

## REPRESENTATION OF NUMBERS IN TERNARY QUADRATIC FORMS

E. ROSENTHALL

We employ integral quaternions  $t = t_0 + t_1i_1 + t_2i_2 + t_3i_3$ , where the coordinates  $t_i$  range over rational integers, while the  $i_1, i_2, i_3$ , satisfy the multiplication table

$$i_1^2 = i_2^2 = -2, \quad i_3^2 = -3, \quad i_2i_3 = 2i_1 - i_2 = (\overline{i_3i_2}),$$

$$i_3i_1 = -i_1 + 2i_2 = (\overline{i_1i_3}), \quad i_1i_2 = -1 + i_3 = (\overline{i_2i_1}),$$

and  $\bar{t} = t_0 - t_1i_1 - t_2i_2 - t_3i_3$  is the conjugate to  $t$ . The norm  $N(t)$  of  $t$  is  $t\bar{t} = \bar{t}t = t_0^2 + 2t_1^2 + 2t_2^2 + 2t_1t_2 + 3t_3^2$ . The norm of a product of two quaternions equals the product of their norms, and  $\overline{vt} = \bar{t}\bar{v}$  for any two quaternions. The associative law  $rs \cdot t = r \cdot st$  holds.

The quaternary quadratic  $Q = t_0^2 + 2t_1^2 + 2t_2^2 + 2t_1t_2 + 3t_3^2$  has determinant 9, the g.c.d. of the literal coefficients of the adjoint to  $Q$  is 3, and the second concomitant of  $Q$  represents no residues 1 modulo 3, and as there is only one form of determinant 9 with these properties in Charve's table\* of reduced quaternary quadratic forms,  $Q$  belongs to a genus of one class. Since  $Q$  represents 1 for two values of  $t_0, \dots, t_3$ , we have,† a proper quaternion being defined as one having coprime coordinates, the following theorem:

**THEOREM 1.** *A proper quaternion  $v = v_0 + v_1i_1 + v_2i_2 + v_3i_3$  whose norm is divisible by a positive integer  $m$  prime to 6 has exactly two right-divisors (left-divisors)  $t$  and  $-t$  of norm  $m$ .*

Every proper pure quaternion  $s = s_1i_1 + s_2i_2 + s_3i_3$  of norm  $km^2$  is of form  $\bar{t}at$  where  $N(a) = k$  and  $N(t) = m$ . For,  $s = vt$  where  $N(t) = m$  by Theorem 1;  $\bar{s} = -s = \bar{t}\bar{v}$ , and  $\bar{t}$  is a left-divisor of  $s$ . Hence, since  $N(v) = km$ ,  $\bar{t}$  is a left-divisor of the proper quaternion  $v$ ,  $v = \bar{t}a$ . Hence  $s = \bar{t}at$ ,  $N(a) = k$ . Clearly  $a$  is pure since  $\bar{t}at = -\bar{t}at$ ,  $\bar{a} = -a$ .

**THEOREM 2.** *Consider the equation  $24n + 1 = x_1^2 + 2x_2^2 + 2x_3^2 - 2x_2x_3$ . If  $24n + 1 = m^2$ , ( $m > 0$ ), then all proper solutions are of type A if  $m \equiv 1 \pmod{4}$  but of type B if  $m \equiv 3 \pmod{4}$ , where*

$$A: x_1 \equiv \pm 1 \pmod{12}, \quad B: x_1 \equiv \pm 5 \pmod{12}.$$

\* L. Charve, *Comptes Rendus de l'Académie des Sciences*, vol. 96 (1883), p. 773.

† G. Pall, *On the factorization of generalized quaternions*, submitted to the *Duke Mathematical Journal*.

If  $24n + 1$  is not a square, there are equally many solutions of each type  $A$  and  $B$ .

A proof for the case in which  $24n + 1 = m^2$  follows. Consider

$$(1) \quad h = x_1^2 + 2x_2^2 + 2x_3^2 - 2x_2x_3.$$

Then

$$3h = 3x_1^2 + 2(-x_2 - x_3)^2 + 2(-x_2 - x_3)(2x_2 - x_3) + 2(2x_2 - x_3)^2.$$

Put  $h = m^2$ , and let  $x = i_1(-x_2 - x_3) + i_2(2x_2 - x_3) + i_3x_1$  represent a solution  $(x_1, x_2, x_3)$  of (1); then all proper pure quaternions  $x$  are given by  $x = \bar{i}at$ ,  $N(t) = m$ ,  $N(a) = 3$ , and from the latter condition we must have  $a = \pm i_3$ . Expanding  $\bar{i}at$  gives  $x_1 = 3t_3^2 - 2t_1^2 - 2t_2^2 - 2t_1t_2 + t_0^2$  where only  $a = i_3$  is considered since  $a = -i_3$  merely changes the sign of  $x_1$  which leaves  $A$  and  $B$  unaltered.

Thus  $x_1 \equiv m \pmod{4}$ . Since  $(m, 3) = 1$ ,  $x_1 \equiv 1 \pmod{3}$ ; hence when  $m \equiv 1 \pmod{4}$ ,  $x_1 \equiv \pm 1 \pmod{12}$ , a solution of type  $A$ , but if  $m \equiv 3 \pmod{4}$ , then  $x_1 \equiv \pm 5 \pmod{12}$ , a solution of type  $B$ .

The case for  $h = 24n + 1$  not a square will now be considered. Let  $x$  be a representative solution of (1) under this condition. We can choose an odd prime  $p$  such that simultaneously

$$(2) \quad (-3h \mid p) = 1, \quad p \equiv 11 \pmod{12}.$$

By the first equation in (2) we can choose  $x_0$  so that  $3x_0^2 + h \equiv 0 \pmod{p}$ . Then by Theorem 1,  $3x_0 + x$  has exactly two right-divisors  $\pm t$  of norm  $p$ , say

$$3x_0 + x = ut, \quad N(t) = p.$$

Then

$$(3) \quad tx\bar{i} = py, \quad \text{where} \quad y = tu - 3x_0,$$

and  $y$  represents another solution of (1). If  $t$  is replaced by  $-t$ ,  $y$  is unchanged.

We shall prove that  $x$  and  $y$  are in opposite classes  $A$  and  $B$  in view of the second equation of (2), and as multiplication by  $p$  does not alter  $A$  or  $B$ , it will suffice to show that  $x$  and  $tx\bar{i}$  are solutions of opposite types.

Setting  $tx\bar{i} = i_1(-y_2 - y_3) + i_2(2y_2 - y_3) + i_3y_1$  and expanding gives

$$y_1 = x_1(t_0^2 + 3t_3^2 - 2t_2^2 - 2t_1^2 - 2t_1t_2) + x_2(6t_2t_3 + 4t_1t_0 + 2t_2t_0) + x_3(-6t_2t_3 - 6t_3t_1 + 2t_2t_0 - 2t_1t_0).$$

In (1),  $x_2$  and  $x_3$  are always even, and thus

$$y_1 \equiv 3x_1 \pmod{4}, \quad y_1 \equiv x_1 \pmod{3}$$

as  $N(\bar{t}) \equiv 11 \pmod{12}$ . Hence  $y$  represents a solution of type opposite to  $x$ .

We can now establish the (1, 1) correspondence. We employ the preceding process for a fixed  $p$ , with  $x_0$  for a solution of type  $A$ , but  $-x_0$  for a solution of type  $B$ . Hence if our process carries  $x$ , a solution of type  $A$ , into  $y$ , then  $y$  is carried into  $x$ . For from (3)

$$3(-x_0) + y = (-\bar{u})\bar{t}, \quad N(\bar{t}) = p.$$

Then,  $\bar{t}yt = px$ ,  $x = ut - 3x_0$ . Further, two distinct solutions of one type cannot correspond to the same solution of the other type.

Application of other types of quaternions furnishes arithmetical proofs of the following additional results:

For representation of  $24n+1$  in  $x_1^2 + 3x_2^2 + 3x_3^2$  the  $A$  and  $B$  relations are

$$A: x_1 \equiv \pm 1 \pmod{12}, \quad x_2 \text{ and } x_3 \equiv 0 \pmod{4}, \\ x_1 \equiv \pm 5 \pmod{12}, \quad x_2 \text{ and } x_3 \equiv 2 \pmod{4},$$

$$B: x_1 \equiv \pm 1 \pmod{12}, \quad x_2 \text{ and } x_3 \equiv 2 \pmod{4}, \\ x_1 \equiv \pm 5 \pmod{12}, \quad x_2 \text{ and } x_3 \equiv 0 \pmod{4}.$$

For  $2(24n+1) = 3x_1^2 + x_2^2 + x_3^2$

$$A: (0; 1, 1), (0; 7, 7), (0; 11, 5), (4; 5, 5), (4; 11, 11), (4; 7, 1), \\ B: (4; 1, 1), (4; 7, 7), (4; 11, 5), (0; 5, 5), (0; 11, 11), (0; 7, 1),$$

where each triplet  $(x_1; x_2, x_3)$  lists the least absolute residues  $x_1 \pmod{8}$ ,  $x_2 \pmod{24}$ ,  $x_3 \pmod{24}$  in a definite order.

For either form if  $24n+1 = m^2$ , ( $m > 0$ ), all solutions are of type  $A$  if  $m \equiv 1 \pmod{6}$ , but of type  $B$  if  $m \equiv 5 \pmod{6}$ . But there are equally many solutions of each type if  $24n+1$  is not a square.

These results were proved in the writer's thesis at McGill University, 1938.

McGILL UNIVERSITY