an odd prime. Then we have the following:*

i) $(\frac{5}{p}) = 1$, *that is* 5 *is a quadratic residue mod p if and only if* $p \equiv \pm 1$ $(mod\ 10)$.

ii) $(\frac{5}{p}) = -1$, *that is* 5 *is a quadratic nonresidue mod p if and only if* $p \equiv \pm 3$ $(mod\ 10)$.

In [9], it was proved that

$$S^{2n} = \begin{pmatrix} -L_{2n-1} & -F_{2n}\sqrt{5} \\ F_{2n}\sqrt{5} & L_{2n+1} \end{pmatrix} \tag{2}$$

and

$$S^{2n+1} = \begin{pmatrix} -F_{2n}\sqrt{5} & -L_{2n+1} \\ L_{2n+1} & F_{2n+2}\sqrt{5} \end{pmatrix} \tag{3}$$

where F_n and L_n denote the nth Fibonacci number and nth Lucas number. For any odd prime p, let us consider S^p in *mod* p. From (3) we have

$$S^p = \begin{pmatrix} -F_{p-1}\sqrt{5} & -L_p \\ L_p & F_{p+1}\sqrt{5} \end{pmatrix}.$$

It is known that $F_{p-1} \equiv 0$ $(mod\ p)$ and $F_p \equiv 1$ $(mod\ p)$, when $\left(\frac{q}{p}\right) = 1$ where $\left(\frac{q}{p}\right)$ is the Legendre symbol, [19]. Then we find $F_{p+1} \equiv 1$ $(mod\ p)$ and $L_p \equiv 1$ $(mod\ p)$. Therefore we have

$$S^p \equiv \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{5} \end{pmatrix} = S\ (mod\ p),$$

that is, $S^{p-1} \equiv I$ $(mod\ p)$. In this case, we can only say that the order of S $(mod\ p)$ divides $p-1$.

Let $\left(\frac{q}{p}\right) = -1$. Then we have $F_p \equiv -1$ $(mod\ p)$, $F_{p+1} \equiv 0$ $(mod\ p)$ and hence we find $F_{p-1} \equiv 1$ $(mod\ p)$. So we get

$$S^p \equiv \begin{pmatrix} -\sqrt{5} & -1 \\ 1 & 0 \end{pmatrix} = -S^{-1}\ (mod\ p),$$

that is, $S^{p+1} \equiv -I$ $(mod\ p)$. In this case, the order of S $(mod\ p)$ divides $p+1$.

Therefore we get the following lemma:

Lemma 2.2.

(i) *Let* $\left(\frac{q}{p}\right) = 1$. *Then* $S^{p-1} \equiv I$ $(mod\ p)$ *and the order of* S, *say* l, *divides* $p-1$.

(ii) *Let* $\left(\frac{q}{p}\right) = -1$. *Then* $S^{p+1} \equiv -I$ $(mod\ p)$ *and the order of* S *divides* $p+1$.

Now we can give our main theorem.

Theorem 2.3. *The quotient groups of the Hecke group* $H(\sqrt{5})$ *by its congruence subgroups* $K_{p,u}(\sqrt{5})$ *and its principal congruence subgroups* $H_p(\sqrt{5})$ *are as follows:*

$$H(\sqrt{5})/K_{p,u}(\sqrt{5}) \cong \begin{cases} PSL(2,p), & p \equiv \pm 1\ (mod\ 10) \\ PGL(2,p), & p \equiv \pm 3\ (mod\ 10) \\ C_2, & p = 5 \\ D_3, & p = 2 \end{cases}$$

and

$$H(\sqrt{5})/H_p(\sqrt{5}) \cong \begin{cases} C_2 \times PSL(2,p), & p \equiv \pm 1\ (mod\ 10) \\ PGL(2,p), & p \equiv \pm 3\ (mod\ 10) \\ C_{10}, & p = 5 \\ D_6, & p = 2 \end{cases}.$$

Proof. *Case 1.* Let $p \neq 2$ and $p \neq 5$, be so that 5 is a square modulo p, that is, 5 is a quadratic residue $mod\ p$. In this case there exists an element u in $GF(p)$ such that $u^2 = 5$. Therefore $\sqrt{5}$ can be considered as an element of $GF(p)$. Let us consider the homomorphism of $H(\sqrt{5})$ reducing all elements of it modulo p. The images of R, S and T under this homomorphism are denoted by r_p, s_p and t_p respectively. Then clearly r_p, s_p and t_p belong to $PSL(2,p)$. Now there is a homomorphism

$$\theta : H(\sqrt{5}) \to PSL(2,p)$$

induced by $\sqrt{5} \to u$. Then our problem is to find the subgroup of $PSL(2,p) = G$, generated by r_p, s_p and t_p.

Following Macbeath's terminology let $k = GF(p)$. Then κ, the smallest subfield of k containing $\alpha = tr(r_p) = 0$, $\beta = tr(s_p) = \sqrt{5}$ and $\gamma = tr(t_p) = 2$, is also $GF(p)$ as $\sqrt{5} \in GF(p)$. In this case, for all p, the $\Gamma_p(\sqrt{5})$−triple (r_p, s_p, t_p) is not singular since the discriminant of the associated quadratic form, which is $-\frac{u^2}{4}$, is not 0 (where $\Gamma_p(\sqrt{5})$ denotes the image of $H(\sqrt{5})$ modulo p, generated by r_p and s_p).

On the other hand, the associated $\mathbb{N}$-triple (giving the orders of its elements) is $(2,l,p)$ where l depends on p. The triple is not exceptional since $p \equiv \pm 1 \ (mod\ 10)$ and $l \neq 2$ (remember that all exceptional triples are $(2,2,n)$, $n \in \mathbb{N}$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$ and $(2,5,5)$ ($(2,3,5)$ is a homomorphic image of $(2,5,5)$), see [5]).

Then by Theorem 4 in [5], (r_p, s_p, t_p) generates a projective subgroup of G, and by Theorem 5 in [5], as $\kappa = GF(p)$ is not a quadratic extension of any other field, this subgroup is the full group $PSL(2,p)$, i.e.

$$H(\sqrt{5})/K_{p,u}(\sqrt{5}) \cong PSL(2,p).$$

Let us now find the quotient of $H(\sqrt{5})$ by the principal congruence subgroup $H_p(\sqrt{5})$ in this case. Recall that, by (1), $H_p(\sqrt{5})$ is a subgroup of the even subgroup $H_e(\sqrt{5})$. Therefore there are no odd elements in $H_p(\sqrt{5})$.

We now want to find the quotient group $K_{p,u}(\sqrt{5})/H_p(\sqrt{5})$. To show that it is not the trivial group, we show that $K_{p,u}(\sqrt{5})$ contains an odd element.

If A is such an element, then

$$A = \begin{pmatrix} x\sqrt{5} & y \\ z & t\sqrt{5} \end{pmatrix}; \ \Delta = 5xt - yz = 1, \ x,y,z,t \in \mathbb{Z}$$

is in $K_{p,u}(\sqrt{5}) - H_p(\sqrt{5})$. Now

$$A^2 = \begin{pmatrix} 5x^2 + yz & \sqrt{5}(xy + yt) \\ \sqrt{5}(xz + tz) & 5t^2 + yz \end{pmatrix}$$

and since $xu \equiv tu \equiv 1$, $y \equiv z \equiv 0 \ mod\ p$, we have $x^2u^2 = 5x^2 \equiv 1 \ mod\ p$ and similarly $t^2u^2 = 5t^2 \equiv 1 \ mod\ p$. Hence A is of exponent two $mod\ H_p(\sqrt{5})$. If B is another such element in $K_{p,u}(\sqrt{5}) - H_p(\sqrt{5})$, then it is easy to see that $AB^{-1} \equiv \pm I \ (mod\ p)$ and hence $AH_p(\sqrt{5}) = BH_p(\sqrt{5})$. Therefore we can write

$$K_{p,u}(\sqrt{5}) = H_p(\sqrt{5}) \cup AH_p(\sqrt{5})$$

as $A \notin H_p(\sqrt{5})$.

Now we want to show that any element $\begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix}$ of $H_e(\sqrt{5})/H_p(\sqrt{5})$ commutes with A. This is true since

$$\begin{pmatrix} x\sqrt{5} & y \\ z & t\sqrt{5} \end{pmatrix} \begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix} = \begin{pmatrix} \sqrt{5}(ax + cy) & 5bx + dy \\ az + 5ct & \sqrt{5}(bz + dt) \end{pmatrix},$$

$$\begin{pmatrix} a & b\sqrt{5} \\ c\sqrt{5} & d \end{pmatrix} \begin{pmatrix} x\sqrt{5} & y \\ z & t\sqrt{5} \end{pmatrix} = \begin{pmatrix} \sqrt{5}(ax+bz) & ay+5bt \\ 5xc+dz & \sqrt{5}(cy+dt) \end{pmatrix}$$

and since $y \equiv z \equiv 0$ and $x \equiv t \ mod\ p$. Therefore we have the following subgroup lattice (see Figure 1) and hence

$$H(\sqrt{5})/H_p(\sqrt{5}) \cong K_{p,u}(\sqrt{5})/H_p(\sqrt{5}) \times H_e(\sqrt{5})/H_p(\sqrt{5}) \cong C_2 \times PSL(2,p).$$

$$\begin{tikzcd}
 & H(\sqrt{5}) \arrow[dl, dash, "PSL(2,p)"'] \arrow[dr, dash, "C_2"] & \\
K_{p,u}(\sqrt{5}) \arrow[dr, dash, "C_2"'] & & H_e(\sqrt{5}) \arrow[dl, dash, "PSL(2,p)"] \\
 & H_p(\sqrt{5}) &
\end{tikzcd}$$

Figure 1

Indeed, $K_{p,u}(\sqrt{5})$ contains an odd element. Let $A = \begin{pmatrix} x\sqrt{5} & y \\ z & t\sqrt{5} \end{pmatrix}$ be as above. We have $\Delta = 5xt - yz = 1$ and $xu \equiv tu \equiv 1$, $y \equiv z \equiv 0$ $(mod\ p)$ where $u \equiv \sqrt{5}\ mod\ p$. Let $v \in GF(p)$ be such that $uv \equiv 1\ mod\ p$. Then we can choose

$$A = T^{-v}RT^{-v}RT^{-v}R = (T^{-v}R)^3 = \begin{pmatrix} v(2-5v^2)\sqrt{5} & 1-5v^2 \\ 5v^2-1 & v\sqrt{5} \end{pmatrix} \in H(\sqrt{5}). \tag{4}$$

That is, it is always possible to find an odd element A of $K_{p,u}(\sqrt{5})$ which does not belong to $H_p(\sqrt{5})$.

Case 2. Now let p be so that 5 is not a square modulo p, i.e. 5 is a quadratic nonresidue $mod\ p$. In this case $\sqrt{5}$ can not be considered as an element of $GF(p)$. Therefore there are no odd elements in the kernel $K_{p,u}(\sqrt{5})$ and hence $K_{p,u}(\sqrt{5}) = H_p(\sqrt{5})$.

Now we shall extend $GF(p)$ to its quadratic extension $GF(p^2)$. Then $u = \sqrt{5}$ can be considered to be in $GF(p^2)$ and there exists a homomorphism $\theta : H(\sqrt{5}) \to PSL(2,p^2)$ induced in a similar way to Case 1.

Let $k = GF(p^2)$. Then κ, the smallest subfield of k containing traces α, β, γ of r_p, s_p and t_p, is also $GF(p^2)$. Then as in Case 1, (r_p, s_p, t_p) is not a singular triple. Let $p > 3$. Then the G_0-triple (r_p, s_p, t_p) is not an exceptional triple and generates $PGL(2,p)$ since κ is the quadratic extension of $\kappa_0 = GF(p)$ and $\gamma = 2$ lies in κ_0 while $\alpha = 0$ and $\beta = \sqrt{5}$ is the square root in κ of 5 which is a non-square in κ_0, that is, $H(\sqrt{5})/K_{p,u}(\sqrt{5}) \cong PGL(2,p)$ (see [5], p.28).

If $p = 3$, (r_p, s_p, t_p) is an exceptional triple since the associated $\mathbb{N}$-triple is $(2,4,3)$ which generates a group isomorphic to the symmetric group S_4 and we get

$$H(\sqrt{5})/K_{3,u}(\sqrt{5}) \cong S_4 \cong PGL(2,3).$$

Consequently, $H(\sqrt{5})/H_p(\sqrt{5}) \cong PGL(2,p)$.

Case 3. Let $p = 5$. As $\sqrt{5}$ can be thought as the zero element of $GF(5) = \{0, 1, 2, 3, 4\}$, $t_5 \equiv I \ mod \ 5$. As $r_5^2 = 1$ as well, we have $H(\sqrt{5})/K_{5,0}(\sqrt{5}) \cong C_2$.

It is easy to show that $S^{2n} \equiv \begin{pmatrix} (-1)^n & (-1)^n n\sqrt{5} \\ (-1)^{n+1} n\sqrt{5} & (-1)^n \end{pmatrix} (mod \ 5)$. Then, we have

$$S^{10} \equiv \begin{pmatrix} -1 & -5\sqrt{5} \\ 5\sqrt{5} & -1 \end{pmatrix} (mod \ 5) \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I(mod \ 5).$$

Thus, in the quotient $H(\sqrt{5})/H_5(\sqrt{5})$ we have the relations $r_5^2 = s_5^{10} = t_5^5 = I$ and $s_5 = r_5 t_5$ as $(\sqrt{5})^2 = 5 \equiv 0 \ (mod \ 5)$. Hence we have $H(\sqrt{5})/H_5(\sqrt{5}) \cong C_{10}$.

Case 4. Let $p = 2$. Then (r_2, s_2, t_2) gives the exceptional $\mathbb{N}$-triple $(2, 3, 2)$ and hence generates a group isomorphic to the dihedral group D_3 of order 6.

Let us now consider the quotient group $H(\sqrt{5})/H_2(\sqrt{5})$. In this case we have the relations $r_2^2 = s_2^6 = t_2^2 = I$. Therefore $H(\sqrt{5})/H_2(\sqrt{5})$ is isomorphic to the dihedral group D_6 of order 12.

Then by Lemma 2.1, the proof is completed. □

Lemma 2.4. *If $p \equiv \pm 1 \ (mod \ 10)$, then we have $K_{p,u}(\sqrt{5}) = K_{p,-u}(\sqrt{5})$.*

Proof. If $p \equiv \pm 1 \ (mod \ 10)$, then $x^2 - 5 \equiv (x - u)(x + u) \ mod \ p$ for some $u \in GF(p)$. In $K_{p,u}(\sqrt{5})$, let us consider the element $A = (T^{-v}R)^3$ obtained in (4). Now we have $R(T^{-v}R)^3 R = (T^v R)^3$. Since $K_{p,u}(\sqrt{5})$ is a normal subgroup, then the equality holds, as required. □

Notice that generators of one of the two principal congruence subgroups corresponding to values u and $-u$ are just the inverses of the generators of the other.

Hence we have found all quotient groups of $H(\sqrt{5})$ with $K_{p,u}(\sqrt{5})$ and with the principal congruence subgroups $H_p(\sqrt{5})$, for all prime p. By means of them we can give the index formula for these two congruence subgroups.

Corollary 2.5. *The indices of the congruence subgroups $K_{p,u}(\sqrt{5})$ and $H_p(\sqrt{5})$ in $H(\sqrt{5})$ are*

$$\left| H(\sqrt{5})/K_{p,u}(\sqrt{5}) \right| = \begin{cases} \frac{p(p-1)(p+1)}{2} & \textit{if } p \equiv \pm 1 \ (mod \ 10) \\ p(p-1)(p+1) & \textit{if } p \equiv \pm 3 \ (mod \ 10) \\ 2 & \textit{if } p = 5 \\ 6 & \textit{if } p = 2 \end{cases}$$

and

$$|H(\sqrt{q})/H_p(\sqrt{q})| = \begin{cases} p(p-1)(p+1) & \textit{if } p \neq 5 \textit{ and } p \neq 2 \\ 10 & \textit{if } p = 5 \\ 12 & \textit{if } p = 2 \end{cases} .$$

We are now able to determine the group theoretical structure of the subgroups $K_{p,u}(\sqrt{5})$ and $H_p(\sqrt{5})$. Recall that $H_p(\sqrt{5}) \triangleleft K_{p,u}(\sqrt{5})$ and also by the definition of $H_p(\sqrt{5})$, $H_p(\sqrt{5}) \triangleleft H_e(\sqrt{5})$. Then we have four cases:

Case 1. Let $p = 5$. We know that $H(\sqrt{5})/K_{5,0}(\sqrt{5}) \cong C_2$. Since R and S are both mapped to the generator of C_2, we find $K_{5,0}(\sqrt{5}) = H_e(\sqrt{5})$.

We also proved that $H(\sqrt{5})/H_5(\sqrt{5}) \cong C_{10}$. The group C_{10} has a presentation

$$\left\langle \alpha, \beta, \gamma; \alpha^2 = \beta^5 = \gamma^{10} = I \right\rangle .$$

Then we have $R \to \alpha$, $S \to \beta$ and therefore $RS \to \alpha\beta$, i.e.

$$\begin{aligned} R &\to (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10) \\ S &\to (1\ 3\ 5\ 7\ 9)(2\ 4\ 6\ 8\ 10) \\ T &\to (1\ 4\ 5\ 8\ 9\ 2\ 3\ 6\ 7\ 10). \end{aligned}$$

By the permutation method and Riemann-Hurwitz formula we find the signature of $H_5(\sqrt{5})$ as $(2; \infty; 2)$.

Case 2. Let $p = 2$. We know that $H(\sqrt{5})/K_{2,u}(\sqrt{5}) \cong D_3$ and $H(\sqrt{5})/H_2(\sqrt{5}) \cong D_6$. In the former one, the quotient group is $D_3 \cong (2, 3, 2)$ and hence by the permutation method it is easy to see that $K_{2,u}(\sqrt{5})$ has the signature $(0; \infty^{(3)}; 2)$ and therefore $K_{2,u}(\sqrt{5}) \cong F_4$, where F_4 denotes a free group of rank four.

Secondly let us consider $H(\sqrt{5})/H_2(\sqrt{5}) \cong D_6 \cong (2, 6, 2)$. In a similar way we obtain the signature of $H_2(\sqrt{5})$ as $(0; \infty^{(6)}; 2)$ and therefore it is a free group of rank seven, i.e. $H_2(\sqrt{q}) \cong F_7$.

Case 3. Let $p \equiv \pm 1$ $(mod\ 10)$. Then the quotient groups are $PSL(2, p)$ and $C_2 \times PSL(2, p)$ as we have proved. Let now r_p, s_p be the images of R, S in $PSL(2, p)$ and $r_p^{'}$, $s_p^{'}$ be the images of R, S in $C_2 \times PSL(2, p)$, respectively. Then the relations $r_p^2 = s_p^l = I$ and $(r_p^{'})^2 = (s_p^{'})^m = I$ are satisfied. Here, l is related to p. As odd powers of S are odd and even powers of S are even, we have $m = 2l$ when l is odd and we have $m = l$ when l is even. From Lemma 2.2, we know that l is a divisor of $p - 1$. So l can be $\frac{p-1}{k}$ for some positive integer k. In this case both $K_{p,u}(\sqrt{5})$ and $H_p(\sqrt{5})$ are free groups. The orders of the parabolic elements $r_p s_p$ and $r_p^{'} s_p^{'}$ are p. Then T goes to an element of order p in both quotient groups. Let μ be the index of the congruence subgroup $K_{p,u}(\sqrt{5})$ in $H(\sqrt{5})$. By the permutation method and Riemann-Hurwitz formula, we find the signature of this subgroup as

$$\left(1 + \frac{p+1}{8}\left((p-2)(p-1) - 2kp\right); \infty^{\left(\frac{(p-1)(p+1)}{2}\right)}; \frac{kp(p+1)}{2}\right).$$

Again, if $\mu^{'}$ is the index of the principal congruence subgroup $H_p(\sqrt{5})$ in $H(\sqrt{5})$, we find the signature of this subgroup as

$$\left(1 + \frac{\mu^{'}}{4pm}(pm - 2p - 2m);\ \infty^{\left(\frac{\mu^{'}}{p}\right)}; \frac{\mu^{'}}{m}\right).$$

Example 2.6. Let $q = 5$, $p = 11$. Then we have $l = 5$ and $m = 10$. These two quotient groups are $PSL(2, 11)$ and $C_2 \times PSL(2, 11)$, respectively. Therefore we find the signature of $K_{11,7}(\sqrt{5})$ as $(70; \infty^{(60)}; 132)$ and the signature of $H_{11}(\sqrt{5})$ as $(205; \infty^{(120)}; 132)$.

Case 4. Let $p \equiv \pm 3 \, mod \, p$. We proved that both quotient groups are isomorphic to $PGL(2, p)$. From Lemma 2.2, we know that the associated $\mathbb{N}-$triple is $(2, \frac{p+1}{k}, p)$ for some positive integer k. As in Case 3, we have the signature of $K_{p,u}(\sqrt{5}) = H_p(\sqrt{5})$ as

$$\left(1 + \frac{p-1}{4}\left((p+1)(p-2) - 2kp\right); \infty^{((p-1)(p+1))}; kp(p-1)\right).$$

Example 2.7. Let $p = 3$. Then we have $H(\sqrt{5})/K_{3,u}(\sqrt{5}) \cong H(\sqrt{5})/H_3(\sqrt{5}) \cong PGL(2, 3) \cong S_4$ and therefore $K_{3,u}(\sqrt{5}) = H_3(\sqrt{5}) \cong (0; \infty^{(8)}; 6)$.

Acknowledgement. The authors wishes to thank the referee for many helpful comments and suggestions.

References

[1] Cangül, İ. N.; Singerman, D.: *Normal Subgroups of Hecke Groups and Regular Maps*. Math. Proc. Camb. Phil. Soc. **123** (1998), 59–74. Zbl 0893.20036

[2] Hecke, E.: *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichungen*. Math. Ann. **112** (1936), 664–699. Zbl 0014.01601

[3] Lang, M. L.; Lim, C. H.; Tan, S. P.: *Principal Congruence Subgroups of the Hecke Groups*. J. Number Theory **85**(2) (2000), 220–230. Zbl 0964.11023

[4] Lyndon, R. C.; Ullman, J. L.: *Pairs of Real 2-by-2 Matrices that Generate Free Products*. Mich. Math. J. **15** (1968), 161–166. Zbl 0159.30602

[5] Macbeath, A. M.: *Generators of The Linear Fractional Groups*. Proc. Symp. Pure. Math. A. M. S. **12** (1969), 14–32. Zbl 0192.35703

[6] Maclachlan, C.: *Maximal Normal Fuchsian Groups*. Illionis J. Math. **15** (1971), 104–113. Zbl 0203.39201

[7] Magnus, W.; Karras, A.; Solitar, D.: *Combinatorial Group Theory*. Dover Publication, Inc., New York 1976. Zbl 0362.20023

[8] Newman, M.: *Integral Matrices*, Academic Press, New York 1972. Zbl 0254.15009

[9] Yılmaz Özgür, N.: *Generalizations of Fibonacci and Lucas Sequences*. Note Mat. **21**(1) (2002), 125–137.

[10] Yılmaz Özgür, N.: *Principal Congruence Subgroups of the Hecke groups* $H(\sqrt{q})$. Submitted.

[11] Yılmaz Özgür, N.; Cangül, İ. N.: *Normal Subgroups of Hecke Group* $H(\sqrt{5})$. Bull. Inst. Math. Acad. Sinica **28**(4) (2000), 277–283. Zbl 0973.20041

[12] Yılmaz Özgür, N.; Cangül, İ. N.: *On the Group Structure and Parabolic Points of the Hecke Group* $H(\lambda)$. Proc. Estonian Acad. Sci. Phys. Math. **51**(1) (2002), 35–46. Zbl 1007.20048

[13] Parson, L. A.: *Generalized Kloosterman Sums and the Fourier Coefficients of Cusp Forms*. Trans. A. M. S. **217** (1976), 329–350. Zbl 0324.10018

[14] Parson, L. A.: *Normal Congruence Subgroups of the Hecke Groups $G(\sqrt{2})$ and $G(\sqrt{3})$*, Pacific J. Math. **70** (1977), 481–487. Zbl 0375.10014

[15] Rose, H. E.: *A Course in Number Theory*. Oxford Science Publications, Second Edition 1998. cf. 1994: Zbl 0818.11001
or 1995: Zbl 0835.11001

[16] Rosen, D.: *A Class of Continued Fractions Associated with Certain Properly Discontinuous Groups*. Duke Math. J. **21** (1954), 549–564. Zbl 0056.30703

[17] Schmidt, T. A.; Sheingorn, M.: *Length Spectra of the Hecke Triangle Groups*. Math. Z. **220**(3) (1995), 369–397. Zbl 0840.11019

[18] Singerman, D.: *Subgroups of Fuchsian Groups and Finite Permutation Groups*. Bull. L.M.S. **2** (1970), 319–323. Zbl 0206.30804

[19] Vajda, S.: *Fibonacci and Lucas Numbers, and the Golden Section: Theory and Applications*. Halsted Press 1989. Zbl 0695.10001

Received September 9, 2002