

## REPRESENTATION OF A BINARY QUADRATIC FORM AS A SUM OF TWO SQUARES

KENNETH S. WILLIAMS

**ABSTRACT.** Let  $\phi(x, y)$  be an integral binary quadratic form. A short proof is given of Pall's formula for the number of representations of  $\phi(x, y)$  as the sum of squares of two integral linear forms.

Let  $\phi(x, y)$  be an integral binary quadratic form. If  $\phi(x, y)$  is expressible as the sum of squares of two integral linear forms then  $\phi(x, y)$  must be positive definite or semidefinite, have an even coefficient of  $xy$ , and be of square determinant. Mordell [1] has proved that a binary quadratic form  $\phi(x, y) = hx^2 + 2kxy + ly^2$  with these properties is the sum of squares of two integral linear forms if and only if  $r_2(d_1) > 0$ , where  $r_2(d_1)$  denotes the number of representations of  $d_1 = \text{G.C.D.}(h, 2k, l)$  as the sum of two squares. Pall [2], using properties of Hermite-matrices, has shown that when  $\phi(x, y)$  is representable in this way, the number of such representations is  $2r_2(d_1)$ , if  $\det(\phi) = hl - k^2 = m^2 \neq 0$ , and is  $r_2(d_1)$ , if  $\det(\phi) = hl - k^2 = m^2 = 0$ . In this note we give a very simple proof of this result.

Since  $hx^2 + 2kxy + ly^2$  can be expressed as the sum of squares of two integral linear forms there exist integers  $a_1, a_2, b_1, b_2$ , such that

$$(1) \quad hx^2 + 2kxy + ly^2 = (a_1x + b_1y)^2 + (a_2x + b_2y)^2.$$

If we write  $\alpha, \beta$  for the gaussian integers  $a_1 + ia_2, b_1 + ib_2$  respectively, (1) becomes

$$(2) \quad hx^2 + 2kxy + ly^2 = (\alpha x + \beta y)(\bar{\alpha}x + \bar{\beta}y),$$

so that

$$(3) \quad h = \alpha\bar{\alpha}, \quad 2k = \alpha\bar{\beta} + \bar{\alpha}\beta, \quad l = \beta\bar{\beta}.$$

The domain of all gaussian integers is denoted by  $Z(i)$ . It is a unique factorization domain. We let  $\gamma \in Z(i)$  denote one of the four associated greatest common divisors of  $\alpha$  and  $\beta$  and write  $\alpha = \gamma\alpha_1, \beta = \gamma\beta_1$ , so that the only common factors of  $\alpha_1$  and  $\beta_1$  are the units  $\pm 1, \pm i$ . Hence from

Received by the editors December 23, 1970.

*AMS 1970 subject classifications.* Primary 10C05, 10J05; Secondary 10E25.

*Key words and phrases.* Binary quadratic form, sum of squares.

© American Mathematical Society 1972

(2) we have

$$\begin{aligned} d_1 &= \text{G.C.D.}(h, 2k, l) = \text{G.C.D.}(\alpha\bar{\alpha}, \alpha\bar{\beta} + \bar{\alpha}\beta, \beta\bar{\beta}) \\ &= \gamma\bar{\gamma} \text{G.C.D.}(\alpha_1\bar{\alpha}_1, \alpha_1\bar{\beta}_1 + \bar{\alpha}_1\beta_1, \beta_1\bar{\beta}_1), \end{aligned}$$

that is

$$(4) \quad d_1 = \gamma\bar{\gamma},$$

and so (2) becomes

$$(5) \quad hx^2 + 2kxy + ly^2 = d_1(\alpha_1x + \beta_1y)(\bar{\alpha}_1x + \bar{\beta}_1y).$$

Moreover we have

$$\begin{aligned} m^2 &= \det(hx^2 + 2kxy + ly^2) = hl - k^2 \\ &= (\alpha\bar{\alpha})(\beta\bar{\beta}) - \left(\frac{\alpha\bar{\beta} + \bar{\alpha}\beta}{2}\right)^2 \quad (\text{from (3)}) \\ &= -\left(\frac{\alpha\bar{\beta} - \bar{\alpha}\beta}{2}\right)^2 = -(\gamma\bar{\gamma})^2 \left(\frac{\alpha_1\bar{\beta}_1 - \bar{\alpha}_1\beta_1}{2}\right)^2 \\ &= -d_1^2 \left(\frac{\alpha_1\bar{\beta}_1 - \bar{\alpha}_1\beta_1}{2}\right)^2 \quad (\text{from (4)}), \end{aligned}$$

that is,

$$(6) \quad m = \pm d_1 i \left(\frac{\alpha_1\bar{\beta}_1 - \bar{\alpha}_1\beta_1}{2}\right).$$

Now the required number of representations is just the number of distinct 4-tuples of integers  $(a'_1, a'_2, b'_1, b'_2)$  such that

$$hx^2 + 2kxy + ly^2 = (a'_1x + b'_1y)^2 + (a'_2x + b'_2y)^2,$$

that is, on writing  $\alpha' = a'_1 + ib'_1 \in Z(i)$ ,  $\beta' = a'_2 + ib'_2 \in Z(i)$  and using (5), the number of distinct pairs of gaussian integers  $(\alpha', \beta')$  such that

$$(\alpha'x + \beta'y)(\bar{\alpha}'x + \bar{\beta}'y) = d_1(\alpha_1x + \beta_1y)(\bar{\alpha}_1x + \bar{\beta}_1y).$$

As  $\alpha_1x + \beta_1y$  is a primitive irreducible element in the unique factorization domain  $Z(i)[x, y]$  we have

$$\alpha_1x + \beta_1y \mid \alpha'x + \beta'y \quad \text{or} \quad \alpha_1x + \beta_1y \mid \bar{\alpha}'x + \bar{\beta}'y.$$

If  $\alpha_1x + \beta_1y \mid \alpha'x + \beta'y$  then  $\alpha'x + \beta'y = \delta(\alpha_1x + \beta_1y)$  for some  $\delta \in Z(i)$ , and so we have

$$(7) \quad (\alpha', \beta') = (\delta\alpha_1, \delta\beta_1), \quad \text{where } \delta\bar{\delta} = d_1.$$

Similarly if  $\alpha_1x + \beta_1y \mid \bar{\alpha}'x + \bar{\beta}'y$  we have

$$(8) \quad (\alpha', \beta') = (\delta'\bar{\alpha}_1, \delta'\bar{\beta}_1), \quad \text{where } \delta'\bar{\delta}' = d_1.$$

If  $m \neq 0$ , so that from (6) we have  $\alpha_1 \bar{\beta}_1 \neq \bar{\alpha}_1 \beta_1$ , then  $(\delta \alpha_1, \delta \beta_1) \neq (\delta' \bar{\alpha}_1, \delta' \bar{\beta}_1)$  and so (7) and (8) give  $2r_2(d_1)$  distinct pairs  $(\alpha', \beta')$  as required. If  $m=0$ , so that from (6) we have  $\alpha_1 \bar{\beta}_1 = \bar{\alpha}_1 \beta_1$ , then  $\bar{\alpha}_1 \sim \alpha_1$ ,  $\bar{\beta}_1 \sim \beta_1$  and the set of ordered pairs given by (7) coincides with that given by (8), thus giving only  $r_2(d_1)$  distinct pairs  $(\alpha', \beta')$  as required.

## REFERENCES

1. L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. **35** (1932), 1–15.
2. G. Pall, *Sums of two squares in a quadratic field*, Duke Math. J. **18** (1951), 399–409. MR **12**, 676.

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA