INTEGERS OF QUADRATIC FIELDS AS SUMS OF SQUARES

BY

IVAN NIVEN

1. **Introduction.** Lagrange proved that every positive rational integer is a sum of four squares of rational integers. Our principal result is that in an imaginary quadratic field every integer of the form

$$a + 2b\theta, \qquad \theta^2 = -m, \tag{1}$$

m being a positive square-free rational integer, is expressible as a sum of three squares of integers of the field. Gaussian integers are treated in §3, integers of the general imaginary quadratic field in §4; necessary and sufficient conditions for two-square sums are given in each case. Section 6 treats real quadratic integers, and §7 interprets some of the results in the theory of Diophantine equations.

It will be recalled that the coefficients of quadratic integers are not always rational integers. Specifically, if the field is an extension of the rational number field by θ in equation (1), and if $m \equiv 3 \pmod 4$, the integers of the field are given by

$$\frac{a}{2} + \frac{b}{2}\theta \tag{2}$$

where a and b are rational integers, both odd or both even. This introduces a special problem, which is dealt with for imaginary fields in §5. Roman letters represent rational integers throughout.

2. **Mordell's theorem.** In this section we prove a theorem which was stated by L. J. Mordell [1], and upon which most of our study is based. Mordell's proof contains an omission of such import that a complete proof is offered here.

THEOREM 1. *If $f(x, y) = ax^2 + 2hxy + by^2$ is a positive binary quadratic form with integral coefficients, necessary and sufficient conditions that f be expressible as a sum of the squares of two linear forms with integral coefficients,*

$$f(x, y) = (a_1x + b_1y)^2 + (a_2x + b_2y)^2, \tag{3}$$

are that $\Delta = ab - h^2$ be a perfect square and that $d = (a, h, b)$ have no prime factor of the form $4n+3$ to an odd power.

To prove that these conditions are necessary, we take equation (3) as our

Presented to the Society, December 29, 1939; received by the editors December 12, 1939.

hypothesis and obtain

$$a = a_1^2 + a_2^2, \qquad h = a_1b_1 + a_2b_2, \qquad b = b_1^2 + b_2^2. \tag{4}$$

It follows that

$$\Delta = ab - h^2 = (a_1b_2 - a_2b_1)^2.$$

There is no loss of generality in assuming d to be square-free. Let p be a prime of the form $4n+3$ dividing d, that is, dividing each of a, b, and h. Using the theory of the decomposition of an integer into the sum of two squares, we note that the first and last equations of (4) imply that p is a divisor of a_1, a_2, b_1, and b_2. Hence p^2 divides a, b, h, and therefore d, which contradicts our hypothesis that d is square-free.

Conversely, let us assume that

$$ab - h^2 = \Delta_0^2, \tag{5}$$

and that d is divisible by no prime of the form $4n+3$ to an odd power, or, what is the same thing, that d is expressible as a sum of two squares of integers. Because of the identity

$$(U^2 + V^2)(u^2 + v^2) = (Uu + Vv)^2 + (Uv - Vu)^2,$$

and because we are attempting to prove that an equation of the form (3) can be set up, we may take

$$d = (a, h, b) = 1. \tag{6}$$

The gap in Mordell's argument occurs at this point. He states (page 5), "Now

$$ab - h^2 = \Delta_0^2, \qquad h^2 \equiv -\Delta_0^2 \pmod{a},$$

and the solution of the congruence for h gives

$$h \equiv -\frac{\Delta_0 a_1}{a_2} \pmod{a}$$

for an appropriate resolution of a as a sum of two integral squares, say,

$$a = a_1^2 + a_2^2."$$

We shall show that a is expressible in the latter form, with

$$a_2h \equiv -\Delta_0 a_1 \pmod{a}. \tag{7}$$

Let p be a prime of the form $4n+3$ which divides ab. Equation (5) shows that ab is a sum of two squares; hence the highest power of p dividing ab is an even one, say $p^{2\alpha}$; it follows that

$$p^\alpha \mid h, \quad p^\alpha \mid \Delta_0.$$

Equation (6) implies that $p^{2\alpha}$ divides a or b, but not both. Treating every prime factor of ab which is congruent to 3 modulo 4 in this fashion, we see that we may write

$$a = P^2A, \qquad b = Q^2B, \qquad h = PQH, \qquad \Delta_0 = PQ\Delta_1, \tag{8}$$

wherein P and Q are odd, prime to each other, and contain only prime factors of the form $4n+3$; also A and B contain no such prime factors. Equation (5) shows that

$$AB = H^2 + \Delta_1^2 = (H + \Delta_1 i)(H - \Delta_1 i). \tag{9}$$

Now each prime factor of A is expressible as a sum of two squares in one and only one way, so that we have

$$A = \prod_{j=1}^{n} (x_j^2 + y_j^2) = \prod_{j=1}^{n} (x_j + y_j i)(x_j - y_j i). \tag{10}$$

Each of the complex factors in the latter product is a prime in the field $R(i)$, the rational number field extended by i. The unique factorization law holds in $R(i)$ so that x_j+y_ji divides one of the two factors

$$H + \Delta_1 i, \qquad H - \Delta_1 i$$

of AB, and x_j-y_ji divides the other. Combining the terms of the product (10) according to this distinction, we may write

$$A = (A_1 - A_2 i)(A_1 + A_2 i) = A_1^2 + A_2^2, \tag{11}$$

where

$$(A_1 - A_2 i) \mid (H + \Delta_1 i), \qquad (A_1 + A_2 i) \mid (H - \Delta_1 i).$$

Similarly we have

$$B = B_1^2 + B_2^2 = (B_1 - B_2 i)(B_1 + B_2 i), \tag{12}$$

these factors dividing $H+\Delta_1 i$ and $H-\Delta_1 i$ respectively. Equations (9), (11), and (12) imply

$$H + \Delta_1 i = (A_1 - A_2 i)(B_1 - B_2 i),$$

whence we obtain

$$H = A_1B_1 - A_2B_2, \qquad \Delta_1 = -A_1B_2 - A_2B_1. \tag{13}$$

If we write

$$a_1 = PA_1, \qquad a_2 = PA_2, \qquad b_1 = QB_1, \qquad b_2 = QB_2,$$

then equations (8), (11), (12), and (13) imply

$$a = a_1^2 + a_2^2, \quad b = b_1^2 + b_2^2, \quad h = a_1b_1 - a_2b_2, \quad \Delta_0 = -a_1b_2 - a_2b_1. \tag{14}$$

It follows that

$$a_2h = a_2a_1b_1 - a_2^2b_2,$$
$$a_2h \equiv a_2a_1b_1 + a_1^2b_2 \pmod{a},$$

and

$$a_2h \equiv -a_1\Delta_0 \pmod{a},$$

which we set out to prove. In fact, equations (14) imply

$$\frac{a_2h + a_1\Delta_0}{a} = -b_2, \qquad \frac{a_1h - a_2\Delta_0}{a} = b_1, \tag{15}$$

and it is easily verified that

$$ax^2 + 2hxy + by^2 = (a_1x + b_1y)^2 + (a_2x - b_2y)^2.$$

3. **Gaussian integers.** Let us consider $a+2bi$, where a and b are rational integers. We have, for an arbitrary integer t,

$$a + 2bi = (a + t) + 2bi + ti^2$$

which may thus be considered as a quadratic form in 1 and i. Mordell's theorem is applicable; first we wish to show that there exists a rational integral value of t such that $t(a+t)-b^2$ is a perfect square.

First let a be even, $a=2A$. We wish to obtain integral t and x to satisfy

$$t(2A + t) - b^2 = x^2,$$

which may be written in the form

$$(t + A)^2 - x^2 = A^2 + b^2. \tag{16}$$

This equation has no solutions if both A and b are odd, but is solvable otherwise.

In case either A or b is odd, we write the solution

$$t + A + x = A^2 + b^2, \qquad t + A - x = 1,$$

so that

$$t = \frac{(A - 1)^2 + b^2}{2}.$$

In our application of Theorem 1, we have (in the case considered) satisfied the condition that the negative of the discriminant of the form be a square.

We now consider the nature of d, the greatest common divisor of t, b, and $a+t$. The above equations show that

$$d = \left(b, \frac{(A-1)^2+b^2}{2}, \frac{(A+1)^2+b^2}{2}\right).$$

Let p be any odd prime dividing d. It is an immediate consequence of the above equation that p divides b, $A-1$, and $A+1$. Hence $p=1$, and d is not divisible by any odd prime.

In case both A and b are even, we write $A=2A_1$, $b=2b_1$, and equation (16) has the solutions

$$t + 2A_1 + x = 2(A_1^2 + b_1^2), \qquad t + 2A_1 - x = 2,$$

so that

$$t = (A_1 - 1)^2 + b_1^2.$$

The value of d is now given by the equation

$$d = (b, (A_1 - 1)^2 + b_1^2, (A_1 + 1)^2 + b_1^2).$$

The argument of the last paragraph applies again to show that d is divisible by no odd prime. This completes the discussion when a is even.

In case a is odd, $a=2A+1$, equation (16) is replaced by

$$(2t + a)^2 - 4x^2 = a^2 + 4b^2. \tag{17}$$

This equation always has rational integral solutions t and x. For if we write

$$2t + a + 2x = a^2 + 4b^2, \qquad 2t + a - 2x = 1,$$

the solution is

$$t = A^2 + b^2.$$

Again we see that d is divisible by no odd prime, because

$$d = (b, A^2 + b^2, (A + 1)^2 + b^2).$$

Recalling the remark after equation (16), we have shown that $a+2bi$ is expressible as a quadratic form in 1 and i satisfying the conditions of Theorem 1 provided that not both $a/2$ and b are integral and odd. Hence if these conditions on a and b are satisfied, the integer $a+2bi$ is expressible as a sum of two squares of Gaussian integers.

Conversely, suppose that the Gaussian integer $a+2bi$ is a sum of two squares,

$$a + 2bi = (c + di)^2 + (e + fi)^2.$$

Setting $t=d^2+f^2$, we have the result

$$(a+t)x^2+2bxy+ty^2=(cx+dy)^2+(ex+fy)^2.$$

Theorem 1 shows that $t(a+t)-b^2$ must be the square of an integer, and the conditions for equations (16) or (17) must be fulfilled for a even or odd, respectively. But equation (16) cannot be satisfied if $a/2$ and b are odd integers. Hence the Gaussian integer $a+2bi$ is not expressible as a sum of two squares if $a/2$ and b are odd rational integers. We have proven the first statement of the following theorem.

THEOREM 2. *A Gaussian integer of the form $a+2bi$ is expressible as a sum of two squares of Gaussian integers if and only if not both $a/2$ and b are odd integers. Every Gaussian integer of the form $a+2bi$ is expressible as a sum of three squares. A Gaussian integer is expressible as a sum of squares of Gaussian integers if and only if its imaginary coordinate is even.*

The last remark is trivial. The second statement is a corollary of the first. For if $a/2$ and b are integral and odd, the integer $a-1+2bi$ is expressible as a sum of two squares, whence $a+2bi$ is a sum of three squares, one of which is unity.

4. **General imaginary quadratic fields.** We now consider integers of the form $\gamma=a+2b\theta$ where a and b are rational integers, and

$$\theta^2=-m, \tag{18}$$

m being an integer greater than unity with no square factors. We note that γ is expressible in infinitely many ways as a quadratic form in 1 and θ,

$$\gamma=(a+tm)+2b\theta+t\theta^2,$$

t being an arbitrary integer. If t can be selected so that this quadratic form is expressible as a sum of two squares of linear forms, then γ is a sum of two squares of integers of the field $R(\theta)$.

On the other hand, if $a+2b\theta$ is a sum of two squares,

$$a+2b\theta=(c+d\theta)^2+(e+f\theta)^2,$$

we set $t=d^2+f^2$ as before and obtain

$$(a+tm)x^2+2bxy+ty^2=(cx+dy)^2+(ex+fy)^2.$$

We have shown, therefore, that the integer γ is a sum of two squares of integers of $R(\theta)$ with rational integral coordinates if and only if the quadratic form $[a+tm, 2b, t]$ is expressible as a sum of two squares of linear forms by means of a suitable choice of the rational integer t. Hence Theorem 1 is applicable.

THEOREM 3. *The integer $a+2b\theta$ is expressible as the sum of the squares of*

two integers of the form $c+d\theta$, *if and only if there exists an integer* t *such that*

$$mt^2 + at - b^2$$

is a perfect square, and such that $(t, b, a+mt)$ *is not divisible by a prime of the form* $4n+3$ *to an odd power.*

We now consider the problem of expressing the integer $a+2b\theta$ as a sum of three squares. The equation

$$a + 2b\theta - (u + v\theta)^2 = (tm + a - u^2) + 2(b - uv)\theta + (t - v^2)\theta^2 \tag{19}$$

leads us to search for integral values of t, u, and v which will make

$$(t - v^2)(tm + a - u^2) - (b - uv)^2 \tag{20}$$

a perfect square. First we set the terms free from t equal to a square,

$$v^2(u^2 - a) - (b - uv)^2 = y^2,$$

so that

$$u = \frac{v^2a + b^2 + y^2}{2bv}. \tag{21}$$

To obtain an integer from this expression for u, we set $v=b$ and $y=2Yb$ or $y=(2Y+1)b$ according as a is odd or even; the integer Y is arbitrary.

The expression (20) is written

$$mt^2 + t(a - u^2 - mb^2) + y^2 = \left(y - \frac{pt}{q}\right)^2,$$

and a solution is

$$t = q(2py + aq - u^2q - mb^2q), \tag{22}$$

provided

$$p^2 - mq^2 = 1. \tag{23}$$

Note that pt/q is an integer.

We shall also need to account for the greatest common divisor of the coefficients of the quadratic form on the right side of equation (19),

$$(b - uv,\ a - u^2 + tm,\ t - v^2) = (b - ub,\ a - u^2 + tm,\ t - b^2). \tag{24}$$

LEMMA. *Let* $\pi_1, \pi_2, \cdots, \pi_r$ *be the primes of the form* $4n+3$ *which divide* b. *Then we can choose* y *in* (21) *so that*

$$u^2 \not\equiv a \pmod{\pi_j}, \qquad j = 1, 2, \cdots, r. \tag{25}$$

First consider a odd, $a=2A-1$. Then $y=2Yb$, and (21) becomes

$$u = A + 2Y^2.$$

In this case (25) becomes

$$(A + 2Y^2)^2 \not\equiv 2A - 1 \pmod{\pi_j}, \qquad j = 1, 2, \cdots, r. \tag{26}$$

When Y ranges over a complete residue system modulo π_j, Y^2 (and therefore $2Y^2+A$) takes on $\frac{1}{2}(\pi_j+1)$ incongruent values modulo π_j. From the theory of quadratic residues it follows that $(2Y^2+A)^2$ takes on at least $[\frac{1}{4}(\pi_j+1)]$ incongruent values modulo π_j, where $[x]$ has the usual number-theoretic meaning, namely, the greatest integer less than or equal to x. Since $[\frac{1}{4}(\pi_j+1)] \geqq 2$ for all primes greater than 5, it is possible to select a value s_j from the complete system of residues modulo π_j, so that (26) is satisfied for all primes greater than 5 provided

$$Y \equiv s_j \pmod{\pi_j} \qquad (j = 1, \cdots, r),\ \pi_j > 5. \tag{27}$$

Since 5 is not a prime of the form $4n+3$, we take $\pi_j = 3$ as the special case. In this case, choose $Y \equiv 0, 1, 2 \pmod 3$ when $A \equiv 0, 1, 2 \pmod 3$ respectively, and (25) is satisfied.

Thus an s_j can be found corresponding to each π_j in (27) including the case $\pi_j = 3$ if it happens to be present, so that values of Y satisfying (26) may be found by use of the Chinese remainder theorem. Hence the lemma is proven in case a is odd.

If $a = 2A$, we have $y = (2Y+1)b$; equations (21) and (25) become

$$u = A + 1 + 2Y^2 + 2Y,$$

and

$$(A + 1 + 2Y^2 + 2Y)^2 \not\equiv 2A \pmod{\pi_j}, \qquad j = 1, \cdots, r, \tag{28}$$

respectively. Again let Y range over a complete residue system modulo π_j; each of the quantities Y^2+Y and $2Y^2+2Y+A+1$ takes on $\frac{1}{2}(\pi_j+1)$ incongruent values modulo π_j. Thus the expression

$$(2Y^2 + 2Y + A + 1)^2$$

takes on at least $[\frac{1}{4}(\pi_j+1)]$ incongruent values modulo π_j. As in the earlier case, a relation of the type (27) is established. In case the prime under discussion is 3, equation (28) is satisfied by choosing $Y \equiv 0, 1, 2 \pmod 3$ when $A \equiv 0, 1, 2 \pmod 3$ respectively. The proof of the lemma is completed by use of the Chinese remainder theorem, as in the previous case.

Having thus chosen a suitable value of u, we note that q in (23) may be selected so that it is divisible by $b(u-1)$. For we may set

$$q = b(u - 1)Q \tag{29}$$

where Q is a solution of

$$p^2 - mb^2(u - 1)^2Q^2 = 1. \tag{30}$$

This is a Pell equation, and is known to have solutions p and Q because $mb^2(u-1)^2$ is not a square.

It is not difficult to show that the expression on the right side of equation (24) has no prime of the form $4n+3$ as a factor. For suppose that π is such a prime dividing $b-ub$. Equation (29) shows that π divides q, and consequently equation (22) implies that π divides t. First, if π divides b, the lemma states that π does not divide u^2-a, and hence $a-u^2+tm$ is prime to π. On the other hand, if π divides $u-1$ but not b, it is clear that π cannot divide the expression $t-b^2$ in equation (24).

We have satisfied the conditions of Theorem 1, and equation (19) may therefore be interpreted as follows:

THEOREM 4. *Every integer of the form $a+2b\theta$ of the quadratic field $R(\theta)$ defined by equation* (18) *is expressible as a sum of three squares of integers of the field.*

5. **A special case.** We now examine more thoroughly the fields $R(\theta)$ where the integer m of equation (19) is of the form $4n+3$.

THEOREM 5. *In case $m\equiv 3 \pmod 4$, the integer $a+b\theta$, with b an odd rational integer, is expressible as a sum of two squares of integers of the field if and only if $4a+4b\theta$ is expressible as a sum of two squares of integers of the type $c+d\theta$ (see Theorem* 3). *Also, the integer $\frac{1}{2}a+\frac{1}{2}b\theta$, with a and b odd rational integers, is expressible as a sum of two squares of integers of the field if and only if $2a+2b\theta$ is expressible as a sum of two squares of integers of the type $c+d\theta$.*

It is obvious that each of these conditions is necessary for the proposed representation. To show that the condition expressed in the first statement is sufficient, we assume that $4a+4b\theta$ is a sum of two squares,

$$4a + 4b\theta = (x_1 + y_1\theta)^2 + (x_2 + y_2\theta)^2. \tag{31}$$

This implies the congruence

$$0 \equiv x_1^2 + x_2^2 - my_1^2 - my_2^2 \pmod 4,$$

or

$$0 \equiv x_1^2 + x_2^2 + y_1^2 + y_2^2 \pmod 4.$$

Hence every one of x_1, x_2, y_1 and y_2 is even, or every one is odd. Equation (31) can be divided by 4 to give the desired result.

We now turn to the second statement of the theorem and assume that

$$2a + 2b\theta = (x_1 + y_1\theta)^2 + (x_2 + y_2\theta)^2. \tag{32}$$

Since a and b are odd, we obtain the congruences

$$2 \equiv x_1^2 + x_2^2 + y_1^2 + y_2^2 \pmod 4, \quad 1 \equiv x_1y_1 + x_2y_2 \pmod 2.$$

These imply that x_1 and y_1 are both even or both odd, and an analogous result for x_2 and y_2. The equation (32) can be divided by 4 to give the desired result, and we have proven the theorem.

THEOREM 6. *In case $m \equiv 3 \pmod 4$, every integer of the field $R(\theta)$ is expressible as a sum of three squares of integers of the field.*

Because of Theorem 4 we need consider only integers of the types

$$a + b\theta, \qquad b \equiv 1 \pmod 2, \tag{33}$$

and

$$\frac{a}{2} + \frac{b}{2}\theta, \qquad a \equiv b \equiv 1 \pmod 2. \tag{34}$$

By Theorem 4 we have

$$4a + 4b\theta = \sum_{j=1}^{3} (x_j + y_j\theta)^2, \tag{35}$$

from which we obtain the congruences

$$0 \equiv x_1^2 + x_2^2 + x_3^2 + y_1^2 + y_2^2 + y_3^2 \pmod 4,$$
$$0 \equiv x_1y_1 + x_2y_2 + x_3y_3 \pmod 2.$$

If there were a disparity between x_1 and y_1 with respect to 2, these congruences would imply

$$3 \equiv x_2^2 + x_3^2 + y_2^2 + y_3^2 \pmod 4,$$
$$0 \equiv x_2y_2 + x_3y_3 \pmod 2,$$

which have no solutions in integers. Hence x_1 and y_1 are both odd or both even, and an analogous argument holds for the pairs x_2, y_2 and x_3, y_3. Our theorem is proven for integers of types (33) by dividing equation (35) by 4.

Turning to integers of the type (34), we write the equation

$$2a + 2b\theta = \sum_{j=1}^{3} (x_j + y_j\theta)^2, \tag{36}$$

using Theorem 4 as our authority. This equation implies the congruences

$$2 \equiv x_1^2 + x_2^2 + x_3^2 + y_1^2 + y_2^2 + y_3^2 \pmod 4,$$
$$1 \equiv x_1y_1 + x_2y_2 + x_3y_3 \pmod 2.$$

If x_1 and y_1 are incongruent modulo 2, we would have

$$1 \equiv x_2^2 + x_3^2 + y_2^2 + y_3^2 \pmod 4, \qquad 1 \equiv x_2y_2 + x_3y_3 \pmod 2,$$

which are manifestly impossible in integers. Hence x_1 and y_1 are both even or both odd; a similar statement holds for the pairs x_2, y_2 and x_3, y_3. Dividing equation (36) by 4, we have completed the proof of the theorem.

6. **Real quadratic fields.** Let

$$f(x, y) = ax^2 + 2hxy + by^2$$

be a positive form with integral coefficients. Mordell [2] has shown that f is expressible as a sum of five squares of linear forms with integral coefficients; also he has shown that f is expressible as a sum of four squares of linear forms with integral coefficients if and only if $ab-h^2$ is a sum of three squares of integers, that is, if and only if $ab-h^2$ is not of the form $4^r(8s+7)$. In case the expression $ab-h^2$ equals zero, the form f is expressible as a sum of four squares of linear forms with integral coefficients.

Let us now consider the field $R(m^{1/2})$, where m is a square-free rational integer greater than unity. The integer $a+2bm^{1/2}$ can be written in the form

$$a + 2bm^{1/2} = (a - tm) + 2bm^{1/2} + t(m^{1/2})^2, \tag{37}$$

a quadratic form in 1 and $m^{1/2}$. If Mordell's theorems above are to apply, we must first inquire whether t can be chosen so that the right side of equation (37) is a *positive* form. The question is whether a positive value of t can be chosen so that

$$D = (a - tm)t - b^2 > 0. \tag{38}$$

If we define K by the equation

$$K = (a^2 - 4mb^2)^{1/2}, \tag{39}$$

it is seen that D vanishes when t has the values

$$\frac{a - K}{2m}, \quad \frac{a + K}{2m}.$$

Furthermore, if K is real, and if t lies between these values, then t and D are positive, and the right side of equation (37) is a positive form; hence the first Mordell theorem stated at the beginning of this section is applicable. On the other hand, if t equals one of the above values, being real, then D is zero, and we apply the last Mordell theorem stated.

THEOREM 7. *The integer $a+2bm^{1/2}$ is expressible as a sum of five squares of integers of the form $c+dm^{1/2}$ if and only if the quantity K defined by* (39) *is real and the closed interval*

$$\left(\frac{a - K}{2m}, \frac{a + K}{2m}\right) \tag{40}$$

contains a rational integer.

Since any integer contained in the interval (40) is of necessity positive, it is clear that these conditions are sufficient. Conversely, let us assume that there exist integral values x_j, y_j $(j=1, \cdots, 5)$ such that

$$a + 2bm^{1/2} = \sum_{j=1}^{5} (x_j + y_j m^{1/2})^2,$$

from which we obtain

$$a = \sum_{j=1}^{5} (x_j^2 + m y_j^2), \qquad b = \sum_{j=1}^{5} x_j y_j.$$

The equation

$$a - 2bm^{1/2} = \sum_{j=1}^{5} (x_j - y_j m^{1/2})^2$$

shows that $a^2 - 4mb^2$ is positive, and consequently K in (39) is real. Consider the function

$$D = -mt^2 + at - b^2,$$

t being looked upon as a continuous variable. Its graph is a parabola. Its zeros are the end-points of the interval (40). Furthermore, any value of t for which D is positive lies in the interval (40). When t is given the integral value $\sum_{j=1}^{5} y^2$; we obtain

$$D = \sum_{j=1}^{5} x_j^2 \sum_{j=1}^{5} y_j^2 - \left(\sum_{j=1}^{5} x_j y_j \right)^2.$$

By the elementary theory of inequalities, this is not negative. Hence we have exhibited an integral value satisfying the conditions of the theorem.

THEOREM 8. *The integer $a+2bm^{1/2}$ is expressible as a sum of four squares of integers of the form $c+dm^{1/2}$ if and only if K defined by* (39) *is real and the closed interval* (40) *contains a rational integer t so that the value of D in equation* (38) *is expressible as a sum of three squares of rational integers.*

This theorem needs no explanation, since it is an immediate extension of Theorem 7, obtained by the use of Mordell's work as outlined at the beginning of this section. It is also possible to state theorems analogous to the last theorem for the situations wherein we wish two-square and three-square sums; this would be done by use of Theorem 1 and other work [3] of Mordell.

7. **Consequences in the theory of Diophantine equations.** The first statement of Theorem 2 may be interpreted as follows:

THEOREM 9. *The Diophantine equations*

$$x^2 + y^2 - z^2 - w^2 = a, \qquad xz + yw = b,$$

are solvable simultaneously if and only if not both $\frac{1}{2}a$ *and* b *are integral and odd.*

The second statement of Theorem 2 together with Theorem 4 leads to the following result.

THEOREM 10. *If* a *and* b *are arbitrary integers, and if* m *is unity or an integer greater than unity which is not a square, then the equations*

$$x^2 + y^2 + z^2 - m(w^2 + u^2 + v^2) = a,$$
$$xw + yu + zv = b,$$

are solvable simultaneously in integers.

Theorem 4 was proven with m a square-free integer, but the proof is valid with the less restrictive hypothesis that m be no square. This hypothesis is needed to insure solutions for the Pell equation (30). Finally we rewrite Theorem 7.

THEOREM 11. *If* a *and* b *are arbitrary integers, and if* m *is any positive integer, then the equations*

$$\sum_{j=1}^{5} (x_j^2 + my_j^2) = a, \qquad \sum_{j=1}^{5} x_j y_j = b$$

have simultaneous solutions in integers if and only if the quantity K *defined by equation* (39) *is real and the closed interval* (40) *contains a rational integer.*

The restriction that m be square-free contained in Theorem 7 is abandoned here because it was not used in the proof. It was included in Theorem 7 merely because quadratic integers are defined in terms of a square-free rational integer.

REFERENCES

1. L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Mathematische Zeitschrift, vol. 35 (1932), pp. 1–15.

2. ———, *A new Waring's problem*, Quarterly Journal of Mathematics, vol. 1 (1930), pp. 276–288.

3. ———, *On binary quadratic forms*, Journal für die reine und angewandte Mathematik, vol. 167 (1932).

UNIVERSITY OF ILLINOIS,
URBANA, Ill.