THE FORMS $ax^2+by^2+cz^2$ WHICH REPRESENT ALL INTEGERS

BY L. E. DICKSON

THEOREM. *$f=ax^2+by^2+cz^2$ represents all integers, positive, negative, or zero, if and only if*: I. *a, b, c are not all of like sign and no one is zero*; II. *no two of a, b, c have a common odd prime factor*; III. *either a, b, c are all odd, or two are odd and one is double an odd*; IV. *$-bc$, $-ac$, $-ab$ are quadratic residues of a, b, c, respectively.*

We shall first prove that I-IV are necessary conditions. Let therefore f represent all integers. It is well known that I follows readily.

If a and b are divisible by the odd prime p, f represents only $1+\frac{1}{2}(p-1)$ incongruent residues cz^2 modulo p. This proves II.

Next, *no one of a, b, c is divisible by* 8. Let $a\equiv 0 \pmod 8$. Every square is $\equiv 0$, 1, or 4 (mod 8). First, let $b=2B$. Since f represents odd integers, c is odd. Since $by^2\equiv 0$ or $2B$ (mod 8) and $cz^2\equiv 0$, c, or $4c$, f has at most six residues modulo 8. If m is a missing residue, f represents no $m+pn$. Second let b and c be odd. Then $4b\equiv 4c\equiv 4 \pmod 8$. Thus the residues of f modulo 8 are obtained by adding each of 0, 4, b to each of 0, 4, c; we get only seven residues 0, 4, b, c, $4+b$, $4+c$, $b+c$.

No one of a, b, c is divisible by 4. Let a be divisible by 4. Since a is not divisible by 8, $a\equiv 4 \pmod 8$. Evidently $f\equiv 0$, b, c, or $b+c$ (mod 4). No two of these are congruent modulo 4. If $b\equiv \pm 1 \pmod 4$, they are 0, ± 1, c, $c\pm 1$. Evidently c is not congruent to 0, ± 1, or ∓ 1. Hence $c\equiv 2 \pmod 4$. Since $b\not\equiv 0$, this proves that one of b and c is $\equiv 2 \pmod 4$. By symmetry, we may take $b\equiv 2 \pmod 4$. If $b\equiv 6 \pmod 8$, we apply our discussion to $-f$ instead of

f. Hence take $b\equiv 2 \pmod 8$. Thus $a\equiv 8n+4$, $b=8m+2$, and c is odd. Since $x^2\equiv 0$ or $1 \pmod 4$, $ax^2\equiv 0$ or $8n+4 \pmod{16}$. Since $y^2\equiv 0$, 1 or $4 \pmod 8$, $by^2\equiv 0$, $8m+2$, or $8 \pmod{16}$. We employ only even residues of f modulo 16. Then z is even, and $cz^2\equiv 0$ or $4c \pmod{16}$. But $c\equiv \pm 1 \pmod 4$, $4c\equiv \pm 4 \pmod{16}$. Evidently ax^2+by^2 has at most 2×3 residues modulo 16. The missing two even residues are seen to be s and $s+4$, where $s=10$ if n and m are both even, $s=2$ if n is even and m odd, $s=6$ if n is odd and m even, $s=14$ if n and m are both odd. According as $4c\equiv 4$ or -4, f is not congruent to $s+4$ or s modulo 16.

No two of a, b, c are even. Let us set $a=2A$, $b=2B$. By the preceding result, A and B are odd. Also, c is odd. If $A=4n-1$, we use $-f$ in place of f. Hence let $A=4n+1$. Then $f\equiv 2x^2+2By^2+cz^2 \pmod 8$. Consider only odd residues of f. Then $cz^2\equiv c \pmod 8$. The residues of $2x^2+2By^2$ are 0, 2, $2B$, $2B+2$. When these are increased by c, the sums must give the four odd residues modulo 8. Hence no two are congruent. Thus no two of 0, 1, B, $B+1$ are congruent modulo 4. Since B is odd and $\not\equiv 1 \pmod 4$, $B\equiv 3$, $B+1\equiv 0$, a contradiction.

This completes the proof of property III. Properties II and III imply the following property.

V. *a, b, c are relatively prime in pairs.*

Thus $cd\equiv -b \pmod a$ has a solution d which is prime to a. Suppose that d were a quadratic non-residue of an odd prime factor p of a. Write $a=pA$. Consider values of x, y, z for which f is divisible by p. Then $z^2\equiv dy^2 \pmod p$, whence y and z are divisible by p. Hence $f=pF$, where $F\equiv Ax^2 \pmod p$. Evidently Ax^2 takes at most $1+\frac{1}{2}(p-1)$ values incongruent modulo p. Hence there is an integer N that is not congruent to one of them. Thus f fails to represent $p(N+pw)$ for any value of w. This contradiction proves that $v^2\equiv d \pmod p$ is solvable. The usual induction shows that it is solvable modulo p^n. Also, $d^2\equiv d \pmod 2$. By means of the Chinese remainder theorem, we see that $w^2\equiv d$ (mod a, is solvable whether a is odd or double an odd integer, Then w is prime to a since d is. Since $(cw)^2 \equiv -bc \pmod{a}$ this proves IV.

We shall now prove that I–IV imply that f represents every integer g. It is known* that I, IV and V imply that $f=0$ has solutions x', y', z' which are relatively prime in pairs. Then the greatest common divisor of the three numbers $\alpha=ax'$, $\beta=by'$, $\gamma=cz'$ is 1. For, if they are all divisible by a prime p, one of x', y', z' is divisible by p (otherwise a, b, c would all be divisble by p). By symmetry, let x' be divisble by p. Then neither y' nor z' is divisible by p. Hence b and c would be divisble by p, contrary to V. Hence† if D is any given integer, ξ, η, ζ may be chosen so that

$$\alpha\xi + \beta\eta + \gamma\zeta = D. \tag{1}$$

We seek a solution of $f=g$ of the form

$$x = nx' + \xi, \qquad y = ny' + \eta, \qquad z = nz' + \zeta. \tag{2}$$

Since $ax'^2 + \cdots = 0$, $f=g$ is satisfied if

$$2Dn = g - e, \tag{3}$$

where

$$e = a\xi^2 + b\eta^2 + c\zeta^2. \tag{4}$$

If ξ', η', ζ' is a second set of solutions of (1), write

$$X = \xi - \xi', \qquad Y = \eta - \eta', \qquad Z = \zeta - \zeta'.$$

Then

$$\alpha X + \beta Y + \gamma Z = 0. \tag{5}$$

We seek the general solution of (5). Let δ be the greatest common divisor of$\alpha=\delta A$ and $\beta=\delta B$. Then δ is prime to γ, whence $Z=-\delta w$. Hence

$$AX + BY = \gamma w, \quad A, B \text{ relatively prime.} \tag{6}$$

There exist integers r, s satisfying

$$Ar + Bs = 1. \tag{7}$$

---

* Dirichlet-Dedekind, *Zahlentheorie*, ed. 4, §157, p. 432 (Supplement X).

† Since the g. c. d. 1 of α, β, γ, is a linear function of them. Multiply the relation by D.

Multiply the second member of (6) by (7). Thus

$$A(X - \gamma rw) + B(Y - \gamma sw) = 0.$$

The quantities in parenthesis are equal to Bm and $-Am$, where m is an integer. The resulting values of X and Y, together with $Z = -\delta w$, give the general solution of (6). Hence if ξ', η', ζ' is one solution of (1), the general solution is

$$(8)\quad \xi = \xi' + \gamma rw + Bm, \quad \eta = \eta' + \gamma sw - Am, \quad \zeta = \zeta' - \delta w,$$

where w and m are arbitrary, while r, s satisfy (7).

First, let a, b, c be all odd. Then $x'+y'+z' \equiv 0 \pmod 2$. But x', y', z' are not all even. Hence just one of them is even. By symmetry, we may take x' even, y' and z' odd. Then α is even, β and γ are odd, δ is odd, A is even, B is odd. Write

$$(9)\qquad e' = a\xi'^2 + b\eta'^2 + c\zeta'^2.$$

When working modulo 2, we may discard the exponents 2 in (4) and (9). Take $w = 0$, $m = 1$. Then, by (8),

$$\xi \equiv \xi' + 1, \quad \eta \equiv \eta', \quad \zeta \equiv \zeta', \qquad \pmod 2,$$

$$e \equiv \xi + \eta + \zeta \equiv e' + 1.$$

For $w = m = 0$, evidently $e = e'$. Hence we may take $e \equiv g \pmod 2$. We may take $D = 1$. Then (3) yields an integral value of n. Hence $f = g$ is solvable.

Second, let a and b be odd, but c the double of an odd integer, whence $c \equiv 2 \pmod 4$. Since $f \equiv x+y \pmod 2$, $x'+y'$ is even. But x' and y' are relatively prime. Hence x' and y' are odd. Thus α and β are odd, γ is even, δ is odd, A and B are odd. By (1) and (4),

$$(10)\qquad D \equiv \xi + \eta \equiv e, \qquad \pmod 2.$$

If g is odd, we take $D = 1$. (See footnote on p. 59.) By (10), $g - e$ is even and (3) yields an integer n.

But if g is even, we take* $D=2$. By (10), $\xi+\eta$ and e are even. In (8), take $w=0$, $m=1$. Then

$$\xi = \xi' + B, \quad \eta = \eta' - A, \quad \zeta = \zeta'. \tag{11}$$

In case ξ' and η' are odd, we replace ξ', η', ζ' by the preceding solution having ξ and η even. Hence we may choose the initial solution ξ', η', ζ' so that ξ' and η' are even. Then (11) gives

$$e \equiv e' + aB^2 + bA^2 \equiv e' + a + b \pmod 4.$$

Hence if $a+b\equiv 2 \pmod 4$, we may choose e so that $e\equiv g \pmod 4$. Then (3) yields an integral value of n. But if $a+b\equiv 0 \pmod 4$, we take $w=1$, $m=0$ in (8) and see that ξ and η are even since γ is even. Then since δ is odd and $c\equiv 2 \pmod 4$,

$$e \equiv 2\zeta^2 = 2(\zeta' - \delta)^2 \equiv 2\zeta'^2 + 2 = e' + 2 \pmod 4.$$

As before, $f=g$ is solvable.

COROLLARY. *If $ax^2+by^2+cz^2$ is not a Null form, it does not represent all integers.*

Examples with $a=1$, $c=-C$, $C>0$.

(i) $b=1$. Then C must be odd or double an odd integer and -1 must be a quadratic residue of C. Then every odd prime factor of C is $\equiv 1 \pmod 4$. A necessary and sufficient condition on C is that it be a sum of two relatively prime squares.

(ii) $b=2$. Then C must be odd and -2 a quadratic residue of C. Then its prime factors are $\equiv 1$ or $3 \pmod 8$. A necessary and sufficient condition on C is that it be of the form r^2+2s^2, r odd, r and s relatively prime.

(iii) $b=3$. Then C must be odd or double an odd integer, C prime to 3, while C and -3 must be quadratic residues of each other. Hence every prime factor of C is $\equiv 1 \pmod 6$. Necessary and sufficient conditions on C are that C be odd and of the form r^2+3s^2, where r and s are relatively prime.

THE UNIVERSITY OF CHICAGO

---

* Elimination of ξ, η, ζ between (1) and (2) gives $\alpha x+\beta y+\gamma z=D$. Here $D\equiv x+y\equiv f \pmod 2$. Hence $D\equiv g \pmod 2$.