World Applied Sciences Journal 2 (1): 45-48, 2007
ISSN 1818-4952

On the Numbers of the Form $n = x^2 + Ny^2$

Nihal Yilmaz Özgür

Department of Mathematics, Balikesir University, 10145 Çagis, Balikesir, Turkey

Abstract: In the present paper we consider the problem when a natural number n can be represented in the form $n = x^2 + Ny^2$. To get some results about this problem we use the group structures of the Hecke groups $H(\sqrt{N}), N \geq 5$ integer.

Key words: Representation of integers . Hecke groups

INTRODUCTION

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

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

where, ? is a fixed positive real number. They were introduced by Hecke, [1]. Hecke showed that when ? = 2 or when ? = $?_q$ = 2cos(p/q), q ∈N, q = 3, the set

$$F_\lambda = \left\{ z \in U : |Re(z)| < \frac{\lambda}{2}, |z| > 1 \right\}$$

is a fundamental region for the group $H(\lambda)$ and also F_λ fails to be a fundamental region for all other $\lambda > 0$. It follows that $H(\lambda)$ is discrete only for these values of λ, [1].

It is well-known that the Hecke groups $H(\lambda_q)$ are isomorphic to the free product of two finite cyclic groups of orders 2 and q, that is, $H(\lambda_q) \cong C_2 * C_q$. For q = 3, we get the modular group $H(\lambda_3)$ = PSL(2, Z). Also it is known that the Hecke groups $H(\lambda)$, $\lambda \geq 2$, are isomorphic to the free product of a cyclic group of order 2 and a free group of rank 1, that is, $H(\lambda) \cong C_2 * Z$, [2, 3].

Let N be a fixed positive integer and x, y are relatively prime integers. Let us consider the problem when a natural number n can be represented in the form $n = x^2 + Ny^2$. For N = 1, the answer of this problem, is given by Fermat's two-square theorem. In [4], Fine proved this theorem by using the group structure of the modular group $H(\lambda_3)$ = PSL(2, Z). In [5], to solve the problem for N = 2 and N = 3, Kern-Isberner and Rosenberger used the some facts about the group structures of the Hecke groups $H(\sqrt{2})$ and $H(\sqrt{3})$ where $?_q$ = 2cos(p/q) and q = 4, 6, respectively. Aside from the modular group, these Hecke groups are the only ones whose elements are completely known, [6]. Also, Kern-Isberner and Rosenberger extended these results for N = 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 37, 58 by considering the groups G_N consisting of all matrices V of type (1) or (2):

$$V = \begin{pmatrix} a\sqrt{N} & b \\ c & d\sqrt{N} \end{pmatrix}; a,b,c,d \in \mathbb{Z},\ adN - bc = 1 \qquad (1)$$

and

$$V = \begin{pmatrix} a & b\sqrt{N} \\ c\sqrt{N} & d \end{pmatrix}; a,b,c,d \in \mathbb{Z}, ad - bcN = 1 \qquad (2)$$

where, a matrix is identified with its negative. It is well-known that $H(\sqrt{N}) = G_N$ for N = 2, 3 [7, 8]. The case N = 4 can be reduced to the two-square theorem as stated in [5]. In [9], it was considered this problem for all integers N = 5 by using the group structures of the Hecke groups $H(\sqrt{N})$, N = 5 integer, generated by the two linear fractional transformations

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

It was given an algorithm that computes the integers x and y for all N = 2. These Hecke groups $H(\sqrt{N})$, N = 5, are Fuchsian groups of the second kind (see [6], [10] and [11] for more details about the Hecke groups).

Corresponding Author: Dr. Nihal Yilmaz Özgür, Department of Mathematics, Balikesir University, 10145 Çagis, Balikesir, Turkey

Here we shall try to determine some values of n which can be written in the form $n = x^2 + Ny^2$. Note that this problem was solved for prime values of n in [12].

RESULTS

From now on we will assume that N is any integer = 5. By identifying the transformation $z \to \frac{Az+B}{Cz+D}$ with the matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, $H(\sqrt{N})$ may be regarded as multiplicative group of 2 × 2 real matrices in which a matrix and its negative are identified. All elements of $H(\sqrt{N})$ have one of the above two forms (1) or (2). But the converse is not true, that is, all elements of the type (1) or (2) need not belong to $H(\sqrt{N})$. In [6], Rosen proved that a transformation

$$V(z) = \frac{Az + B}{Cz + D} \in H(\sqrt{N})$$

if and only if A/C is a finite $\sqrt{N}$-fraction. In $H(\sqrt{N})$, the set of all elements of the form (2) forms a subgroup of index 2 called the even subgroup. It is denoted by $H_e(\sqrt{N})$. Having index two, $H_e(\sqrt{N})$ is a normal subgroup of $H(\sqrt{N})$. Also, $H_e(\sqrt{N})$ is the free product of two infinite cyclic groups generated by T and RTR, [11].

Throughout the paper, we assume that n > 0, n ? N and (n, N) = 1. In [9], it was shown that the following two conditions are necessary to get some results about the problem under consideration by using the group structure of the Hecke group $H(\sqrt{N})$:

- -N is a quadratic residue mod n
- n is a quadratic residue mod N.

In fact, these conditions are not sufficient to solve the problem for all numbers n and N. Indeed, we can consider the following example.

Example 2.1: Let N = 11 and n = 23. Observe that -11 is a quadratic residue mod 23 and 23 is a quadratic residue mod 11. But it can be easily checked that the number 23 can not be represented in the form $23 = x^2 + 11y^2$ with (x, y) = 1.

Here we can try to find sufficient conditions.

Let -N be a quadratic residue mod n. Since (n, N) = 1, there are k, l ∈ Z such that kN - nl = 1. Hence we have kN = 1 + nl and kN ≡ 1 (mod n) and so -k is a quadratic residue mod n, too. Therefore we have $u^2 \equiv -k$ (mod n) for some u ∈ Z. We get $u^2N \equiv -kN$ (mod n), $u^2N \equiv -1$ (mod n) and so we have

$$u^2N = -1 + qn \qquad (3)$$

for some q ∈ Z. Now we consider the matrix

$$B = \begin{pmatrix} -u\sqrt{N} & -q \\ n & u\sqrt{N} \end{pmatrix} \qquad (4)$$

of which determinant $-u^2N + qn = 1$. We know that $B \in H(\sqrt{N})$ if and only if $-\frac{u\sqrt{N}}{n}$ is a finite $\sqrt{N}$-fraction. If $B \in H(\sqrt{N})$, then our problem can be solved using the group structure of $H(\sqrt{N})$. Indeed, B has order 2 as tr(B) = 0. Since $H(\sqrt{N}) \cong C_2 * Z$, each element of order 2 in $H(\sqrt{N})$ is conjugate to the generator R. That is,

$$B = VRV^{-1} \qquad (5)$$

for some $V \in H(\sqrt{N})$. We may assume that V is a matrix of type (2), $V = \begin{pmatrix} a & b\sqrt{N} \\ c\sqrt{N} & d \end{pmatrix}$; $a,b,c,d \in \mathbb{Z}, ad - bcN = 1$. Then we obtain

$$B = \begin{pmatrix} (ac + bd)\sqrt{N} & -(a^2 + Nb^2) \\ d^2 + Nc^2 & -(ac + bd)\sqrt{N} \end{pmatrix} \qquad (6)$$

Comparing the entries, we have $n = d^2 + Nc^2$ for some integers d, c. From the discriminant condition, clearly we get (d, c) = 1.

Therefore if we can find the conditions that determine whether $-\frac{u\sqrt{N}}{n}$ is a finite $\sqrt{N}$-fraction or not, then we can get some more results about this problem using the group structure of $H(\sqrt{N})$. Note that we are unable to give the exact conditions. But, from Lemma 4 in [3], we know that A/C is a finite $\sqrt{N}$-fraction if and only if there is a sequence a_k such that:

$$\frac{A}{C} = \frac{a_{k+1}}{a_k} \text{ or } -\frac{a_{k-1}}{a_k} \qquad (7)$$

for some k. The sequence a_k is defined by:

$$a_0 = 1,$$

$$a_1 = s_1\sqrt{N}, \qquad (8)$$

$$a_{k+1} = s_{k+1}\sqrt{N}a_k - a_{k-1}, k \geq 2,$$

where, s_k's are nonzero integers. Here we use this lemma to find some values of n which can be written in the form $n = x^2 + Ny^2$.

In (5), if we choose V such that $V \in H(\sqrt{N})$, then $B = VRV^{-1} \in H(\sqrt{N})$ and we find some values of n. Let us start by choosing $s_1 = x$ and $s_2 = y$ in (8). We get

$$a_0 = 1,$$

$$a_1 = x\sqrt{N}, \tag{9}$$

$$a_2 = xyN-1.$$

Now $-\frac{a_1}{a_2} = -\frac{x\sqrt{N}}{xyN-1}$ is a finite $\sqrt{N}$-fraction and hence the matrix

$$V = \begin{pmatrix} -x\sqrt{N} & 1 \\ xyN-1 & -y\sqrt{N} \end{pmatrix}$$

is in $H(\sqrt{N})$. If we compute the matrix VRV^{-1}, we find

$$B = \begin{pmatrix} * & -(1+Nx^2) \\ (xyN-1)^2 + Ny^2 & * \end{pmatrix}.$$

Comparing the entries we have

$$n = (xyN-1)^2 + Ny^2 \text{ and } q = 1 + Nx^2. \tag{10}$$

Notice that n = 1 (mod N) in this case. But the converse statement is not true everywhen. In Example 2.1, we have seen that 23 = 1 (mod 11) and 23 can not be written in the form $23 = x^2 + 11y^2$.

From now on, without loss of generality we will assume that c > 0.

Lemma 2.2: $\xi \in U$ is a fixed point of an elliptic element $E \in H(\sqrt{N})$ if and only if $\xi = \frac{-d\sqrt{N}+i}{c}$ where $d^2N + 1 \equiv 0 \pmod{c}$, c (>N) is a quadratic residue mod N and $-\frac{d\sqrt{N}}{c}$ is a finite $\sqrt{N}$-fraction.

Proof: We know that any elliptic element E in $H(\sqrt{N})$ is conjugate to the generator $R(z) = -1/z$ and an odd element of the form

$$E = \begin{pmatrix} -d\sqrt{N} & b \\ c & d\sqrt{N} \end{pmatrix}; -d^2N - bc = 1$$

since tr(E) = 0. The fixed points of E are given by $\frac{-d\sqrt{N} \pm i}{c}$ and $-d^2N - bc = 1$. Clearly $\xi = \frac{-d\sqrt{N}+i}{c} \in U$ and $-\frac{d\sqrt{N}}{c}$ is a finite $\sqrt{N}$-fraction. Let $E = VRV^{-1}$ for some $V \in H(\sqrt{N})$. If V is of the form (1) then we have

$$E = \begin{pmatrix} \alpha\sqrt{N} & \beta \\ \gamma & \delta\sqrt{N} \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \delta\sqrt{N} & -\beta \\ -\gamma & \alpha\sqrt{N} \end{pmatrix} = \begin{pmatrix} (\alpha\gamma+\beta\delta)\sqrt{N} & * \\ \gamma^2+\delta^2N & * \end{pmatrix}.$$

Comparing the entries we have c is of the form $\gamma^2 + \delta^2N$ for some integers γ, δ. This shows that $c \equiv \gamma^2 \pmod{N}$ and so c is a quadratic residue mod N. If V is of the form (2), it can be similarly checked that c is a quadratic residue mod N.

Conversely, assume that c divides $d^2N + 1$, c (>N) is a quadratic residue mod N and $-\frac{d\sqrt{N}}{c}$ is a finite $\sqrt{N}$-fraction. Then the element

$$E = \begin{pmatrix} -d\sqrt{N} & -(d^2N+1)/c \\ c & d\sqrt{N} \end{pmatrix} \in H(\sqrt{N})$$

is elliptic of order 2 and fixes $\xi = \frac{-d\sqrt{N}+i}{c}$.

Lemma 2.3: $\xi \in U$ is a fixed point of an elliptic element $E \in H(\sqrt{N})$ if and only if ξ is equivalent to the point i in $H(\sqrt{N})$.

Proof: There exists a unique point $\eta \in F_{\sqrt{N}}$ equivalent to ξ. If we write ξ = V(η), then η is fixed by the transformation $\hat{E} = V^{-1}EV \in H(\sqrt{N})$. If E is elliptic then so is Ê. But i is the only elliptic fixed point in $F_{\sqrt{N}}$. Hence ξ is equivalent to the point i.

Conversely, if $\xi = V(i), V \in H(\sqrt{N})$ and E is the elliptic element fixing i, then ξ is fixed by the elliptic element VEV^{-1}.

Remark 2.4: Observe that for $V = \begin{pmatrix} \alpha\sqrt{N} & \beta \\ \gamma & \delta\sqrt{N} \end{pmatrix} \in H(\sqrt{N})$ with γ and δ are relatively prime, we have:

$$V(i) = \frac{(\alpha\gamma+\beta\delta)\sqrt{N}+i}{\gamma^2+\delta^2N} \tag{11}$$

and for $V = \begin{pmatrix} \alpha & \beta\sqrt{N} \\ \gamma\sqrt{N} & \delta \end{pmatrix} \in H(\sqrt{N})$ with γ and δ are relatively prime, we have:

$$V(i) = \frac{(\alpha\gamma+\beta\delta)\sqrt{N}+i}{\gamma^2 N+\delta^2}. \qquad (12)$$

Now we prove the following theorem:

Theorem 2.5: Let c (> N) be any positive divisor of $d^2N + 1$. Assume that c is a quadratic residue mod N and $-\frac{d\sqrt{N}}{c}$ is a finite $\sqrt{N}$-fraction. Then c can be written as $c = x^2 + Ny^2$ with $x, y \in Z$ and $(x, y) = 1$.

Proof: Suppose that c satisfies the conditions given in the statement of the theorem. Then by the sufficiency of Lemma 2.2, $\xi = \frac{-d\sqrt{N}+i}{c}$ is an elliptic fixed point. Hence, by the necessity of Lemma 2.3 and by the equations (11) and (12), ξ can be written in the form

$$\xi = \frac{-d\sqrt{N}+i}{c} = \frac{(\alpha\gamma+\beta\delta)\sqrt{N}+i}{\gamma^2+\delta^2 N}$$

or

$$\xi = \frac{-d\sqrt{N}+i}{c} = \frac{(\alpha\gamma+\beta\delta)\sqrt{N}+i}{\gamma^2 N+\delta^2}.$$

Comparing the imaginary parts, we see that $c = x^2 + Ny^2$ for some integers x, y with $(x, y) = 1$.

Remark 2.6: Notice that if $d^2N + 1 \equiv 0 \pmod c$, then clearly $-N$ is a quadratic residue mod c.

For the converse of Theorem 2.5, we have the following result.

Theorem 2.7: If $c = x^2 + Ny^2$ with $(x, y) = 1$, then there exists an integer d such that $d^2N \equiv -1 \pmod c$ and c is a quadratic residue mod N.

Proof: It must be $(x, N) = 1$, otherwise it would be $(c, N) \neq 1$. Since $(x, y) = 1$, we have $(x, yN) = 1$. Then there exist integers a and b so that $ayN - bx = 1$. Let

$$d = ax + by. \qquad (13)$$

It can be easily checked that

$$d^2N + 1 = (x^2 + Ny^2)(a^2N + b^2).$$

That is, we have $d^2N \equiv -1 \pmod c$. Clearly, c is a quadratic residue mod N since $c = x^2 + Ny^2$.

Remark 2.8: In Theorem 2.7, we can not guarantee that $-\frac{d\sqrt{N}}{c}$ is a finite $\sqrt{N}$-fraction everywhen.

REFERENCES

1. Hecke, E., 1936. Über die bestimmung Dirichletscher reihen durch ihre funktionalgleichung, Math. Ann. 112: 664-699.
2. Lyndon, R.C. and J.L. Ullman, 1968. Pairs of real 2×2 matrices that generate free products, Michigan Math. J., 15: 161-166.
3. Yilmaz Özgür, N. and I.N. Cangül, 2002. On the group structure and parabolic points of the Hecke group $H(\lambda)$, Proc. Estonian Acad. Sci. Phys. Math., 51: 35-46.
4. Fine, B., 1977. A note on the two-square theorem, Canad. Math. Bull., 20: 93-94.
5. Kern-Isberner, G. and G. Rosenberger, 1984. A note on numbers of the form $n = x^2 + Ny^2$, Arch. Math. (Basel) 43: 148-156.
6. Rosen, D., 1954. A class of continued fractions associated with certain properly discontinuous groups, Duke Math. J., 21: 549-563.
7. Hutchinson, J.I., 1902. On a class of automorphic functions, Trans. Amer. Math. Soc., 3: 1-11.
8. Young, J., 1904. On the group of sign (0, 3; 2, 4, 8) and the functions belonging to it, Trans. Amer. Math. Soc., 5: 81-104.
9. Yilmaz Özgür, N., On the numbers of the form $n = x^2 + Ny^2$ and the Hecke groups $H(\sqrt{N})$, submitted.
10. Schmidt, T.A. and M. Sheingorn, 1995. Length spectra of the Hecke triangle groups, Math. Z., 220: 369-397.
11. Yilmaz Özgür, N., 2006. Principal congruence subgroups of Hecke Groups $H(\sqrt{q})$, Acta Math. Sin. (Engl. Ser.) 22: 383-392.
12. Cox, D.A., 1989. Primes of the form $x^2 + Ny^2$, John Wiley and Sons, Inc., New York.