ON THE TWO-SQUARE THEOREM AND THE MODULAR GROUP

NİHAL YILMAZ ÖZGÜR

ABSTRACT. Given a positive integer n such that -1 is a quadratic residue mod n, we give an algorithm that computes the integers u and v which satisfy the equation $n = u^2 + v^2$. To do this we use the group structure of the Modular group $\Gamma = PSL(2, \mathbb{Z})$.

1. INTRODUCTION

Fermat's two-square theorem states that a prime p is expressible as the sum of two squares if and only if -1 is a quadratic residue mod p, [5]. In [2], Fine gave a new proof of this theorem using the group structure of the Modular group $\Gamma = PSL(2, \mathbb{Z})$ which is one of the Hecke groups. Fine's result extends the two-square theorem for an arbitrary positive integer n.

The Hecke groups $H(\lambda)$ are the discrete subgroups of $PSL(2, \mathbb{R})$ 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, [6]. 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, $H(\lambda_q) \cong C_2 * C_q$. The Modular group Γ is the Hecke group $H(\lambda_3)$. Γ and its normal subgroups have especially been of great interest in many fields of mathematics, for example number theory, automorphic function theory and group theory, (see [1]-[4] and [7]-[10]).

2000 *Mathematics Subject Classification*. Primary 11D85, 11F06, 20H10, 11E25.

Key words and phrases. Representation of integers, two-square theorem, Modular group.

The Modular group Γ consists of all linear fractional transformations

$$z \to \frac{az+b}{cz+d}, \; a, \; b, \; c, \; d \in \mathbb{Z} \text{ and } ad-bc=1.$$

All elements of Γ can also be considered as projective matrices $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a, b, c, d rational integers and $ad - bc = 1$.

Using the group structure of the Modular group, Fine proved the following theorem, [2]:

Theorem 1.1. *A positive integer n is the sum of 2 squares if -1 is a quadratic residue mod n. Conversely if $n = u^2 + v^2$ with $(u, v) = 1$ then -1 is a quadratic residue mod n.*

In this paper, given a positive integer n such that -1 is a quadratic residue mod n, we give an algorithm that computes the integers u and v in the theorem. To do this, we use the some facts about the structure of the Modular group.

2. The Algorithm

Before giving the algorithm that computes the integers u and v, we summarize the technique used in the proof of Theorem 1.1. Let $n > 0$, $n \in \mathbb{Z}$. Assume that -1 is a quadratic residue mod n. Then there are integers l, k with $l^2 = -1 + kn$. Now we consider the matrix

$$A = \begin{pmatrix} -l & n \\ -k & l \end{pmatrix} \tag{2.1}$$

of which determinant $1 = -l^2 + kn$. Clearly $A \in \Gamma$. Also A has order 2 as $trA = 0$. Since $\Gamma \cong C_2 * C_3$, each element of order 2 in Γ is conjugate to the generator R, that is, $A = BRB^{-1}$ for some $B \in \Gamma$. If $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$; $\alpha, \beta, \gamma, \delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1$, then we obtain

$$A = \begin{pmatrix} -(\alpha\gamma + \beta\delta) & \alpha^2 + \beta^2 \\ -(\gamma^2 + \delta^2) & (\alpha\gamma + \beta\delta) \end{pmatrix}.$$

Comparing the entries, we have $n = \alpha^2 + \beta^2$ for some integers α, β. From the determinant condition, clearly we get $(\alpha, \beta) = 1$. Also we find that $k = \gamma^2 + \delta^2$, $l = \alpha\gamma + \beta\delta$.

We now present the algorithm. First we need the following result which follows directly from the discussion above and the proof of Theorem 1.1. We let

$$R = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

As mentioned in the introduction, the Modular group Γ is generated by R and T.

Proposition 2.1. *Let n be a positive integer such that -1 is a quadratic residue mod n and let l, k be the integers satisfying the equation $l^2 = -1 + kn$. Now let A be the matrix*

$$A = \begin{pmatrix} -l & n \\ -k & l \end{pmatrix}$$

and let B be the projective matrix such that

$$A = BRB^{-1}.$$

If

$$B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

then the following equations are satisfied:

$$\begin{aligned} n &= \alpha^2 + \beta^2, \\ k &= \gamma^2 + \delta^2, \\ l &= \alpha\gamma + \beta\delta. \end{aligned} \tag{2.2}$$

There is a standard algorithm (see [9] and [3]) to express any projective matrix $M \in \Gamma$ in terms of the generators R, T. From this algorithm we get the algorithm to find the integers u, v such that $n = u^2 + v^2$.

Proposition 2.2. *Let n and B be as in Proposition 2.1. Then given A there is an effective algorithm to determine B. From B the integers u, v can then be determined.*

Proof. Apply the standard algorithm as described in [9] or [3] to express A as a word in R and T. Now let $V = RT$ so that $T = RV$ and rewrite the expression for A as a word in R and V. R and V form a free product basis for Γ so the expression for A in terms of R and V is unique. Since $A = BRB^{-1}$ it follows that the expression for B in terms of R and V can be read directly off of the expression for A. Rewriting in terms of a matrix gives B as a matrix.

This standard algorithm can be implemented for B in the following way: Define the functions

$$
\begin{aligned}
f &: (a,b,c,d) \to (d,-c,-b,a) \\
g &: (a,b,c,d) \to (a-c, 2a+b-c, c, c+d)\,.
\end{aligned}
\tag{2.3}
$$

Given A start with $(-l, n, -k, l)$. Apply f if the first coordinate is positive and apply g if not. Proceed and eventually $(0,1,-1,0)$ will be obtained. Write R for f and T^{r_i} for r_i times g. The matrix B is then $B = T^{r_0}RT^{r_1}R$ ... RT^{r_n} where only r_0 and r_n may be zero ([9] or [3]). □

Since $T^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, T^rR = \begin{pmatrix} -r & 1 \\ -1 & 0 \end{pmatrix}$ and $RT^r = \begin{pmatrix} 0 & 1 \\ -1 & -r \end{pmatrix}$ for any integer r, it is easy to compute the matrix B. The following example illustrates the algorithm defined in Proposition 2.2.

Example 2.1. *Let* $n = 1649$. *Observe that* -1 *is a quadratic residue mod* 1649. *We can find the integers* 463, 130 *such that* $(463)^2 = -1 + 1649.130$. *We have*

$$(-463, 1649, -130, 463) \underset{\to}{g} (-333, 853, -130, 333) \underset{\to}{g} (-203, 317, -130, 203)$$
$$\underset{\to}{g} (-73, 41, -130, 73) \underset{\to}{g} (57, 25, -130, -57) \underset{\to}{f} (-57, 130, -25, 57)$$
$$\underset{\to}{g} (-32, 41, -25, 32) \underset{\to}{g} (-7, 2, -25, 7) \underset{\to}{g} (18, 13, -25, -18) \underset{\to}{f} (-18, 25, -13,$$
$$\underset{\to}{g} (-5, 2, -13, 5) \underset{\to}{g} (8, 5, -13, -8) \underset{\to}{f} (-8, 13, -5, 8) \underset{\to}{g} (-3, 2, -5, 3)$$
$$\underset{\to}{g} (2, 1, -5, -2) \underset{\to}{f} (-2, 5, -1, 2) \underset{\to}{g} (-1, 2, -1, 1) \underset{\to}{g} (0, 1, -1, 0).$$

Then we obtain $B = T^4RT^3R(T^2R)^2T^2$. *If we compute the matrix* B, *we get*

$$
\begin{aligned}
B &= \begin{pmatrix} -4 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -3 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -2 & 1 \\ -1 & 0 \end{pmatrix}^2\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 25 & 32 \\ 7 & 9 \end{pmatrix}.
\end{aligned}
$$

By (2.2), we find

$$1649 = (25)^2 + (32)^2, 130 = (7)^2 + (9)^2 \text{ and } 463 = 25.7 + 32.9.$$

Remark 2.1. *In* [1], *Beck showed that there is a one to one correspondence between the family of* 2×2 *matrices over* $\mathbb{Z}^+$ *whose determinant equals 1, and the family of partially ordered paths. Then using this correspondence Beck also gave an another algorithm that computes the integers* u *and* v *in the Theorem 1.1. Our algorithm uses matrix multiplication and works easily even for large values of* n *as in the Example 2.1.*

Acknowledgement. The author is thankful to the referees for valuable suggestions for improvement of this paper.

References

[1] I. Beck, *Partial Orders and the Modular Group*, Linear Algebra Appl. 120 (1989), 139-147.

[2] B. Fine, *A Note on the Two-Square Theorem*, Canad. Math. Bull. **20** (1) (1977), 93-94.

[3] B. Fine, *Algebraic theory of the Bianchi groups*, Monographs and Textbooks in Pure and Applied Mathematics, 129. Marcel Dekker, Inc., New York, 1989.

[4] B. Fine, *Trace classes and quadratic forms in the modular group*, Canad. Math. Bull., Vol. **37** (2) (1994), 202-212.

[5] G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers*, Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[6] E. Hecke, *Über die bestimmung Dirichletscher reihen durch ihre funktionalgleichungen*, Math. Ann. **112** (1936), 664-699.

[7] M. Newman, *The structure of some subgroups of the modular group*, Illinois J. Math., **6** (1962), 480-487.

[8] M. Newman, *Classification of normal subgroups of the modular group*, Trans. Amer. Math. Soc. **126** (1967), 267-277.

[9] M. Newman, *Integral matrices*, Pure and Applied Mathematics, Vol. 45. Academic Press, New York-London, 1972.

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

Balikesir University, Department of Mathematics, 10145 Balikesir, TURKEY
E-mail address: nihal@balikesir.edu.tr