Acta Math. Univ. Comenianae
Vol. LXXIV, 2(2005), pp. 205–209

REPRESENTATION OF INTEGERS BY HERMITIAN FORMS

A. TEKCAN

Abstract. In this paper we consider the representation of (positive) integers by the Hermitian forms C_n, $C_{k,l}$ and $C^*_{k,l}$.

1. Introduction

Let Γ be the *modular group* $\mathrm{PSL}(2,\mathbb{Z})$, i.e. the set of the transformations

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

Picard group P is a group which consists of all transformations of the form

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

P is generated by the transformations $S(z)=-z$, $T(z)=z-1$, $U(z)=-\frac{1}{z}$, $V(z)=-z-i$, and has a presentation

$$P = \left\langle \begin{array}{rl} S,T,U,V : S^2 = & U^2 = V^2 = (US^{-1})^2 = (VT^{-1})^2 \\ = & (ST^{-1})^2 = (UT^{-1})^3 = (VU^{-1})^3 = I \end{array} \right\rangle.$$

P is sometimes denoted by $\mathrm{PSL}(2,\mathbb{Z}[i])$ and can be thought as 3-dimensional version of the modular group Γ (see [**1**], [**3**] and [**4**]).

A *binary Hermitian form* is a form of the type

$$C:\ az\overline{z} + bz + \overline{b}\overline{z} + c$$

for $a,c \in \mathbb{Z}$ and $b \in \mathbb{Z}[i]$. Taking $z=x+iy$ and $b=b_1+ib_2$ for $x,y,b_1,b_2 \in \mathbb{Z}$, we have

$$C : a\left(x^2+y^2\right) + 2b_1x - 2b_2y + c. \tag{1}$$

This form is denoted by $C=(a,b_1,b_2,c)$. The *discriminant* of C is defined by the formula $b_1^2+b_2^2-ac$ and is denoted by Δ. If $a \neq 0$, then the Hermitian form $C=(a,b_1,b_2,c)$ of discriminant $\Delta > 0$ represents a circle in the complex plane centered at $\left(\frac{-b_1}{a},\frac{b_2}{a}\right)$ with radius $r=\frac{\sqrt{\Delta}}{|a|}$.

Received March 15, 2004.
2000 *Mathematics Subject Classification.* Primary 11E16, 11E25.
Key words and phrases. Hermitian forms, Picard group, representation of integers by Hermitian forms.

A Hermitian form of positive discriminant represents a circle for $a \neq 0$ and a circle corresponds to a Hermitian form of positive discriminant. If $r = 1$, then $C = (a, b_1, b_2, c)$ is called a *unit Hermitian form.*

Two Hermitian forms are said to be *equivalent* if there exists a transformation in the Picard group taking one to the other (see [**2**] and [**4**]).

Let $C = (a, b_1, b_2, c)$ be a Hermitian form, and let n be any integer. If there exist integers x and y such that

$$C(x, y) = a\left(x^2 + y^2\right) + 2b_1x - 2b_2y + c = n,$$

then we say that n is *represented* by C.

2. Representation of Integers by Hermitian Forms.

Representation of integers by binary quadratic forms[1] and Hermitian forms has an important role in the theory of numbers and was studied by many authors. In the present paper, we consider the representation of integers by Hermitian forms.

For any given positive integer n, we define the *n-form* C_n as

$$C_n = (n, n^2, n, n).$$

Then the discriminant of C_n is n^4. So C_n represents a circle centered at $(-n, 1)$ with radius n. Then we have the following theorem.

Theorem 2.1. *Every positive integer can be represented by* C_n.

Proof. Let n be any positive integer. Consider the Diophantine equation

$$C_n(x, y) = n\left(x^2 + y^2\right) + 2n^2x - 2ny + n = n.$$

This equation has a solution for $(x, y) = (-n-1, 1-n)$, that is $C_n(-n-1, 1-n) = n$. Therefore every positive integer can be represented by C_n. □

Example 2.1. Let $n = 7$. Then we have $C_7 = (7, 49, 7, 7)$ and thus $C_7(-8, -6) = 7$.
For $n = 12$ we have $C_{12} = (12, 144, 12, 12)$ and thus $C_{12}(-13, -11) = 12$.

Let n be any positive integer. Consider the following circles with radius n:

$$\begin{aligned} C^x_{1,1} &= (n, -n, n^2, n), \\ C^x_{1,4} &= (n, -n, -n^2, n), \\ C^x_{-1,2} &= (n, n, n^2, n), \\ C^x_{-1,3} &= (n, n, -n^2, n) \end{aligned}$$

[1] A real binary quadratic form F is a polynomial in two variables x and y of the type $F(x, y) = ax^2 + bxy + cy^2$ with real coefficients a, b, c.

and

$$\begin{aligned} C^y_{1,1} &= (n, -n^2, n, n), \\ C^y_{1,2} &= (n, n^2, n, n), \\ C^y_{-1,3} &= (n, n^2, -n, n), \\ C^y_{-1,4} &= (n, -n^2, -n, n), \end{aligned}$$

where for the circle $C^t_{u,v}$; t represents the axis x or y, u represents a line that is perpendicular to x or y axis, and v represents the number of quadrants in the plane. We denote the family of these circles by Φ. The circles $C^x_{1,1}$ and $C^x_{1,4}$ are tangent to the x-axis at $x = 1$ and the circles $C^x_{-1,2}$ and $C^x_{-1,3}$ are tangent to the $x-$axis at $x = -1$. The points $x = 1$ and $x = -1$ are called *attractive points* of these circles. Similarly, the circles $C^y_{1,1}$ and $C^y_{1,2}$ are tangent to the y-axis at $y = 1$ and the circles $C^y_{-1,3}$ and $C^y_{-1,4}$ are tangent to the $y-$axis at $y = -1$. The points $y = 1$ and $y = -1$ are called *attractive points* of these circles.

Theorem 2.2. *Every positive integer can be represented by each of the forms in Φ.*

Proof. Let n be a positive integer. Consider the Diophantine equation

$$C^x_{1,1}(x, y) = n\left(x^2 + y^2\right) - 2nx - 2n^2y + n = n.$$

This equation has a solution for $(x, y) = (1-n,\ n-1)$, that is $C^x_{1,1}(1-n,\ n-1) = n$. Therefore n can be represented by $C^x_{1,1}$. Similarly,

$$\begin{aligned} C^x_{1,4}(1-n, -n-1) &= n, \\ C^x_{-1,2}(-n-1, n-1) &= n, \\ C^x_{-1,3}(-n-1, -n-1) &= n, \\ C^y_{1,1}(n-1, n+1) &= n, \\ C^y_{1,2}(-n-1, 1-n) &= n, \\ C^y_{-1,3}(-n-1,\ n-1) &= n, \\ C^y_{-1,4}(n-1, -n-1) &= n \end{aligned}$$

can be obtained. □

Let $C = (a, b_1, b_2, c)$ be a circle centered at $\left(\frac{-b_1}{a}, \frac{b_2}{a}\right)$ with radius $r = \frac{\sqrt{\Delta}}{|a|}$. Then the transformation

$$W(z) = z + \left(\frac{b_1 - b_2}{a}\right) + i\left(\frac{b_1 - b_2}{a}\right)$$

sends C to (a, b_2, b_1, c), which is again a circle centered at $\left(\frac{-b_2}{a}, \frac{b_1}{a}\right)$ with radius $r = \frac{\sqrt{\Delta}}{|a|}$.

Theorem 2.3. *Each of the circles in the family Φ is equivalent to C_n.*

Proof. The transformation $W_n(z) = z + (n-1) + i(n-1)$ is an element of P since $n-1$ is an integer. We know that P is generated by the transformations $S(z) = -z, T(z) = z-1, U(z) = -\frac{1}{z}$ and $V(z) = -z-i$. Hence

$$\begin{aligned} W_n(C_n) &= C^x_{-1,2}, \\ UW_n(C_n) &= C^x_{1,1}, \\ SW_n(C_n) &= C^x_{1,4}, \\ USW_n(C_n) &= C^x_{-1,3} \end{aligned}$$

and

$$\begin{aligned} U(C_n) &= C^y_{1,1}, \\ S(C_n) &= C^y_{-1,4}, \\ SU(C_n) &= C^y_{-1,3}, \\ (SU)^2(C_n) &= C^y_{1,2} \end{aligned}$$

for $C_n = (n, n^2, n, n)$. Therefore each of the circles in the family Φ is equivalent to C_n. □

From Theorem 2.3,

Corollary 2.4. *All of the circles in the family Φ are equivalent.*

Let k and l be any two integers. We define the *k,l-form* $C_{k,l}$ as

$$C_{k,l} = \left(-n,\ nk,\ -nl, n\left(1-k^2-l^2\right)\right)$$

for an integer n. The discriminant of $C_{k,l}$ is n^2. Therefore $C_{k,l}$ represents a circle centered at (k,l) with radius 1. So $C_{k,l}$ is a unit Hermitian form.

Theorem 2.5. *Every integer can be represented by $C_{k,l}$.*

Proof. Let n be any integer. Consider the Diophantine equation

$$C_{k,l}(x,y) = -n\left(x^2+y^2\right) + 2nkx + 2nly + n\left(1-k^2-l^2\right) = n.$$

This equation has a solution for $(x,y) = (k,l)$, that is $C_{k,l}(k,l) = n$. Therefore every integer can be represented by $C_{k,l}$. □

Example 2.2. Let $n = 10$. Then n can be represented by

$$C_{3,4} = (-10, 30, -40, -240).$$

n also can be represented by

$$C_{-2,-6} = (-10, -20, 60, -390).$$

In fact, there are infinitely many unit Hermitian forms $C_{k,l}$ representing n.

In Theorem 2.7 we will show that there exists a unique unit Hermitian form $C_{k,l}$, up to equivalency, representing n.

For distinct integers k and l we define the Hermitian form $C^*_{k,l}$ as

$$C^*_{k,l} = (n, -nk, nl, 2nkl)$$

for an integer n. The discriminant of $C^*_{k,l}$ is $(nk-nl)^2$. So $C^*_{k,l}$ represents a circle in $\mathbb{C}$ centered at (k,l) with radius $r=|k-l|$. Then we have the following theorem.

Theorem 2.6. *Every integer can be represented by* $C^*_{k,l}$.

Proof. Let n be any integer. Then the Diophantine equation

$$C^*_{k,l}(x,y)=n\left(x^2+y^2\right)-2nkx-2nly+2nkl=n$$

has a solution for $(x,y)=(k-1,k)$, that is $C^*_{k,l}(k-1,k)=n$. Therefore every integer can be represented by $C^*_{k,l}$. □

Example 2.3. Let $n=17$. Then n can be represented by

$$C^*_{2,4}=(17,-34,68,272).$$

n also can be represented by

$$C^*_{-3,-8}=(17,51,-136,816).$$

In fact, there are infinitely many Hermitian forms $C^*_{k,l}$ representing n.

Let $C_{r,s}$ and $C_{t,u}$ be two circles with the same radius centered at (r,s) and (t,u), respectively, for $r,s,t,u\in\mathbb{Z}$. Then the transformation

$$W(z)=z+(t-r)+i(u-s)$$

is an element of P since $t-r$ and $u-s$ are integers. $W(z)$ sends $C_{r,s}$ to $C_{t,u}$. Therefore $C_{r,s}$ and $C_{t,u}$ are equivalent under $W(z)$. Hence we can say that circles of the same radius are equivalent under $W(z)$. Therefore from Theorem 2.5,

Theorem 2.7. *There exists a unique unit Hermitian form* $C_{k,l}$*, up to equivalency, representing* n.

References

1. Coxexter H. S. M. and Moser W. O. J., *Generators and Relations for Discrete Groups.* Springer-Berlin, 1957.

2. Earnest A. G. and Khosravani A., *Universal Binary Hermitian Forms.* Mathematics of Computation, **66**(219) (1997), 1161–1168.

3. Flath D. E., *Introduction to Number Theory.* Wiley, 1989.

4. Harding S. J., *Some Arithmetic and Geometric Problems Concerning Discrete Groups.* Ph. D. Thesis, Southampton University, 1985.

A. Tekcan, Department of Mathematics, Faculty of Science University of Uludag, Görükle 16059, Bursa, Turkey, *e-mail*: fahmet@uludag.edu.tr