BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 40(4), 479-494

Principal congruence subgroups of the Hecke groups and related results

Sebahattin Ikikardes, Recep Sahin and I. Naci Cangul

Abstract. In this paper, first, we determine the quotient groups of the Hecke groups $H(\lambda_q)$, where $q \geq 7$ is prime, by their principal congruence subgroups $H_p(\lambda_q)$ of level p, where p is also prime. We deal with the case of $q = 7$ separately, because of its close relation with the Hurwitz groups. Then, using the obtained results, we find the principal congruence subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$ for $q \geq 5$ prime. Finally, we show that some of the quotient groups of the Hecke group $H(\lambda_q)$ and the extended Hecke group $\overline{H}(\lambda_q)$, $q \geq 5$ prime, by their principal congruence subgroups $H_p(\lambda_q)$ are M^*-groups.

Keywords: principal congruence subgroups, Hecke groups, extended Hecke groups.

Mathematical subject classification: 11F06, 20H05, 30F50.

1 Introduction

The Hecke groups $H(\lambda)$ are defined to be the maximal discrete subgroups of $PSL(2, \mathbb{R})$ generated by two linear fractional transformations

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

where λ is a fixed positive real number. Let $S = TW$, i.e.

$$S(z) = -\frac{1}{z+\lambda}.$$

By identifying the transformation $\dfrac{az+b}{cz+d}$ with the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $H(\lambda)$ may be regarded as a multiplicative group of 2×2 matrices in which a matrix is

Received 19 August 2008.

identified with its negative. Notice that T and S have matrix representations

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

respectively.

E. Hecke [13] showed that $H(\lambda)$ is Fuchsian if and only if $\lambda = \lambda_q = 2\cos\frac{\pi}{q}$, for $q \geq 3$ integer, or $\lambda \geq 2$. We are going to be interested in the former case. The Hecke groups $H(\lambda_q)$ have a presentation, see [8],

$$H(\lambda_q) = \langle T, S \mid T^2 = S^q = I \rangle. \tag{1}$$

These groups are isomorphic to the free product of two finite cyclic groups of orders 2 and q. As the signature of $H(\lambda_q)$ is $(0; 2, q, \infty)$, the quotient space $\mathcal{U}/H(\lambda_q)$ where $\mathcal{U}$ is the upper half plane, is a sphere with one puncture and two elliptic fixed points of order 2 and q. Therefore all Hecke groups $H(\lambda_q)$ can be considered as a triangle group. Hence the Hecke surface $\mathcal{U}/H(\lambda_q)$, is a Riemann surface.

The first few Hecke groups are $H(\lambda_3) = \Gamma = PSL(2, \mathbb{Z})$ (the modular group), $H(\lambda_4) = H(\sqrt{2})$, $H(\lambda_5) = H\left(\frac{1+\sqrt{5}}{2}\right)$, and $H(\lambda_6) = H(\sqrt{3})$. It is clear from the above that $H(\lambda_q) \subset PSL(2, \mathbb{Z}[\lambda_q])$, but unlike in the modular group case (the case $q = 3$), the inclusion is strict and the index $[PSL(2, \mathbb{Z}[\lambda_q]) : H(\lambda_q)]$ is infinite as $H(\lambda_q)$ is discrete whereas $PSL(2, \mathbb{Z}[\lambda_q])$ is not for $q \geq 4$.

The extended Hecke groups $\overline{H}(\lambda_q)$ have been defined by adding the reflection $R(z) = 1/\overline{z}$ to the generators of the Hecke groups $H(\lambda_q)$, for $q \geq 3$ integer, in [27] and [28] . Thus the extended Hecke group $\overline{H}(\lambda_q)$ has the presentation, see [31],

$$\overline{H}(\lambda_q) = \langle T, S, R \mid T^2 = S^q = R^2 = (RT)^2 = (RS)^2 = I \rangle \cong D_2 *_{\mathbb{Z}_2} D_q.$$

If we take

$$R_1(z) = \frac{1}{\overline{z}}, \qquad R_2(z) = -\overline{z}, \qquad R_3(z) = -\overline{z} - \lambda_q,$$

where

$$T = R_2 R_1 = R_1 R_2 \quad \text{and} \quad S = R_1 R_3,$$

then we get the alternative presentation

$$\overline{H}(\lambda_q) = \langle R_1, R_2, R_3 \mid R_1^2 = R_2^2 = R_3^2 = (R_1 R_2)^2 = (R_1 R_3)^q = I \rangle.$$

The signature of the extended Hecke group $\overline{H}(\lambda_q)$ is $(0; +; [-]; \{2, q, \infty\})$. Since the extended Hecke groups $\overline{H}(\lambda_q)$ contain a reflection, they are non-Euclidean crystallographic (NEC) groups, which are discrete subgroups $\overline{H}(\lambda_q)$ of the group $PGL(2, \mathbb{R})$ of isometries of $\mathcal{U}$ such that the quotient space $\mathcal{U}/\overline{H}(\lambda_q)$ is a Klein surface. Also $\mathcal{U}/H(\lambda)$ is the canonical double cover of $\mathcal{U}/\overline{H}(\lambda_q)$.

In [29], Sahin, Ikikardes and Koruoglu studied some normal subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$, $q \geq 3$ prime, and some relations between them (see also [30] and [31]). They came across an interesting general fact when they were studying these subgroups. All of their findings concerning extended Hecke group $\overline{H}(\lambda_3)$ coincide with known results related to M^*-groups. Now, we briefly recall some definitions about the M^*-groups.

Let X be a compact bordered Klein surface of algebraic genus $g \geq 2$. May proved in [21] that the automorphism group G of X is finite, and the order of G is at most $12(g-1)$. Groups isomorphic to the automorphism group of such a compact bordered Klein surface with this maximal number of automorphisms are called M^*-groups. Thus, see [21], a finite group G is called an M^*-group if it is generated by three distinct non-trivial elements r_1, r_2, r_3 which satisfy the relations

$$r_1^2 = r_2^2 = r_3^2 = (r_1 r_2)^2 = (r_1 r_3)^3 = I$$

and other relations which make the group finite. These groups were investigated intensively [2, 4, 5, 11, 19–21]. The article in [3] contains a nice survey of known results about M^*-groups.

Also, in [21], May proved that a finite group of order ≥ 12 is an M^*-group if and only if it is the homomorphic image of the extended modular group $\overline{H}(\lambda_3)$. In fact, by using known results about normal subgroups of the extended modular group, he found some examples which are M^*-groups.

In this paper, we consider the case that $q \geq 5$ is a prime number. We determine the quotient groups of the Hecke groups $H(\lambda_q)$ by their principal congruence subgroups $H_p(\lambda_q)$, for prime p, using a classical method introduced by Macbeath [19]. For the cases $q = 3, 4, 5, 6$ and $q \geq 7$ prime, the principal congruence subgroups $H_p(\lambda_q)$ of the Hecke groups $H(\lambda_q)$ has been studied in detail by Cangül (third author) in his PhD Thesis, [6, Chapter 7]. But, most of his results are not published and later found by other authors by means of other techniques. Many properties of the principal congruence subgroups $H_p(\lambda_q)$ of the Hecke groups $H(\lambda_q)$ have been studied in the literature. For examples of these studies see [1, 13–17, 22–24]. Since the case $q = 5$ have been studied in detail in [6], [18] and [10], we will only give some known results for this case. Also, the case $q = 7$ will be significant and different from the others, and therefore it will be dealt with separately. Indeed in this special case, with only one exception, all quotient groups of $H(\lambda_7)$ by the principal congruence subgroups of prime level are Hurwitz groups − i.e. the groups of $84(g-1)$ automorphisms on a Riemann surface of genus g (for more information about Hurwitz groups, see [9]).

In section 2, after recalling some results from [19], we give all quotient groups of $H(\lambda_7)$ by the principal congruence subgroup $H_p(\lambda_7)$ and a list of their indices. Also we obtain the quotient groups of the Hecke groups $H(\lambda_q)$ by their principal congruence subgroups $H_p(\lambda_q)$ where $q > 7$ and p are arbitrary primes. In section 3, using some results given in Section 2, we find the principal congruence subgroups $\overline{H}_p(\lambda_q)$ of the extended Hecke groups $\overline{H}(\lambda_q)$. Also, we show that some of the quotient groups of the Hecke group $H(\lambda_q)$ and the extended Hecke group $\overline{H}(\lambda_q)$, $q \geq 5$ prime, by their principal congruence subgroups $H_p(\lambda_q)$ are M^*-groups.

Remark 1.1. For the case $q > 3$ is an odd integer, the principal congruence subgroups $H_p(\lambda_q)$ of the Hecke groups $H(\lambda_q)$ have been studied in detail by Lang, Lim and Tan in [18]. To find an explicit formula for the index $\left[H(\lambda_q) : H_p(\lambda_q)\right]$ in the case when p is a prime, they used the results of Dickson [11] on the subgroups of two-dimensional special linear groups over an algebraically closed field of characteristic p. Also they gave a complete list of the indices of the congruence subgroups of $H(\lambda_5)$. In this paper, apart from their method, we use some results of Macbeath [19] and the minimal polynomial of λ_q to obtain the quotients of $H(\lambda_q)$ by the principal congruence subgroups. Notice that for prime $q > 7$, Theorem 2.9 coincides with the main theorem of [18].

2 Principal congruence subgroups of $H(\lambda_q)$ for $q \geqslant 5$ is a prime number

The purpose of this section is to give the principal congruence subgroups of Hecke groups $H(\lambda_q)$ for $q \geqslant 5$ is a prime number. In each case we shall find the quotient group of $H(\lambda_q)$ by the principal congruence subgroups. Our main tool will be [19]. We shall recall some results from this work to use in determining the required quotient groups.

We start by defining *the principal congruence subgroup of level p, p prime*, of $H(\lambda_q)$, by

$$\begin{aligned} H_p(\lambda_q) &= \left\{T \in H(\lambda_q) : T \equiv \pm I \pmod{p}\right\}, \\ &= \left\{\begin{pmatrix} a & \lambda_q b \\ \lambda_q c & d \end{pmatrix} : a \equiv d \equiv \pm 1,\ b \equiv c \equiv 0 \pmod{p},\ ad - \lambda_q^2 bc = 1\right\}. \end{aligned}$$

It is well-known that each principal congruence subgroup $H_p(\lambda_q)$ of $H(\lambda_q)$ is always normal and of finite index.

A subgroup of $H(\lambda_q)$ 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 $H(\lambda_q)$.

Notice that $H_p(\lambda_q)$ is the kernel of the reduction homomorphism induced by reducing entries modulo p.

Let $\wp$ be an ideal of $\mathbb{Z}\left[\lambda_q\right]$ which is an extension of the ring of integers by the algebraic number λ_q. Then the natural ring epimorphism

$$\Theta_{\wp} : \mathbb{Z}\left[\lambda_q\right] \to \mathbb{Z}\left[\lambda_q\right]/\wp$$

induces a group homomorphism

$$H(\lambda_q) \to PSL(2, \mathbb{Z}\left[\lambda_q\right]/\wp)$$

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

Let now s be an integer such that $P_q^*(\lambda_q)$, the minimal polynomial of λ_q, has solutions in $GF(p^s)$. It is well known that such an s exists and satisfies $1 \leq s \leq d = \deg P_q^*(\lambda_q)$. Let u be a root of $P_q^*(\lambda_q)$ in $GF(p^s)$. Let us take $\wp$ to be the ideal generated by u in $\mathbb{Z}\left[\lambda_q\right]$. As above, we can define

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

as the group homomorphism induced by the assignment $\lambda_q \to u$. $K_{p,u}(\lambda_q) = Ker(\Theta_{p,u,q})$ is a normal subgroup of $H(\lambda_q)$.

Given p, as $K_{p,u}(\lambda_q)$ 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 the Kummer's theorem that if u, v are roots of the same irreducible factor of $P_q^*(\lambda_q)$ over $GF(p)$, then $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$. Even if u, v are roots of different factors of $P_q^*(\lambda_q)$, we may have $K_{p,u}(\lambda_q) = K_{p,v}(\lambda_q)$.

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

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

Therefore $H_p(\lambda_q) \trianglelefteq \bigcap_{all\ u} K_{p,u}(\lambda_q)$. In general, $H_p(\lambda_q)$ and $K_{p,u}(\lambda_q)$ are different. However the equality $H_p(\lambda_q)=K_{p,u}(\lambda_q)$ holds in our case because q is odd prime. Thus, in all cases we only determine the quotient of $H(\lambda_q)$ by $K_{p,u}(\lambda_q)$. To do this, we use some results of Macbeath [19]. As we shall use these results intensively, we now briefly recall them here.

2.1 Macbeath's results

Let $k = GF(p^n)$ be a field with p^n elements, where p is prime and k_1 be its unique quadratic extension. Let $G_0 = SL(2,k)$ and $G = PSL(2,k)$ so that $G \approxeq G_0/\{\pm I\}$. We shall also consider the subgroup G_1 of $SL(2,k_1)$ consisting of the matrices of the form $\begin{pmatrix} a & b \\ b^q & a^q \end{pmatrix}$ where $a, b \in k_1$ and $a^{q+1} - b^{q+1} = 1$. Macbeath classifies the G_0-triples (A, B, C^{-1}), $C = AB$, 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^{-1}) will be a k-triple (α, β, γ). Also to each G_0-triple (A, B, C^{-1}) there is an associated 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 epimorphism $\phi : G_0 \to G$ he 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^{-1}).

In the Hecke group case, we have $A = t_p$, $B = s_p$ and $C = w_p$, where t_p, s_p and w_p denote the images of T, S and W, respectively, under the homomorphism φ_p^* reducing all elements of $H(\lambda_q)$ modulo p. Hence the corresponding k-triple is $(0, u, 2)$, where u is a root of the minimal polynomial $P^*(\lambda_q)$ *modulo* p in $GF(p)$ or in a suitable extension field. Also the corresponding N-triple is $(2, q, n)$, where n is the level (i.e. the least positive integer so that W^n belongs to the subgroup).

Macbeath obtained three kinds of subgroups of G: affine, exceptional and projective groups. We now consider them in connection with the Hecke groups.

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

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

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 denoted by G_0. By mapping it to G via the natural homomorphism ϕ we obtain a subgroup A_1 of G. Now consider the set of matrices $\begin{pmatrix} w & 0 \\ 0 & w^q \end{pmatrix}$, $w \in k_1$, $w^{q+1} = 1$ in G_1. This is conjugate to a subgroup of $SL(2, k_1)$. 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 $k-$triple (α, β, γ) is singular. A group generated by a singular G_0-triple is an *affine group.*

From now on we restrict ourselves to the case $k = GF(p)$, p prime.

For $H(\lambda_q)$, with generators $T(z) = -1/z$ and $W(z) = z + \lambda_q$ the above determinant is equal to $-\lambda_q^2/4$ and therefore it vanishes only when $\lambda_q^2 \equiv 0 \pmod{p}$. For $q \geqslant 5$ a prime number, we need to find all primes p such that $\lambda_q^2 \equiv 0 \pmod{p}$ to determine the singular G_0-triples. To do this we shall consider minimal polynomial $P_q^*(\lambda_q)$ of λ_q over $\mathbb{Q}$ and specially its constant term c. It is easy to see that if $q \geq 5$ is a prime number then $|c| = 1$ (see [7]). Therefore there are no singular triples when $q \geq 5$ prime number.

The triples $(2, 2, n), n \in \mathbb{N}, (2, 3, 3), (2, 3, 4), (2, 3, 5)$ and $(2, 5, 5)$ – as $(2, 3, 5)$ is a homomorphic image of $(2, 5, 5)$ – which are the associated 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. For example when $q = 3$, we obtain exceptional triples for $p = 2, 3$ and 5. If $q > 5$ is prime then it is easy to see that the only exceptional triples are obtained for $p = 2$.

The last class of subgroups of G is the class of projective subgroups. It is known that there are two kinds of them: $PSL(2, k_s)$ and $PGL(2, k_s)$, where k_s is a subfield of k, the latter containing the former with index 2, except for $p = 2$ where both groups are equal. The groups $PSL(2, k_s)$ for all subfields of k, and whenever possible, the groups $PGL(2, k_s)$, together with their conjugates in $PGL(2, k)$ will be called *projective subgroups* of G.

Dickson [11], 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 (t_p, s_p, w_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 [19].

Theorem 2.1. *A G_0-triple which is neither singular nor exceptional generates a projective subgroup of G.*

Theorem 2.2. *If a G_0-triple with associated k-triple (α, β, γ) 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* *subfield of k containing α, β and γ, and κ_0 is a subfield, if any, of which, κ is a quadratic extension.*

There are some $k-$triples which are neither exceptional nor singular. These are called *irregular* by Macbeath, i.e. a k-triple 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 2.3. *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.*

For the case $q = 5$, principal congruence subgroups of Hecke groups $H(\lambda_5)$ has been studied by Cangül in [6, Theorem 7.7, p. 150]. Using the Macbeath's results he gave the following theorem.

Theorem 2.4. *The quotient groups of the Hecke group $H(\lambda_5)$ by its principal congruence subgroups $K_{p,u}(\lambda_5)$ are the following:*

$$\frac{H(\lambda_5)}{K_{p,u}(\lambda_5)} \approxeq \begin{cases} D_5 & \text{if} \quad p = 2, \\ A_5 & \text{if} \quad p = 3, 5, \\ PSL(2,p) & \text{if} \quad p \equiv \pm 1 \mod 10, \\ PSL(2,p^2) & \text{if} \quad p \equiv \pm 3 \mod 10 \quad \text{and} \quad p \neq 3. \end{cases}$$

Notice that this result coincides with the ones given by Lang et al. in [18, p. 230, Corollary 2] and by Demirci et al. [10] for the Hecke group $H(\lambda_5)$.

2.2 The case $q = 7$

In this case, we shall show that all of quotients $H(\lambda_q)/K_{p,u}(\lambda_q)$, except for $p = 2$, are Hurwitz groups.

Since by Theorem 2.2, there are no exceptional or singular triples for $p > 2$, the triple (t_p, s_p, w_p) generates a projective subgroup. Now the minimal polynomial $P_7^*(x)$ has degree three which is odd. Hence the field κ which is either $GF(p)$ or $GF(p^3)$ cannot be a quadratic extension of any other field κ_0. Therefore by Theorem 2.3 no projective general linear group occurs as a quotient of $H(\lambda_7)$ by a principal congruence subgroup. That is, the only possible projective group generated by the G_0-triple (t_p, s_p, w_p) is $PSL(2,p^3)$. Let us now give the following theorem which is a special case of the main theorem of [18].

Theorem 2.5. *The quotient groups of the Hecke group $H(\lambda_7)$ by its principal congruence subgroups $K_{p,u}(\lambda_7)$ are the following:*

$$\frac{H(\lambda_7)}{K_{p,u}(\lambda_7)} \cong \begin{cases} D_7 & \text{if} \quad p = 2, \\ PSL(2,7) & \text{if} \quad p = 7, \\ PSL(2,p) & \text{if} \quad p \equiv \pm 1 \mod 7, \\ PSL(2,p^3) & \text{if} \quad p \not\equiv \pm 1 \mod 7, p \neq 2. \end{cases}$$

Proof. Case 1: $p = 2$. In this case we have an exceptional N-triple $(2, 7, 2)$ which gives

$$H(\lambda_7)/K_{2,u}(\lambda_7) \cong D_7.$$

Case 2: $p = 7$. Now the minimal polynomial $P_7^*(x)$ has a root, $u = 5$, of multiplicity three in $GF(7)$. Indeed

$$(x-5)^3 \equiv (x+2)^3 \equiv x^3 - x^2 - 2x + 1 = P_7^*(x) \mod 7$$

Since (R_7, S_7, T_7) is neither exceptional nor singular, it generates, by Theorem 2.2, $PSL(2, 7)$. Therefore the quotient group

$$H(\lambda_7)/K_{7,u}(\lambda_7) \cong PSL(2,7)$$

is a Hurwitz group.

Case 3: $p \equiv \pm 1 \mod 7$. This is equivalent to saying that $p \equiv \pm 1 \mod 14$. Since 7 is prime and divides the order of $PSL(2, p)$, there are elements of order 7 in $PSL(2, p)$. That is, there is a homomorphism of $H(\lambda_7)$ to $PSL(2, p)$ for each of the three roots u_1, u_2 and u_3 of $P_q^*(\lambda_7)$ whenever $p \equiv \pm 1 \mod 14$. Since (t_p, s_p, w_p) is neither exceptional, singular nor irregular, by Theorem 2.2, it generates the whole group $PSL(2, p)$. Therefore, $H(\lambda_7)$ has three normal congruence subgroups $K_{7,u_i}(\lambda_7)$, $i = 1, 2, 3$ with quotient $PSL(2, p)$.

Case 4: Finally let $p \not\equiv \pm 1 \mod 7$, and $p \neq 2$. In that case, 7 does not divide the order of $PSL(2, p)$ implying that there is no homomorphism from $H(\lambda_7)$ to $PSL(2, p)$. In another words, the minimal polynomial $P_7^*(x)$ has no roots in $GF(p)$. Hence we have a homomorphism $H(\lambda_7) \to PSL(2, p^3)$ induced as before. By Theorems 2.1 and 2.2, (t_p, s_p, w_p) generates $PSL(2, p^3)$ which is a Hurwitz group.

Hence we have found all quotients of the Hecke group $H(\lambda_7)$ with the principal congruence subgroups $K_{p,u}(\lambda_7)$, for all prime p. By means of these we can give the index formula for this congruence subgroup.

Corollary 2.6. *The indices of the principal congruence subgroups $K_{p,u}(\lambda_7)$ in $H(\lambda_7)$ are*

$$\left[H(\lambda_7) : K_{p,u}(\lambda_7)\right] \cong \begin{cases} 14 & \text{if} \quad p = 2, \\ 168 & \text{if} \quad p = 7, \\ \frac{p(p-1)(p+1)}{2} & \text{if} \quad p \equiv \pm 1 \mod 7, \\ \frac{p(p^5-1)(p^5+p^4+p^3+p^2+p+1)}{2} & \text{if} \quad p \not\equiv \pm 1 \mod 7, p \neq 2. \end{cases}$$

2.3 The prime q case where $q > 7$

Now we consider the prime q case where $q > 7$. Of course all ideas in this case are also valid for $q = 3$, 5 and 7. Recall that for $q = 7$ and $p \equiv \pm 1 \mod 7$, we obtained three homomorphisms from $H(\lambda_7)$ to $PSL(2, p)$ one for each root of $P_7^*(x)$ in $GF(p)$, and these homomorphisms provided three non-conjugate normal subgroups of $H(\lambda_7)$. A similar thing seems to happen when $q > 7$. Whenever we reduce $P_q^*(x)$ *modulo* p, it splits linearly either in $GF(p)$ or in a finite extension of $GF(p)$. That is, the roots of $P_q^*(x)$ *modulo* p are in $GF(p)$ or in a finite extension of $GF(p)$. If a particular root u is in $GF(p)$, then there is a homomorphism from $H(\lambda_q)$ to $PSL(2, p)$, whose kernel is $K_{p,u}(\lambda_q)$. Similarly, if a root u lies in $GF(p^n)$ where n is less than or equal the degree d of the minimal polynomial $P_q^*(x)$, then there is a homomorphism from $H(\lambda_q)$ to $PSL(2, p^n)$ with kernel $K_{p,u}(\lambda_q)$. Therefore for each root u, we have a way to obtain another normal subgroup $K_{p,u}(\lambda_q)$.

In subsection 2.1 we have shown the necessary and sufficient condition for the generators of $H(\lambda_q)$ to constitute a singular triple is that $\lambda_q^2 \equiv 0 \mod p$. Therefore, there are no singular triples when q is prime > 7.

Since (t_p, s_p, w_p) is neither exceptional nor singular for $p > 2$, it generates, by Theorem 2.1, a projective subgroup of G. To find which projective subgroup is generated by this triple, we must consider the field k and its smallest subfield κ, containing the traces α, β and γ, *modulo* p, of t_p, s_p and w_p, respectively. Here we have four possible cases:

Case 1: $p = 2$. In this case we have already seen that the G_0-triple (t_p, s_p, w_p) generates an exceptional subgroup. Then the quotient group $H(\lambda_q)/K_{2,u}(\lambda_q)$ is associated with the N-triple $(2, q, 2)$ which is dihedral of order $2q$.

Case 2: $p = q$. In this case $x_0 = q - 2$ is the only root of the minimal polynomial $P_q^*(x) \mod p$. To prove this we show that -1 is the only root of

$$\Phi_p(x) = \frac{x^p + 1}{x + 1} = x^{p-1} - x^{p-2} + x^{p-3} - \cdots + x^2 - x + 1.$$

Consider the expansion of $(x+1)^{p-1}$. The binomial coefficients are congruent to ± 1 m mod p:

$$\binom{p-1}{r} = \frac{(p-1).....(p-r)}{r!} \equiv (-1)^r.\frac{r!}{r!} = (-1)^r$$

Therefore $\Phi_p(x)$ is congruent to $(x+1)^{p-1}$. Hence all $p-1$ roots of $\Phi_p(x)$ are congruent to -1 *modulo* p, as required. Therefore all roots are in $GF(p)$. Then there is a homomorphism from $H(\lambda_q)$ to $PSL(2,p)$ for each root u. Again by a similar argument we find

$$\frac{H(\lambda_q)}{K_{q,u}(\lambda_q)} \cong PSL(2,q)$$

for each u.

Case 3: Let $p \equiv \pm 1 \mod q$. Since q is odd prime, this is equivalent to say that $p \equiv \pm 1 \mod 2q$; i.e. $p = kq \pm 1$ with $k \in \mathbb{N}$ is even. Now

$$\frac{p(p-1)(p+2)}{2} : q = \frac{p(p-1)(p+2)}{2} : \frac{p \pm 1}{2} \in \mathbb{N}$$

and therefore q divides the order of $PSL(2,p)$; there are elements of order q in $PSL(2,p)$. Then there exists a homomorphism

$$\theta : H(\lambda_q) \to PSL(2,p)$$

for each root u in $GF(p)$. Therefore there are $d = \deg P_q^*(x)$ normal congruence subgroups $K_{p,u}(\lambda_q)$ of $H(\lambda_q)$. This implies

Theorem 2.7. *If $p \equiv \pm 1 \mod q$, then there exists a homomorphism $\theta : H(\lambda_q) \to PSL(2,p)$ for each root $u \in GF(p)$. The kernel of this homomorphism is $K_{q,u}(\lambda_q)$.*

Case 4: Let $p \neq \pm 1 \mod q$ and $p \neq 2, q$. Then q does not divide the order of $PSL(2,p)$ and therefore no homomorphism from $H(\lambda_q)$ to $PSL(2,p)$ exists, i.e. $P_q^*(x)$ has no roots in $GF(p)$. We extend $GF(p)$ to $GF(p^n)$ where n is less than or equal to the degree d of the minimal polynomial $P_q^*(x)$ which is

$$d = \frac{q-1}{2}$$

as q is an odd prime. Let u be a root of $P_q^*(x)$ in $GF(p^n)$. Then by Theorems 2.1 and 2.2, we have a homomorphism of $H(\lambda_q)$ to $PSL(2, p^n)$ if n is odd and to $PGL(2, p^{\frac{n}{2}})$ if n is even. The kernel of this homomorphism is $K_{q,u}(\lambda_q)$.

We have thus completed the discussion of the principle congruence subgroups of $H(\lambda_q)$. At the end we have the following result:

Theorem 2.8. *The quotient groups of the Hecke group $H(\lambda_q)$ by its principal congruence subgroups $K_{p,u}(\lambda_q)$ are the following:*

$$\frac{H(\lambda_q)}{K_{p,u}(\lambda_q)} \cong \begin{cases} D_q & \textit{if } p = 2, \\ PSL(2,p) & \textit{if } p = q \textit{ or if } p \equiv \pm 1 \mod q, \\ PSL(2,p^n) & \textit{if } p \neq \pm 1 \mod q \textit{ and } p \neq 2, q, \textit{ and } n \textit{ is odd}, \\ PGL(2,p^{n/2}) & \textit{if } p \neq \pm 1 \mod q \textit{ and } p \neq 2, q, \textit{ and } n \textit{ is even}, \end{cases}$$

where n is less than or equal to the degree d of the minimal polynomial.

3 Principal congruence subgroups of $\overline{H}(\lambda_q)$ and their applications

In this section we determine the principal congruence subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$ where $q \geq 5$ is a prime number. The *principal congruence subgroups of level p*, p prime, of $\overline{H}(\lambda_q)$ are defined in [27], as

$$\overline{H}_p(\lambda_q) = \left\{ M \in \overline{H}(\lambda_q) : M \equiv \pm I \pmod p \right\},$$

$$= \left\{ \begin{pmatrix} a & b\lambda_q \\ c\lambda_q & d \end{pmatrix} : a \equiv d \equiv \pm 1, b \equiv c \equiv 0 \pmod p), ad - \lambda_q^2 bc = \pm 1 \right\}.$$

$\overline{H}_p(\lambda_q)$ is always a normal subgroup of finite index in $\overline{H}(\lambda_q)$. It is easily seen that

$$H_p(\lambda_q) = \overline{H}_p(\lambda_q) \cap H(\lambda_q).$$

By [27], we know that if $p \geq 3$ is a prime number, then

$$\overline{H}_p(\lambda_q) = H_p(\lambda_q) \quad \text{and} \quad \overline{H}(\lambda_q)/\overline{H}_p(\lambda_q) = \overline{H}(\lambda_q)/H_p(\lambda_q) \cong C_2 \times G,$$

where $H(\lambda_q)/H_p(\lambda_q) \cong G$ and if $p = 2$, then $\overline{H}(\lambda_q)/\overline{H}_2(\lambda_q) \cong H(\lambda_q)/H_2(\lambda_q)$. Using these results, we can give the following theorems without proof.

Theorem 3.1. *The quotient groups of the extended Hecke group $\overline{H}(\lambda_5)$ by its principal congruence subgroups $\overline{H}_p(\lambda_5)$ are the following:*

$$\frac{\overline{H}(\lambda_5)}{\overline{H}_p(\lambda_5)} \approx \begin{cases} D_5 & \textit{if } p = 2, \\ C_2 \times A_5 & \textit{if } p = 3, 5, \\ C_2 \times PSL(2,p) & \textit{if } p \equiv \pm 1 \mod 10, \\ C_2 \times PSL(2,p^2) & \textit{if } p \equiv \pm 3 \mod 10, \textit{ and } p \neq 3. \end{cases}$$

Theorem 3.2. *The quotient groups of the extended Hecke group $\overline{H}(\lambda_7)$ by its principal congruence subgroups $\overline{H}_p(\lambda_7)$ are the following:*

$$\frac{\overline{H}(\lambda_7)}{\overline{H}_p(\lambda_7)} \cong \begin{cases} D_7 & \text{if} \quad p = 2, \\ C_2 \times PSL(2,7) & \text{if} \quad p = 7, \\ C_2 \times PSL(2,p) & \text{if} \quad p \equiv \pm 1 \mod 7, \\ C_2 \times PSL(2,p^3) & \text{if} \quad p \not\equiv \pm 1 \mod 7,\, p \neq 2. \end{cases}$$

Theorem 3.3. *The quotient groups of the extended Hecke group $\overline{H}(\lambda_q)$, $q > 7$ prime, by its principal congruence subgroups $\overline{H}_p(\lambda_q)$ are as follows:*

$$\frac{H(\lambda_q)}{K_{p,u}(\lambda_q)} \cong \begin{cases} D_q & \text{if } p = 2, \\ C_2 \times PSL(2,p) & \text{if } p = q \text{ or if } p \equiv \pm 1 \mod q, \\ C_2 \times PSL(2,p^n) & \text{if } p \not\equiv \pm 1 \mod q \text{ and } p \neq 2, q \text{ and } n \text{ is odd} \\ C_2 \times PGL(2,p^{n/2}) & \text{if } p \not\equiv \pm 1 \mod q \text{ and } p \neq 2, q \text{ and } n \text{ is even}, \end{cases}$$

where n is less than or equal to the degree d of the minimal polynomial.

The above results can be applied to the theory of Klein surfaces. Recall that a bordered compact Klein surface of algebraic genus $g \geq 2$ has at most $12(g-1)$ automorphisms [20]. When this maximal bound is attained by a surface, its group of automorphisms is called an M^*-group [21]. May proved [21] that there is a relationship between the extended modular group and M^*-groups. The relationship says that a finite group of order at least 12 is an M^*-group if and only if it is a homomorphic image of the extended modular group $\overline{H}(\lambda_3)$. In fact, by using known results about normal subgroups of the extended modular group, he found an infinite family of M^*-groups. For example, the quotient group $\overline{H}(\lambda_3)/\overline{H}_p(\lambda_3)$ of the extended Hecke group $\overline{H}(\lambda_3)$ (extended modular group Γ) by its principal congruence subgroup $\overline{H}_p(\lambda_3)$ is an M^*-group where $p \geq 2$ is a prime number.

On the other hand, Singerman showed in [32] that for p prime, $PSL(2,p)$ is an M^*-group if and only if $p \neq 2, 3, 7, 11$ and $PSL(2,p^2)$ is an M^*-group if and only if $p \neq 3$. Also, Bujalance et al. proved [5] that for prime $p \neq 2, 3, 7, 11$, $C_2 \times PSL(2,p)$ are M^*-groups.

Thus, it is easily seen that some of the quotient groups of the Hecke group $H(\lambda_q)$ and the extended Hecke group $\overline{H}(\lambda_q)$, $q \geq 5$ prime, by their principal congruence subgroups $H_p(\lambda_q)$ are M^*-groups. Therefore there is a relationship between (extended) Hecke groups and M^*-groups. Using this relation we can obtain following results.

Theorem 3.4. *Let $p > 2$ be a prime number.*

(i) *Let $q = 5$. If $p = 3$ or 5, then $H(\lambda_5)/H_p(\lambda_5) \approxeq A_5$ is an M^*-group. If $p \equiv \pm 1 \bmod 10$ and $p \neq 11$, then $H(\lambda_5)/H_p(\lambda_5) \approxeq PSL(2, p)$ is an M^*-group. If $p \equiv \pm 3 \bmod 10$ and $p \neq 3$, then $H(\lambda_5)/H_p(\lambda_5) \approxeq PSL(2, p^2)$ is an M^*-group.*

(ii) *Let $q = 7$. If $p \equiv \pm 1 \bmod 7$, then $H(\lambda_7)/H_p(\lambda_7) \approxeq PSL(2, p)$ is an M^*-group.*

(iii) *Let $q > 7$ be a prime number. If $p \equiv \pm 1 \bmod q$, then $H(\lambda_q)/H_p(\lambda_q) \approxeq PSL(2, p)$ is an M^*-group.*

Theorem 3.5. *Let $p > 2$ be a prime number.*

(i) *Let $q = 5$. If $p = 3$ or 5, then $\overline{H}(\lambda_5)/\overline{H}_p(\lambda_5) \approxeq C_2 \times A_5$ is an M^*-group. If $p \equiv \pm 1 \bmod 10$ and $p \neq 11$ then $\overline{H}(\lambda_5)/\overline{H}_p(\lambda_5) \approxeq C_2 \times PSL(2, p)$ is an M^*-group.*

(ii) *If $q = 7$ and $p \equiv \pm 1 \bmod 7$, then $\overline{H}(\lambda_7)/\overline{H}_p(\lambda_7) \approxeq C_2 \times PSL(2, p)$ is an M^*-group.*

(iii) *If $q > 7$ prime number and $p \equiv \pm 1 \bmod q$, then $\overline{H}(\lambda_q)/\overline{H}_p(\lambda_q) \approxeq C_2 \times PSL(2, p)$ is an M^*-group.*

Example 3.6.

(i) $\overline{H}(\lambda_5)/\overline{H}_{19}(\lambda_5) \approxeq C_2 \times PSL(2, 19)$ is an M^*-group.

(ii) $\overline{H}(\lambda_{11})/\overline{H}_{23}(\lambda_{11}) \approxeq C_2 \times PSL(2, 23)$ is an M^*-group.

References

[1] O. Bizim and I.N. Cangül. Congruence subgroups of some Hecke groups. Bull. Inst. Math. Acad. Sinica, **30**(2) (2002), 115–131.

[2] E. Bujalance, J.J. Etayo, J.M. Gamboa and G. Gromadzki. *Automorphisms groups of compact bordered Klein surfaces. A Combinatorial Approach.* Lecture Notes in Math., **1439** (1990), Springer Verlag.

[3] E. Bujalance, F.J. Cirre and P. Turbek. *Groups acting on bordered Klein surfaces with maximal symmetry*. Proceedings of Groups St. Andrews 2001 in Oxford. Vol. I, 50–58, London Math. Soc. Lecture Note Ser., 304, Cambridge, U.K. Cambridge University Press (2003).

[4] E. Bujalance, F.J. Cirre and P. Turbek. *Subgroups of M^*-groups.* Q.J. Math., **54**(1) (2003), 49–60.

[5] E. Bujalance, F. J. Cirre and P. Turbek. *Automorphism criteria for M^*-groups.* Proc. Edinb. Math. Soc., **47**(2) (2004), 339–351.

[6] I.N. Cangül. *Normal subgroups of Hecke groups.* Ph.D. Thesis, University of Southampton, Faculty of Mathematical Studies, December (1993).

[7] I.N. Cangül. *The minimal polynomials of* $\cos(2\pi/n)$ *over* $\mathbb{Q}$. Problemy Mat., **15** (1997), 57–62.

[8] I.N. Cangül and D. Singerman. *Normal subgroups of Hecke groups and regular maps.* Math. Proc. Camb. Phil. Soc., **123** (1998), 59–74.

[9] M.D.E. Conder. *Hurwitz groups: a brief survey.* Bull. Amer. Math. Soc., **23** (1990), 359–370.

[10] M. Demirci and I.N. Cangül. *A class of congruence subgroups of Hecke group* $H(\lambda_5)$. Bull. Inst. Math. Acad. Sin. (N.S.), **1**(4) (2006), 549–556.

[11] L.E. Dickson. *Linear Groups with an Exposition of the Galois Field Theory*, printed by Dover (1960).

[12] N. Greenleaf and C.L. May. *Bordered Klein surfaces with maximal symmetry.* Trans. Amer. Math. Soc., **274**(1) (1982), 265–283.

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

[14] I. Ivrissimtzis and D. Singerman. *Regular maps and principal congruence subgroups of Hecke groups.* European J. Combin., **26**(3-4) (2005), 437–456.

[15] M.L. Lang. *The signatures of the congruence subgroups* $G_0(\tau)$ *of the Hecke groups* G_4 *and* G_6. Comm. Algebra, **28**(8) (2000), 3691–3702.

[16] M.L. Lang. *The structure of the normalizers of the congruence subgroups of the Hecke Group* G_5. Bull. London Math. Soc., **39**(1) (2007), 53–62.

[17] M.L. Lang, C.H. Lim and S.P. Tan. *Independent generators for congruence subgroups of Hecke groups.* Math. Z., **220**(4) (1995), 569–594.

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

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

[20] C.L. May. *Automorphisms of compact Klein surfaces with boundary.* Pacific J. Math., **59** (1975), 199–210.

[21] C.L. May. *Large automorphism groups of compact Klein surfaces with boundary.* Glasgow Math. J., **18** (1977), 1–10.

[22] C.L. May. *A family of M^*-groups.* Canad. J. Math., **38**(5) (1986), 1094–1109.

[23] C.L. May. *Supersolvable M^*-groups.* Glasgow Math. J., **30**(1) (1988), 31–40.

[24] D.L. McQuillan. *Classification of normal subgroups of the modular group.* Amer. J. Math., **87** (1965), 285–296.

[25] M. Newman. *Normal congruence subgroups of the modular group.* Amer. J. Math., **85** (1963), 419–427.

[26] L.A. Parson. *Normal Congruence subgroups of the Hecke groups $G(2^{(1/2)})$ and $G(3^{(1/2)})$.* Pacific J. of Math., **70** (1977), 481–487.

[27] R. Sahin and O. Bizim. *Some subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$.* Acta Math. Sci. Ser. B, Engl. Ed., **23**(4) (2003), 497–502.

[28] R. Sahin, O. Bizim and I.N. Cangül. *Commutator subgroups of the extended Hecke groups $\overline{H}(\lambda_q)$.* Czechoslovak Math. J., **54**(129), no. 1, (2004), 253–259.

[29] R. Sahin, S. İkikardes and Ö. Koruoğlu. *Some normal subgroups of the extended Hecke groups $\overline{H}(\lambda_p)$.* Rocky Mountain J. Math., **36**(3) (2006), 1033–1048.

[30] R. Sahin, S. İkikardes and Ö. Koruoğlu. *Generalized M^*-groups.* Internat. J. Algebra Comput., **16**(6) (2006), 1211–1219.

[31] R. Sahin, S. İkikardes and Ö. Koruoğlu. *Extended Hecke groups $\overline{H}(\lambda_q)$ and their fundamental regions.* Adv. Stud. Contemp. Math. (Kyungshang), **15**(1) (2007), 87–94.

[32] D. Singerman. *$PSL(2, q)$ as an image of the extended modular group with applications to group actions on surfaces.* Proc. Edinb. Math. Soc., **30** (1987), 143–151.

Sebahattin Ikikardes and **Recep Sahin**
Balikesir Universitesi
Fen-Edebiyat Fakultesi
Matematik Bolumu
10145 Balikesir
TURKEY

E-mail: skardes@balikesir.edu.tr /
rsahin@balikesir.edu.tr

I. Naci Cangul
Uludag Universitesi
Fen-Edebiyat Fakultesi
Matematik Bolumu
16059 Bursa
TURKEY

E-mail: cangul@uludag.edu.tr