ACTA ARITHMETICA
XII (1966)

The representation of numbers by some quaternary quadratic forms

by

L. J. MORDELL (Cambridge)

Let

$$(1)\qquad f = f(x, y, z, w) = Ax^2+By^2+Cy^2+Dw^2,$$

where A, B, C, D are integers. The question of the representation of integers $m > 0$ by such forms has received much attention [1]. When f is definite, results are given by the classical theory of quadratic forms. When f is indefinite, Siegel [2] has shown that m is representable by f if the congruence

$$(2)\qquad f \equiv m \pmod{p^r}$$

is solvable for all primes p and integers $r \geqslant 1$ with $(x, y, z, w, p) = 1$.

Many special results are known when f is definite. Some of these give the number of representations and are found in various ways, e.g. by the classical theory, the application of elliptic and modular functions, Liouville's method, and some miscellaneous methods.

Other methods prove the existence of solutions for given m, and then there is no loss of generality in supposing that m is now and hereafter square free. The classic instance is when $A=B=C=D=1$, and the proof is due to Lagrange. Other proofs of this case have been given by using the geometry of numbers. There is really no need to use this since its only object is to find an estimate for the least number represented by a quadratic form. An estimate, however, is given by arithmetic processes much more elementary, but the bound may not be so small. One can also use the precise estimate for the minimum but this requires more technique.

[1] See Dickson, *History of the Theory of Numbers*, Vol. III, Chapter 11.

[2] Siegel, *Indefinite quadratische Formen und Funktionen Theorie, I*, Math. Ann. 124 (1951), pp. 17-54. See also, G. L. Watson, *Integral quadratic forms*, 1960, p. 81.

Most of the special results for the existence of a representation of all m by (1) consider only the case when $A > 0$, $B > 0$, $C > 0$, $D > 0$ [3]. The method now presented gives results also when some of A, B, C, D are negative. Some such results are trivial.

Thus for

$$(3)\qquad x^2+y^2-z^2-w^2 = m,$$

if $m \not\equiv 2 \pmod 4$, it suffices to take $y = w = 0$, and if $m \equiv 2 \pmod 4$, it suffices to take $y = 1$, $w = 0$.

For

$$x^2+y^2-2z^2-2w^2 = m,$$

we write

$$(4)\qquad x^2+y^2-(z+w)^2-(z-w)^2 = m.$$

It suffices to show that solutions of (3) exist in which $z \not\equiv w+1 \pmod 2$. This cannot occur if $m \equiv 2 \pmod 4$. If $m \not\equiv 2 \pmod 4$, we need only take $y = w$ and $w \equiv z \pmod 2$.

We consider from now on the special forms given by

$$(5)\qquad f = f(x, y, z, w) = x^2+bcy^2+caz^2+abw^2.$$

These forms admit a composition process [4]. Thus if

$$f_1 = f(x_1, y_1, z_1, w_1) = x_1^2+bcy_1^2+abw_1^2+caz_1^2,$$

then

$$ff_1 = f(x_2, y_2, z_2, w_2),$$

where

$$\begin{aligned} x_2 &= xx_1-(bcyy_1+cazz_1+abww_1),\\ y_2 &= yx_1+y_1x+a(zw_1-z_1w),\\ z_2 &= zx_1+z_1x+b(wy_1-w_1y),\\ w_2 &= wx_1+w_1x+c(yz_1-y_1z). \end{aligned}$$

This shows at once that if f represents m and m_1, then f represents mm_1.

We prove now the

LEMMA. *There exist integers $(x, y, z, w) \neq (0, 0, 0, 0)$ such that*

$$(6)\qquad f(x, y, z, w) = Mm, \qquad |M| \leqslant \sqrt{2|abc|},$$

[3] In particular, Ramanujan has shown by the theory of the definite ternary quadratic form that this holds for only 55 sets of values for A, B, C, D; *Collected works* (1927), pp. 169-178.

[4] Bachmann, *Die Arithmetik der Quadratischen Formen, I* (1898), p. 13.

provided that the congruence

$$(7)\qquad cA^2+bB^2+a \equiv 0 \pmod m$$

is solvable.

It is well known that this is so if $(m, abc) = 1$, since $m \not\equiv 0 \pmod 4$. Put

$$(8)\qquad x = cAX+bBY+mZ, \quad y = BX-AY+mW, \quad z = X, \quad w = Y.$$

Then since from (6),

$$\begin{gathered} c^2A^2+bcB^2+ca \equiv 0 \pmod m,\\ b^2B^2+bcA^2+ab \equiv 0 \pmod m,\\ f(x, y, z, w) = Mm. \end{gathered}$$

A crude estimate $|M| < 4\sqrt{|abc|}$ arises by applying Minkowski's theorem on linear forms to (8) [5] of determinant m^2. Thus integers $(X, Y, Z, W) \neq (0, 0, 0, 0)$ exist such that

$$\sqrt[4]{|abc|}\,|x| < \sqrt{|abc|\,m}, \qquad \sqrt[4]{|abc|}\,|y| \leqslant \sqrt{|a|\,m},$$
$$\sqrt[4]{|abc|}\,|z| \leqslant \sqrt{|b|\,m}, \qquad \sqrt[4]{|abc|}\,|w| \leqslant \sqrt{|c|\,m}.$$

The estimate (6) follows from the known results of Korkine and Zolotareff with a slight extension to indefinite forms, that if D is the determinant of $f(x, y, z, w) = F(X, Y, Z, W)$ expressed as a quadratic form in X, Y, Z, W, then $f(x, y, z, w)$ represents a number with modulus $\leqslant \sqrt[4]{|4D|}$. In our case, $D = m^4a^2b^2c^2$.

We commence with the case $c = 1$ and so

$$(9)\qquad f = x^2+by^2+az^2+abw^2 = Mm, \qquad |M| \leqslant \sqrt{2|ab|},$$

and

$$(10)\qquad A^2+bB^2+a \equiv 0 \pmod m.$$

This is solvable if $(m, ab) = 1$, also if $b = 1$ since m is square free. The classical case is $a = b = 1$. Also $M = 1$.

If we had used the cruder estimate $M < 4$, then $M = 1, 2, 3$.

But $M = 2$ gives

$$x^2+y^2+z^2+w^2 = 2m.$$

Since either all x, y, z, w are even or only two are even, say x, y,

$$\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+w}{2}\right)^2+\left(\frac{z-w}{2}\right)^2 = m.$$

[5] Bachmann, *Die Arithmetik der quadratischen Formen*, 1923, p. 268.

If $M = 3$, we may suppose $x \equiv 0 \pmod{3}$, $y \equiv z \equiv w \equiv 1 \pmod{3}$. Then

$$\left(\frac{y+z+w}{3}\right)^2 + \left(\frac{x+y-z}{3}\right)^2 + \left(\frac{x+z-w}{3}\right)^2 + \left(\frac{x+w-y}{3}\right)^2 = m.$$

This could have been deduced by composition from

$$0^2+1^2+1^2+1^2 = 3.$$

The next cases $b = 1$, $a = \pm 2$ are easily reduced to the cases $b = 1$, $a = \pm 1$.

The cases $b = 1$, $a = \pm 3$, $|M| < \sqrt{6} = 0, 1, 2$. Clearly $M = 0$ is impossible.

Take $a = 3$. If $M = 2$,

$$x^2+y^2+3(z^2+w^2) = 2m.$$

If $x \equiv y \pmod{2}$, then $z \equiv w \pmod{2}$ and

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{z+w}{2}\right)^2 + 3\left(\frac{z-w}{2}\right)^2 = m,$$

i.e. the case $M = 1$.

If $x \equiv y+1 \pmod{2}$, then $z \equiv w+1 \pmod{2}$, so $1+3 \equiv 2m \pmod{4}$, i.e. $m \equiv 0 \pmod{2}$. Hence $M = 1$ if $m \equiv 1 \pmod{2}$. If $m \equiv 0 \pmod{2}$, $M = 1$ for $m/2$ and since 2 is representable, so is m.

Take next $a = -3$. Since $1^2+1^2-3\cdot 1^2 = -1$, we need only examine $M = 2$ and so

$$x^2+y^2-3z^2-3w^2 = 2m.$$

The argument above applies when $x \equiv y \pmod{2}$, $z \equiv w \pmod{2}$. We need only consider $x \equiv 1 \pmod{2}$, $y \equiv 0 \pmod{2}$, $z \equiv 1 \pmod{2}$, $w \equiv 0 \pmod{2}$.

Since $1^2-3\cdot 1^2 = -2$, we have

$$\left(\frac{x+3z}{2}\right)^2 - 3\left(\frac{x+z}{2}\right)^2 + \left(\frac{y+3w}{2}\right)^2 - 3\left(\frac{y+w}{2}\right)^2 = -m,$$

i.e. the case $M = -1$.

When $m \equiv 0 \pmod{3}$, the result holds for $a = \pm 3$, since we can take $x = y = 0 \pmod{3}$.

The case $b = 1$, $a = 5$ is of some interest. Here

$$x^2+y^2+5(z^2+w^2) = Mm, \quad M = 1, 2, 3, \quad (m, 5) = 1.$$

Clearly $M \neq 1$ for all m since 3 cannot be represented. It can be shown from the theory of the ternary quadratic that all integers > 3 are representable with $M = 1$. The present method shows that all integers > 0 are representable with $M = 2$. Thus if $M = 1$,

$$(x+y)^2+(x-y)^2+5(z+w)^2+5(z-w)^2 = 2m.$$

If $M = 3$, compound with $1^2+5\cdot 1^2 = 6$, then

$$\left(\frac{x+5z}{3}\right)^2 + 5\left(\frac{x-z}{3}\right)^2 + \left(\frac{y+5w}{3}\right)^2 + 5\left(\frac{y-w}{3}\right)^2 = 2m$$

gives an integral representation. For

$$x^2+y^2 \equiv z^2+w^2 \pmod{3},$$

and we can take $x \equiv y \equiv 1$, $z \equiv w \equiv 1 \pmod{3}$, and

$$x \equiv 0, \quad y \equiv 1, \quad z \equiv 0, \quad w \equiv 1 \pmod{3}.$$

If $m \equiv 0 \pmod{5}$, say $m = 5m_1$, then

$$x_1^2+y_1^2+z^2+w^2 = 2m_1.$$

and

$$(2x_1+y_1)^2+(x_1-2y_1)^2+5(z^2+w^2) = 10m_1.$$

Next $b = 1$, $a = -5$ and so

$$x^2+y^2-5(z^2+w^2) = m.$$

It is simpler here to proceed as follows suggested by Dr. Birch. Since $2^2-5\cdot 1^2 = -1$, multiplication gives

$$(2x-5z)^2-5(x-2z)^2-y^2+5w^2 = -m,$$

or

$$AB-5CD = -m,$$

where

$$A = 2x-5z+y, \quad B = 2x-5z-y, \quad C = x-2z+w, \quad D = x-2z-w.$$

For given A, B, C, D, we have integer values of x, y, z, w if $A \equiv B \pmod{2}$, $C \equiv D \pmod{2}$. Hence if $m \equiv 1 \pmod{2}$, it suffices to take $C \equiv D \equiv 0 \pmod{2}$, and if $m \equiv 0 \pmod{2}$, to take $C \equiv D \equiv 1 \pmod{2}$. When $m \equiv 0 \pmod{5}$ it suffices to take $x \equiv y \equiv 0 \pmod{5}$.

Next $b = 1$, $a = -7$. Clearly $M \neq 0$. Then $|M| = 1, 2, 3$. Since $3^2+2^2-7(1^2+1^2) = -1$, we need only take $M = 2, 3$. First,

$$x^2+y^2-7(z^2+w^2) = 2m.$$

The result for $x \equiv y \pmod 2$, $z \equiv w \pmod 2$ follows as for $a = 3$, and so we need only consider the case when $x \equiv 1$, $y \equiv 0$, $z \equiv 1$, $w \equiv 0$ all to mod 2. Since $3^2 - 7\cdot 1^2 = 2$, we have

$$\left(\frac{3x+7z}{2}\right)^2 - 7\left(\frac{x+3z}{2}\right)^2 + \left(\frac{3y+7w}{2}\right)^2 - 7\left(\frac{y+3w}{2}\right)^2 = m.$$

Take next

$$x^2+y^2-7(z^2+w^2) = 3m.$$

Hence $2^2-7\cdot 1^2 = -3$, and so

$$(2x+7z)^2-7(x+2z)^2+(2y+7w)^2-7(y+2w)^2 = -9m.$$

Now

$$x^2+y^2 \equiv z^2+w^2 \pmod 3.$$

Hence, all to mod 3, either $x^2+y^2 \equiv 1$, $z^2+w^2 \equiv 1$, and we can take $x \equiv 1$, $y \equiv 0$, $z \equiv 1$, $w \equiv 0$, or $x^2+y^2 \equiv 2$, $z^2+w^2 \equiv 2$, and we can take $x \equiv y \equiv z \equiv w \equiv 1$.

In all cases $2x+7y$, $x+2z$, $2y+7w$, $y+2w \equiv 0 \pmod 3$, and so we have a representation with $M = -1$ and so $M = 1$. The result also holds when $m \equiv 0 \pmod 7$.

Let us take $b = 1$, $a = -11$ for a final example of this type. Then

$$x^2+y^2-11(z^2+w^2) = Mm, \qquad |M| < \sqrt{22} = 2, 3, 4.$$

Since $3^2+1^2-11\cdot 1^2 = -1$, we need only take $M = 2, 3, 4$, since clearly $M \neq 0$.

Suppose first that $M = 2$. Then $x+y+z+w \equiv 0 \pmod 2$. If $x \equiv y$, $z \equiv w \pmod 2$, we have

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 - 11\left(\left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2\right) = m.$$

We may suppose then that $x \equiv 1$, $y \equiv 0$, $z \equiv 1$, $w \equiv 0 \pmod 2$. Since $3^2-11\cdot 1^2 = -2$, we have

$$\left(\frac{3x+11z}{2}\right)^2 - 11\left(\frac{x+3z}{2}\right)^2 + \left(\frac{3y+11w}{2}\right)^2 - 11\left(\frac{y+3w}{2}\right)^2 = -m,$$

that is, the case $M = -1$.

Suppose next that $M = 4$, and so $x \equiv y \equiv z \equiv w \pmod 2$. We need only consider odd x and so by the above, we are reduced to the case of $M = -2$, and then again to the case $M = 1$.

Suppose that next $M = 3$. Then we have to mod 3, either $x^2+y^2 \equiv 1$, $z^2+w^2 \equiv -1$ and it suffices to take $(x, y, z, w) \equiv (0, 1, -1, -1)$, or $x^2+y^2 \equiv -1$, $z^2+w^2 \equiv 1$ and it suffices to take $(x, y, z, w) = (1, 1, 1, 0)$.

Take $(x_1, y_1, z_1, w_1) = (0, 5, 1, 1)$, and then

$$x_2 = -5y+11z+11w, \qquad y_2 = 5x-11z+11w,$$
$$z_2 = x+5w-y, \qquad w_2 = x+y-5z.$$

In all cases $x_2 \equiv y_2 \equiv z_2 \equiv w_2 \equiv 0 \pmod 3$, and we have again the case $M = 1$. The result holds when $m \equiv 0 \pmod{11}$.

We now consider the cases $a = \pm 2$, $b = \pm 3$, $c = 1$. It is well known that the case $a = 2$, $b = 3$ is the same as $a = b = 1$.

Consider the equations

$$\text{(A)} \qquad x^2-3y^2-2z^2+6w^2 = Mm,$$
$$\text{(B)} \qquad x^2+3y^2-2z^2-6w^2 = Mm,$$
$$\text{(C)} \qquad x^2-3y^2+2z^2-6w^2 = Mm.$$

Hence $|M| = 0, 1, 2, 3$. Since each of the forms in (A), (B), (C) represents -1, we need only take $M = 2, 3$. We show that the equations (A) and (B) each imply the other. Multiply (A) by $1^2-2\cdot 1^2 = -1$. Then

$$(x+2z)^2-2(x+z)^2+3y^2-6w^2 = -Mm.$$

Since $x+2z = X$, $x+z = Z$ gives a 1-1 correspondence between integer sets x, z and X, Z we have (B) with M replaced by $-M$. Clearly $M \neq 0$ in (A), as is obvious from $x = 3X$, $z = 3Z$.

Take (A) with $M = 3$ and so since $x^2-2z^2 \equiv 0 \pmod 3$, we have $x = 3X$, $z = 3Z$, say, and then

$$3X^2-y^2-6Z^2+2w^2 = m,$$

i.e. again (A) with $M = -1$.

Take next $M = 2$. Then $x \equiv y \pmod 2$. If $x = 2X$, $y = 2Y$,

$$2X^2-6Y^2-z^2+3w^2 = m.$$

This is (A) with $M = -1$. Suppose then $x \equiv y \equiv 1 \pmod 2$. Apply composition with $1^2-3\cdot 1^2-2\cdot 1^2+6\cdot 1^2 = 2$. Then

$$x_2 = x+3y+2z-6w, \qquad y_2 = y+x-2(z-w),$$
$$z_2 = z+x-3(w-y), \qquad w_2 = w+x+y-z.$$

Hence if $w \equiv z \pmod 2$, $x_2 \equiv y_2 \equiv z_2 \equiv w_2 \equiv 0 \pmod 2$, and we have (A) with $M = 1$.

We may suppose now that $w \equiv z+1$, $x \equiv y \equiv 1 \pmod 2$. Then (A) gives

$$-2-2(w-1)^2+6w^2 \equiv 2m \pmod 4,$$

and so $m \equiv 0 \pmod 2$.

Hence (A) holds with $M = 1$ if m is odd. But if m is even, (A) holds for $m/2$ with $M = 1$. Since (A) represents 2, (A) also represents m. If $m \equiv 0 \pmod 3$, $x = 3X$, $z = 3Z$ and we have again (A).

Take finally (C) and multiply by $1^2 - 3\cdot 1^2 = -2$. Then

$$(x-3y)^2 - 3(x-y)^2 - 4z^2 + 12w^2 = -2m.$$

Write this as

$$AB - 3CD = -2m, \tag{11}$$

where

$$A = x-3y+2z, \quad B = x-3y-2z, \quad C = x-y+2w, \quad D = x-y-2w.$$

We require the condition that x, y, z, w be integers for given integers A, B, C, D. These are obviously,

$$A \equiv B \pmod 4), \quad C \equiv D \pmod 4;$$

and

$$A+B-C-D \equiv 0 \pmod 4, \quad \text{i.e.,} \quad A \equiv C \pmod 2,$$

since

$$x - 3y = \frac{A+B}{2}, \quad x - y = \frac{C+D}{2}.$$

Hence

$$A^2 - 3C^2 \equiv -2m \pmod 4.$$

If $m \equiv 1 \pmod 2$, we take $A \equiv C \equiv 1 \pmod 2$. Then we can satisfy formula (11) by taking $A \equiv B \equiv C \equiv D \equiv 1 \pmod 4$.

If $m \equiv 0 \pmod 2$, (C) holds for $m/2$ and also for 2 with $M = 1$, and so also for m.

A similar argument holds when $m \equiv 0 \pmod 3$.

There is no need to give further instances of the method.

ST. JOHNS COLLEGE,
CAMBRIDGE, ENGLAND

Reçu par la Rédaction le 17. 1. 1966

ACTA ARITHMETICA
XII (1966)

Uniform distribution of sequences in GF$[q, x]$*

by

JOHN H. HODGES (Boulder, Colorado)

1. Introduction and preliminaries. Let $\Phi = \mathrm{GF}[q, x]$, denote the ring of polynomials in an indeterminate x over an arbitrary finite field GF(q) of q elements. Throughout this paper italic capitals $A, B, M, H, \ldots$ will denote elements of Φ, except as indicated.

Let M be any element of Φ of degree $m > 0$. Then a complete residue system modulo M (in Φ) contains q^m elements. One such complete residue system consists of all elements of Φ of degree $< m$. (For this purpose, the zero polynomial may be regarded as having degree $< m$ for all $m > 0$.) Let $\theta = \{A_i\}$ be an infinite sequence of elements of Φ. For any $B \epsilon \Phi$ and any integer $n \geqslant 1$, define $\theta(n, B, M)$ as the number of terms among $A_1, \ldots, A_n$ such that $A_i \equiv B \pmod M$. Then following Niven ([5], § 1) we say that the sequence θ is *uniformly distributed modulo* M, abbreviated as u.d. (mod M), if and only if

$$\lim_{n\to\infty} \theta(n, B, M)/n = q^{-m} \quad (\text{all } B \epsilon \Phi). \tag{1.1}$$

Furthermore, we say that the sequence θ is *uniformly distributed*, abbreviated as u.d., if and only if it is u.d. (mod M) for every M of degree > 0 in Φ.

For certain questions of interest concerning sequences in Φ, a somewhat weaker condition than (1.1) must be used. Let $\theta = \{A_i\}$ be any infinite sequence of elements of Φ in which no element of Φ appears infinitely many times. For any $B \epsilon \Phi$, any integer $n \geqslant 1$ and any $M \epsilon \Phi$ of degree $m > 0$, let

$$\begin{cases} \theta(n) = \text{number of terms of } \theta \text{ such that } \deg A_i < n, \\ N(\theta, n, B, M) = \text{number of terms of } \theta \text{ such that } \deg A_i < n \\ \qquad\qquad \text{and } A_i \equiv B \pmod M. \end{cases} \tag{1.2}$$

* Supported by NSF Research Grant GP 2542 and NSF Science Faculty Fellowship 64203.