CRITERIA FOR THE SOLUTION OF A CERTAIN QUADRATIC DIOPHANTINE EQUATION

BY R. G. ARCHIBALD

1. *Introduction.* The interesting diophantine equation,

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

in which a, b, c, d are integers, all different from zero, and x, y, z, u are the unknowns, has already been treated in the literature. It is, however, desirable to have a complete treatment and definite statement of criteria for solvability directly applicable to a given equation.

In 1884 A. Meyer* stated, though somewhat obscurely, necessary and sufficient conditions for the solvability of equation (1), but his proof, as well as P. Bachmann's† treatment, is restricted to the case in which a, b, c, d are all odd integers. In 1930 an account of this equation was given by L. E. Dickson;‡ but, as he points out himself, his work is incomplete in the case in which exactly two of the coefficients are even integers and $abcd/4 \equiv 5 \pmod 8$. Recently a paper§ by L. J. Mordell has appeared in which a complete and independent derivation of conditions for solvability is given. His conditions, however, are not always directly applicable to a given equation: more explicitly, his condition II may not be satisfied by a given equation and yet the equation may possess a solution. According to the scheme there presented, restrictions are placed on the values of the unknowns, and it may happen that a set of diophantine equations have to be tested to determine whether the given one is solvable or not. This is best illustrated by an example.

His method is not directly applicable to the equation

$$110x^2+770y^2-z^2-u^2=0,$$

which is solvable for $x=2$, $y=1$, $z=11$, $u=33$). We enquire,

* Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 29 (1884), pp. 209–222.

† *Zahlentheorie*, Part IV, *Die Arithmetik der Quadratischen Formen*, I, pp. 259–266.

‡ *Studies in the Theory of Numbers*, pp. 70–76.

§ Journal für Mathematik, vol. 164 (1931), pp. 40–49.

without loss of generality, whether this equation has a solution such that x, y, z, u have no common factor.

Since Mordell's condition II is not satisfied, we may gather that either the equation has no (non-trivial) solution or both z and u have either the factor 5 or the factor 11, or both. If z and u both have the factor 5, we are led to the equation $22x^2+154y^2-5z_1^2-5u_1^2=0$, for which again condition II is not satisfied. (By our assumption that x, y, z, u have no common factor we know that x and y are not divisible by 5.)

If the equation just mentioned has a solution, both z_1 and u_1 must have the factor 11; consequently we are led to the equation $2x^2+14y^2-55z_2^2-55u_2^2=0$. Here, again, condition II is not satisfied. Thus, the original equation either possesses no solution, or z and u do not have the factor 5.

Next, we may suppose that both z and u have the factor 11 and obtain the equation $10x^2+70y^2-11z_0^2-11u_0^2=0$, for which the condition II is satisfied. Hence the original equation, as tested by Mordell's criterion, has a solution.

It is our object here to obtain, as a special case and application of important considerations* of H. Hasse, necessary and sufficient conditions, which can be directly applied to a given equation, for the solvability in integers, not all zero, of equation (1) with integral (rational) coefficients a, b, c, d, all different from zero.

2. *Necessary and Sufficient Conditions for Solvability. Preliminary Conditions.* Without loss of generality we may assume that†

(i) Each of a, b, c, d is without a squared factor >1.

(ii) No three of a, b, c, d have a common factor >1.

Necessary and sufficient conditions‡ for the solvability of equa-

---

* *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, Journal für Mathematik, vol. 152 (1923), pp. 129–148. This paper was brought to the writer's attention by Hasse.

† See, for example, Meyer, loc. cit., pp. 209–210, or Dickson, loc. cit., pp. 68–71.

‡ We employ the notation used by Meyer; namely,

$$a = (a, b)(a, c)(a, d)\alpha, \qquad b = (a, b)(b, c)(b, d)\beta,$$
$$c = (a, c)(b, c)(c, d)\gamma, \qquad d = (a, d)(b, d)(c, d)\delta,$$

where (f, g) denotes the greatest common divisor of f and g.

tion (1), with a, b, c, d non-zero integers, satisfying the above preliminary conditions are the following:

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

II (i) $-(a, c)(a, d)(b, c)(b, d)\gamma\delta$ is a quadratic residue of every odd prime p dividing either (a, b) or (c, d) such that at the same time Legendre's symbol $(\alpha\beta\gamma\delta/p) = +1$;

(ii) $-(a, b)(a, d)(b, c)(c, d)\beta\delta$ is a quadratic residue of every odd prime p dividing either (a, c) or (b, d) for which $(\alpha\beta\gamma\delta/p) = +1$;

(iii) $-(a, b)(a, c)(b, d)(c, d)\beta\gamma$ is a quadratic residue of every odd prime p dividing either (a, d) or (b, c) for which $(\alpha\beta\gamma\delta/p) = +1$.

III Either

(i) $abcd \equiv 2, 3, 5, 6, 7 \pmod 8$;

or

(ii) $abcd \equiv 1$ and $a+b+c+d \equiv 0 \pmod 8$;

or

(iii) $abcd \equiv 4 \pmod 8$, and, if a and b are even and c and d odd, either $abcd/4 \equiv 3, 5, 7 \pmod 8$, or $abcd/4 \equiv 1 \pmod 8$ and

$$\frac{a}{2} + \frac{b}{2} + c + d \equiv \frac{(cd)^2 - 1}{2} \pmod 8.$$

3. *Application of Hasse's Work.* By the *discriminant* of a quadratic form we mean the determinant $D = |a_{ij}|$ of its set of coefficients. We shall consider only forms which have non-zero discriminant. By the *rational kernel* of a number m, different from zero, in the field $K(1)$ of all rational numbers, we mean the uniquely determined reduced number obtained by removing all rational squared factors from m. Similarly, the *p-adic kernel* of a number $m(\neq 0)$ in the field* $K(p)$ of p-adic numbers is the reduced number obtained by removing from m all squared factors occurring in the field $K(p)$. The rational kernels are integral positive or negative numbers without squared factors. Rationally equivalent forms have the same rational kernel for their discriminants, and p-adically equivalent forms have the same p-adic kernel for their discriminants. The p-adic kernels, say d_p, of the discriminant of one and the same form in the field

* See K. Hensel, *Zahlentheorie*, 1913, Chapter 6.

$K(1)$ are at the same time the p-adic kernels of the rational kernel, d, of the discriminant. We speak of the *invariants* d and d_p.

Consider a ternary quadratic form f. We define for a form equivalent, in the algebraic sense, to f and without cross-product terms (which always exists), let us say $f_0 = by^2+cz^2+du^2$, the quantity $\check{c}_p$ as the generalized Hilbert* norm residue symbol

$$\check{c}_p = \check{c}_p(f_0) = \left(\frac{-bc, -bd}{p}\right).$$

This quantity $c_p(f_0)$ is an invariant with respect to p-adic transformations and can be denoted by $\check{c}_p(f)$. We consider now Hasse's theorem† that a quaternary quadratic form (with rational coefficients) of invariant d represents zero rationally if and only if in any form whatever of the special type $ax^2+\phi(y, z, u)$ rationally equivalent to it, $\check{c}_p(\phi) = +1$ whenever the generalized symbol‡ of Legendre (d/p) has the value $+1$, this holding true for every finite prime p and also§ for $p = p_\infty$. For our purpose let $f = ax^2+by^2+cz^2+du^2$ and $\phi = by^2+cz^2+du^2$, whence

$$\check{c}_p(\phi) = \left(\frac{-bc, -bd}{p}\right).$$

In the form $ax^2+by^2+cz^2+du^2$, with integral rational coefficients, let us assume $abcd \neq 0$ and the preliminary conditions (i) and (ii) to hold. Hence, the invariant d is $\alpha\beta\gamma\delta$.

Our equation (1), *then, with* $abcd \neq 0$ *and with the preliminary conditions* (i) *and* (ii) *satisfied, is solvable in rational numbers* (*or, what is equivalent, in integers*) *if, and only if, for every finite prime* p *and for* $p = p_\infty$, *the Hilbert symbol*

$$\left(\frac{-bc, -bd}{p}\right) = +1 \tag{2}$$

when the generalized Legendre symbol $((\alpha\beta\gamma\delta)/p) = +1$.

Now we have

$$-bc = -(b, c)^2(a, b)(b, d)(a, c)(c, d)\beta\gamma,$$

$$-bd = -(b, d)^2(a, b)(b, c)(a, d)(c, d)\beta\delta.$$

* Hensel, loc. cit., Chapter 12, §§4–6.

† Hasse, loc. cit., p. 143.

‡ Hasse, loc. cit., p. 134.

§ See Hensel, loc. cit., Chapter 12, §1.

In the first place, consider the field $K(p_\infty)$, that is, the case $p=p_\infty$. Now $(\alpha\beta\gamma\delta/p_\infty)=+1$ when and only when $\alpha\beta\gamma\delta>0$. But when $p=p_\infty$, $((-bc, -bd)/p_\infty)=+1$ if at least one of $-bc$, $-bd$ is positive. Hence, whenever $\alpha\beta\gamma\delta>0$, either β and γ must be of opposite sign or β and δ are of opposite sign; and whenever $\alpha\beta\gamma\delta<0$, the condition (2) is obviously satisfied. Hence, in this case the condition (2) is equivalent to saying that not all of a, b, c, d are of the same sign (our condition I).

Secondly, let p be an *odd* prime. Now, since a squared factor cannot occur in $\alpha\beta\gamma\delta$, and since, if p itself divided $\alpha\beta\gamma\delta$, then $(\alpha\beta\gamma\delta/p)\neq+1$, we need only consider primes not dividing $\alpha\beta\gamma\delta$; that is, only odd primes not dividing $abcd$, and those odd primes dividing exactly two of a, b, c, d.

(i) Let p be an odd prime dividing either (a, b) or (c, d). Then*

$$\left(\frac{-bc, -bd}{p}\right)=\left(\frac{-(b,d)(a,c)(b,c)(a,d)\gamma\delta}{p}\right).$$

It follows, therefore, that in this case our condition states that $-(b, d)(a, c)(b, c)(a, d)\gamma\delta$ is a quadratic residue of every odd prime factor p of either (a, b) or (c, d) such that the relation $(\alpha\beta\gamma\delta/p)=+1$ holds (our condition II (i)).

(ii) Let p be an odd prime dividing either (a, c) or (b, d). Then

$$\left(\frac{-bc, -bd}{p}\right)=\left(\frac{-(a,b)(b,c)(a,d)(c,d)\beta\delta}{p}\right).$$

It follows, therefore, that in this case, our condition states that $-(a, b)(b, c)(a, d)(c, d)\beta\delta$ is a quadratic residue of every odd prime factor p of either (a, c) or (b, d) such that the relation $(\alpha\beta\gamma\delta/p)=+1$ holds (our condition II (ii)).

(iii) Let p be an odd prime dividing either (a, d) or (b, c). Then

$$\left(\frac{-bc, -bd}{p}\right)=\left(\frac{-(a,b)(b,d)(a,c)(c,d)\beta\gamma}{p}\right).$$

Hence our condition states that $-(a, b)(b, d)(a, c)(c, d)\beta\gamma$ is a quadratic residue of every odd prime factor p of either (a, d) or (b, c) such that $(\alpha\beta\gamma\delta/p)=+1$ (our condition II (iii)).

* Hensel, loc. cit., p. 317.

Thirdly, let p be an odd prime dividing *none* of a, b, c, d. Then $((-bc, -bd)/p)$ is automatically equal to $+1$.

Fourthly, let p be the prime $p=2$.

(i) Let 2 be a factor of one only of a, b, c, d. The condition is vacuously satisfied since $(\alpha\beta\gamma\delta/2) \neq +1$. Hence, if $abcd \equiv 2$ or 6 (mod 8), no further condition is required (part of condition III (i)).

(ii) Let 2 be a factor of precisely two of a, b, c, d. Without loss of generality, let us suppose that a and b are even and that c and d are odd (that is, $(a/2)(b/2)cd \equiv 1, 3, 5, 7 \pmod 8$). We desire to have $((-bc, -bd)/2) = +1$ whenever $(\alpha\beta\gamma\delta/2) = +1$. But $(\alpha\beta\gamma\delta/2) = +1$ if and only if $\alpha\beta\gamma\delta \equiv 1 \pmod 8$; that is, if and only if $(a/2)(b/2)cd \equiv 1 \pmod 8$. Hence, employing the usual methods of evaluating the symbol $((f, g)/2)$, we desire

$$\frac{\left\{-(b,c)^2\frac{(a,b)}{2}(b,d)(a,c)(c,d)\beta\gamma\right\}^2-1}{8}$$

$$+\frac{\left\{-(b,d)^2\frac{(a,b)}{2}(b,c)(a,d)(c,d)\beta\delta\right\}^2-1}{8}$$

$$+\frac{\left\{-(b,c)^2\frac{(a,b)}{2}(b,d)(a,c)(c,d)\beta\gamma-1\right\}}{2}$$

$$\cdot\frac{\left\{-(b,d)^2\frac{(a,b)}{2}(b,c)(a,d)(c,d)\beta\delta-1\right\}}{2}$$

to be *even* when $\alpha\beta\gamma\delta \equiv 1 \pmod 8$. Now, since for two *odd* integers A and B,

$$\frac{A^2-1}{2}+\frac{B^2-1}{2} \equiv \frac{(AB)^2-1}{2} \pmod{32},$$

we have finally, remembering that the square of an odd number is of the form $8M+1$ and that $(a/2)(b/2)cd \equiv 1 \pmod 8$ (whence $(b/2)c+1 \equiv (a/2)d+d^2 \pmod 8$),

$$d^2 \cdot \frac{(cd)^2 - 1}{2} + cd + \frac{b}{2} d + \frac{a}{2} d + d^2 \equiv 0 \pmod 8$$

when $\alpha\beta\gamma\delta \equiv 1 \pmod 8$, that is, when $(a/2)(b/2)cd \equiv 1 \pmod 8$. We note that

$$-d \cdot \frac{(cd)^2 - 1}{2} \equiv \frac{(cd)^2 - 1}{2} \pmod 8,$$

and obtain on simplification the condition that

$$\frac{a}{2} + \frac{b}{2} + c + d \equiv \frac{(cd)^2 - 1}{2} \pmod 8$$

when $(a/2)(b/2)cd \equiv 1 \pmod 8$. If $(a/2)(b/2)cd \equiv 3, 5, 7 \pmod 8$, that is, $\alpha\beta\gamma\delta \equiv 3, 5, 7 \pmod 8$, we saw that $(\alpha\beta\gamma\delta/2) \neq +1$. Hence we have our condition III (iii).

(iii) Finally, let each of a, b, c, d be odd. Then

$$\left(\frac{-bc, -bd}{2}\right) = (-1)^s,$$

where

$$s = \frac{-(b, c)^2(a, b)(b, d)(a, c)(c, d)\beta\gamma - 1}{2} \cdot \frac{-(b, d)^2(a, b)(b, c)(a, d)(c, d)\beta\delta - 1}{2}.$$

Hence we desire s to be even whenever $(\alpha\beta\gamma\delta/2) = +1$. But $(\alpha\beta\gamma\delta/2) = +1$ when and only when $abcd \equiv 1 \pmod 8$. The condition is therefore vacuously satisfied when $abcd \equiv 3, 5, 7 \pmod 8$ (part of condition III (i)). Thus, when $abcd \equiv 1 \pmod 8$, we desire

$$\{(b, c)^2(a, b)(b, d)(a, c)(c, d)\beta\gamma + 1\} \cdot \{(b, d)^2(a, b)(b, c)(a, d)(c, d)\ \beta\delta + 1\} \equiv 0 \pmod 8.$$

That is, $cd+bc+bd+abcd \equiv 0 \pmod 8$; or, in other words, since $abcd \equiv 1 \pmod 8$, $a+b+c+d \equiv 0 \pmod 8$. This is our condition III (ii).

All possible values of p have been considered. The set of conditions I, II, and III is therefore necessary and sufficient for the solvability of equation (1) in integers.

THE UNIVERSITY OF GÖTTINGEN