The next stage of the reduction is analogous except that we have no local conditions to trouble us. It enables us to write

$$f_4 = x_5 x_6 + f_6(x_7, \ldots, x_{11}), \qquad g_4 = b_5 \xi_5^2 + g_5(x_6, \ldots, x_{11})$$

with $\xi_5 = x_5 + c_{56} x_6 + \ldots$; and if g_6 is the restriction of g_5 to $x_6 = 0$ then f_6, g_6 are non-singular and no form of the pencil generated by them has rank less than 3. Moreover we may assume that $b_5 \neq 0$; for otherwise we can obtain a rational solution of $f = g = 0$ by putting $x_5 = 1$, $\xi_1 = \xi_3 = x_2 = x_4 = x_6 = \ldots = 0$.

Now let $\mathscr{S}'$ be the finite set of these primes p such that $b_1 \xi_1^2 + b_3 \xi_3^2 + b_5 \xi_5^2$ does not represent zero over the p-adic numbers. We have arranged that $\mathscr{S}'$ contains no prime of $\mathscr{S}$, and we can therefore apply the result of Lemma 4 to the forms f_6 and $b_1 b_3 b_5 g_6$ for each $p \in \mathscr{S}'$. For each of them we obtain a p-adic point P_{7p} on $f_6 = 0$ such that $b_1 b_3 b_5 g_6(P_{7p})$ is not a p-adic square. Let P_7 be a rational point on $f_6 = 0$ so near to each P_{7p} that it has the same properties; by a further change of variables we may take it to be $(1, 0, 0, 0, 0)$. Let $b_7 = g_6(P_7) \neq 0$ and consider the linear subspace given by

$$x_2 = x_4 = x_6 = x_8 = x_9 = x_{10} = x_{11} = 0.$$

On this we have $f = 0$ identically; and since ξ_1, ξ_3, ξ_5, x_7 are an acceptable system of homogeneous coordinates we can write the restriction of g in the form

$$b_1 \xi_1^2 + b_3 \xi_3^2 + b_5 \xi_5^2 + b_7 x_7^2.$$

But this is an indefinite quadratic form which represents zero in every p-adic field. (The only difficulty is with the $p \in \mathscr{S}'$, for which we appeal to the theorem that a quaternary quadratic form which does not represent zero in a p-adic field must have determinant a p-adic square.) Hence it represents zero over the rationals; and this representation extends in an obvious way to a rational solution of $f = g = 0$. This completes the proof of the theorem.

References

[1] B. J. Birch, D. J. Lewis and T. G. Murphy, Amer. J. Math. 84 (1962), pp. 110-115.

[2] V. B. Demyanov, Izv. Akad. Nauk. SSSR 20 (1956), pp. 307-324.

[3] L. J. Mordell, Hamb. Abh. 23 (1959), pp. 126-143.

[4] C. V. H. Rao, Proc. Lond. Math. Soc. 17 (1919), pp. 272-305.

[5] C. Segre, Math. Ann. 24 (1884), pp. 313-444.

TRINITY COLLEGE, CAMBRIDGE

Reçu par la Rédaction le 20. 12. 1963

ACTA ARITHMETICA
IX (1964)

Simultaneous representation by adjoint quadratic forms

by

G. Pall (Baton Rouge, La)

Dedicated to Professor L. J. Mordell

1. Introduction. Consider an n-ary quadratic form φ with real coefficients, and its adjoint form φ'. Denote their matrices by $A = (a_{ij})$ and $A' = (a'_{ij})$, so that a'_{ij} is the cofactor of the element a_{ij} in the determinant of A. Two real numbers m and m' are said to be *simultaneously represented by φ and φ'* if there exist integers x_i, z'_i $(i = 1, \ldots, n)$ such that

$$(1) \qquad m = \sum_{i,j=1}^{n} a_{ij} x_i x_j, \qquad m' = \sum_{i,j=1}^{n} a'_{ij} z'_i z'_j, \qquad 0 = \sum_{i=1}^{n} x_i z'_i.$$

The pair of column vectors $x = (x_i)$ and $z' = (z'_i)$ is called a *simultaneous representation*. The representation is termed *primitive* if each vector is primitive, that is the n components of each vector are relatively prime.

The notion of simultaneous representation was first introduced by G. Eisenstein [1], as part of an expression for his invariant system for a genus of ternary quadratic forms. The extension of Eisenstein's idea to n-ary quadratic forms, due to H. J. S. Smith [2] and H. Minkowski [3], involved the sequence of leading minor determinants in the matrix of A. It is interesting that the definition we have given above allows a quantitative development, which is the main purpose of this article. An algorithm will be given which produces all the simultaneous representations of given m and m' by φ and φ', each *set* of primitive representations (a set being an aggregate Wx, $W'z'$, W running over the unimodular automorphs of φ) being associated with a unique class of quadratic forms in $n-2$ variables and a certain set of solutions of certain quadratic congruences modulo m and m'. A formula similar to those of Smith, Minkowski, and Siegel [4] for the weighted number of simultaneous representations by a genus, exists for the weighted number of simultaneous representations by the system of classes of a genus and the adjoint genus.

As an example, the number of simultaneous, primitive solutions of

$$(2) \qquad m = x_1^2 + x_2^2 + x_3^2, \qquad m' = y_1^2 + y_2^2 + y_3^2, \qquad 0 = x_1 y_1 + x_2 y_2 + x_3 y_3,$$

where m and m' are coprime positive integers, is $24gg'$, where g and g'

denote the numbers of solutions t and t' of the respective congruences

$$t^2 \equiv -m' \pmod{m}, \qquad t'^2 \equiv -m \pmod{m'}.$$

As a second example, if m and m' are coprime positive odd integers, then the number of simultaneous and primitive solutions of

$$m = x_1^2+x_2^2+x_3^2+3x_4^2, \quad m' = 3y_1^2+3y_2^2+3y_3^2+y_4^2, \quad 0 = x_1y_1+\ldots+x_4y_4,$$

if $m' \equiv 1 \pmod 3$, and of

$$m = x_1^2+x_2^2+2x_3^2+2x_3x_4+2x_4^2, \qquad m' = 3y_1^2+3y_2^2+2y_3^2-2y_3y_4+2y_4^2,$$

with $0 = x_1y_1+x_2y_2+x_3y_3+x_4y_4$, if $m' \equiv 2 \pmod 3$, is equal to

$$\begin{array}{lll}
12, & \text{if } m = m' = 1; & \\
24h, & \text{if } mm' \equiv 1 \bmod 4 & \text{and } mm' > 1; \\
48h, & \text{if } mm' \equiv 3 \bmod 8 & \text{and } (-1 \mid m) = (m' \mid 3); \\
16h, & \text{if } mm' \equiv 3 \bmod 8 & \text{and } (-1 \mid m) = -(m' \mid 3); \\
96h, & \text{if } mm' \equiv 7 \bmod 8 & \text{and } (-1 \mid m) = (m' \mid 3); \\
0, & \text{if } mm' \equiv 7 \bmod 8 & \text{and } (-1 \mid m) = -(m' \mid 3).
\end{array}$$

Here $h = h(mm')$ denotes the number of properly primitive classes of positive binary quadratic forms of determinant mm'.

A third example: if m and m' are coprime positive integers, then the number of solutions, with $(x_1, \ldots, x_4) = 1 = (y_1, \ldots, y_4) = 1$, of

$$m = x_1^2+x_2^2+x_3^2+x_4^2, \qquad m' = y_1^2+y_2^2+y_3^2+y_4^2,$$

$$0 = x_1y_1+x_2y_2+x_3y_3+x_4y_4,$$

is equal to

$$\begin{array}{llll}
48, & \text{if } mm' = 1; & 96h, & \text{if } mm' \equiv 1 \text{ or } 2 \bmod 4,\ mm' > 1; \\
64h, & \text{if } mm' \equiv 3 \bmod 8; & 0, & \text{if } mm' \equiv 0,\ 4, \text{ or } 7 \bmod 8.
\end{array}$$

I. Ternary quadratic forms

2. The algorithm for ternaries. This section, the special case $n = 3$ of Part II, will serve to illuminate what follows and has noteworthy features of its own.

THEOREM 1. *Let $x = (x_i)$ and $z = (z_i')$ be primitive column vectors, with three components, such that $x^\top z' = 0$ (1). Then there exists a unimodular*

(1) Notations. The superscript $^\top$ marks the transpose of a matrix. A *unimodular* matrix is one which is integral and has determinant $+1$. The term *Adjoint* (with a capital A) indicates the matrix of cofactors, not transposed; thus $\operatorname{adj} T$ is the transpose of $\operatorname{Adj} T$. It should be recalled that if $B = T^\top AT$, then $\operatorname{Adj} B = (\operatorname{Adj} T)^\top (\operatorname{Adj} A)\ (\operatorname{Adj} T)$; and that $\operatorname{Adj}(TX) = (\operatorname{Adj} T)(\operatorname{Adj} X)$. Parentheses surrounding matrices may, for convenience of typing and printing, be sufficiently indicated as shown in (3).

matrix T such that x is the first column of T and z' is the third column of the Adjoint matrix T'. If T is one such matrix, then every matrix with these properties is given by TX, where

$$X = \begin{pmatrix} 1 & h & k \\ 0 & 1 & h' \\ 0 & 0 & 1 \end{pmatrix}, \tag{3}$$

with h, k, and h' arbitrary integers. This means, if T and T' are indicated columnwise by

$$T = (x\ \ y\ \ z), \qquad T' = (x'\ \ y'\ \ z'), \tag{4}$$

that y can be replaced by $y+hx$, and y' by $y'-h'z'$, with h and h' arbitrary integers; and that, if y and y' are fixed, then z is uniquely determined up to an added integral multiple of x, or alternatively, x' is uniquely determined up to an added integral multiple of z'.

Proof. See the more general Theorem 4.

Our idea is to apply the transformation T to φ, and to see what remains invariant when T is replaced by the general matrix TX. We have $m = x^\top Ax$ and $m' = z'^\top A'z'$, and assume that $d = |A| \neq 0$, and that $mm' \neq 0$. If $B = T^\top AT$, then the Adjoint of B is $T'^\top A'T'$, and we can write

$$B = \begin{pmatrix} m & t & s \\ t & q & r \\ s & r & k \end{pmatrix}, \qquad B' = \begin{pmatrix} . & . & . \\ . & q' & t' \\ . & t' & m' \end{pmatrix}, \tag{5}$$

where the dots indicate parts of the matrix for which names are not needed. If y and y' are replaced by $y+hx$ and $y'+h'z'$, then t and t' become $t+hm$ and $t'+h'm'$. Thus there are associated with the primitive representations x and z' two uniquely determined real numbers t and t' such that

$$-\tfrac{1}{2}|m| < t \leqslant \tfrac{1}{2}|m|, \qquad -\tfrac{1}{2}|m'| < t' \leqslant \tfrac{1}{2}|m'|. \tag{6}$$

If we so fix t and t', then replacing z by $z+k_1x$ will replace s by $s+k_1m$. Hence there is also associated a real number s such that

$$-\tfrac{1}{2}|m| < s \leqslant \tfrac{1}{2}|m|. \tag{6'}$$

If x and z' are replaced by Wx and $W'z'$, where W is any unimodular automorph of φ and W' is Adj W, then T and T' can be replaced by WT and $W'T'$. Hence the same matrices B and B', consequently the same real numbers t, t', s are associated with the set of representations Wx and $W'z'$, where W ranges over the unimodular automorphs of φ.

There are thus associated with every set of simultaneous and primitive representations of m and m' by φ and φ' three real numbers t, t', s satisfying (6) and (6′). Conversely, to every triple t, t', s satisfying (6) and (6′) correspond a unique set of simultaneous and primitive representations of m and m' by certain forms, but not necessarily by φ and φ'. Indeed, for given t, t', s we can find real numbers q, q', r, and k such that

$$(7)\qquad mq-t^2 = m', \quad m'q'-t'^2 = md, \quad st-mr = t', \quad mk-s^2 = q',$$

and form from these the matrix B in (5). If then the matrices A and B are not *equivalent*[2], then no representations of m and m' are associated with t, t', s. But if A and B are equivalent, let T be one unimodular transformation of A into B. Then the most general such transformation is WT, where W is any unimodular automorph of A. Then the first columns of WT with the third columns of $W'T'$ constitute a set of simultaneous, primitive representations of m and m' by φ and φ', associated with t, t', and s.

THEOREM 2. *The number of sets of simultaneous and primitive representations of m and m' by a ternary form φ and its adjoint φ' equals the number of complexes t, t', s satisfying* (6) *and* (6′) *for which B constructed by* (7) *is equivalent to the matrix of φ.*

The possible triples t, t', s are considerably restricted if A is integral. Then m and m' must be integers, as also the elements of B and B', whence t, t', s are solutions of the congruences

$$(8)\qquad t^2 \equiv -m' \,(\mathrm{mod}\, m), \qquad -\tfrac{1}{2}|m| < t \leqslant \tfrac{1}{2}|m|;$$

$$(9)\qquad t'^2 \equiv -md \,(\mathrm{mod}\, m'), \qquad -\tfrac{1}{2}|m'| < t' \leqslant \tfrac{1}{2}|m'|;$$

$$(10)\qquad st \equiv t' \,(\mathrm{mod}\, m), \qquad s^2 \equiv -q' \,(\mathrm{mod}\, m), \qquad -\tfrac{1}{2}|m| < s \leqslant \tfrac{1}{2}|m|;$$

with q' defined by $m'q' = t'^2+dm$.

If m and m' are coprime integers the number of solutions t, t', s of (8)-(10) is equal to the number of solutions t, t' of (8)-(9). For then $(t, m) = 1$, and the unique solution s of $st \equiv t' \bmod m$ satisfies $s^2+q' = (s^2m'+q'm')/m' \equiv (t'^2-s^2t^2+dm)/m' \equiv 0 \bmod m$.

It is easily seen for any solution of (8)-(10) that B constructed as in (5) has determinant d. The index of B is fixed by the signs of m, m', d.

(2) Equivalence is used in the Gauss sense, that $A = U^{\top}BU$ for some unimodular U.

Hence all the solutions of (8)-(10) are associated with simultaneous representations of m and m' by forms f and f' with f of determinant d and index determined by the signs of m, m', d. To obtain the number of sets of simultaneous primitive representations by the system of classes of a genus and its adjoint, it is only necessary to prescribe conditions to assure that B is in that genus. Thus m and m' may be so restricted that their values fix the generic characters, and then all solutions will refer to a specific genus with its adjoint.

Since there is only one class of positive integral ternaries of determinant 1, it follows that the number of sets of solutions of (2) is gg', if m and m' are positive coprime integers. Since $x_1^2+x_2^2+x_3^2$ has 24 unimodular automorphs, each set consists of 24 distinct representations, in view of the following theorem:

THEOREM 3. *If x and z' are simultaneous primitive representations of nonzero numbers m, m' by φ and φ', then as W ranges over the unimodular automorphs of φ, the vectors Wx and $W'z'$ never repeat their pair of values for different W's.*

Proof. Since the W's form a group it suffices to show that $Wx = x$ and $W'z' = z'$ imply that W is the identity I. Our previous discussion showed that the matrix T such that x is the first column of T and z' is the third column of T' is uniquely determined by the condition that (6) and (6′) are satisfied by

$$T^{\top}AT = \begin{pmatrix} m & t & s \\ t & . & . \\ s & . & . \end{pmatrix} \quad\text{and}\quad T'^{\top}A'T' = \begin{pmatrix} . & . & . \\ . & . & t' \\ . & t' & m' \end{pmatrix}.$$

If $T = (x\ \ y\ \ z)$ and $T' = (x'\ \ y'\ \ z')$ are the unique matrices with the specified properties, then $WT = (x\ \ .\ \ .)$ and $W'T' = (.\ \ .\ \ z')$ have the same properties. Hence $WT = T$ and $W = I$.

As a second example consider the two positive classes of determinant 3, containing $f_1 = x_1^2+x_2^2+3x_3^2$ and $f_2 = 2x_1^2+2x_1x_2+2x_2^2+x_3^2$ with the adjoints $f_1' = 3y_1^2+3y_2^2+y_3^2$ and $f_2' = 2y_1^2-2y_1y_2+2y_2^2+3y_3^2$. We assume m and m' positive, $(m, m') = 1$, $(m', 3) = 1$. Then the representations are by f_1 and f_1' if $m' \equiv 1 \bmod 3$, and by f_2 and f_2' if $m' \equiv 2 \bmod 3$. The number of primitive representations in each case is equal to w times the number of solutions of

$$t^2 \equiv -m' \,(\mathrm{mod}\, m), \qquad t'^2 \equiv -3m \,(\mathrm{mod}\, m'),$$

w (the number of unimodular automorphs) being 8 for f_1, 12 for f_2 ([5]).

II. n-ary quadratic forms

3. A theorem on integral matrices. We shall prove

THEOREM 4. *Let x and z' be primitive column vectors with n components, $x^{\top}z' = 0$. There exists a unimodular matrix T such that x is the first column of T and z' is the last column of $T' = \operatorname{Adj} T$. If T is one such matrix the most general is TX, where*

$$X = \begin{pmatrix} 1 & \alpha^{\top} & t \\ 0 & U & \beta \\ 0 & 0 & 1 \end{pmatrix}; \tag{11}$$

here U is any unimodular matrix of order $n-2$, $\alpha^{\top}$ and β are row and column vectors with $n-2$ integer components, t is an integer, and the 0's are zero matrices.

To prove that T exists we first choose a unimodular matrix Q such that $Qx = e_1$, with e_1 the first column of the identity I. Then if $Q' = \operatorname{Adj} Q$, $x^{\top}Q^{\top}Q'z' = 0$, whence the first element of $Q'z'$ is 0. Choose a unimodular matrix R, with first row and column the same as those of I, to satisfy $R'Q'z' = e_n$, where e_n is the last column of I. Then, if $P = RQ$, $Px = e_1$ and $P'z' = e_n$. Hence the first column of $T = P^{-1}$ is x and the last column of T' is z'.

Since $X'X^{\top} = I$, the Adjoint of X is

$$X' = \begin{pmatrix} 1 & 0 & 0 \\ \gamma & V & 0 \\ u & \delta^{\top} & 1 \end{pmatrix}, \tag{12}$$

where $V = U'$, $\gamma = -V\alpha$, $\delta = -V^{\top}\beta$, and $u+t = \beta^{\top}V\alpha$; hence TX and $T'X'$ have the desired properties with T and T'. To prove that TX is the most general such matrix it will suffice to show that if S and T are two such, then $T^{-1}S$ has the form of X. We can partition S and T, S' and T', as follows,

$$T = (x \;\; Y \;\; z), \qquad T' = (x' \;\; Y' \;\; z'), \qquad S = (x \;\; Y_1 \;\; z_1), \qquad S' = (x_1' \;\; Y_1' \;\; z'),$$

the Y's being integral matrices with n rows and $n-2$ columns. Since $T'^{\top}T = I = S'^{\top}S$, we have $x'^{\top}x = 1$, $Y'^{\top}x = 0$, $z'^{\top}x = 0$, $z'^{\top}Y_1 = 0$, $z'^{\top}z_1 = 1$, and hence

$$T^{-1}S = \begin{pmatrix} x' \\ Y' \\ z' \end{pmatrix}(x \;\; Y_1 \;\; z_1) = \begin{pmatrix} 1 & \alpha^{\top} & t \\ 0 & U & \beta \\ 0 & 0 & 1 \end{pmatrix}, \tag{13}$$

where α, β, t, and U are integral matrices defined by this equation. Obviously U is unimodular with $T^{-1}S$.

4. The class of $(n-2)$-ary forms associated with Wx and $W'z'$. If T and T' have x and z' as first and last columns respectively, and $m = x^{\top}Ax$ and $m' = z'^{\top}A'z'$, then $B = T^{\top}AT$ and $B' = T'^{\top}A'T'$ can be given the notations

$$B = \begin{pmatrix} m & \varkappa^{\top} & l \\ \varkappa & B_2 & \lambda \\ l & \lambda^{\top} & s \end{pmatrix}, \qquad B' = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & C_2 & \mu \\ \cdot & \mu^{\top} & m' \end{pmatrix}, \tag{14}$$

where B_2 and C_2 are symmetric matrices of order $n-2$; $\varkappa$, λ, and μ have $n-2$ components; s and l are numbers. We investigate what remains invariant in (14) when T is replaced by the "most general" matrix TX, and hence B is replaced by

$$X^{\top}BX = \begin{pmatrix} m & \varkappa^{\top}U + m\alpha^{\top} & l+\varkappa^{\top}\beta+mt \\ U^{\top}\varkappa + m\alpha & m\alpha\alpha^{\top}+U^{\top}\varkappa\alpha^{\top}+\alpha\varkappa^{\top}U+U^{\top}B_2U & \cdot \\ l+\beta^{\top}\varkappa+mt & \cdot & \cdot \end{pmatrix}, \tag{15}$$

and B' by

$$X'^{\top}B'X' = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & V^{\top}C_2V+\delta\mu^{\top}V+V^{\top}\mu\delta^{\top}+m'\delta\delta^{\top} & V^{\top}\mu+m'\delta \\ \cdot & \mu^{\top}V+m'\delta^{\top} & m' \end{pmatrix}. \tag{16}$$

THEOREM 5. *In the notation of* (14), *set*

$$G = mB_2 - \varkappa\varkappa^{\top}, \qquad F = m'C_2 - \mu\mu^{\top}. \tag{17}$$

If T is replaced by TX, G and F are replaced by the equivalent matrices $U^{\top}GU$ and $V^{\top}FV$ respectively, where $V = U'$. Also,

$$|G| = m^{n-3}m', \qquad |F| = mm'^{n-3}d^{n-2}, \qquad GF = FG = mm'dI_2, \qquad \operatorname{Adj} G = m^{n-4}F/d, \tag{18}$$

where $d = |A|$ and I_2 is the identity matrix of order $n-2$.

Proof. To complete squares relative to m in (15) is to apply the transformation which differs from I only in having the first row

$$\big(1 \quad -m^{-1}(\varkappa^{\top}U+m\alpha^{\top}) \quad -m^{-1}(l+\varkappa^{\top}\beta+mt)\big),$$

and thus to replace the matrix (15) by the matrix E whose first row is $(m \;\; 0 \;\; 0)$ and "middle row" is $(0 \;\; m^{-1}U^{\top}GU \;\; .)$. Then (16) must be transformed by the Adjoint matrix, differing from I only in having its first column the transpose of

$$\big(1 \quad m^{-1}(\varkappa^{\top}U+m\alpha^{\top}) \quad m^{-1}(l+\varkappa^{\top}\beta+mt)\big),$$

and accordingly (16) is replaced by E' $(=\operatorname{Adj} E)$, which differs from (16) at most in its first row and column. Since m' is the value of the leading determinant of order $n-1$ in E, and $d^{n-2}m$ is the value of the last determinant of order $n-1$ in E', $m'=m|m^{-1}G|$, and the first row of E' is $(m^{-1}d\ \ 0\ \ 0)$. Next we apply to E' the transformation which differs from I only in having the last row

$$(0\ \ -m'^{-1}(\mu^{\top}V+m'\delta^{\top})\ \ 1),$$

and thus (applying the Adjoint to E) replace E and E' by

$$\begin{pmatrix} m & 0 & 0\\ 0 & m^{-1}U^{\top}GU & 0\\ 0 & 0 & m'^{-1}d\end{pmatrix},\qquad \begin{pmatrix} m^{-1}d & 0 & 0\\ 0 & m'^{-1}V^{\top}FV & 0\\ 0 & 0 & m'\end{pmatrix}.$$

Since these have the product dI the theorem follows.

The matrices G and F are best remembered as the matrices obtained by completing squares relative to m and m' respectively, in the first minor of order $n-1$ in B, and in the last minor of order $n-1$ in B'.

We need the explicit result of completing squares relative to m in (14). This replaces B and B' by

$$\begin{pmatrix} m & 0 & 0\\ 0 & m^{-1}G & \lambda-l\varkappa/m\\ 0 & \lambda^{\top}-l\varkappa^{\top}/m & s-l^2/m\end{pmatrix},\qquad \begin{pmatrix} m^{-1}d & 0 & 0\\ 0 & C_2 & \mu\\ 0 & \mu^{\top} & m'\end{pmatrix}.$$

Since the product of these matrices is dI, we have in particular

$$(19)\qquad G\mu+(m\lambda-l\varkappa)m'=0,\qquad \mu^{\top}(m\lambda-l\varkappa)+(ms-l^2)m'=dm.$$

5. The algorithm, in general. There are thus associated with any given simultaneous, primitive representations x and z' of m and m' by φ and φ', an aggregate of quadruplets

$$(20)\qquad \{U^{\top}GU,\ U^{\top}\varkappa+m\alpha,\ V^{\top}\alpha+m'\delta,\ l+\varkappa^{\top}\beta+mt\},$$

which can be generated (as is evident from Theorem 4, and can be verified directly) from any particular quadruplet $\{G,\varkappa,\mu,l\}$ of the aggregate by use of an arbitrary unimodular U, arbitrary integral vectors α and β, and an arbitrary integer t. Here $V=\operatorname{Adj} U$ and $\delta=-U^{-1}\beta$. Since the same matrices B and B' are derived from Wx and $W'z'$, as from x and z', the entire set Wx and $W'z'$ (W ranging over the unimodular automorphs of φ) is associated with the same aggregate (20).

Conversely, for any given $G,\varkappa,\mu,l$, we can define F by (18_4), B_2 and C_2 by (17), can solve for λ from (19_1) and for s from (19_2). Thus a matrix B is constructed. If A and B happen to be equivalent, let T denote a unimodular transformation of A into B; then the first and last columns of WT and $W'T'$ constitute a set of simultaneous and primitive representations of m and m' by φ and φ' associated with the quadruplet $\{G,\varkappa,\mu,l\}$, and with the aggregate (20) which it generates. But if A and B are not equivalent no representation of m and m' by φ and φ' is associated with $\{G,\varkappa,\mu,l\}$.

Consider (20) with U fixed. We can choose α and β $(=-U\delta)$ uniquely so that — the inequalities being satisfied by each component —

$$-\tfrac{1}{2}|m|<U^{\top}\varkappa+m\alpha\leqslant\tfrac{1}{2}|m|,\qquad -\tfrac{1}{2}|m'|<V^{\top}\mu+m'\delta\leqslant\tfrac{1}{2}|m'|.$$

For this choice of α,β, $l+\varkappa^{\top}\beta+mt$ is uniquely determined modulo m. Thus every aggregate of quadruplets contains one $\{G,\varkappa,\mu,l\}$ in which (componentwise)

$$(21)\qquad -\tfrac{1}{2}|m|<\varkappa\leqslant\tfrac{1}{2}|m|,\qquad -\tfrac{1}{2}|m'|<\mu\leqslant\tfrac{1}{2}|m'|,\qquad -\tfrac{1}{2}|m|<l\leqslant\tfrac{1}{2}|m|.$$

Two quadruplets $\{G,\varkappa,\mu,l\}$ and $\{G,\varkappa_1,\mu_1,l_1\}$, with the same G, and both satisfying (21), will belong to the same aggregate if and only if there exists a unimodular automorph U of G such that

$$(22)\qquad (\varkappa_1-U^{\top}\varkappa_1)/m,\quad (\mu_1-V^{\top}\mu)/m'\quad\text{and}\quad (l_1-l+\varkappa^{\top}U\delta)/m\ \text{are integral},$$

δ denoting the quotient $(\mu_1-V^{\top}\mu)/m'$. For a given matrix G, the set of all triplets $\{\varkappa,\mu,l\}$ satisfying (21) and (22) for some U, derived from a given triplet $\{\varkappa_1,\mu_1,l_1\}$, will be called a *G-set.*

THEOREM 6. *Every set of simultaneous and primitive representations of nonzero numbers m and m' by the real nonsingular n-ary quadratic form φ and its adjoint φ' is associated with a unique class of matrices G of order $n-2$, and if we select a particular matrix G in this class, with a unique G-set. One such set of representations obtains for every matrix G and accompanying G-set for which the matrix B constructed as explained above is equivalent to the matrix of φ.*

If φ has an integral matrix the possible values for $G,\varkappa,\mu,l$ are greatly resticted. Then m and m' are integers, B and B' are integral, and $\varkappa$ and μ are integral solutions of the congruences

$$(23)\qquad \varkappa\varkappa^{\top}\equiv -G\ (\operatorname{mod} m),\qquad \mu\mu^{\top}\equiv -F\ (\operatorname{mod} m').$$

Here G is an integral matrix of determinant $m^{n-3}m'$, and it suffices to take one matrix in each of the finite number of classes (class being defined under unimodular transformations) of this determinant. The index of G must be such that the direct sum of the matrices m, $m^{-1}G$, $m'^{-1}d$

has the index of A. Also, $F = d(\operatorname{Adj} G)/m^{n-4}$ must be integral. And the genus of G must allow (23) to be solvable.

By (19_1), μ must satisfy the additional congruence

$$G\mu \equiv 0 \pmod{m'}, \tag{24}$$

and for each pair of vectors $\varkappa$ and μ, l must satisfy

$$l\varkappa \equiv G\mu/m' \pmod{m}; \tag{25}$$

and λ is then determined as an integral vector by

$$\lambda = (l\varkappa - G\mu/m')/m. \tag{26}$$

On substituting this expression for λ into (19_2) we obtain

$$-\mu^\top G\mu/m' + (ms - l^2)m' = dm. \tag{27}$$

Hence μ must also satisfy the congruence

$$\mu^\top G\mu/m' \equiv -md \pmod{m'}, \tag{28}$$

and l must also satisfy

$$l^2 \equiv -(dm + \mu^\top G\mu/m')/m' \pmod{m}. \tag{29}$$

Then s can be determined from (27) as an integer.

A simple situation occurs if m and m' are coprime. Then no prime factor p of m can divide all the elements of G. For else p would divide the leading determinant of order $n-1$ in B (in (14)), and hence p would divide m'. For such a matrix G the solutions $\varkappa$ of (23) are primitive modulo m, and (25), being equivalent to

$$l\varkappa \equiv -\varkappa\varkappa^\top \mu/m' \pmod{m},$$

has the unique solution $l \equiv -\varkappa^\top \mu/m' \pmod{m}$. This satisfies (29) since $\varkappa^\top\mu = \mu^\top\varkappa$,

$$l^2 \equiv \mu^\top\varkappa\cdot\varkappa^\top\mu/m'^2 \equiv -\mu^\top G\mu/m'^2 \pmod{m}.$$

For each suitable matrix G we may consider the solutions $\varkappa$ and l modulo m, and μ modulo m', for which the preceding systems of congruences are satisfied and the associated matrix B is in the class, genus, or order in which we desire the representations. It then becomes necessary to arrange the solutions in G-sets, or at least, if the number of sets of representations is sought, to find the number of triples in each G-set. It might be surmised that if G has a finite number u of unimodular automorphs each G-set will contain u triples. This is not true in general, but

fortunately any diminution in the number of triples in a G-set is compensated by a corresponding reduction in the associated set of representations, in accordance with the following theorem (see [6]):

THEOREM 7. *Let the representations x and z' be associated in the preceding algorithm with the quadruplet $\{G, \varkappa, \mu, l\}$. Let Σ_1 denote the subgroup of unimodular automorphs W of φ such that $Wx = x$ and $W'z' = z'$. Let Σ_2 denote the subgroup of unimodular automorphs U of G such that*

$$U^\top\varkappa \equiv \varkappa \pmod{m}, \qquad U'^\top\mu \equiv \mu \pmod{m'},$$
$$\varkappa^\top(\mu - U'^\top\mu)/m' \equiv 0 \pmod{m}. \tag{30}$$

There is a one-one correspondence between the sets Σ_1 and Σ_2.

Proof. Notice that in (30), $\varkappa$ and μ may be considered only modulo m and m' respectively, and that it is not necessary to assume (21). For if μ is replaced by $\mu + m'\tau$, where τ denotes an integral vector, then $\varkappa^\top(\mu - V^\top\mu)/m'$ is increased by $(\varkappa^\top - \varkappa^\top V^\top)\tau$, which is divisible by m since by (30_1), as $VU^\top = I$, $\varkappa^\top \equiv \varkappa^\top V^\top \pmod{m}$. Hence, if $(m, m') = 1$, (30_3) is a consequence of (30_1) and (30_2).

Consider Adjoint unimodular transformations $T = (x\ Y\ z)$ and $T' = (x'\ Y'\ z')$ replacing A and A' by B and B' (in (14)). If $Wx = x$ and $W'z' = z'$, then WT and $W'T'$ also have x and z' as first and last columns respectively. By Theorem 4, $WT = TX$, and hence $X = T^{-1}WT$ is a unimodular automorph of B, of the type displayed in (11). On forming $X^\top BX = B$ and $X'^\top B'X' = B'$, we have (compare (14), (15), and (16))

$$U^\top GU = G, \quad \varkappa = U^\top\varkappa + m\alpha, \quad \mu = V^\top\mu + m'\delta, \quad \varkappa^\top U\delta = -mt. \tag{31}$$

Hence U is a unimodular automorph of G satisfying (30).

Conversely, let $U^\top GU = G$ and let (30) hold. Then we can define integral vectors α and β, and an integer t, by (31). The resulting integral matrix X and its Adjoint X' replace B and B' by the matrices in (15) and (16), so far as they are explicitly shown; and these displayed parts coincide with the corresponding parts of B and B'. However, the rest of B is determined by the parts of B and B' thus given and by the determinant d, since $BB' = dI$. Hence X is a unimodular automorph of B, and $W = TXT^{-1}$ is a unimodular automorph of A such that $Wx = x$ and $W'z' = z'$.

This establishes the one-one correspondence. We do not need the property, no doubt also true, that the correspondence is preserved under multiplication.

The number ν of elements in Σ_2 may be finite or infinite, but the index, which we will denote by ε, of Σ_2 within the group of all unimodular automorphs U of G is finite. Indeed, ε is equal to the number of incongruent triples $\{\varkappa, \mu, l\}$ to respective moduli m, m', m in a G-set. If the number u of automorphs U of G is finite, $u = \nu\varepsilon$. If also the number w of automorphs W of A is finite, then by Theorem 7,

$$(32)\qquad \frac{1}{\nu} = \frac{\text{number of distinct pairs } Wx,\ W'z' \text{ in a set}}{w} = \frac{\varepsilon}{u}.$$

If w is finite, the *weight* of the representation x and z' (by φ and φ') is defined to be $1/w$. By (32), the sum of the weights of the representations in a set (Wx and $W'z'$) is $1/\nu$. Now ν is finite, even though w may be infinite, provided u is finite. It is consistent and natural to define the *weight of a set of representations* (Wx and $W'z'$) to be $1/\nu$, if ν is finite. This makes it possible for example to apply the preceding theory quantitatively to indefinite forms if the matrices G are definite.

In some cases our algorithm will associate a set of nonequivalent matrices $A_1, \ldots, A_h$ with a set of nonequivalent matrices $G_1, \ldots, G_s$, each G_j being accompanied by one or more G_j-sets. For example, if $A_1, \ldots, \ldots, A_h$ are representatives (one from each class) of a given determinant d, then $G_1, \ldots, G_s$ will be certain matrices previously characterized. If $A_1, \ldots, A_h$ are representatives of the classes of a genus, then $G_1, \ldots, G_s$ will consist of the classes of one or more genera. Sometimes, not every triplet of solutions $\{\varkappa, \mu, l\}$ of the system of congruences with $G = G_j$ will be such that the matrices B constructed therefrom are in the prescribed genus, and one must specify those solutions.

Let the numbers u_j of unimodular automorphs of the G_j be assumed finite ($j = 1, \ldots, s$). Denote by $A_i\ (m, m')$ the sum of the weights of all sets of simultaneous and primitive representations of m and m' by A_i and A_i'; and let $\varrho(G_j)$ denote the number of incongruent triples $\varkappa, \mu$ and l (mod m, m', m), obtained with $G = G_j$, and such that the corresponding matrix B is equivalent to one of $A_1, \ldots, A_h$. Then, summing up from (32), we have

$$(33)\qquad \sum_{i=1}^{h} A_i(m, m') = \sum_{j=1}^{s} \varrho(G_j)/u_j.$$

If the numbers $w_1, \ldots, w_h$ of unimodular automorphs of $A_1, \ldots, A_h$ are finite, then the left member has the form $\sum A_i[m, m']/w_i$, where $A_i[m, m']$ denotes the number of simultaneous and primitive representations by A_i and A_i'.

6. An example. Let $n = 4$, $d = 3$, and let φ denote $f_1 = x_1^2 + x_2^2 + x_3^2 + 3x_4^2$ or $f_2 = x_1^2 + x_2^2 + 2x_3^2 + 2x_3x_4 + 2x_4^2$, which ([7]) are forms of the two classes of positive classic quaternaries of determinant 3. Each of f_1, f_2 may be shown to have 48 unimodular automorphs. The genera

of f_1 and f_2 are distinct, since clearly $f_1' = 3y_1^2 + 3y_2^2 + 3y_3^2 + y_4^2$ represents no $3k+2$, and $f_2' = 3y_1^2 + 3y_2^2 + 2y_3^2 - 2y_3y_4 + 2y_4^2$ represents no $3k+1$. We shall assume $(m', 3) = 1$, whence all simultaneous representations will be by f_1 and f_1' if $m' \equiv 1 \bmod 3$, and by f_2 and f_2' if $m' \equiv 2 \bmod 3$. We also assume that m and m' are positive, odd, and relatively prime.

Let ψ denote the binary quadratic form of matrix G. The solvability of $\varkappa\varkappa^\top \equiv -G \pmod m$ fixes the generic character $(\psi \mid p)$ of ψ for every odd prime p dividing m. We noticed above that no prime factor of m may divide the four elements of G. By (18_4), $F = 3$ Adj G, $|G| = mm'$. If m' and μ could have a common prime factor p, p would divide the last determinant of order $n-1$ in B', here equal to $9m$. Since, for binaries, G and Adj G are equivalent, the solvability of $\mu\mu^\top \equiv -F \pmod{m'}$ implies that ψ is primitive also modulo m', and that $(\psi \mid p) = (-3 \mid p)$ for every odd prime p in m'. Thus the generic characters of ψ are completely determined. It is necessary to see whether these generic characters are consistent with the conditions for the existence of a binary quadratic genus.

These conditions are here as follows. Write $mm' = p_1p_2 \ldots p_r$ as a product of (not necessarily distinct) primes. If ψ is properly primitive, the condition is that the product of the generic characters $(\psi \mid p_i)$ shall equal 1 if $mm' \equiv 3 \bmod 4$, but $(-1 \mid \psi)$ if $mm' \equiv 1 \bmod 4$. This merely assigns the value of the generic character $(-1 \mid \psi)$ if $mm' \equiv 1 \bmod 4$, but in view of the preceding values of $(\psi \mid p)$, imposes the condition

$$(34)\qquad (m' \mid 3) = (-1 \mid m), \quad \text{if } mm' \equiv 3 \bmod 4 \quad \text{and} \quad \psi \text{ is p. p.}$$

If ψ is improperly primitive, the condition is that the product of the symbols $(\frac{1}{2}\psi \mid p_i)$ shall equal 1. This reduces as follows:

$$(35)\qquad (m' \mid 3) = (-1 \mid m)(2 \mid mm'), \quad \text{if } \psi \text{ is i.p. (hence } mm' \equiv 3 \bmod 4).$$

In particular there are no simultaneous representations of m and m' by f_1 and f_1' if $m \equiv 3 \bmod 4$ and $mm' \equiv 7 \bmod 8$; and there are no simultaneous representations of m and m' by f_2 and f_2' if $m \equiv 1 \bmod 4$ and $mm' \equiv 7 \bmod 8$.

Let h_1 denote the number of classes in the properly primitive genus of determinant mm' with the generic characters designated above, if $mm' \equiv 1 \bmod 4$ or if $(m' \mid 3) = (-1 \mid m)$; and let h_2 denote the number of classes in the similarly designated improperly primitive genus, if $mm' \equiv 3 \bmod 4$ and $(m' \mid 3) = (-1 \mid m)(2 \mid mm')$. Also let ϱ denote the number of distinct odd primes dividing m and σ the number dividing m'.

For either of these genera there exists in the class of ψ a form which is congruent coefficientwise to $-x_1^2 - mm'x^2 \pmod{m^2}$ and to $-3x_1^2-$

$-(mm'/3)x_2^2 \pmod{m'^2}$. Then if $\varkappa^\top$ and $\mu^\top$ are given the notations $(k_1\ k_2)$ and $(m_1\ m_2)$, (23) becomes

$$k_1^2 \equiv 1, \quad k_1k_2 \equiv 0, \quad k_2^2 \equiv 0 \pmod{m},$$
$$m_1^2 \equiv 0, \quad m_1m_2 \equiv 0, \quad m_2^2 \equiv 9 \pmod{m'}.$$

Hence k_1 has 2^ϱ residues mod m, while $k_2 \equiv 0$; m_2 has 2^σ residues mod m', while $m_1 \equiv 0$. Both (24) and (28) are seen to be automatically satisfied.

To sum up, there are $48\cdot 2^{\varrho+\sigma}\, h_1/u$ simultaneous and primitive representations of m and m' by φ and φ' if $mm' \equiv 1 \bmod 4$, or if $mm' \equiv 3 \bmod 8$ and $(m' \mid 3) = (-1 \mid m)$. There are $48\cdot 2^{\varrho+\sigma}(h_1+h_2)/2$ such representations if $mm' \equiv 7 \bmod 8$ and $(m' \mid 3) = (-1 \mid m)$. There are $48\cdot 2^{\varrho+\sigma}\times$ $\times h_2/u$ such representations if $mm' \equiv 3 \bmod 8$ and $(m' \mid 3) = -(-1 \mid m)$.

Now, if h denotes the number of properly primitive classes of positive binaries of determinant mm', then it is known that

$$h = \begin{cases} 2^{\varrho+\sigma}h_1 & \text{if} \quad mm' \equiv 1 \pmod 4, \\ 2^{\varrho+\sigma-1}h_1 & \text{if} \quad mm' \equiv 3 \pmod 4; \end{cases} \tag{36}$$

and, if $mm' \equiv 3 \pmod 4$,

$$h_1 = \begin{cases} h_2 & \text{if} \quad mm' = 3, \\ \big(2-(2 \mid mm')\big)h_2 & \text{if} \quad mm' > 3. \end{cases} \tag{37}$$

Also, u (the number of unimodular automorphs of G) is 6 if ψ is i.p. and $mm' = 3$; 4 if $mm' = 1$; and otherwise $u = 2$.

The result stated in the Introduction readily follows.

References

[1] G. Eisenstein, Jour. für Mathematik 35 (1847), pp. 117-136.

[2] H. J. S. Smith, Proc. Roy. Soc. London 16 (1867), pp. 197-208; Collected Mathematical Papers, I, pp. 510-523; II, pp. 623-680.

[3] H. Minkowski, Gesamm. Abh., I.

[4] C. L. Siegel, Annals of Mathematics 36 (1935), pp. 527-606; formula (5).

[5] Any table of positive ternary quadratic forms; e. g. B. W. Jones, Bulletin 97 National Research Council. or see G. Pall, Bull. Amer. Math. Soc., 47 (1941), pp. 641-650.

[6] G. Pall, Canadian Jour. of Math. 1 (1949), pp. 344-364; (Theorem 3).

[7] This follows from the fact that the minimum cannot exceed $(4d)^{1/4}$, hence must be 1, and from the corresponding result for ternaries.

LOUISIANA STATE UNIVERSITY

Reçu par la Rédaction le 28. 12. 1963

ACTA ARITHMETICA
IX (1964)

On Catalan's problem

by

K. Inkeri (Turku)

1. Catalan's well-known conjecture that 8 and 9 are the only two consecutive integers larger than 1 which are powers of other integers would be proved if it could be shown that the Diophantine equation

$$x^p - y^q = 1 \tag{1}$$

has only the obvious solutions (x or $y = 0$) for all pairs of prime numbers p and q except for the pair $p = 2$, $q = 3$, for which also $x = \pm 3$, $y = 2$ are solutions. Up to the present this has been proved only for certain special pairs p, q. The case $p = q$ is naturally obvious. Lebesgue [6] has treated the case $q = 2$ and Nagell [7] the cases $p = 3$ and $q = 3$. On the other hand the case $p = 2$ still awaits its final clarification, even though certain strict conditions have been presented. There is, as Obláth [9] has shown, at most one solution. If x, y is the solution, then [5]

$$x \equiv 0 \pmod{q^2}, \qquad y \equiv -1 \pmod{q^3} \tag{2}$$

and (cf. e.g. [4]), in addition,

$$2^q \equiv 2 \pmod{q^2}. \tag{3}$$

As of the primes not exceeding 200183, [10], only 1093 and 3511 fulfil (3), equation (1) is seen not to have a solution for a large number of pairs 2, q.

In this paper we limit ourselves to prime exponents $p > 3$, $q > 3$, of which at least one is of the form $4m+3$ and present proofs for two theorems which yield necessary conditions for the existence of a non-trivial solution of equation (1) that are similar to congruences (2) and (3). As an application, we show that equation (1) is not soluble in non-zero integers for a fairly large number of pairs p, q.