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

$$f_i = a_i x_1 + f_i(x_1, \ldots, x_n), \quad g_i = b_i x_1^2 + g_i(x_1, \ldots, x_n)$$

with $x_i = x_1 + c_i x_1 + \ldots$; and if $g_i$ is the restriction of $g_i$ to $x_1 = 0$ then $f_i, g_i$ are non-singular and no form of the pencil generated by them has rank less than 3. Moreover we may assume that $b_1 \neq 0$; for otherwise we can obtain a rational solution of $f = g = 0$ by putting $x_1 = 1, x_1 = 2, \ldots = 0$.

Now let $\mathcal{O}$ be the finite set of these primes $p$ such that $b_1 x_1^2 + b_1 x_1^2 + b_2 x_2^2$ does not represent zero over the $p$-adic numbers. We have arranged that $\mathcal{O}$ contains no prime of $\mathcal{O}$, and we can therefore apply the result of Lemma 4 to the forms $f$ and $b_1 b_2 g_i$ for each $p \in \mathcal{O}$. For each of them we obtain a $p$-adic point $P_n$ on $f = 0$ such that $b_i b_1 b_2 g_i(P_n)$ is not a $p$-adic square. Let $P_n$ be a rational point on $f = 0$ so near to each $P_n$ that it has the same properties; by a further change of variables we may take it to be $(1, 0, 0, 0, 0)$. Let $b_i = g_i(P_n) \neq 0$ and consider the linear subspace given by

$$a_i = a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = a_8 = a_9 = 0.$$ 

On this we have $f = 0$ identically; and since $x_1, x_2, x_3, x_4$ are an acceptable system of homogeneous coordinates we can write the restriction of $g$ in the form

$$b_1 x_1^2 + b_1 x_1^2 + b_1 x_1^2 + b_2 x_2^2.$$

But this is an indefinite quadratic form which represents zero in every $p$-adic field. (The only difficulty is with the $p \in \mathcal{O}$, 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 rational field; and this representation extends in an obvious way to a rational solution of $f = g = 0$. This completes the proof of the theorem.

References


Simultaneous representation by adjoint quadratic forms

by G. PALL (Baton Rouge, LA)

Dedicated to Professor L. J. Mordell

1. Introduction. Consider an r-ary quadratic form $f$ with real coefficients, and its adjoint form $f'$. 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 $f$ and $f'$ if there exist integers $x_i, x_i' (i = 1, \ldots, n)$ such that

$$m = \sum_{i=1}^{n} a_{ij} x_i, m' = \sum_{i=1}^{n} a'_{ij} x_i', \quad 0 = \sum_{i=1}^{n} a_i x_i.$$ 

The pair of column vectors $x = (x_i)$ and $x' = (x_i')$ 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 r-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 $f$ and $f'$, each set of primitive representations (a set being an aggregate $W x, W x'$, $W$ running over the unimodular automorphs of $f$) 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

$$m = a_1 + a_2 + a_3, \quad m' = a_1' + a_2' + a_3', \quad 0 = a_1 y_1 + a_2 y_2 + a_3 y_3,$$

where $m$ and $m'$ are coprime positive integers, is $24 g g'$, where $g$ and $g'$
denote the numbers of solutions \( t \) and \( t' \) of the respective congruences
\[
t' = -m' \pmod{m}, \quad t'' = -m \pmod{m}.
\]

As a second example, if \( m \) and \( m' \) are coprime positive odd integers, then the number of simultaneous and primitive solutions of
\[
m = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad m' = 3y_1^2 + 3y_2^2 + y_3^2 + y_4^2,
\]
with \( 0 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \), if \( m' \equiv 1 \pmod{3} \), and
\[
m = x_1^2 + x_2^2 + x_3^2 + 2x_4x_5 + 2x_6x_7, \quad m' = 3y_1^2 + 3y_2^2 + 2y_3^2 - 2y_4y_5 + 2y_6y_7,
\]
with \( 0 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \), if \( m' \equiv 2 \pmod{3} \), is equal to
\[
\begin{align*}
12, & \quad \text{if } m = m' = 1; \\
24h, & \quad \text{if } mm' \equiv 1 \pmod{4} \text{ and } mm' > 1; \\
48h, & \quad \text{if } mm' \equiv 3 \pmod{8} \text{ and } (-1 | m) = (m' | 3); \\
16h, & \quad \text{if } mm' \equiv 3 \pmod{8} \text{ and } (-1 | m) = -(m' | 3); \\
96h, & \quad \text{if } mm' \equiv 7 \pmod{8} \text{ and } (-1 | m) = (m' | 3); \\
0, & \quad \text{if } mm' \equiv 7 \pmod{8} \text{ and } (-1 | m) = -(m' | 3).
\end{align*}
\]
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 \( (x_1, \ldots, x_5) = 1 \), of
\[
m = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad m' = y_3^2 + y_4^2 + y_5^2 + y_6^2,
\]
with \( 0 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \), is equal to
\[
\begin{align*}
48, & \quad \text{if } mm' = 1; \\
96h, & \quad \text{if } mm' \equiv 1 \pmod{4}, 2 \text{ or } 3 \pmod{8}, mm' > 1; \\
64h, & \quad \text{if } mm' = 3 \pmod{8}; \\
0, & \quad \text{if } mm' = 0, 4, \text{ or } 7 \pmod{8}.
\end{align*}
\]

1. 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 \( \varphi = (x_1) \) and \( \varphi = (x_2) \) be primitive column vectors, with three components, such that \( \varphi' \varphi' = 0 \). \(^{(1)}\) Then there exists a unimodular

\[^{(1)}\] Notations. The superscript \( T \) 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 Adj \( T \) is the transpose of Adj \( T \). It should be recalled that if \( B = T' A T \), then Adj \( B \) = (Adj \( T \))\(^T\) (Adj \( A \)) (Adj \( T \)); and that Adj \( (T X) \) = (Adj \( T \)) (Adj \( X \)). Parentheses surrounding matrices may, for convenience of typing and printing, be sufficiently indicated as shown in (3).
real numbers $t, t', s$ are associated with the set of representations $W_{m'}$ and $W_{m''}$, where $W$ ranges over the unimodular automorphs of $\varphi$.

There are thus associated with every set of simultaneous and primitive representations of $m$ and $m'$ by $q$ and $q'$ 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 $q$ and $q'$. Indeed, for given $t, t', s$ we can find real numbers $q, q', r$, and $k$ such that

$$mq - t^2 = m', \quad m'q - t'^2 = m'd, \quad st - mw = t', \quad mk - s^2 = q',$$

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 $W'T$, where $W$ is any unimodular automorph of $A$. Then the first columns of $W'T$ with the third columns of $W'T$ constitute a set of simultaneous, primitive representations of $m$ and $m'$ by $q$ and $q'$, associated with $t, t', s$ and $s$.

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

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

$$t^2 \equiv -m' \pmod{m}, \quad -\frac{1}{2}|m| < t \leq \frac{1}{2}|m|;$$

$$t'^2 \equiv -md \pmod{m'}, \quad -\frac{1}{2}|m'| < t' \leq \frac{1}{2}|m'|;$$

$$st \equiv t' \pmod{m}, \quad s^2 \equiv -q' \pmod{m}, \quad -\frac{1}{2}|m| < s \leq \frac{1}{2}|m|;$$

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

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 $m, m', d$.


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 integer ternaries of determinant 1, it follows that the number 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 $q$ and $q'$, then as $W$ ranges over the unimodular automorphs of $q$, the vectors $Wx$ and $Wz'$ never repeat their pair of values for different $W$.

*Proof.* Since the $W$s form a group it suffices to show that $Wx$ and $Wz'$ 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 second column of $T$ equals the unique matrix determined by the condition that (8) and (10) are satisfied by

$$T'AT = t \quad \text{and} \quad T'AT' = t'$$

$$s \quad \text{and} \quad t' \quad m'.$$

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

As a second example consider the two positive classes of determinant 3, containing $f_1 = x_1^2 + x_2^2 + x_3^2$ and $f_2 = 2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2$ with the adjoints $f_1' = 3y_1^2 + 3y_2^2 + y_3^2$ and $f_2' = 2y_1^2 + 2y_2^2 + 2y_3^2 + 3y_4^2$. We assume $m$ and $m'$ positive, $(m, m') = 1$, $(m', 3) = 1$. Then the representations are by $f_1$ and $f_1'$ if $m' = 1 \pmod{3}$, and by $f_2$ and $f_2'$ if $m' = 2 \pmod{3}$. The number of primitive representations in each class is equal to $w$ times the number of solutions of

$$t \equiv -m' \pmod{m}, \quad t'^2 \equiv -3m \pmod{m},$$

$w$ (the number of unimodular automorphs) being 8 for $f_1$, 12 for $f_2$ (5).
II. \(m\)-ary quadratic forms

3. A theorem on integral matrices. We shall prove

Theorem 4. Let \(x\) and \(x'\) be primitive column vectors with \(n\) components, \(x^t x' = 0\). There exists a unimodular matrix \(T\) such that \(T^t x = x\) is the first column of \(T\) and \(x' = x\) is the last column of \(T^t = \text{Adj} T\). If \(T\) is one such matrix the most general is \(T X\), where

\[
\begin{pmatrix}
1 & a^t \\
X^t & \\
0 & U & \beta \\
& 0 & 1
\end{pmatrix}
\]

where \(U\) is any unimodular matrix of order \(n-2\), \(a^t\) and \(\beta\) 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 \(Q^t e_1 = e_1\), with \(e_1\) the first column of the identity \(I\). Then if \(Q^t = \text{Adj} Q\), \(x^t Q^t Q x' = 0\), whence the first element of \(Q x'\) is 0. Choose a unimodular matrix \(F\), with first row and column the same as those of \(G\), to satisfy \(F Q x' = e_1\), where \(e_1\) is the last column of \(I\). Then, if \(P = F Q\), \(P x' = e_1\) and \(P x' = e_1\). Hence the first column of \(T = P^{-1} x\) is \(x\) and the last column of \(T^t\) is \(x'\).

Since \(X^t X = I\), the Adjoint of \(X\) is

\[
\begin{pmatrix}
0 & 0 \\
\gamma & V \\
\delta & 1
\end{pmatrix}
\]

where \(V = U\), \(\gamma = -V a\), \(\delta = -V^t \beta\), and \(u + t = \beta^t V a\); hence \(T X\) and \(T^t X\) have the desired properties with \(T\) and \(T^t\). To prove that \(T X\) 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,

\[
T = (x \ Y \ z), \quad T' = (x' \ Y' \ z'), \quad S = (x_1 \ Y_1 \ z_1), \quad S' = (x'_1 \ Y'_1 \ z'_1),
\]

the \(Y\)'s being integral matrices with \(n\) rows and \(n-2\) columns. Since \(T^t T = I = S^{-1} S\), we have \(x^t x = 1, \quad y^t x = 0, \quad x^t x' = 0, \quad x^t y_1 = 0, \quad x^t z_1 = 1\), and hence

\[
\begin{pmatrix}
x' \\
1 & a^t \\
x^t & 0 & U & \beta \\
0 & 0 & 1
\end{pmatrix}
\]

where \(a, \beta, t,\) 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 \(W x\) and \(W x'\).

If \(T\) and \(T'\) have \(x\) and \(x'\) as first and last columns respectively, and \(m = x^t A x\) and \(m' = x'^t A' x'\), then \(B = T^t A T\) and \(B' = T'^t A' T'\) can be given the notations

\[
\begin{pmatrix}
m & x^t \\
1 & \beta \\
\end{pmatrix}
\]

where \(B_2\) and \(C_2\) are symmetric matrices of order \(n-2\); \(x, \beta, s,\) and \(t\) are numbers. We investigate what remains invariant in (14) when \(T\) is replaced by the "most general" matrix \(T X\), and hence \(B\) is replaced by

\[
\begin{pmatrix}
m & x^t U + a^t \\
1 + x^t t + s & \beta + m t
\end{pmatrix}
\]

and \(B'\) by

\[
\begin{pmatrix}
m & x^t U + a^t \\
1 + x^t t + s & \beta + m t
\end{pmatrix}
\]

Theorem 5. In the notation of (14), set

\[
G = m B_2 - x a^t, \quad F = m C_2 - \mu a^t.
\]

If \(T\) is replaced by \(T X\) and \(F\) by \(G\), and \(U\) are replaced by the equivalent matrices \(U^t G U\) and \(V^t F V\) respectively, where \(V = U\). Also,

\[
|G| = m^{n-1} m, \quad |F| = m^{n-2} m^{n-1}, \quad GF = FU = mm'd I_n, \quad \text{Adj} G = m^{n-1} F[c, d],
\]

where \(d = |A|\) and \(I_n\) is the identity matrix of order \(n-2\).

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

\[
(1 - m^{-1}(a^t U + a^t) - m^{-1}(1 + x^t \beta + m t)),
\]

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

\[
(1 - m^{-1}(a^t U + a^t) - m^{-1}(1 + x^t \beta + m t)),
\]
and accordingly (16) is replaced by $E' (= \text{Adj } E)$, 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 $d^{m'-m}$ is the value of the last determinant of order $n-1$ in $E'$, $m' = m|d^{m'-m}|$, and the first row of $E'$ is $(m' - d, 0)$. Next we apply $E'$ the transformation which differs from $I$ only in having the last row
\[ \begin{pmatrix} 0 & m' - d & (m' + m' V + m' \delta_1) \\ m & 0 & 0 \\ 0 & m' - d & 0 \\ 0 & 0 & m' \delta \\ 0 & 0 & m' \delta \\ 0 & 0 & m' \delta \end{pmatrix}, \]
and thus (applying the Adjoint to $E$) replace $E$ and $E'$ by
\[ \begin{pmatrix} m & 0 & 0 & m' - d & 0 & 0 \\ 0 & m' - d & 0 & 0 & m' - d & 0 \\ 0 & 0 & m' - d & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \end{pmatrix}. \]
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
\[ \begin{pmatrix} m & 0 & 0 & m' - d & 0 & 0 \\ 0 & m' - d & 0 & 0 & m' - d & 0 \\ 0 & 0 & m' - d & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \\ 0 & 0 & 0 & m' \delta \end{pmatrix}. \]
Since the product of these matrices is $dI$, we have in particular
\[ G_{\mu} + (m-\lambda \beta) m' = 0, \quad \mu^T (m-\lambda \beta) + (m' - \beta \delta) m' = -\bar{d} m. \]

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

\[ \begin{pmatrix} U \Sigma U^T, U \Sigma x + ma, V \Sigma a + m' \delta, l + x' \beta + m' \delta \end{pmatrix}, \]

which can be generated (as is evident from Theorem 4, and can be verified directly) from any particular quadruplet $(G, x, \mu, l)$ of the aggregate by use of an arbitrary unimodular $U$, arbitrary integer vectors $x$ and $\beta$, and an arbitrary integer $l$. Here $V = \text{Adj } U$ and $L = -U^{-1} \beta$.

Since the same matrices $B$ and $B'$ are derived from $Wz$ and $Wz'$, as from $x$ and $x'$, the entire set $Wz$ and $Wz'$ (with $l^T |d|$ ranging over the unimodular automorphs of $\varphi$) is associated with the same aggregate (20).

Conversely, for any given $G, x, \mu, l$, we can define $F$ by (18), $B_2$ and $C_0$ by (17), can solve for $l$ from (19), and for $x$ from (19). 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 $\varphi$ and $\varphi'$ associated with the quadruplet $(G, x, \mu, l)$, and with the aggregate (20) which it generates. But if $A$ and $B$ are not equivalent, no representation of $m$ and $m'$ by $\varphi$ and $\varphi'$ is associated with $(G, x, \mu, l)$.

Consider (20) with $U$ fixed. We can choose $\alpha$ and $\beta = (-U \delta)$ uniquely so that — the inequalities being satisfied by each component
\[ -\frac{1}{2} |m| < U^T x + ma < \frac{1}{2} |m|, \quad -\frac{1}{2} |m'| < V^T x + m' \delta < \frac{1}{2} |m'|. \]

For this choice of $\alpha, \beta, l + x' \beta + m'$ is uniquely determined modulo $m$. Thus every aggregate of quadruplets contains one $(G, x, \mu, l)$ in which (componentwise)
\[ (21)\quad -\frac{1}{2} |m| < x < \frac{1}{2} |m|, \quad -\frac{1}{2} |m'| < \mu < \frac{1}{2} |m'|, \quad -\frac{1}{2} |m| < l < \frac{1}{2} |m|. \]

Two quadruplets $(G, x, \mu, l)$ and $(G, x, \mu, l')$ 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
\[ (22)\quad (x_1 - U^T x_1) / m, \quad (x_1 - U^T x_1) / m' \text{ and } (x_1 - U^T x_1) / m' \text{ are integral, } \delta \text{ denoting the quotient } (a_1 - U^T a_1) / m'. \]

For a given matrix $G$, the set of all triplets $(x, \mu, l)$ satisfying (21) and (22) for some $U$, derived from a given triplet $(x_1, \mu_1, l_1)$, 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 quartic form $\varphi$ and its adjoint $\varphi'$ 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 $\varphi$.

If $\varphi$ has an integral matrix the possible values for $G, x, \mu, l$ are greatly restricted. Then $m$ and $m'$ are integers, $B$ and $B'$ are integral, and $x$ and $\mu$ are integral solutions of the congruences
\[ (23)\quad x \equiv 0 \pmod{m}, \quad \mu \equiv 0 \pmod{m}. \]

Here $G$ is an integral matrix of determinant $m'^{-1} m'$, 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 $m^{-1} G$, $m'^{-1} G$
has the index of \( A \). Also, \( F = d(\text{Adj}(G))/m^{n-1} \) must be integral. And the genus of \( G \) must allow (23) to be solvable.

By (19a), \( \mu \) must satisfy the additional congruence

\[ \tag{24} \mu \mu = 0 \pmod{m'}, \]

and for each pair of vectors \( \alpha \) and \( \mu \), \( \lambda \) must satisfy

\[ \tag{25} \lambda = \mu \mu \pmod{m}; \]

and \( \lambda \) is then determined as an integer vector by

\[ \tag{26} \lambda = (\lambda - \mu \mu) m. \]

On substituting this expression for \( \lambda \) into (19a) we obtain

\[ \tag{27} \mu \mu = \mu \mu \pmod{m} = \mu \mu \pmod{m}. \]

Hence \( \mu \) must also satisfy the congruence

\[ \tag{28} \mu \mu = \mu \mu \pmod{m}. \]

and \( \mu \) must also satisfy

\[ \tag{29} \mu \mu = \mu \mu \pmod{m}. \]

Then \( \lambda \) 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 each \( p \) 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 \( \lambda \) of (23) are primitive modulo \( m \), and (25), being equivalent to

\[ \lambda = -\alpha \mu \pmod{m}, \]

has the unique solution \( \lambda = -\alpha \mu \pmod{m} \). This satisfies (29) since \( \alpha \mu = \mu \mu \pmod{m} \).

For each suitable matrix \( G \) we may consider the solutions \( \lambda \) and \( \mu \) modulo \( m \), and \( \mu \) 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 \( s \) 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 (63)).

**Theorem 7.** Let the representations \( x \) and \( x' \) be associated in the preceding algorithm with the quadruplet \((G, \kappa, \mu, l)\). Let \( \Sigma_1 \) denote the subgroup of unimodular automorphs \( W \) of \( \varphi \) such that \( W x = x \) and \( W x' = x' \). Let \( \Sigma_2 \) denote the subgroup of unimodular automorphs \( U \) of \( G \) such that

\[ \tag{30} U T = x \pmod{m}, \quad U T \mu = \mu \pmod{m}, \]

\[ \mu = \mu \pmod{m}. \]

There is a one-one correspondence between the sets \( \Sigma_1 \) and \( \Sigma_2 \).

**Proof.** Notice that in (30), \( x \) and \( \mu \) may be considered only modulo \( m \) and \( m' \) respectively, and that it is not necessary to assume (21). For if \( \mu \) is replaced by \( \mu + m' \), where \( \tau \) denotes an integral vector, then \( x' = (x' - V T \mu) \pmod{m} \). \( m' \) is increased by \( \mu \) since \( \mu \) is divisible by \( m \) by (29), \( x' = x' \pmod{m' \mu} \). Hence, \( \mu \pmod{m} \) is a consequence of (30), and (30) is a consequence of (30), (30), and (30).

Consider Adjoint unimodular transformations \( T = (x Y x) \) and \( T' = (x Y' x) \) replacing \( A \) by \( B \) and \( B' \) (in (14)). If \( W x = x \) and \( W x' = x' \), then \( W T \) and \( W T' \) also have \( \alpha \) and \( \alpha' \) as first and last columns respectively. By Theorem 4, \( W T = T X \), and hence \( X = V T \). \( V T \) is a unimodular automorph of \( B \), of the type displayed in (11). On forming \( X = X X' = B \) and \( X' \), we have (compare (14), (15), and (16))

\[ \tag{31} U T G = T \pmod{m}, \quad \mu = \mu \pmod{m}, \quad \mu = \mu \pmod{m}, \quad \mu = \mu \pmod{m}. \]

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

Conversely, let \( U T G = G \) and let (30) hold. Then we can define integral vectors \( \alpha \) and \( \beta \), and an integer \( l \), 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 \( \delta \), since \( B' = B \delta \). Hence \( X \) is a unimodular automorph of \( B \), and \( W = X T X' \) is a unimodular automorph of \( A \) such that \( W x = x \) and \( W x' = x' \).

This establishes the one-one correspondence. We do not need the property, nor do we doubt that, the correspondence is preserved under multiplication.

The number \( v \) of elements in \( \Sigma_1 \) may be finite or infinite, but the index, which we will denote by \( s \), of \( \Sigma_1 \) within the group of all unimodular automorphs \( U \) of \( G \) is finite. Indeed, \( s \) is equal to the number of
incongruent triples \((s, \mu, \ell)\) to respective moduli \(m, m', m''\) in a \(G\)-set.

If the number \(w\) of automorphs \(U\) of \(G\) is finite, \(w = w(e)\). If also the number \(w\) of automorphs \(W\) of \(A\) is finite, then by Theorem 7,

\[
\frac{1}{w} \sum_{x \in W} \sum_{y \in W} \sum_{z \in W} = \frac{\mu}{w}
\]

If \(w\) is finite, the weight of the representation \(x\) and \(x'\) (by \(y\) and \(y')\) is defined to be \(1/w\). By (32), the sum of the weights of the representations in a set \((W_x \times W_{x'})\) is \(1/w\). Now \(v\) is finite, even though \(w\) may be infinite, provided \(v\) is finite. It is consistent and natural to define the weight of a set of representations \((W_x \times W_{x'})\) to be \(1/v\), if \(v\) 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 one-equivalent matrices \(A_1, \ldots, A_s\) with a set of one-equivalent matrices \(G_1, \ldots, G_s\), each \(G_i\) being accompanied by one or more \(G_i\)-sets. For example, if \(A_1, \ldots, A_s\) are representatives (one from each class) of a given determinant \(d\), then \(G_1, \ldots, G_s\) will be certain matrices previously characterized. If \(A_1, \ldots, A_s\) 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 triple of solutions \((s, \mu, \ell)\) of the system of congruences with \(G = G_i\) will be such that the matrices \(B_i\) constructed therefore are in the prescribed genus, and one must specify those solutions.

Let the numbers \(w_1\) of unimodular automorphs of the \(G_i\) be assumed finite \((i = 1, 2, \ldots, s)\). 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 \(g(G_i)\) denote the number of incongruent triples \((s, \mu, \ell)\) obtained with \(G = G_i\), and such that the corresponding matrix \(B_i\) is equivalent to one of \(A_1, \ldots, A_s\). Then, summing up from (32), we have

\[
\sum_{i=1}^{s} A_i(m, m') = \sum_{i=1}^{s} g(G_i)/w_i.
\]

If the numbers \(w_1, \ldots, w_s\) of unimodular automorphs of \(A_1, \ldots, A_s\) 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 \(x\) denote \(f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2\) or \(f_2 = x_1^2 + x_2^2 + x_3^2 + 2x_2x_3 + 2x_2x_4\), which (17) are forms of the two classes of positive classical 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 \(f_2 = 3y_1^2 + 3y_2^2 + 2y_3^2 + 2y_4^2 + 2y_5^2\) represents no \(3k + 1\).

We shall assume \((m', 3) = 1\), whence all simultaneous representations will be by \(f_1\) if \(m' = 1\) mod \(3\), and by \(f_2\) if \(m' = 3\) mod \(3\). We also assume that \(m\) and \(m'\) are positive, odd, and relatively prime.

Let \(x\) denote the binary quadratic form of matrix \(G\). The solvability of \(x = G(\text{mod } m)\) fixes the characteristic \((x, p)\) of \(x\) for any odd prime \(p\) dividing \(m\). We noticed above that no prime factor of \(m\) may divide the four elements of \(G\). By \((14), p = 3\) \(\text{Adj } G\) \(_{(x)} = m'\).

If \(m'\) and \(m\) could have a common prime factor \(p\), \(p\) would divide the last determinant of order \(s - 1\) in \(B\), here equal to \(3m\). Since, for binaries, \(G\) and \(\text{Adj } G\) are equivalent, the solvability of \(3x = G(\text{mod } m)\) implies that \(x\) is primitive modulo \(m'\), and that \((x, p) = (-1, 3p)\) for every odd prime \(p\) in \(m'\). Thus the generic characters of \(x\) 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 \(m = m'p_1p_2\ldots p_s\) as a product of (not necessarily distinct) primes. If \(x\) is properly primitive, the condition is that the product of the generic characters \((x, p_i)\) shall equal 1 if \(m = m'p_i\) \(\text{mod } 4\), and \((-1, x)\) if \(m'p_i\) \(\text{mod } 4\). This merely assigns the value of the generic character \((-1, x)\) if \(m'p_i\) \(\text{mod } 4\), but in view of the preceding values of \((x, p_i)\), imposes the condition

\[
(x, m) = (-1, m)\quad \text{if} \quad m = m'p_1p_2\ldots p_s\quad \text{and} \quad x = p_1p_2\ldots p_s.
\]

If \(x\) is improperly primitive, the condition is that the product of the symbols \((x, p)\) shall equal 1. This reduces as follows:

\[
(x, m) = (-1, m)\quad \text{if} \quad m = m'p_1p_2\ldots p_s\quad \text{and} \quad x = p_1p_2\ldots p_s\quad \text{for} \quad x = p_1p_2\ldots p_s.
\]

In particular there are no simultaneous representations of \(m\) and \(m'\) by \(f_1\) and \(f_2\) if \(m = 3\) mod \(4\) and \(m' = 1\) mod \(4\); and there are no simultaneous representations of \(m\) and \(m'\) by \(f_1\) and \(f_2\) if \(m = 1\) mod \(4\) and \(m' = 7\) mod \(8\).

Let \(A_i\) denote the number of classes in the properly primitive genus of determinant \(mm'\) with the generic characters designated above, if \(mm' = 1\) mod \(4\) or if \(m' = 5\) mod \(4\); and let \(B_i\) denote the number of classes in the similarly designated improperly primitive genus, if \(mm' = 3\) mod \(4\) and \(m' = 5\) mod \(4\).

Also let \(g\) denote the number of distinct odd primes dividing \(m\) and \(w\) the number dividing \(m'\).

For either of these genera there exists in the class of \(x\) a form which is congruent coefficientwise to \(-x_1^2 - x_2^2\) (mod \(m'\)) and to \(-x_1^2 - x_2^2\) (mod \(m'\)).
(mod m^2). Then if x^T and y^T are given the notations (b_1, b_2)
and (m, m_0), (23) becomes

\[ \begin{align*}
& b_1 = 1, \quad b_2 \equiv 0, \quad b_3 \equiv 0 \pmod{m}, \\
& m_1 = 0, \quad m_2 = 0, \quad m_3 = 9 \pmod{m}. 
\end{align*} \]

Hence b_1 has 2^r residues mod m, while b_2 = 0; m_0 has 2^r residues mod m',
while m_0 = 0. Both (24) and (25) are seen to be automatically satisfied.

To sum up, there are 48·2^{r+1}·2^{r+1} such simultaneous and primitive repre-
sentations of m and m by p and q if mm' = 1 mod 4, or if mm' = 3 mod 8
and (m') = (−1 mod m). There are 48·2^{r+1}·(b_1 + b_2)/2 such representa-
tions if mm' = 7 mod 8 and (m') = (−1 mod m). There are 48·2^{r+1}·
×b_3/2 such representations if mm' = 3 mod 8 and (m') = (−1 mod m).

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

\[ h = \begin{cases} 
2^{r+1} b_1 & \text{if } mm' = 1 \pmod{4}, \\
2^{r+1} & \text{if } mm' = 3 \pmod{4},
\end{cases} \]

and, if mm' = 3 (mod 4),

\[ h = \begin{cases} 
b_1 & \text{if } mm' = 3, \\
2 - (2 | m') & h_2 \text{ if } mm' > 3.
\end{cases} \]

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

The result stated in the Introduction readily follows.

References

[5] Any table of positive ternary quadratic forms; e.g. B. W. Jones, Bul-
letin 97 National Research Council. or see G. Pall, Bull. Amer. Math. Soc.,
47(1941), pp. 641-650.
[7] This follows from the fact that the minimum cannot exceed (mm')^{1/4}, hence
must be 1, and from the corresponding result for ternaries.

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

\[ x^p - y^q = 1 \]

has only the obvious solutions \((x, y) = (2, 3)\) for all pairs of prime
numbers \(p\) and \(q\) except for the pair \(p = 2, q = 3\), for which also \(x = ±3, y = 2\) are solutions. Up to the present this has been proved only for
certain special pairs \(p, q\); the case \(p = q = 3\) 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 Oblath [9] has shown, at most one solution. If \(x, y\) is the solution,
then [5]

\[ x = 0 \pmod{q^2}, \quad y = -1 \pmod{q^2} \]

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

\[ 2^q \equiv 2 \pmod{q^2}. \]

As of the primes not exceeding 200183, [10], only 1093 and 3511 fulfill
(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 \(p, q\).