Journal of Number Theory 130 (2010) 1274–1281

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On numbers of the form $n = x^2 + Ny^2$ and the Hecke groups $H(\sqrt{N})$

Nihal Yılmaz Özgür

Balıkesir University, Department of Mathematics, 10145 Balıkesir, Turkey

ARTICLE INFO

Article history:
Received 3 October 2006
Revised 14 December 2009
Available online 23 March 2010
Communicated by D. Zagier

MSC:
11D85
11F06
20H10

Keywords:
Hecke groups
Representation of integers

ABSTRACT

We consider the Hecke groups $H(\sqrt{N})$, $N \geqslant 2$ integer, to get some results about the problem when a natural number n can be represented in the form $n = x^2 + Ny^2$. Given a natural number n, we give an algorithm that computes the integers x and y satisfying the equation $n = x^2 + Ny^2$ for all $N \geqslant 2$.

1. Introduction

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

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

where $\lambda \in \mathbb{R}$, $\lambda \geqslant 2$ or $\lambda = \lambda_q = 2\cos(\frac{\pi}{q})$, $q \in \mathbb{N}$, $q \geqslant 3$. These values of λ are the only ones that give discrete groups, by a theorem of Hecke [3]. 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, $H(\lambda_q) \cong C_2 * C_q$. Let N be a fixed positive integer and x, y are integers. For $N = 1$, the answer of the question when a natural number n can be represented in the form $n = x^2 + Ny^2$, is given by Fermat's

E-mail address: nihal@balikesir.edu.tr.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.01.002

two-square theorem. In [2], B. Fine proved this theorem using the group structure of the modular group $H(\lambda_3) = PSL(2,\mathbb{Z})$. To solve the problem for $N = 2$ and $N = 3$, in [5], G. Kern-Isberner and G. Rosenberger dealt with the Hecke groups $H(\sqrt{2})$ and $H(\sqrt{3})$ where $\lambda_q = 2\cos\frac{\pi}{q}$ and $q = 4, 6$, respectively. Aside from the modular group, these Hecke groups are the only ones whose elements are completely known [7]. Also, G. Kern-Isberner and G. 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 U of type (1.1) or (1.2):

$$U = \begin{pmatrix} a & b\sqrt{N} \\ c\sqrt{N} & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}, \qquad ad - Nbc = 1, \tag{1.1}$$

$$U = \begin{pmatrix} a\sqrt{N} & b \\ c & d\sqrt{N} \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}, \qquad adN - bc = 1, \tag{1.2}$$

where a matrix is identified with its negative. It is known that $H(\sqrt{N}) = G_N$ for $N = 2, 3$ (see [4,11]). Note that the case $N = 4$ can be reduced to the two-square theorem as stated in [5]. Here we consider this problem for all integers $N \geqslant 5$. To do this we shall consider the Hecke groups $H(\sqrt{N})$, $N \geqslant 5$ integer, generated by two linear fractional transformations

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

These Hecke groups $H(\sqrt{N})$ are Fuchsian groups of the second kind (see [7,8] for more details about the Hecke groups). For a given n, we give an algorithm that computes the integers x and y satisfying the equation $n = x^2 + Ny^2$ for all $N \geqslant 2$.

Note that the problem "given a positive integer N, which primes p can be expressed in the form $p = x^2 + Ny^2$, where x and y are integers?" was considered in [1]. Also, in [10], the present author gave an algorithm that computes the integers x and y satisfying the equation $n = x^2 + y^2$ for a given positive integer n such that -1 is a quadratic residue *mod n* using the group structure of the modular group $H(\lambda_3) = PSL(2,\mathbb{Z})$.

2. Main results

From now on we will assume that N is any integer $\geqslant 5$ unless otherwise stated. By identifying the transformation $z \to \frac{Az+B}{Cz+D}$ with the matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, $H(\sqrt{N})$ may be regarded as a 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 (1.1) or (1.2). But the converse is not true, that is, all elements of the type (1.1) or (1.2) need not belong to $H(\sqrt{N})$. In [7], Rosen proved that a transformation $V(z) = \frac{Az+B}{Cz+D} \in H(\sqrt{N})$ if and only if $\frac{A}{C}$ is a finite $\sqrt{N}$-fraction. Recall that a finite $\sqrt{N}$-fraction has the form

$$(r_0\sqrt{N}, -1/r_1\sqrt{N}, \ldots, -1/r_n\sqrt{N}) = r_0\sqrt{N} - \cfrac{1}{r_1\sqrt{N} - \cfrac{1}{r_2\sqrt{N} - \cdots - \cfrac{1}{r_n\sqrt{N}}}}, \tag{2.1}$$

where r_i $(i \geqslant 0)$ are positive or negative integers and r_0 may be zero. Also it is known that the Hecke group $H(\sqrt{N})$ is isomorphic to the free product of a cyclic group of order 2 and a free group of rank 1 (see [6,9]), that is,

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

Here, we use this group structure of $H(\sqrt{N})$. Throughout the paper, we assume that $n > 0$, $n \in \mathbb{N}$ and $(n, N) = 1$.

Let $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$. Since n and N are relatively prime, we have $(Ny, x) = 1$. Then we can find numbers $z, t \in \mathbb{Z}$ with $Nyt - xz = 1$. Therefore the matrix $U = \begin{pmatrix} y\sqrt{N} & x \\ z & t\sqrt{N} \end{pmatrix}$ is in G_N. Conjugating R by U gives an element A of G_N:

$$A = \begin{pmatrix} -(yz + xt)\sqrt{N} & x^2 + Ny^2 \\ -(z^2 + Nt^2) & (yz + xt)\sqrt{N} \end{pmatrix} = \begin{pmatrix} -\alpha\sqrt{N} & n \\ \beta & \alpha\sqrt{N} \end{pmatrix}; \quad \alpha, \beta \in \mathbb{Z}$$

with $\det(A) = 1 = -N\alpha^2 - n\beta$ which implies that $-N$ is a quadratic residue *mod* n. Notice that the equation $n = x^2 + Ny^2$ implies $n \equiv x^2$ *mod* N and hence n is a quadratic residue *mod* N, too. In this case we need not to $H(\sqrt{N})$ and therefore we obtain the following theorem for all n and N using the transformations of the group G_N.

Theorem 2.1. *Let N be a fixed positive integer and let n be a positive integer relatively prime to N. If $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$, then $-N$ is a quadratic residue mod n and n is a quadratic residue mod N.*

Conversely, assume that $-N$ is a quadratic residue *mod* n. Since $(n, N) = 1$, there are $k, l \in \mathbb{Z}$ such that $kN - \ln = 1$. Hence we have $kN = 1 + \ln$, and $kN \equiv 1$ *mod* n, and so $-k$ is a quadratic residue *mod* n, too. Therefore we have $u^2 \equiv -k$ *mod* n for some $u \in \mathbb{Z}$. We get $u^2N \equiv -kN$ *mod* n, $u^2N \equiv -1$ *mod* n, and so we have

$$u^2N = -1 + qn \tag{2.2}$$

for some $q \in \mathbb{Z}$. Now we consider the matrix

$$B = \begin{pmatrix} -u\sqrt{N} & n \\ -q & u\sqrt{N} \end{pmatrix} \tag{2.3}$$

of which determinant $-u^2N + qn = 1$. Clearly $B \in G_N$. In [5], for $N = 2$, G. Kern-Isberner and G. Rosenberger solved the problem for all natural numbers n using the fact that B must be conjugate to the generator R in G_2. If -2 is a quadratic residue *mod* n, they proved that n can be written as $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$. For the values $N = 3, 5, 6, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 37, 58$, G. Kern-Isberner and G. Rosenberger proved that B must be conjugate to R in G_N by consideration of the additional assumption n is also quadratic residue *mod* N. Therefore n can be written as $n = x^2 + Ny^2$ for these values of N under the extra hypothesis n is a quadratic residue *mod* N. For $N = 7$, they obtained that if n is an odd number and if -7 is a quadratic residue *mod* n, then n can be written as $n = x^2 + 7y^2$.

At this point we want to use the group structure of the Hecke groups $H(\sqrt{N})$ to get similar results for the values of $N \geqslant 5$ other than stated above. Notice that the matrix B cannot be always in $H(\sqrt{N})$. If $\frac{u\sqrt{N}}{q}$ is a finite $\sqrt{N}$-fraction, then B is an element of $H(\sqrt{N})$. Also B has order 2 as $tr\, B = 0$. Since $H(\sqrt{N}) \cong C_2 * \mathbb{Z}$, each element of order 2 in $H(\sqrt{N})$ is conjugate to the generator R, that is, $B = VRV^{-1}$ for some $V \in H(\sqrt{N})$. We may assume that V is a matrix of type (1.1), $V = \begin{pmatrix} a & b\sqrt{N} \\ c\sqrt{N} & d \end{pmatrix}$; $a, b, c, d \in \mathbb{Z}$, $ad - Nbc = 1$. Then we obtain

$$B = \begin{pmatrix} -(ac + bd)\sqrt{N} & a^2 + Nb^2 \\ -(d^2 + Nc^2) & (bd + ac)\sqrt{N} \end{pmatrix}. \tag{2.4}$$

Comparing the entries, we have $n = a^2 + Nb^2$ for some integers a, b. From the discriminant condition, clearly we get $(a, b) = 1$. Therefore, if we can find the conditions that determine whether $\frac{u\sqrt{N}}{q}$ is a finite $\sqrt{N}$-fraction or not, then it is possible to get some more results about this problem.

Note that we are unable to give the explicit conditions which determine whether $\frac{u\sqrt{N}}{q}$ is a finite $\sqrt{N}$-fraction or not. But, from Lemma 4 in [9], we know that $\frac{A}{C}$ is a finite $\sqrt{N}$-fraction if and only if there is a sequence a_k such that

$$\frac{A}{C} = \frac{a_{k+1}}{a_k} \quad \text{or} \quad -\frac{a_{k-1}}{a_k} \tag{2.5}$$

for some k. The sequence a_k is defined by

$$\begin{aligned} a_0 &= 1, \\ a_1 &= s_1\sqrt{N}, \\ a_{k+1} &= s_{k+1}\sqrt{N}a_k - a_{k-1}, \quad k \geqslant 2, \end{aligned} \tag{2.6}$$

where s_k's come from any sequence of non-zero integers. Here we will use this lemma to get some examples.

We start with an algorithm that computes the integers x and y for the cases $N = 2$ and $N = 3$.

Theorem 2.2. *Let $N = 2$ or $N = 3$. For $N = 2$, let n be a natural number such that -2 is a quadratic residue mod n and for $N = 3$, let n be a natural number such that -3 is a quadratic residue mod n and n is a quadratic residue mod 3. In either case, let u and q $(>N)$ be the integers satisfying the equation $Nu^2 = -1 + qn$. Define the following functions*:

$$\begin{aligned} f &: (a, b, c, d) \to (d, -c, -b, a), \\ g &: (a, b, c, d) \to (a - c, 2Na + b - Nc, c, c + d). \end{aligned} \tag{2.7}$$

Start with the quadruple $(-u, n, -q, u)$, and apply f if the first coordinate is positive and apply g if not. Proceed likewise until the quadruple $(0, 1, -1, 0)$ is obtained. For f write R and for r_i times g write T^{r_i}. Then compute the matrix $V = T^{r_0}RT^{r_1}R \ldots RT^{r_n}$ where only r_0 and r_n may be zero. If $V = \begin{pmatrix} x & y\sqrt{N} \\ z\sqrt{N} & t \end{pmatrix}$, then the following equations are satisfied:

$$\begin{aligned} n &= x^2 + Ny^2, \\ q &= Nz^2 + t^2, \\ u &= xz + yt. \end{aligned} \tag{2.8}$$

If $V = \begin{pmatrix} x\sqrt{N} & y \\ z & t\sqrt{N} \end{pmatrix}$, then the following equations are satisfied:

$$\begin{aligned} n &= Nx^2 + y^2, \\ q &= z^2 + Nt^2, \\ u &= xz + yt. \end{aligned} \tag{2.9}$$

Proof. The proof is based on the fact that the matrix B, defined in (2.3), must be conjugate to R in G_N for $N=2,3$. Then $B=VRV^{-1}$ for some $V\in G_N$. If V is a matrix of type (1.1), $V=\begin{pmatrix} x & y\sqrt{N} \\ z\sqrt{N} & t\end{pmatrix}$, $a,b,c,d\in\mathbb{Z}$, $ad-Nbc=1$, then we obtain $B=\begin{pmatrix} (-xz-yt)\sqrt{N} & x^2+Ny^2 \\ -(Nz^2+t^2) & (xz+yt)\sqrt{N}\end{pmatrix}$. Comparing the entries, we have $n=x^2+Ny^2$, $q=Nz^2+t^2$, $u=xz+yt$. From the discriminant condition, clearly we get $(x,y)=1$. Our method is to find the matrix V such that $B=VRV^{-1}$ and so $V^{-1}BV=R$. To do this we use the group structure of G_N. Every element of G_N can be expressed as a word in R and T. So $V=T^{r_0}RT^{r_1}R\ldots RT^{r_n}$ where the r_i $(0<i<n)$ are integers and only r_0 and r_n may be zero. Then we have

$$\begin{aligned} R=V^{-1}BV&=\left(T^{-r_n}R\ldots RT^{-r_1}RT^{-r_0}\right)B\left(T^{r_0}RT^{r_1}R\ldots RT^{r_n}\right)\\ &=\left(T^{-r_n}R\ldots RT^{-r_1}R\right)\left(T^{-r_0}BT^{r_0}\right)\left(RT^{r_1}R\ldots RT^{r_n}\right).\end{aligned}$$

If f represents the coefficients of the matrix RXR and g represents ones for the matrix $T^{-1}XT$ for any matrix $X=\begin{pmatrix} a\sqrt{N} & b \\ c & d\sqrt{N}\end{pmatrix}\in G_N$, then the proof follows easily using the fact that conjugate matrices have equal traces.

As $T^r=\begin{pmatrix} 1 & r\sqrt{N} \\ 0 & 1\end{pmatrix}$, $T^rR=\begin{pmatrix} -r\sqrt{N} & 1 \\ -1 & 0\end{pmatrix}$ and $RT^r=\begin{pmatrix} 0 & 1 \\ -1 & -r\sqrt{N}\end{pmatrix}$ for any integer r, it is easy to compute the matrix V.

If V is a matrix of type (1.2), the proof follows similarly. □

The following examples illustrate the algorithm defined in Theorem 2.2.

Example 2.1. Let $N=2$ and $n=89$. Observe that -2 is a quadratic residue *mod* 89. We can find the integers $20,9$ such that $2(20)^2=-1+89.9$. We have

$$\begin{aligned} &(-20,89,-9,20)\underset{\rightarrow}{g}(-11,27,-9,11)\underset{\rightarrow}{g}(-2,1,-9,2)\\ &\underset{\rightarrow}{g}(7,11,-9,-7)\underset{\rightarrow}{f}(-7,9,-11,7)\underset{\rightarrow}{g}(4,3,-11,-4)\underset{\rightarrow}{f}(-4,11,-3,4)\\ &\underset{\rightarrow}{g}(-1,1,-3,1)\underset{\rightarrow}{g}(2,3,-3,-2)\underset{\rightarrow}{f}(-2,3,-3,2)\underset{\rightarrow}{g}(1,1,-3,-1)\\ &\underset{\rightarrow}{f}(-1,3,-1,1)\underset{\rightarrow}{g}(0,1,-1,0).\end{aligned}$$

Then $V=T^3RTRT^2RTRT$. If we compute the matrix V, we obtain

$$\begin{aligned} V&=\begin{pmatrix} 1 & 3\sqrt{2} \\ 0 & 1\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -\sqrt{2}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -2\sqrt{2}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -\sqrt{2}\end{pmatrix}^2\\ &=\begin{pmatrix} 9 & 2\sqrt{2} \\ 2\sqrt{2} & 1\end{pmatrix}.\end{aligned}$$

By (2.8), we find

$$89=(9)^2+2(2)^2,\qquad 9=2(2)^2+1^2,\qquad 20=9.2+2.1.$$

Example 2.2. Let $N=3$ and $n=172$. -3 is a quadratic residue *mod* 172 and 172 is a quadratic residue *mod* 3. We can find the integers $33,19$ such that $3(33)^2=-1+172.19$. We have

$$(-33,172,-19,33)\underset{\rightarrow}{g}(-14,31,-19,14)\underset{\rightarrow}{g}(5,4,-19,-5)$$
$$\underset{\rightarrow}{f}(-5,19,-4,5)\underset{\rightarrow}{g}(-1,1,-4,1)\underset{\rightarrow}{g}(3,7,-4,-3)\underset{\rightarrow}{f}(-3,4,-7,3)$$
$$\underset{\rightarrow}{g}(4,7,-7,-4)\underset{\rightarrow}{f}(-4,7,-7,4)\underset{\rightarrow}{g}(3,4,-7,-3)\underset{\rightarrow}{f}(-3,7,-4,3)$$
$$\underset{\rightarrow}{g}(1,1,-4,-1)\underset{\rightarrow}{f}(-1,4,-1,1)\underset{\rightarrow}{g}(0,1,-1,0).$$

Then $V=(T^2R)^2(TR)^3T$. If we compute the matrix V, we obtain

$$V=\begin{pmatrix}-2\sqrt{3} & 1\\ -1 & 0\end{pmatrix}^2\begin{pmatrix}-\sqrt{3} & 1\\ -1 & 0\end{pmatrix}^3\begin{pmatrix}1 & \sqrt{3}\\ 0 & 1\end{pmatrix}$$
$$=\begin{pmatrix}7\sqrt{3} & 5\\ 4 & \sqrt{3}\end{pmatrix}.$$

By (2.9), we find

$$172=3(7)^2+(5)^2,\qquad 19=(4)^2+3(1)^2,\qquad 33=7.4+5.1.$$

Remark 2.1. Since the case $N=4$ can be reduced to the two-square theorem and the corresponding Hecke group $H(\sqrt{N})$ is a subgroup of the modular group $H(\lambda_3)=PSL(2,\mathbb{Z})$, the similar algorithm given in [10] can be used to compute the integers x and y in this case. That is, if -4 is a quadratic residue *mod n*, then one can find the integers u and q (>4) satisfying the equation $u^2 4=-1+qn$. The matrix B defined in (2.3), is an element of the modular group and hence it must be conjugate to R. Then the similar algorithm given in [10] works in this case, too.

If $B\in H(\sqrt{N})$, $N\geqslant 5$, then the method given in Theorem 2.2 is also valid for all N. For all $N\geqslant 5$, we use this algorithm. Now observe that the matrix

$$C=\begin{pmatrix}u\sqrt{N} & 1\\ -qn & -u\sqrt{N}\end{pmatrix}$$

is in $H(\sqrt{N})$. Indeed, using the equation $-u^2N+qn=1$ given in (2.2), it can be easily verified that

$$-\frac{u\sqrt{N}}{qn}=-\frac{1}{u\sqrt{N}+\frac{1}{u\sqrt{N}}}.$$

Therefore we get $-\frac{u\sqrt{N}}{qn}$ is a finite $\sqrt{N}$-fraction and so C is an element of $H(\sqrt{N})$, more explicitly $C=RT^uRT^{-u}R$. Also C has order 2 as $tr\,C=0$. Since each element of order 2 in $H(\sqrt{N})$ is conjugate to the generator R, if $B\in H(\sqrt{N})$, then B must be conjugate to C. In this case $C=DBD^{-1}$ for some $D\in H(\sqrt{N})$. We may assume that D is a matrix of type (1.1), $D=\left(\begin{smallmatrix}a & b\sqrt{N}\\ c\sqrt{N} & d\end{smallmatrix}\right)$; $a,b,c,d\in\mathbb{Z}$, $ad-Nbc=1$. We have

$$DBD^{-1}=\begin{pmatrix}* & (2uab+b^2q)N+a^2n\\ * & *\end{pmatrix}=\begin{pmatrix}u\sqrt{N} & 1\\ -qn & -u\sqrt{N}\end{pmatrix}.$$

Comparing the second entries, we obtain that $(2uab+b^2q)N+a^2n=1$ and $a^2n\equiv 1$ *mod N*. Hence if $B\in H(\sqrt{N})$, then n must be a quadratic residue *mod N*. Therefore the conditions $-N$ is a quadratic residue *mod* n and n is a quadratic residue *mod* N are necessary to get some results about the problem under consideration by using the group structure of the Hecke group $H(\sqrt{N})$. Note that these conditions are not the sufficient conditions. Also it must be $B \in H(\sqrt{N})$, that is, $\frac{u}{q}\sqrt{N}$ must be a finite $\sqrt{N}$-fraction. For example, for $N = 17$ and $n = 52$, observe that 52 is a quadratic residue *mod* 17 and -17 is a quadratic residue *mod* 52. But it is easily checked that 52 cannot be written in the form $52 = x^2 + 17y^2$ where $(x, y) = 1$.

For all $N \geqslant 5$, we can use the algorithm given in Theorem 2.2. For $N = 7$, if n is an odd number and if -7 is a quadratic residue *mod* n; for other values of $N \geqslant 5$, if $-N$ is a quadratic residue *mod* n and n is a quadratic residue *mod* N, then one can find the integers u and q $(>N)$ satisfying the equation $u^2N = -1 + qn$. If $\frac{u\sqrt{N}}{q}$ is a finite $\sqrt{N}$-fraction, then $B \in H(\sqrt{N})$ and the algorithm defined in Theorem 2.2 is valid. One can use the nearest integer algorithm to find the expansion of $\frac{u\sqrt{N}}{q}$ in an $\sqrt{N}$-fraction (for more details about this algorithm, see [7]).

Finally we give an example explaining our method.

Example 2.3. Let $N = 11$ and $n = 991$. -11 is a quadratic residue *mod* 991 and 991 is a quadratic residue *mod* 11. We can find the integers 100, 111 such that $11(100)^2 = -1 + 991.111$. We find the expansion of $\frac{100\sqrt{11}}{111}$ in a finite $\sqrt{11}$-fraction as

$$\frac{100\sqrt{11}}{111} = \sqrt{11} - \cfrac{1}{\sqrt{11} - \cfrac{1}{\sqrt{11} + \cfrac{1}{\sqrt{11} - \cfrac{1}{\sqrt{11}}}}}.$$

Therefore $\frac{100\sqrt{11}}{111}$ is a finite $\sqrt{11}$-fraction and $B = \begin{pmatrix} -100\sqrt{11} & 991 \\ -111 & 100\sqrt{11} \end{pmatrix} \in H(\sqrt{11})$. Using the algorithm defined in Theorem 2.2, we have

$$\begin{aligned} &(-100, 991, -111, 100) \underset{\rightarrow}{g} (11, 12, -111, -11) \underset{\rightarrow}{f} (-11, 111, -12, 11) \\ &\quad \underset{\rightarrow}{g} (1, 1, -12, -1) \underset{\rightarrow}{f} (-1, 12, -1, 1) \underset{\rightarrow}{g} (0, 1, -1, 0). \end{aligned}$$

Then $V = (TR)^2T$. If we compute the matrix V, we obtain

$$\begin{aligned} V &= \begin{pmatrix} -\sqrt{11} & 1 \\ -1 & 0 \end{pmatrix}^2 \begin{pmatrix} 1 & \sqrt{11} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 10 & 9\sqrt{11} \\ \sqrt{11} & 10 \end{pmatrix}. \end{aligned}$$

By (2.8), we find

$$991 = (10)^2 + 11(9)^2, \qquad 111 = 11(1)^2 + (10)^2, \qquad 100 = 10.1 + 9.10.$$

Remark 2.2. Notice that this algorithm can be used for all N and n without any restriction. Even for large values of n this method works easily.

References

[1] D.A. Cox, Primes of the Form $x^2 + Ny^2$, John Wiley, 1989.
[2] B. Fine, A note on the two-square theorem, Canad. Math. Bull. 20 (1) (1977) 93–94.
[3] E. Hecke, Über die bestimmung Dirichletscher reihen durch ihre funktionalgleichung, Math. Ann. 112 (1) (1936) 664–699.

[4] J.I. Hutchinson, On a class of automorphic functions, Trans. Amer. Math. Soc. 3 (1902) 1–11.
[5] G. Kern-Isberner, G. Rosenberger, A note on numbers of the form $n = x^2 + Ny^2$, Arch. Math. 43 (2) (1984) 148–156.
[6] R.C. Lyndon, J.L. Ullman, Pairs of real 2×2 matrices that generate free products, Michigan Math. J. 15 (1968) 161–166.
[7] D. Rosen, A class of continued fractions associated with certain properly discontinuous groups, Duke Math. J. 21 (1954) 549–563.
[8] T.A. Schmidt, M. Sheingorn, Length spectra of the Hecke triangle groups, Math. Z. 220 (3) (1995) 369–397.
[9] N. Yılmaz Özgür, I.N. Cangül, On the group structure and parabolic points of the Hecke group $H(\lambda)$, Proc. Estonian Acad. Sci. Phys. Math. 51 (1) (2002) 35–46.
[10] N. Yılmaz Özgür, On the two-square theorem and the modular group, Ars Combin. 94 (2010) 251–255.
[11] J. Young, On the group of sign $(0, 3; 2, 4, \infty)$ and the functions belonging to it, Trans. Amer. Math. Soc. 5 (1) (1904) 81–104.