Acta Mathematica Sinica, English Series
Mar., 2006, Vol. 22, No. 2, pp. 383–392
Published online: Oct. 17, 2005
DOI: 10.1007/s10114-005-0609-2
Http://www.ActaMath.com

Acta Mathematica Sinica, English Series

Principal Congruence Subgroups of Hecke Groups $H(\sqrt{q})$

Nihal YILMAZ ÖZGÜR
Department of Mathematics, Balikesir University, 10100 *Balikesir, Turkey*
E-mail: nihal@balikesir.edu.tr

Abstract Using the notion of quadratic reciprocity, we discuss the principal congruence subgroups of the Hecke groups $H(\sqrt{q}), q > 5$ prime number.

Keywords Hecke group, Principal congruence subgroup, Congruence subgroup
MR(2000) Subject Classification 11F06; 20H05, 20H10

1 Introduction

The Hecke groups $H(\lambda)$ are the discrete subgroups of $PSL(2,\mathbb{R})$ (the group of 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 [1] (for more information about the Hecke groups, see [2–7] and [8]). 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 an infinite cyclic group where $\lambda \geq 2$ (see [9] and [10]). In other words

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

Here, we consider only the case $\lambda = \sqrt{q},\ q > 5$ prime number. We determine the quotient groups of the Hecke groups $H(\sqrt{q})$ by their principal congruence subgroups using a classical method, defined by Macbeath [11]. Then we compute signatures of these normal subgroups using the permutation method and Riemann–Hurwitz formula (see [12] and [13]). We make use of the notion of quadratic reciprocity and the number sequences related to Fibonacci and Lucas sequences. Note that in [14], principal congruence subgroups of the Hecke group $H(\sqrt{5})$ were investigated by using Fibonacci and Lucas numbers.

Our argument depends on determining all the powers of S which is one of the generators of $H(\sqrt{q})$. To answer the question that for what values of n the congruence $S^n \equiv \pm I(\text{mod } p)$, p being an odd prime, holds, we need to compute the n-th power of S, for every integer n. It is hard to compute S^n easily. In [15], for each $q \geq 5$, it was introduced two new sequences denoted by $\mathscr{U}_n^q$ and $\mathscr{V}_n^q$, and proved that

$$S^{2n} = \begin{pmatrix} -\mathscr{V}_{2n-1}^q & -\mathscr{U}_{2n}^q\sqrt{q} \\ \mathscr{U}_{2n}^q\sqrt{q} & \mathscr{V}_{2n+1}^q \end{pmatrix} \tag{1}$$

and

$$S^{2n+1} = \begin{pmatrix} -\mathscr{U}_{2n}^q\sqrt{q} & -\mathscr{V}_{2n+1}^q \\ \mathscr{V}_{2n+1}^q & \mathscr{U}_{2n+2}^q\sqrt{q} \end{pmatrix}. \tag{2}$$

Received October 10, 2003, Accepted February 17, 2005

For $q = 5$, $\mathscr{U}_n^5 = F_n$ and $\mathscr{V}_n^5 = L_n$, where F_n denotes the n-th Fibonacci number and L_n denotes n-th Lucas number. The sequences $\mathscr{U}_n^q$ and $\mathscr{V}_n^q$ are not generalized Fibonacci sequences except for $q = 5$. These new sequences have similar properties to those of Fibonacci and Lucas sequences, some of them the same as ones for Fibonacci and Lucas. For example in [15], it was shown that

$$\mathscr{V}_p^q = \mathscr{U}_{p+1}^q + \mathscr{U}_{p-1}^q. \tag{3}$$

In a sense, $\mathscr{U}_n^q$ is a generalization of F_n and $\mathscr{V}_n^q$ is a generalization of L_n (see [15] and [16], for more details about the $\mathscr{U}_n^q$ and $\mathscr{V}_n^q$). In [14], some facts were used about the Fibonacci and Lucas numbers. Here we use some basic properties of the sequences $\mathscr{U}_n^q$ and $\mathscr{V}_n^q$.

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

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

where $S = RT$ and the signature of $H(\sqrt{q})$ is $(0; 2, \infty; 1)$. By identifying the transformation $w = \frac{az+b}{cz+d}$ with the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $H(\sqrt{q})$ 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

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

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

(i) $\left(\begin{smallmatrix} a & b\sqrt{q} \\ c\sqrt{q} & d \end{smallmatrix}\right)$; $a, b, c, d \in \mathbb{Z}$, $ad - qbc = 1$; (ii) $\left(\begin{smallmatrix} a\sqrt{q} & b \\ c & d\sqrt{q} \end{smallmatrix}\right)$; $a, b, c, d \in \mathbb{Z}$, $qad - bc = 1$.

Those of type (i) are called even while those of type (ii) are called odd. R and S, the generators of $H(\sqrt{q})$, are both odd. The set of all odd elements is not closed as the product of two odd elements is always even. Similarly we have odd.even = odd, even.odd = odd, even.even = even. Therefore we guarantee that this classification is a partition. As each element V of $H(\sqrt{q})$ is a product of generators, we conclude that V is either odd or even. But the converse statement is not true. That is, all elements of type (i) or (ii) need not be in $H(\sqrt{q})$. In [7], Rosen proved that $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in H(\lambda)$ if and only if $\frac{A}{C}$ is a finite λ-fraction (see [7] for more details).

The set of all even elements forms a subgroup of index 2 called the even subgroup. It is denoted by $H_e(\sqrt{q})$. Having index two, $H_e(\sqrt{q})$ is a normal subgroup of $H(\sqrt{q})$. Also, $H_e(\sqrt{q})$ is the free product of two infinite cyclic groups generated by $T = RS$ and $U = SR$. Indeed, being odd elements, R and S both go to 2-cycles under the homomorphism

$$H(\sqrt{q}) \to H(\sqrt{q})/H_e(\sqrt{q}) \cong C_2,$$

that is, $R \to (1\ \ 2)$, $S \to (1\ \ 2)$, $T \to (1)(2)$, so by the permutation method and Riemann–Hurwitz formula, the signature of $H_e(\sqrt{q})$ is $(0; \infty^{(2)}; 1)$. If we choose $\{I, R\}$ as a Schreier transversal for $H_e(\sqrt{q})$, then by the Reidemeister–Schreier method (see [17]), $H_e(\sqrt{q})$ has the parabolic generators T and $U = SR$. As $R \notin H_e(\sqrt{q})$, it is clear that

$$H(\sqrt{q}) = H_e(\sqrt{q}) \cup RH_e(\sqrt{q}).$$

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

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

2 Principal Congruence Subgroups

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

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

In general, this is equivalent to

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

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

$$H_p(\sqrt{q}) \lhd H_e(\sqrt{q}). \tag{4}$$

A subgroup of $H(\sqrt{q})$ 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 $H(\sqrt{q})$.

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

Let $\wp$ be an ideal of $\mathbb{Z}[\sqrt{q}]$ which is an extension of the ring of integers by the algebraic number $\sqrt{q}$. Then the natural map $\Theta_\wp : \mathbb{Z}[\sqrt{q}] \to \mathbb{Z}[\sqrt{q}]/\wp$ induces a map $H(\sqrt{q}) \to PSL(2, \mathbb{Z}[\sqrt{q}]/\wp)$, whose kernel is called the principal congruence subgroup of level $\wp$.

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

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

as the homomorphism induced by $\sqrt{q} \to u$. Let $K_{p,u}(\sqrt{q}) = \mathrm{Ker}(\Theta_{p,u,q})$.

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

Given p, as $K_{p,u}(\sqrt{q})$ 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 Kummer's theorem that if u, v correspond to the same irreducible factor f of $x^2 - q$ over $GF(p^s)$, then $K_{p,u}(\sqrt{q}) = K_{p,v}(\sqrt{q})$. Even when $u, \ v$ give different factors of $x^2 - q$, we may have $K_{p,u}(\sqrt{q}) = K_{p,v}(\sqrt{q})$. In Lemma 2.3, we show that $K_{p,u}(\sqrt{q}) = K_{p,-u}(\sqrt{q})$ when q is a quadratic residue mod p.

It is easy to see that $K_{p,u}(\sqrt{q})$ is a normal congruence subgroup of level p of $H(\sqrt{q})$, that is, $H_p(\sqrt{q}) \trianglelefteq K_{p,u}(\sqrt{q})$. Therefore $H_p(\sqrt{q}) \leq \bigcap_{\text{all } u} K_{p,u}(\sqrt{q})$. When the index of $H_p(\sqrt{q})$ in $K_{p,u}(\sqrt{q})$ is not 1, i.e., when they are different, we shall use $K_{p,u}(\sqrt{q})$ to calculate $H_p(\sqrt{q})$. We first try to find the quotient of $H(\sqrt{q})$ with $K_{p,u}(\sqrt{q})$. It is then easy to determine $H(\sqrt{q})/H_p(\sqrt{q})$. To determine both quotients we use some results of Macbeath [11]. After finding the quotients of $H(\sqrt{q})$ by the principal congruence subgroups, we find the group-theoretic structure of them. For notions and terminology see [11] and [12]. Also for the notion of quadratic reciprocity see [18].

Before stating our main results we need the following observations and lemma.

In [16], it was shown that $\mathscr{U}_{2n}^q$ and $\mathscr{V}_{2n+1}^q$ are in the following formulas for all n:

$$\mathscr{U}_{2n}^q = \frac{1}{\sqrt{q(q-4)}} \left[\left(\frac{\sqrt{q-4} + \sqrt{q}}{2} \right)^{2n} - \left(\frac{\sqrt{q-4} - \sqrt{q}}{2} \right)^{2n} \right] \tag{5}$$

and

$$\mathscr{V}_{2n+1}^q = \frac{1}{\sqrt{q-4}} \left[\left(\frac{\sqrt{q-4} + \sqrt{q}}{2} \right)^{2n+1} + \left(\frac{\sqrt{q-4} - \sqrt{q}}{2} \right)^{2n+1} \right]. \tag{6}$$

For any odd prime p, let us consider S^p in mod p. In $H(\sqrt{q})$, from (2) we have

$$S^p = \begin{pmatrix} -\mathscr{U}_{p-1}^q \sqrt{q} & -\mathscr{V}_p^q \\ \mathscr{V}_p^q & \mathscr{U}_{p+1}^q \sqrt{q} \end{pmatrix}.$$

From (6), we get

$$\begin{aligned}
\mathscr{V}_p^q &= \frac{1}{\sqrt{q-4}}\left[\left(\frac{\sqrt{q-4}+\sqrt{q}}{2}\right)^p+\left(\frac{\sqrt{q-4}-\sqrt{q}}{2}\right)^p\right] \\
&= \frac{1}{2^p\sqrt{q-4}}\Bigg[(\sqrt{q-4})^p+\begin{pmatrix} p \\ 1 \end{pmatrix}(\sqrt{q-4})^{p-1}\sqrt{q} \\
&\quad +\cdots+\begin{pmatrix} p \\ p-1 \end{pmatrix}\sqrt{q-4}(\sqrt{q})^{p-1}+(\sqrt{q})^p+(\sqrt{q-4})^p \\
&\quad -\begin{pmatrix} p \\ 1 \end{pmatrix}(\sqrt{q-4})^{p-1}\sqrt{q}+\cdots+\begin{pmatrix} p \\ p-1 \end{pmatrix}\sqrt{q-4}(\sqrt{q})^{p-1}-(\sqrt{q})^p)\Bigg] \\
&= \frac{1}{2^{p-1}}\left[(\sqrt{q-4})^{p-1}+\begin{pmatrix} p \\ 2 \end{pmatrix}(\sqrt{q-4})^{p-3}(\sqrt{q})^2+\cdots+\begin{pmatrix} p \\ p-1 \end{pmatrix}(\sqrt{q})^{p-1}\right].
\end{aligned}$$

As we have $\binom{p}{n} \equiv 0 (\mathrm{mod}\ p)$ for $1 \leq n \leq p-1$ and $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$, we find

$$\mathscr{V}_p^q \equiv (q-4)^{\frac{p-1}{2}} (\mathrm{mod}\ p). \tag{7}$$

Similarly, from (5) we have

$$\mathscr{U}_{p+1}^q = \frac{1}{2^p}\left[\begin{pmatrix} p+1 \\ 1 \end{pmatrix}(\sqrt{q-4})^{p-1}+\begin{pmatrix} p+1 \\ 3 \end{pmatrix}(\sqrt{q-4})^{p-3}q+\cdots+\begin{pmatrix} p+1 \\ p \end{pmatrix}(q)^{\frac{p-1}{2}}\right].$$

As $\binom{p+1}{n} \equiv 0 (\mathrm{mod}\ p)$ for $2 \leq n \leq p-1$ and $\binom{p+1}{1} \equiv \binom{p+1}{p} \equiv 1 (\mathrm{mod}\ p)$, we obtain

$$2^p \mathscr{U}_{p+1}^q \equiv \left[(q-4)^{\frac{p-1}{2}}+(q)^{\frac{p-1}{2}}\right] (\mathrm{mod}\ p). \tag{8}$$

Now we have two cases:

Case 1 Let us take $\left(\frac{q}{p}\right) = 1$, where $\left(\frac{q}{p}\right)$ is the Legendre symbol. Then we have $(q)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$ by the Euler criteria [18]. If $p \mid (q-4)$, then $q-4 \equiv 0 (\mathrm{mod}\ p)$ and $(q-4)^{\frac{p-1}{2}} \equiv 0 (\mathrm{mod}\ p)$. So we get $\mathscr{V}_p^q \equiv 0 \,(\mathrm{mod}\ p)$ and $2\mathscr{U}_{p+1}^q \equiv 1 (\mathrm{mod}\ p)$ since $2^p \equiv 2 (\mathrm{mod}\ p)$. As $q-4 \equiv 0 (\mathrm{mod}\ p)$, then $q \equiv 4 (\mathrm{mod}\ p)$. Hence we can take $\sqrt{q} \equiv \pm 2 (\mathrm{mod}\ p)$ and so $\sqrt{q}\mathscr{U}_{p+1}^q \equiv \pm 1 (\mathrm{mod}\ p)$. By (3), we find $-\sqrt{q}\mathscr{U}_{p-1}^q \equiv \pm 1 (\mathrm{mod}\ p)$. Finally we get

$$S^p \equiv \pm I \,(\mathrm{mod}\ p). \tag{9}$$

Clearly, the order of $S (\mathrm{mod}\ p)$ is p in this case.

Let $(q-4, p) = 1$. Then by the Euler theorem, $(q-4)^{\varphi(p)} \equiv 1 (\mathrm{mod}\ p)$, i.e., $(q-4)^{p-1} \equiv 1 (\mathrm{mod}\ p)$ and so $(q-4)^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\ p)$. If $(q-4)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$, then $\mathscr{V}_p^q \equiv 1 (\mathrm{mod}\ p)$ and $\mathscr{U}_{p+1}^q \equiv 1 (\mathrm{mod}\ p)$. From (3), we get $\mathscr{U}_{p-1}^q \equiv 0 (\mathrm{mod}\ p)$. Therefore we have

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

i.e., $S^{p-1} \equiv I (\mathrm{mod}\ p)$. Similarly, if $(q-4)^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$, then we have $\mathscr{V}_p^q \equiv -1 (\mathrm{mod}\ p)$ and $\mathscr{U}_{p+1}^q \equiv 0 (\mathrm{mod}\ p)$ as $2^p \equiv 2 (\mathrm{mod}\ p)$. Since $\mathscr{U}_{p-1}^q \equiv -1 (\mathrm{mod}\ p)$, we have $S^p \equiv S^{-1} (\mathrm{mod}\ p)$, i.e., $S^{p+1} \equiv I (\mathrm{mod}\ p)$. In this case, we can say only that the order of $S (\mathrm{mod}\ p)$ divides $p-1$ or $p+1$.

Case 2 Let $\left(\frac{q}{p}\right) = -1$. Then $(q)^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$. In this case, p can not be divided by $q-4$. For, if $p \mid (q-4)$, then $q \equiv 4 (\mathrm{mod}\ p)$ and q would be a quadratic residue mod p. Thus we have $(q-4, p) = 1$ and $(q-4)^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\ p)$. If $(q-4)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$, then we have $\mathscr{V}_p^q \equiv 1 (\mathrm{mod}\ p)$, $\mathscr{U}_{p+1}^q \equiv 0 (\mathrm{mod}\ p)$ and $\mathscr{U}_{p-1}^q \equiv 1 (\mathrm{mod}\ p)$. So we get

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

i.e., $S^{p+1} \equiv -I(\text{mod } p)$. If $(q-4)^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, then we have $\mathscr{V}_p^q \equiv -1(\text{mod } p)$, $\mathscr{U}_{p+1}^q \equiv -1(\text{mod } p)$ and $\mathscr{U}_{p-1}^q \equiv 0(\text{mod } p)$. Therefore we get $S^p \equiv -S(\text{mod } p)$ and so $S^{p-1} \equiv -I(\text{mod } p)$. In this case, the order of $S(\text{mod } p)$ divides $p-1$ or $p+1$.

Therefore we get the following lemma:

Lemma 2.1 (i) *Let* $\left(\frac{q}{p}\right) = 1$. *If* $p \mid (q-4)$, *then* $S^p \equiv \pm I(\text{mod } p)$ *and the order of* S *is* p *in* mod p. *If* $(q-4, p) = 1$ *and* $(q-4)^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, *then* $S^{p-1} \equiv I(\text{mod } p)$. *If* $(q-4, p) = 1$ *and* $(q-4)^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, *we have* $S^{p+1} \equiv I(\text{mod } p)$. *Then the order of* S, *say* l, *divides* $p-1$ *or* $p+1$.

(ii) *Let* $\left(\frac{q}{p}\right) = -1$. *If* $(q-4)^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, *we have* $S^{p+1} \equiv -I(\text{mod } p)$ *and if* $(q-4)^{\frac{p-1}{2}} \equiv -1(\text{mod } p)$, *we have* $S^{p-1} \equiv I(\text{mod } p)$. *Then the order of* S *divides* $p-1$ *or* $p+1$.

Now we can give our main theorem.

Theorem 2.2 *The quotient groups of the Hecke groups* $H(\sqrt{q})$ *by their congruence subgroups* $K_{p,u}(\sqrt{q})$ *and their principal congruence subgroups* $H_p(\sqrt{q})$ *are as follows*:

$$H(\sqrt{q})/K_{p,u}(\sqrt{q}) \cong \begin{cases} PSL(2,p) & \text{if } q \text{ is a quadratic residue mod } p, \\ PGL(2,p) & \text{if } q \text{ is a quadratic nonresidue mod } p, \\ C_2 & \text{if } p = q, \\ D_3 & \text{if } p = 2, \end{cases}$$

and

$$H(\sqrt{q})/H_p(\sqrt{q}) \cong \begin{cases} C_2 \times PSL(2,p) & \text{if } q \text{ is a quadratic residue mod } p, \\ PGL(2,p) & \text{if } q \text{ is a quadratic nonresidue mod } p, \\ C_{2q} & \text{if } p = q, \\ D_6 & \text{if } p = 2. \end{cases}$$

Proof

Case 1 Let $p \neq 2$ be so that q is a square modulo p, that is, q is a quadratic residue mod p and let $p \neq q$. In this case, there exists an element u in $GF(p)$ such that $u^2 = q$. Therefore $\sqrt{q}$ can be considered as an element of $GF(p)$. Let us consider the homomorphism of $H(\sqrt{q})$ reducing all its elements 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 $\theta : H(\sqrt{q}) \to PSL(2,p)$ induced by $\sqrt{q} \to u$. 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 $\alpha = \text{tr}(r_p) = 0$, $\beta = \text{tr}(s_p) = \sqrt{q}$ and $\gamma = \text{tr}(t_p) = 2$, is also $GF(p)$ as $\sqrt{q} \in GF(p)$. In this case, for all p, the $\Gamma_p(\sqrt{q})$-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 $\Gamma_p(\sqrt{q})$ denotes the image of $H(\sqrt{q})$ 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 and q. Now we want to know when the triple is exceptional (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 [11]). Note that l can not be 2 since $S^2 = \begin{pmatrix} -1 & -\sqrt{q} \\ \sqrt{q} & q-1 \end{pmatrix}$. It would be $S^2 \equiv \pm I$ only when p is a multiple of q, but in this case we would have $\left(\frac{q}{p}\right) = 0$. Firstly, let $p = 3$. If q is a quadratic residue mod 3, then $q \equiv 1(\text{mod } 3)$ by the Euler criteria. Since $q - 4 \equiv 0(\text{mod } 3)$, then by Lemma 2.1(i), we have $S^3 \equiv \pm I(\text{mod } 3)$. Therefore we find the exceptional triple $(2,3,3)$.

Let $p = 5$. Similarly, if q is a quadratic residue mod 5, then we have $q^2 \equiv 1(\text{mod } 5)$, so $q \equiv \mp 1(\text{mod } 10)$. In this case, it can be $l = 3$ or $l = 5$. If $q \equiv 1(\text{mod } 10)$, then $(q-4, 5) = 1$ and

it is easy to check that $S^3 \equiv -I(\text{mod } 5)$ (notice that $(q-4)^{\frac{5-1}{2}} \equiv -1(\text{mod } 5)$ and the order of S divides 6). If $q \equiv -1(\text{mod } 10)$, then $5 \mid (q-4)$, and by Lemma 2.1(i) we have $S^5 \equiv \mp I(\text{mod } 5)$.

Consequently, if $q \equiv 1(\text{mod } 3)$, we have the exceptional triple $(2,3,3)$. So (r_3, s_3, t_3) generates a group which is isomorphic to A_4 of order 12 and we obtain

$$H(\sqrt{q})/K_{3,u}(\sqrt{q}) \cong A_4 \cong PSL(2,3).$$

If $q \equiv \pm 1 \pmod{10}$, we have the exceptional triples $(2,3,5)$ and $(2,5,5)$. Therefore (r_5, s_5, t_5) generates a group which is isomorphic to A_5 of order 60. So we obtain

$$H(\sqrt{q})/K_{5,u}(\sqrt{q}) \cong A_5 \cong PSL(2,5).$$

If (r_p, s_p, t_p) is not exceptional, then by Theorem 4 in [11], (r_p, s_p, t_p) generates a projective subgroup of G, and by Theorem 5 in [11], as $\kappa = GF(p)$ is not a quadratic extension of any other field, this subgroup is the whole $PSL(2,p)$, i.e., $H(\sqrt{q})/K_{p,u}(\sqrt{q}) \cong PSL(2,p)$.

Let us now find the quotient of $H(\sqrt{q})$ by the principal congruence subgroup $H_p(\sqrt{q})$ in this case. Note that, by (4), $H_p(\sqrt{q})$ is a subgroup of the even subgroup $H_e(\sqrt{q})$. Therefore there are no odd elements in $H_p(\sqrt{q})$.

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

If A is such an element, then

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

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

$$A^2 = \begin{pmatrix} qx^2 + yz & \sqrt{q}(xy + yz) \\ \sqrt{q}(xz + tz) & qt^2 + yz \end{pmatrix},$$

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

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

$$\begin{pmatrix} x\sqrt{q} & y \\ z & t\sqrt{q} \end{pmatrix}\begin{pmatrix} a & b\sqrt{q} \\ c\sqrt{q} & d \end{pmatrix} = \begin{pmatrix} \sqrt{q}(ax + cy) & bxq + dy \\ az + qct & \sqrt{q}(bz + dt) \end{pmatrix}$$

and

$$\begin{pmatrix} a & b\sqrt{q} \\ c\sqrt{q} & d \end{pmatrix}\begin{pmatrix} x\sqrt{q} & y \\ z & t\sqrt{q} \end{pmatrix} = \begin{pmatrix} \sqrt{q}(ax + bz) & ay + btq \\ qxc + dz & \sqrt{q}(cy + dt) \end{pmatrix},$$

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

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

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

$$A = (T^{-v}R)^3 = \begin{pmatrix} v(2 - v^2q)\sqrt{q} & 1 - qv^2 \\ qv^2 - 1 & v\sqrt{q} \end{pmatrix} \in H(\sqrt{q}). \tag{10}$$

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

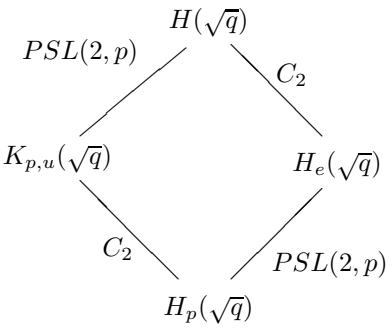

Figure 1

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

Now we shall extend $GF(p)$ to its quadratic extension $GF(p^2)$. Then $u = \sqrt{q}$ can be considered to be in $GF(p^2)$ and there exists a homomorphism $\theta : H(\sqrt{q}) \to PSL(2, p^2)$ induced similarly 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, t_p, is also $GF(p^2)$. Then as in Case 1, (r_p, s_p, t_p) is not a singular triple. If the G_0-triple (r_p, s_p, t_p) is not an exceptional triple, since κ is the quadratic extension of $\kappa_0 = GF(p)$ and $\gamma = 2$ lies in κ_0 while $\alpha = 0$, and $\beta = \sqrt{q}$ is the square root in κ of q which is a non-square in κ_0, (r_p, s_p, t_p) generates $PGL(2, p)$, i.e., $H(\sqrt{q})/K_{p,u}(\sqrt{q}) \cong PGL(2, p)$ (see [11, p. 28]).

If $p = 3$ or 5, (r_p, s_p, t_p) can be an exceptional triple. So we want to know for what values of q, $(\frac{q}{3}) = -1$ or $(\frac{q}{5}) = -1$. If $(\frac{q}{3}) = -1$, we have $q \equiv -1 (\mathrm{mod}\ 3)$, and if $(\frac{q}{5}) = -1$, we have $q^2 \equiv -1 \pmod 5$, so $q \equiv \pm 2 (\mathrm{mod}\ 5)$.

If $q \equiv -1 \pmod 3$, we have $q - 4 \equiv 1 (\mathrm{mod}\ 3)$. Again, it is easy to check that $S^4 \equiv -I (\mathrm{mod}\ 3)$. Thus we have the $\mathbb{N}$-triple $(2, 4, 3)$ which generates a group isomorphic to the symmetric group S_4 and we get $H(\sqrt{q})/K_{3,u}(\sqrt{q}) \cong S_4 \cong PGL(2, 3)$.

Similarly, if $q \equiv -2 \pmod 5$, we have $S^6 \equiv -I \pmod 5$, and if $q \equiv 2 \pmod 5$, we have $S^4 \equiv -I \pmod 5$. Therefore we get the $\mathbb{N}$-triples $(2, 6, 5)$ and $(2, 4, 5)$ when $q \equiv \mp 2 \pmod 5$. These triples are not exceptional. In this case (r_5, s_5, t_5) generates $PGL(2, p)$.

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

In this case, we have observed that the order of $S \bmod p$ is always $p - 1$ or $p + 1$ in examples. At this point, we conjecture that the order of $S \bmod p$ is $p-1$ or $p+1$ according to $(q-4)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$ or $(q-4)^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$, respectively. But we have not proved yet this conjecture.

Case 3 Let $p = q$. As $\sqrt{q}$ can be thought of as the zero element of $GF(q) = \{0, 1, 2, \ldots, q-1\}$, we have $t_q \equiv I \bmod q$. As $r_q^2 = 1$ as well, we have $H(\sqrt{q})/K_{q,0}(\sqrt{q}) \cong C_2$.

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

$$S^{2q} \equiv \begin{pmatrix} -1 & -q\sqrt{q} \\ q\sqrt{q} & -1 \end{pmatrix} (\mathrm{mod}\ q) \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I (\mathrm{mod}\ q).$$

So, in the quotient $H(\sqrt{q})/H_q(\sqrt{q})$ we have the relations $r_q^2 = s_q^{2q} = t_q^q = I$, $s_q = r_q t_q$ as $(\sqrt{q})^2 = q \equiv 0 \pmod q$. Then we have $H(\sqrt{q})/H_q(\sqrt{q}) \cong C_{2q}$.

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

Lemma 2.3 *Let q be a quadratic residue mod p. Then we have $K_{p,u}(\sqrt{q}) = K_{p,-u}(\sqrt{q})$.*

Proof If q is a quadratic residue mod p, then $x^2 - q \equiv (x-u)(x+u) \bmod p$ for some $u \in GF(p)$. In $K_{p,u}(\sqrt{q})$, let us consider the element $A = (T^{-v}R)^3$ obtained in (10). Now we have $R(T^{-v}R)^{-3}R = (T^vR)^3$. Since $K_{p,u}(\sqrt{q})$ 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.

Now using the Legendre symbol and the law of quadratic reciprocity, it is easy to prove the following lemma:

Lemma 2.4 *Let p be an odd prime. Then $(\frac{7}{p}) = 1$ if and only if $p \equiv \pm 1, \pm 3, \pm 9 \bmod 28$. If $p \equiv \pm 5, \pm 11, \pm 13 \bmod 28$, we have $(\frac{7}{p}) = -1$.*

Example 2.5 By Theorem 2.2 and Lemma 2.4, we have the quotient groups of the Hecke group $H(\sqrt{7})$ by its congruence subgroups $K_{p,u}(\sqrt{7})$ and its principal congruence subgroups $H_p(\sqrt{7})$ are as follows:

$$H(\sqrt{7})/K_{p,u}(\sqrt{7}) \cong \begin{cases} PSL(2,p), & p \equiv \pm 1, \pm 3, \pm 9 \bmod 28, \\ PGL(2,p), & p \equiv \pm 5, \pm 11, \pm 13 \bmod 28, \\ C_2, & p = 7, \\ D_3, & p = 2, \end{cases}$$

and

$$H(\sqrt{7})/H_p(\sqrt{7}) \cong \begin{cases} C_2 \times PSL(2,p), & p \equiv \pm 1, \pm 3, \pm 9 \bmod 28, \\ PGL(2,p), & p \equiv \pm 5, \pm 11, \pm 13 \bmod 28, \\ C_{10}, & p = 7, \\ D_6, & p = 2. \end{cases}$$

Note that we are unable to give conditions when q is a quadratic residue mod p or not, for any prime p and any q.

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

Corollary 2.6 *The indices of the congruence subgroups $K_{p,u}(\sqrt{q})$ and $H_p(\sqrt{q})$ in $H(\sqrt{q})$ are*

$$|H(\sqrt{q})/K_{p,u}(\sqrt{q})| = \begin{cases} \dfrac{p(p-1)(p+1)}{2} & \text{if } q \text{ is a square} \bmod p \text{ and } p \neq q, \\ p(p-1)(p+1) & \text{if } q \text{ is not a square} \bmod p, \\ 2 & \text{if } p = q, \\ 6 & \text{if } p = 2, \end{cases}$$

and

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

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

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

We also proved that $H(\sqrt{q})/H_q(\sqrt{q}) \cong C_{2q}$. C_{2q} has a presentation

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

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

$R \to (1\ 2)(3\ 4)\ \cdots\ (2q{-}1\ 2q)$, $\quad S \to (1\ 3\ 5\ \cdots\ 2q{-}1)(2\ 4\ 6\ \cdots\ 2q)$, $\quad T \to (1\ 4\ 5\ 8\ \cdots\ 2q)$.

By the permutation method and Riemann–Hurwitz formula we find the signature of $H_q(\sqrt{q})$ as $(\frac{q-1}{2}; \infty; 2)$.

Case 2 Let $p = 2$. We know that $H(\sqrt{q})/K_{2,u}(\sqrt{q}) \cong D_3$ and $H(\sqrt{q})/H_2(\sqrt{q}) \cong D_6$. 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 $K_{2,u}(\sqrt{q})$ has the signature $(0; \infty^{(3)}; 2)$ and therefore $K_{2,u}(\sqrt{q}) \cong F_4$, where F_4 denotes a free group of rank four.

Secondly let us consider $H(\sqrt{q})/H_2(\sqrt{q}) \cong D_6 \cong (2, 6, 2)$. In a similar way we obtain the signature of $H_2(\sqrt{q})$ 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 q is a quadratic residue mod p, $p \neq q$, $p \neq 2$. 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 depends on p and q. 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. In this case both $K_{p,u}(\sqrt{q})$ and $H_p(\sqrt{q})$ are free groups.

If $(q-4) \equiv 0 (\mathrm{mod}\ p)$ then from Lemma 2.1(i), we know that $l = p$ and so $m = 2p$. If $p \mid (q-4)$, then the signature of $K_{p,u}(\sqrt{q})$ is

$$\left(1 + \frac{(p-1)(p+1)(p-4)}{8}; \infty^{(\frac{(p-1)(p+1)}{2})}; \frac{(p-1)(p+1)}{2}\right)$$

and the signature $H_p(\sqrt{q})$ is

$$\left(1 + \frac{(p-1)(p+1)(p-3)}{4};\ \infty^{((p-1)(p+1))}; \frac{(p-1)(p+1)}{2}\right).$$

If $(q-4, p) = 1$, then $S^{p-1} \equiv I (\mathrm{mod}\ p)$ or $S^{p+1} \equiv I (\mathrm{mod}\ p)$ according to $(q-4)^{\frac{p-1}{2}} \equiv \pm 1 (\mathrm{mod}\ p)$. But, l may be a divisor of $p-1$ or $p+1$ since $\sqrt{q}$ can be considered as an element u of $GF(p)$. So l can be $\frac{p-1}{k}$ or $\frac{p+1}{k}$ for some positive integer k. 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 $K_{p,u}(\sqrt{q})$ in $H(\sqrt{q})$. By the permutation method and Riemann–Hurwitz formula, we find the signature of this subgroup as

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

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

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

Example 2.7 Let $q = 7$ and $p = 19$. We have $l = m = 10$ and $\mu = 3420$, $\mu' = 6840$. The signature of $K_{19,8}(\sqrt{7}) = K_{19,11}(\sqrt{7})$ is $(595; \infty^{(180)}; 342)$ and the signature of $H_{19}(\sqrt{7})$ is $(1189; \infty^{(360)}; 684)$.

Case 4 Let q be a quadratic nonresidue mod p. We prove that both quotient groups are isomorphic to $PGL(2,p)$. From Lemma 2.1(ii), we know that the associated $\mathbb{N}$-triple is $(2, \frac{p+1}{k}, p)$ or $(2, \frac{p-1}{k}, p)$ for some positive integer k according to $(q-4)^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$ or $(q-4)^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$, respectively. As in Case 3, we have the signature of $K_{p,u}(\sqrt{q}) =$

$H_p(\sqrt{q})$ as

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

or

$$\left(1+\frac{(p+1)(p^2-(2k+3)p+2)}{4};\ \infty^{((p-1)(p+1))};kp(p+1)\right),$$

respectively.

Example 2.8 (i) Let $q=7$ and $p=5$. In this case we have $H(\sqrt{7})/K_{5,u}(\sqrt{7}) \cong H(\sqrt{7})/H_5(\sqrt{7}) \cong PGL(2,5)$. As $3^2 \equiv -1(\text{mod } 5)$, we get the signature of $K_{5,u}(\sqrt{7}) = H_5(\sqrt{7})$ as $(4;\infty^{(24)};30)$.

(ii) Let $q=7$ and $p=11$. As $3^5 \equiv 1(\text{mod } 11)$, we have $K_{11,u}(\sqrt{7}) = H_{11}(\sqrt{7}) \cong (216;\infty^{(120)};110)$.

Finally, we can give the following corollary:

Corollary 2.9 *All principal congruence subgroups of the Hecke group $H(\sqrt{q})$, $q \geq 5$ prime number, are free groups.*

References

[1] Hecke, E.: Über die bestimmung dirichletscher reihen durch ihre funktionalgleichung. *Math. Ann.*, **112**, 664–699 (1936)

[2] Cangül, İ. N., Singerman, D.: Normal Ssubgroups of Hecke groups and regular maps. *Math. Proc. Camb. Phil. Soc.*, **123**(1), 59–74 (1998)

[3] Lang, M. L., Lim, C. H., Tan, S. P.: Principal congruence subgroups of the Hecke groups. *J. Number Theory*, **85**(2), 220–230 (2000)

[4] Newman, M.: Integral Matrices, Academic Press, New York, 1972

[5] Parson, L. A.: Generalized Kloosterman sums and the Fourier coefficients of cusp forms. *Trans. A.M.S.*, **217**, 329–350 (1976)

[6] Parson, L. A.: Normal congruence subgroups of the Hecke groups $G(\sqrt{2})$ and $G(\sqrt{3})$. *Pacific J. Math.*, **70**, 481–487 (1977)

[7] Rosen, D.: A class of continued fractions associated with certain properly discontinuous groups. *Duke Math. J.*, **21**, 549–563 (1954)

[8] Schmidt, T. A., Sheingorn, M.: Length spectra of the Hecke triangle groups. *Math. Z.*, **220**(3), 369–397 (1995)

[9] Lyndon, R. C., Ullman, J. L.: Pairs of real 2-by-2 matrices that generate free products. *Mich. Math. J.*, **15**, 161–166 (1968)

[10] 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), 35–46 (2002)

[11] Macbeath, A. M.: Generators of the linear fractional groups. *Proc. Symp. Pure. Math. A.M.S.*, **12**, 14–32 (1969)

[12] Singerman, D.: Subgroups of Fuchsian Groups and finite permutation groups. *Bull. London Math. Soc.*, **2**, 319–323 (1970)

[13] Maclachlan, C.: Maximal normal Fuchsian groups. *Illionis J. Math.*, **15**, 104–113 (1971)

[14] Yılmaz Özgür, N., Cangül, İ. N.: On the principal congruence subgroups of the Hecke group $H(\sqrt{5})$. *Beiträge Algebra Geom.*, **45**(1), 75–85 (2004)

[15] Yılmaz Özgür, N.: Generalizations of Fibonacci and Lucas sequences. *Note Mat.*, **21**(1), 113–125 (2002)

[16] Yılmaz Özgür, N.: On the sequences related to Fibonacci and Lucas numbers. *J. Korean Math. Soc.*, **42**(1), 135–151 (2005)

[17] Magnus, W., Karras, A., Solitar, D.: Combinatorial Group Theory, Dover Publication, Inc., New York, 1976

[18] Rose, H. E.: A Course in Number Theory, Oxford Science Publications, Second Edition, Oxford, 1998