NOTE ON THE DIOPHANTINE EQUATION $ax^2 + by^2 + cz^2 + dt^2 = 0$

BY L. J. MORDELL

Suppose that the constants a, b, c, d are integers none of which is zero, and that

I. *a, b, c, d have no squared factors;*

II. *no three of a, b, c, d have a common factor, that is, $[a, b, c] = 1$, etc.*

Then, if we suppose the restrictions I, II apply throughout the paper, the equation

$$ax^2 + by^2 + cz^2 + dt^2 = 0 \tag{1}$$

has integer solutions not all zero, if, and only if,

III. *a, b, c, d are not all of the same sign,*

IV. *every odd prime factor p_{ab} of $[a, b]$ for which*

$$\left(\frac{-cd}{p_{ab}}\right) = -1, \tag{2}$$

must also satisfy

$$\left(\frac{-ab/p_{ab}^2}{p_{ab}}\right) = 1, \tag{3}$$

together with five corresponding conditions derived by permuting the letters. The symbol is that of quadratic residuacity.

V. (1) *Either* $abcd \equiv 2, 3, 5, 6, 7 \pmod 8$,

V. (2) *or* $abcd \equiv 1 \pmod 8$, $a+b+c+d \equiv 0 \pmod 8$;

these mean that we must exclude

$$a \equiv b \pmod 8, \quad c \equiv d \pmod 8, \quad a \equiv c \pmod 4,$$

and the corresponding sets derived by permuting the letters;

V. (3) *or two of a, b, c, d are even, say a, b, and we must have*

V. (3.1) *either* $\frac{1}{4}abcd \equiv 3, 5, 7 \pmod 8$,

V. (3.2) *or* $\frac{1}{4}abcd \equiv 1 \pmod 8$, and $\frac{1}{2}a + \frac{1}{2}b + c + d \equiv (c^2d^2 - 1)/2 \pmod 8$; these mean that we must exclude the sets

$$\frac{1}{2}a \equiv \frac{3}{2}b \pmod 8, \quad \acute{c} \equiv 3d \pmod 8,$$

or

$$\frac{1}{2}a \equiv \frac{1}{2}b \pmod 8, \quad c \equiv d \pmod 8, \quad \frac{1}{2}a \equiv c \pmod 8,$$

or

$$\frac{1}{2}a \equiv \frac{5}{2}b \pmod 8, \quad c \equiv 5d \pmod 8, \quad \frac{1}{2}a \equiv -c \pmod 8.$$

If in equation (1), we impose the restrictions that

$$[z, t, a, b] = 1 \text{ or } 2 \tag{4}$$

together with the five similar ones obtained by permuting the letters, the only difference in the conditions is that IV must be replaced by

VI. *$-cd$ is a quadratic residue of $[a, b]$, written as $-cd\ R\ [a, b]$, and so of every odd prime factor of $[a, b]$; together with the five conditions obtained by permuting the letters.*

In a recent number of this Bulletin, R. G. Archibald* deduces the conditions III, IV, V in a slightly different form (it is not difficult to see that his II is equivalent to my IV) as a particular case of an important general result due to Hasse. He also refers, *inter alia*, to my recent paper† where I show that III, V, VI are the necessary and sufficient conditions for integer solutions of (1) subject to the restrictions typified by (2).

The first results on (1) were due to Meyer who assumes not only that a, b, c, d satisfy the conditions I, II, which it may be remarked involve no loss of generality and simplify the results, but also the further condition that no primes p_{ab} exist for which (2) holds, that is, his results applied to (1) limited only by I, II really give the solutions as restricted by my condition (4). Both his results and mine are really general in that it is very easy to transform a given equation into the required form. But the methods employed in my paper are so elementary, depending only on Legendre's criteria for the solvability of the equation

* *Criteria for the solution of a certain quadratic diophantine equation*, this Bulletin, vol. 37 (1931), pp. 608–614.

† *The condition for integer solutions of $ax^2+by^2+cz^2+dt^2=0$*, Journal für Mathematik, vol. 164 (1931), pp. 40–49. References to the literature are given here and also in Archibald's note.

$$Ax^2 + By^2 + Cz^2 = 0,$$

that it may be desirable to remove the restriction (4) and to deduce the condition IV instead of VI.

Let p_{ab}, p'_{ab}, etc. be the odd prime factors of $[a, b]$. Then (4) is equivalent to

$$[z, t] \not\equiv 0 \pmod{p_{ab} \text{ or } p'_{ab} \text{ etc.} \cdots},$$

that is, the 2 in (4) is really no restriction since c, d have no squared factors.

We now find the condition that (1) should be solvable subject to the six restrictions typified by (4) except that for a particular odd factor q of $[a, b]$, we are not excluding $[z, t] \equiv 0 \pmod{q}$. If we set

$$z = qz', \quad t = qt', \quad x = x', \quad y = y',$$

the equation (1) becomes

$$a'x'^2 + b'y'^2 + c'z'^2 + d't'^2 = 0, \tag{5}$$

where $a' = a/q$, $b' = b/q$, $c' = cq$, $d' = dq$. Since a', b', c', d' still satisfy I, II, we may assume that $[x', y', z', t'] = 1$ and so no three of x', y', z', t' can have a common factor. Hence x', y' are both prime to q, that is,

$$[x', y', c', d'] = 1 \text{ or } 2.$$

Hence it is clear that (5) is subject to the appropriate six restrictions typified by (4) and we can apply V and VI. But the corresponding condition V for (5) is exactly the same as V since $a'b'c'd' = abcd$ and

$$a' + b' + c' + d' = \frac{a}{q} + \frac{b}{q} + cq + dq \equiv 0 \pmod{8},$$

since $q^2 \equiv 1 \pmod{8}$.

Since $c'd' = cdq^2$, $a'b' = ab/q^2$, $a'c' = ac$, etc., the corresponding ing condition VI, on noting that $-(ab/q^2)Rq[c, d]$ means that $-(ab/q^2)Rq$ and $-(ab/q^2)R[c, d]$, becomes

$$-cdR\left[\frac{a}{q}, \frac{b}{q}\right], \quad -\frac{ab}{q^2}Rq \tag{6}$$

together with the five conditions

$$(7)\qquad \begin{array}{lll} -abR[c,d], & -acR[b,d], & -adR[b,c], \\ -bcR[a,d], & -bdR[a,c]. & \end{array}$$

If $[a, b]$ is divisible by a prime p_{ab} which is not a factor of q and for which

$$(8)\qquad \left[\frac{-cd}{p_{ab}}\right] = -1,$$

(6) will not hold. Hence (6) can be satisfied only if q is divisible by every prime p_{ab} for which (2) holds. For these primes, the condition $-(ab/q^2)Rq$ becomes

$$(9)\qquad -\frac{ab}{p_{ab}^2}Rp_{ab}.$$

If there are such primes p_{ab}, VI shows that (1) is not solvable unless $[z, t] \equiv 0 \pmod{p_{ab}}$, and that it is solvable if q is the product of these p_{ab}. Hence the equation (1) has solutions subject to the five restrictions

$$(10)\qquad \begin{array}{lll} [x,y,c,d] = 1, 2; & [x,z,b,d] = 1, 2; & [x,t,b,c] = 1, 2; \\ [y,z,a,d] = 1, 2; & [y,t,a,c] = 1, 2; & \end{array}$$

if and only if III and V hold and if every odd prime factor p_{ab} of $[a, b]$ for which (2) holds also satisfies (3), together with the five conditions (7).

It is clear that we can proceed now with equation (1) as restricted by (10) and remove in turn the restrictions $[x, y, c, d] = 1, 2$, etc. Thus if we now allow

$$[x, y, c, d] = r > 2,$$

and put

$$x = rx'', y = ry'', z = z'', t = t'',$$
$$a'' = ar, b'' = br, c'' = c/r, d'' = d/r,$$

then

$$a''x''^2 + b''y''^2 + c''z''^2 + d''t''^2 = 0.$$

If this has solutions subject to the five restrictions typified by (10), that is $[x'', y'', c'', d''] = 1, 2$, etc., the first condition in (7) becomes $-abr^2R(c/r, d/r)$ while the other four remain unchanged. Hence r must include among its factors the odd prime factors p'_{cd}, of $[c, d]$, if any, for which

$$\left(\frac{-ab}{p'_{cd}}\right) = -1.$$

To the condition below (10), must be added the one arising since $[a'', b''] = r[a, b]$, that if

$$\left(\frac{-\dfrac{cd}{r^2}}{p'_{cd}}\right) = -1 \tag{11}$$

then also

$$\left(\frac{-abr^2/p'^2_{cd}}{p_{cd}}\right) = 1; \tag{12}$$

that is,

$$\left(\frac{-ab}{p'_{cd}}\right) = 1. \tag{13}$$

But then there is no need to take p_{cd} as a factor of r, and we must have

$$\left(\frac{-cd/p'^2_{cd}}{p'_{cd}}\right) = 1. \tag{14}$$

Hence (1) has solutions subject to the last four restrictions in (10) if and only if III and V hold together with the last four conditions in (7), and also that (3) holds when (2) holds; and (14) holds when (13) holds. We thus arrive at the condition IV when (1) is not restricted by the six conditions typified by (4).

It may be remarked that condition IV could be deduced more simply by noting the fact pointed out in my paper that my method showed that necessary and sufficient conditions for the solvability in integers not all zero of $f(x, y, z, t) = 0$, where f is an indefinite quaternary (or for that matter a ternary) quadratic form with integer coefficients and non-zero determinant, is that the congruence $f(x, y, z, t) \equiv 0 \pmod{p^n}$ should be solvable with $[x, y, z, t] \not\equiv 0$ mod p, for all primes $p \geqq 2$ and integers $n \geqq 0$, and that this requires a condition for only a finite number of values of p, n. Thus for (1) we need only take $p^n = 2^4, p_{ab}^2, p_{ac}^2, \cdots$. The condition V arises from $p^n = 2^4$, and the condition IV on taking $p^n = p_{ab}^2$ and applying the result that the congruence

$$Ax^2 + By^2 + Cz^2 \equiv 0 \pmod{p^n}$$

is possible for all odd primes p if $ABC \not\equiv 0 \pmod{p}$.

Archibald's numerical example is

$$110x^2 + 770y^2 - z^2 - t^2 = 0.$$

Here only the primes p_{ab} exist and $p_{ab} = 5, 11$, since

$$[110, 770] \equiv 0 \pmod{p_{ab}}.$$

For $p_{ab} = 11$,

$$\left(\frac{-cd}{p_{ab}}\right) = \left(\frac{-1}{11}\right) = -1,$$

but

$$\left(\frac{-ab/p_{ab}}{p_{ab}}\right) = \left(\frac{-700}{11}\right) = \left(\frac{-7}{11}\right) = 1.$$

For $p_{ab} = 5$,

$$\left(\frac{-cd}{p_{ab}}\right) = 1,$$

and no other condition arises. Hence IV is satisfied. Clearly V is satisfied since

$$\tfrac{1}{2}a \equiv -1 \pmod{8}, \quad \tfrac{1}{2}b \equiv 1 \pmod{8}, \quad c \equiv d \pmod{8}.$$

Hence the equation is solvable. Archibald gives the solution $x = 2, y = 1, z = 11, t = 33$.

THE UNIVERSITY, MANCHESTER, ENGLAND