Nach (46) bekommt man also für $0 < q \leq b - a$

\[(340) \quad a^{-1}S(a, b) \leq (a/q)^{1/2} + (q/a)^{1/2} + (q/a^{1/2} + (a^{1/2}q)^{1/2}).\]

Hierzu bemerken wir, daß wegen (49) und (50) die Ungleichung

\[(341) \quad (a/q)^{1/2} \leq (a/q)^{1/2} \quad für \quad 0 < q \leq b - a\]

gilt.

Nun sei speziell
\[q = a^{1/2}t^{-1/2}.\]

Dann stimmen die beiden ersten Terme auf der rechten Seite von (340) überein. Wenn also außerdem $q < b - a$ ist, so folgt in Verbindung mit (341)

\[(342) \quad a^{-1/2}S(a, b) \leq (at)^{1/2} + (at)^{1/2} + (a^{-1/2}t^{1/2}).\]

Dies gilt aber auch im Falle $q > b - a$, da dann aus (49) und (50) mit der trivialen Abschätzung

\[a^{-1/2}S(a, b) \leq q + 1 = a^{1/2}t^{-1/2} + 1 \leq (at)^{1/2}\]

damit ist (342) unter den Voraussetzungen (49) und (50) bewiesen. Nun folgt aber aus (339)

\[(ar)^{1/2} \leq a^{1/2}t^{1/2},\]

Im Falle $a > t^{1/2}$ ist

\[(ar)^{1/2}a^{-1/2} = a^{1/2}t^{1/2} \leq t^{1/2},\]

und wegen $a \geq 1$ ist jedenfalls

\[(a^{-1/2}t^{1/2}) \leq t^{1/2} \leq a^{1/2}t^{1/2}.\]

Die Abschätzung (336) folgt also im Falle $a > t^{1/2}$ aus (342). Im Falle $a < t^{1/2}$ ist (336) trivial.

Wegen (48) ist damit unser Hauptsatz bewiesen.

Literaturverzeichnis


Reçu par la Réduction le 27. 2. 1953

On the genera of quadratic and hermitian forms over an algebraic number field

by V. C. NANDA (Bombay)

§ 1. Introduction. Pursuing the study of the theory of genera of quadratic forms initiated by Gauss, Minkowski [6] defined a genus of rational integral quadratic forms, in any number of variables, to consist of all forms which are equivalent in the real number field and modulo all positive integers. He then showed that all forms in a genus have the same signature, determinant $s$ and class mod $s^2$, and that these finitely many invariants determine a genus completely. C. L. Siegel [7] gave an alternative proof of this result, and also obtained a finite set of genus invariants for forms with coefficients in an algebraic number field [8].

The converse problem of proving the existence of a genus of rational integral quadratic forms with prescribed invariants was also solved by Minkowski. H. Braun [1] later gave another set of invariants and a solution of the corresponding converse problem. She [2] also extended the results of Minkowski to hermitian forms over an imaginary quadratic extension of the rational number field.

In this paper we consider quadratic and hermitian forms over an arbitrary algebraic number field. We prove that a genus of hermitian forms can be defined by means of a finite set of invariants. We also prove the existence of genera of quadratic and hermitian forms with prescribed invariants. We use the methods of H. Braun in the proof of our results.

The main difficulty in this discussion is caused by the fact that, unlike in the case of the rational number field, the ring of integers in an algebraic number field is not, in general, a principal ideal domain, so that it is also necessary to take into account singular matrices. For this purpose, the reciprocity formula for Gauss sums (an important tool in the proof), is generalized to cover the case of singular matrices (Lemma 5). This formula appears to be of interest, independently of the application that we make of it.
Our results can be applied to simplify, and to generalize to arbitrary quadratic or hermitian forms over any algebraic number field, a formula originating in the work of Gauss, and proved for totally definite forms over totally real fields by Siegel [8], Lemmas 92, 93. This formula constitutes an important step in the proof of Siegel's main theorem. We hope to give this generalization elsewhere. The author wishes to express his sincere thanks to Professor K. G. Ramanathan for constant encouragement and guidance throughout the preparation of this paper.

§ 2. Notation and definitions. Let $K$ be an algebraic number field with an automorphism $\tau$ satisfying $\tau^2 = 1$ the identity automorphism. Let $k$ be the fixed field of $\tau$. If $\tau = 1$, then $k = K$. If $\tau \neq 1$, $K$ is the field of rational functions of the square root of a number $a + b\sqrt{d}$, where $a, b \in k$. Let $\mathfrak{d}$ and $\mathfrak{D}$ denote respectively, the rings of integers in $k$ and $K$. We choose $d \in \mathfrak{d}$, not divisible by the square of an integer, other than a unit. In case $\tau = 1$, we always assume that $d = 1$.

Let $\mathfrak{a}$ denote the extension to $K$ of an ideal in $k$ briefly denoted as a $k$-ideal. For an integral $k$-ideal $\mathfrak{a}$, denote by $R(\mathfrak{a})$, the residue class ring $\mathfrak{D}/\mathfrak{a}$. It is easy to see that $\tau$ gives rise in a natural way to an automorphism of $R(\mathfrak{a})$. We denote this automorphism also by $\tau$.

Let $R$ denote any of the rings $K$, $\mathfrak{D}$, $R(\mathfrak{a})$. Let $S = (\mathfrak{a})$ be a matrix with $s_1 \in R$ (we use the notation $S \in R$ to express this fact, the number of rows and columns being, in general, understood from the context). If $S = \bigoplus S'_{\tau}$, then $S$ is defined to be a hermitian matrix (h-matrix), and the expression $S'[X] = X'AX$ a hermitian form (h-form); here $X'_\tau = (x_1, ..., x_n)$ is a row varying over $R$ (in particular, therefore, $S$ has $m_n$ rows and columns). In the particular case when $\tau = 1$, $S$ is symmetric (s-matrix) and $S[X]$ is a quadratic form (q-form). In the following, the statements about h-forms will, in general, include statements about q-forms.

Let $S[X]$, where $X' = (y_1, ..., y_m)$ be another h-form in $R$. We say that $S$ represents $T$ in $R$ or that $S[T]$ represents $T[X]$ in $R$ (all statements made about h-matrices are also assumed made about h-forms), if there exists a matrix $C \in R$ such that $S[C] = T$. $C$ is called a representation of $T$ by $S$ in $R$. If $T$ also represents $S$ in $R$, then we say that $S$ and $T$ are equivalent in $R$ (or $S \sim T$ in $R$). This is an equivalence relation and a class in $R$ is defined to be a complete set of equivalent matrices.

In $R$, all equivalent matrices have the same rank, called the rank of the class. It may be shown as in [2], Lemma 5, that if further, every ideal in $R$ is a finite $R$-module, generated by $r$ elements, then in every class of rank $m$, there is a matrix of $r_m$ rows. If $R$ is a field of characteristic either zero, or coprime with $2d$, then there is a diagonal matrix of $m$ rows in a class of rank $m$.

For a matrix $A \in R$, a matrix $E_A \in \mathfrak{D}$ is called a right unit (r-unit) if rank $r(E_A)$ of $E_A = r(A)$ and $AE_A = A$. For a left unit (l-unit), similarly defined, we use the notation $E_A^\tau$. Siegel [8], Lemma 9) has proved the existence of these units. For an r-unit $E_A$ and an l-unit $E_A$ of $A = \mathfrak{D}$, the unique solution $X$ in $K$ ([8], Lemma 12) of $AX = E_A$, $E_A X = X$ is called the parallel $E_A E_A \tau$ inverse of $A$. We denote this matrix by $A^{-1}$ if there no danger of confusion. For $A \in R$ of rank $m$, $\delta(A) = $ determinant of $A$ is defined to be the ideal generated by all the $m$-ranked subdeterminants of $A$. For an h-matrix $S$, $\delta(S)$ is a h-ideal.

Let $S, T \in R$ be two h-matrices. A representation $B$ of $T$ by $S$ in $R$ is called an $E_B E_T$ reduced representation if $E_B E_T = B$. Any representation $B$, one can construct a reduced representation $B = E_B E_T E_T$. A matrix $U \in \mathfrak{D}$ is called (a) unimodular if $|U| \neq 0$, and $U^{-1} \in \mathfrak{D}$, (b) primitive if $|U| = 1$ and (c) primitive modulo an integral $k$-ideal $\mathfrak{a}$ if $|U|, a = 0$.

We adopt the notation $k^{(1)}, ..., k^{(n)}$ for the $r_1$ real and $k^{(r_1 + l_1)}, k^{(r_2 + r_1 + l_1)}, ..., k^{(r_1 + r_2 + \cdots + r_l)}$ for the $r_2$ conjugate-complex pairs of conjugates of $k$. For a $k$, $k^{(0)}$ denotes the conjugate of a belonging to $k^{(0)}$. In case $\tau = 1$, we further, the notation is chosen that $d^{(0)} < 0$ for $0 \leq l \leq r_1$. Define

$$ r - \begin{cases} r_1 & \text{if } \tau \neq 1, \\ r_1 & \text{if } \tau = 1. \end{cases} $$

For a matrix $A = (\mathfrak{a}) \subset A$, $A^{(0)}$ is defined to be $(a_{00})$.

Let $S \in K$ be an h-matrix. Let $\text{rg}(S) = m$, so that $S \sim T$ in $K$, where $T = (t_1, ..., t_m)$ is the diagonal matrix with $t_1, ..., t_m$ on the diagonal, $|T| \neq 0$ and $t_1 \neq 0$, then for $1 \leq i \leq m$, let $w_i, \eta_i$ denote respectively the number of positive and negative elements of $T^{(0)}$. We define $\text{sg}(S) = \text{the system of signatures of the h-matrix } S$ by

$$ \text{sg}(S) = \{(w_1, \eta_1)_{t_1 = 1, ..., t_m}, \text{ or briefly, } (w_1, \eta_1). $$

For a number $c \in k$, $\text{sg}(a)$ is defined by

$$ \text{sg}(a) = \left\{ \begin{array}{ll} a^{(0)} & \text{if } a > 0, \\ \eta \text{ or } a^{(0)} & \text{if } a < 0. \end{array} \right. $$

Let $S \in K$ be an h-matrix of rank $m$. Let $T$ be a non-singular matrix such that $T = \left[ \begin{array}{cc} T & 0 \\ 0 & A \end{array} \right]$, $A = \mathfrak{D}$. Let $B$ denote the matrix of the first $m$ rows of $A$. Then $T = \tau[B]$. It can be shown as in [8], Lemma 31, that the class of the ideal $\delta(B)$ is uniquely fixed by $S$. We call it the ideal class of $S$. Also fixed uniquely, therefore, is the set $\langle T, \alpha \rangle$, $\alpha \in K$, or briefly $\langle T \rangle$, called the kernel of $S$, denoted by $\mathfrak{K}(S)$. 


$h$-matrices $S, T \in K$ are said to belong to the same genus if and only if $S \sim T$ modulo all integral $k$-ideals and $\text{sig}(S) = \text{sig}(T)$.

In this section, we prove several lemmas, which we use later in the proof of the main theorem in \S 4.

Lemma 1. Let $S, T \in \mathcal{O}$ be $h$-matrices of rank $m$. Let $\delta(S) = \delta(T) = s_0$. Let $q$ be a $k$-ideal such that $4q^2 | q$. Let $p$ be the extension to $K$ of a prime ideal in $k$ (briefly called a $k$-prime ideal), and let $p^n | q$ (i.e., $p^n | q$ and $p^{n+1} | q$ with rational integral $a \geq b$). Then $S \sim T$ modulo $p^l \sim T$ modulo $p^{l+1}$ for $l > a + 1$.

Proof. Let us suppose $C_1$ is an integral matrix satisfying
\begin{equation}
S(C_1) = T \cdot p^l,
\end{equation}
$E_0 C_1 E_T = C_1$.

Let $S^{-1}$ denote the $E_0 E_T$ inverse of $S$, $C_1^{-1}$ the $E_0 E_T$ inverse of $C_1$, and $S_1 = S(C_1) - T$. From (3.1), $S_1 p^l$ and $E_0 S_1 E_T = S_1$. Define
\begin{equation}
C_{l+1} = C_1 - S^{-1} C_1^{-1} S_1.
\end{equation}

Then $S(C_{l+1})$ modulo $p^{l+1}$ and $C_{l+1}$ is $E_0 E_T$ reduced. Also, since $l \geq a + 1$, the denominators of elements of $C_{l+1}$ are coprime with $p$.

By repeating the procedure $a$, we see that $S$ represents $T$ modulo $p^{l+1}$.

Interchanging the roles of $S$ and $T$, we get the lemma.

Lemma 2. Let $S, T, s_0$ be as in Lemma 1. Let $p$ be a $k$-prime ideal such that $p \not| 2s_0$. In case $\tau = 1$, let us assume further that $K(S) = K(T)$.

Then $S \sim T$ modulo $p$.

Proof. Case I: $\tau = 1$. The result follows trivially from [8], Lemma 56.

Case II: $\tau = 1$. We may, without loss of generality, assume $S, T$ to be diagonal matrices. So that let $S = [s_1 \ldots s_m]$, $T = [t_1 \ldots t_m]$ where $s_i, t_i \in \mathcal{O}$. Further, $p, s_i \in \mathcal{O}$.

Then we have that for a prime ideal $p$ $\not| (2s_i)$, every element of $q$, which is coprime with $p$ is congruent mod $p$ to the relative norm of an element in $\mathcal{O}$. This is shown exactly as in [3], \S 47.

This completes the proof of Lemma 2.
their respective determinants. Then \( (a_1, \ldots, a_t) = b \). Since \( S = T[A] \),
the matrices \( T[A_k] \) are all integral, and therefore \( A_k \) are all integral.
The result follows from the fact that \( \beta b = \ldots = a_1 a_1 a_2 \).

This finishes the proof of Lemma 4.

In the remainder of this section, we restrict ourselves to the case \( r = 1 \). We prove here a reciprocity formula for generalized Gauss sums, defined below; deriving it from a general \( \theta \)-transformation formula.

Let \( S = (a_i) \in k \) be an \( s \)-matrix. Let \( a \) be an integral ideal satisfying
1) \( a \mid m \) and \( 2a \) are integral for all \( i, j \) if \( a \mid b \), and
2) if \( a \mid b \) and \( a \not\mid \) is integral then \( a \mid b \). The ideal \( a \) is then called the
denominator of the \( s \)-matrix \( S \) (den \( s \)).

Let \( g \in k \) such that \( gb = ab^{-1} \), \( a, b \) coprime integral ideals and \( b \)
the different of \( b \). For an \( s \)-matrix \( S \) such that \( \text{den} (S) = a \), we define the
Gauss sum (see [3]) \( G \) by

\[
G = \sum_{X \mod b} \exp \left( 2 \pi \sigma (g b(X)) \right)
\]

where the sum is over a complete set of incongruent \( \mod b \) columns \( X \),
satisfying \( b \mid X \), \( b \) being an \( r \)-unit of \( S \). This is a generalization of the
Gauss sum for non-singular \( S \). It is independent of the choice
of the representative \( X \) of the residue class \( \mod b \) and the \( r \)-unit \( b \).
It has the following properties, which are simple to prove.

(i) Let the matrix \( B \) be either primitive \( \mod b \) satisfying \( b \mid B \),
or unimodular. Then \( G = G \).

(ii) Let \( b \) be an odd integral ideal (i.e. \( b \not\mid 2 \)). Then \( G = G \).

(iii) Let \( b \mid b \). Then \( G = G \).

(iv) Let \( b = b \) with \( b, c = 0 \) and \( c \). Let \( a, c \) be integral
ideals such that \( b_a = (a), a \mid k \) and \( (a, c) = 0 \). Define \( b = \sigma \).

Then \( G = G = G \).

We now derive the reciprocity formula for the Gauss sums from the
general \( \theta \)-transformation formula. The denominator of an ideal \( \theta \)
(den \( \theta \)) is defined to be an ideal \( c_1 \) such that \( c_1 \) is integral and prime
to \( c_1 \). The system of indices of an \( s \)-matrix \( S \) (ind \( S \)), is defined to be the
set \( (i) \) where \( f_i = u_i - c_1 \) if \( \sigma \).
We notice here that

\[
\sum_{X \mod a} \exp \left( 2 \pi \sigma (g b(X)) \right)
\]

where \( \text{sgn} (g) = (a_i), \text{ind} (S) = (a), \delta \), \( \sigma = \text{den} (b) \), and \( a \in \text{den} (b) \) and \( a \in \delta \) is such that \( a \) is integral and prime to \( a \).

Proof. Corresponding to \( S \), \( \sigma \), \( 1, \ldots, r, \sigma \), we define \( D \) as
follows. Let \( S = T[A] \), \( A \in k \), \( A \not\mid 0 \), \( |T| = 0 \).

For \( 1 \leq r \), define \( D \) to be a real positive symmetric solution of
\( \sum_r b^r \sum_r b^r = T \), and for \( 1 \leq \sigma \), define \( D \) to be a positive
hermitian solution of \( \sum_r b^r \sum_r b^r = T \). These solutions are known
to exist. Now define \( D \) for \( 1 \leq r \), \( D \) for \( 1 \leq \sigma \).

Clearly \( D b^r \sum_r b^r = \sigma \) and \( D \sigma \sum_r b^r = D \). For <t>0</t>, \( \sigma \) an
integral ideal; \( Y \in k \) a column satisfying \( b \mid Y \), \( \xi = \sum \xi a_i \) is a basis of \( \sigma \) and \( \xi, \xi_1, \ldots, \xi_n \) are arbitrary real numbers; define

\[
\sum_{X \mod \xi} \exp \left( - \pi \sigma (P(X + Y)) \right) + 2 \pi \sigma (g b(X + Y)) \right)
\]

where \( \sigma \) now denotes the trace in the obvious sense.

Define \( X_1 = A X \), \( X_1 = A X \)

where \( A \) is defined in (3.3). Let \( N(a) = \sigma \). Then the set of all \( X_1 \),
contains all \( m \)-rowed columns \( a \), and is contained in the set of
integral \( m \)-rowed columns \( Z \). This proves i) the set of all \( X_1 \) form a lattice \( L \)
of dimension \( 1 \), and ii) the sum (3.4) converges absolutely, since

\[
\sum_{X \mod \xi} \exp \left( - \pi \sigma (Q(Z)) \right)
\]

for \( Q > 0 \) (see [3]). Thus

\[
\sum_{X \mod \xi} \exp \left( - \pi \sigma (Q(Z)) \right)
\]

Applying the well known \( \theta \)-transformation formula for non-singular matrices, we get

\[
\theta = \theta \}

\[
\sum_{X \mod \xi} \exp \left( - \pi \sigma (Q(Z)) \right)
\]

for \( Q > 0 \) (see [3]). Thus

\[
\sum_{X \mod \xi} \exp \left( - \pi \sigma (Q(Z)) \right)
\]
where

$$
\Phi(t, E) = \prod_{e=1}^{n} \left( t^{e} - 2\sqrt{2} t^{e-1} - 2^{e-1} \right) \cdot \prod_{e=1}^{n} \left( t^{e} + 2^{e-1} \right) \cdot \prod_{e=1}^{n} \left( t^{e} + 4 \sqrt{2} t^{e-1} \right) \cdot \prod_{e=1}^{n} \left( t^{e} + 4 \right),
$$

where the signs of the square roots are chosen so as to be positive when the quantities are real and positive, \( \delta(L) \) is the discriminant of the lattice \( L = a^{-n}N(g(b)^{3}) \), and \( \bar{L} \) is the lattice complementary to \( L \). Now if \( P' = A^{-1} g^{-1} \) where \( A^{-1} \) is the inverse of \( A \), using (3.5) we have the general \( \theta \)-transformation formula

(3.8) \( \theta (S, P'; g, \bar{L}, \phi(T), \bar{Y}) = N(\bar{L}^{-1} g^{-1} \bar{b}^{-1} \bar{b}^{-1} \bar{b}^{-1} \bar{L} \bar{T} \bar{Y}) \times \exp \left( -2 \pi \sum_{\omega, \mu \in \mathbb{Z}, \omega \neq \mu} \left( \frac{t^{(\omega - P' - 2\bar{b}^{-1})} - 2\bar{b}^{-1} \bar{Y}}{t^{-1} + 4|\bar{c}|^{-2}} \right) \right) \).

Now consider \( \tau \)-transformation \( \tau (S, P; g, \bar{L}, \phi(T), \bar{Y}) \). Taking the limit as \( t \to \infty \) and using (3.8), we get for the usual way (see [1]), the result of Lemma 5.

By an argument similar to that in [1], formula 8, p. 37 we get

**COROLLARY 1.** Let \( S(C) = T, C \in \mathcal{C}, \bar{E}_{0} \mathcal{C}_{2} = \mathcal{C}, \delta (C) = C \). Let \( \phi \) be as in Lemma 5. If \( \left( \text{den} (\frac{1}{2} \frac{1}{2} \frac{1}{2} \frac{1}{2} C) \right) = 0 \), then

$$
\tau (S, T) = N(C) \cdot \tau (S, T).
$$

**§ 4. The Genus theorem.** In this section, we prove our main result, concerning the existence of a genus of \( h \)-forms with given invariants.

**THEOREM.** Suppose that we are given the following:

i) a natural number \( m \),

ii) a set of pairs of non-negative rational integers \( (u_{i}, v_{i}) \) for \( i = 1, \ldots, m \), or equivalently \( f_{i} = w_{i} - v_{i} \) and \( u_{i} + v_{i} = m_{i} \),

iii) integral \( h \)-ideals \( a \) and \( q \) satisfying \( \delta \bar{S} \mathcal{B} \psi \) and \( q \), where \( \mathcal{B} \) is defined in (3.5),

iv) a set \( \langle (\phi_{q}) \rangle = \left\{ \begin{array}{ll}
\psi \in \mathbb{K} & \text{if } \psi = a \mathcal{B} \psi \mod q, \quad (x, q) = \mathbb{D} \text{ if } \tau = 1, \\
\psi \in \mathcal{B} \psi & \text{if } \tau = 1
\end{array} \right\} \)

where the representative \( \psi \) satisfies \( \sigma(x) = -1 \), \( q_{h}^{-1} \in \mathbb{C} \) with \( (S, q) = \mathbb{D} \), and

v) a class \( \mathcal{S}(q) \) of \( h \)-matrices modulo \( q \), where the representative \( \mathcal{S} \) is chosen \( m \)-rowed, integral.

Then there exists an integral \( h \)-matrix \( S \in \mathcal{S}(q) \), such that

$$
\tau (S) = m, \quad \delta (S) = a, \quad \sigma (S) = \langle (u_{i}, v_{i}) \rangle, \quad K (S) = \langle \phi_{q} \rangle
$$

if and only if

(4.1) \( \left| S \right| = a \mathcal{B} \psi \mod q, \quad x \in K, \quad (x, q) = \mathbb{D} \).

and, in addition, if \( \tau = 1 \),

(4.2) \( \theta (S, T) = \exp \left( \frac{m}{4} \sum_{i} \phi_{q, i} \right) N(2a q^{n} g^{-1} \bar{b}^{-1} \bar{Y}) \frac{1}{| \mathbb{D} |} \left( \frac{\mathcal{B} \psi \mod q}{| \mathbb{D} |} \right)^{m} \),

where

(4.3) \( \phi \in \mathcal{B}, \quad g = g^{-1}, \quad (g, \mathcal{S}) = 0, \quad \sigma (g) = \{ q_{1} \}, \quad \omega \in \mathcal{B} \) is such that \( \omega d \) is integral and prime to \( g \), and \( \omega \) is the generalised Jacobi symbol.

**Remark.** As a result of this theorem, the invariants uniquely determine a genus, namely the genus containing \( S \). The uniqueness follows from the fact that if \( S \in \mathcal{S}(q) \) has rank \( m \) system of signatures \( (u_{i}, v_{i}) \), discriminant \( a \), and kernel \( \langle \phi_{q} \rangle \), then \( S \) and \( S' \) are in the same genus, in view of Lemma 5.

For the proof of the theorem, we need

**LEMMA 6.** Let \( S, \langle (\phi_{q}) \rangle, q \) have the same meaning as in the conclusion of Lemma 5. Let \( m \geq 2 \), let \( \mathcal{C} \in \mathcal{C} \) be searchable and let \( | \mathcal{S} | = a \mathcal{B} \psi \mod q \) with \( (x, q) = \mathbb{D} \). Let \( (a) = a_{1} a_{2} \) where \( a_{1} a_{2} \) are \( k \)-ideals satisfying \( (a_{1}) = D \) and \( a_{1} \) is divisible only by such prime ideals as already divide \( q \). In case \( m = 2, \tau = 1 \), we further assume that \( a_{1} \) is a \( h \)-prime ideal and \( -a_{1} \equiv q^{2} \mod q_{a_{2}} \).

Then there exists \( S_{1} = S \mod q \), such that \( S_{1} \) represents a primitive \( \mathcal{B} \psi \mod q_{a_{2}} \) for any natural number \( b \) and

$$
| S_{1} | = a_{1} a_{2} \mathcal{B} \psi \mod q_{a_{2}}, \quad (x_{1}, q) = \mathbb{D}.
$$

**Proof of Lemma 6.** As in [1], define \( D = \begin{pmatrix} \delta_{1} & 0 \\ 0 & B \end{pmatrix} \), where \( B \) is the \( (m-1) \)-rowed identity matrix. Let \( \lambda, \mu \in \mathcal{B} \) satisfy

(4.4) \( \lambda \equiv 0 \mod q^{2}, \quad \mu \equiv 0 \mod q \),

Define

(4.5) \( S_{1} = S \lambda + \mu D \).

We will show that this is the required \( S_{1} \).

In view of the meaning of \( \lambda, \mu \), we have, trivially, \( S_{1} = S \mod q \) and

(4.6) \( \left| S_{1} \right| = \left| a_{1} a_{2} \mathcal{B} \psi \mod q_{a_{2}} \right|, \quad (x, q) = \mathbb{D} \).

Let \( a_{1} = h a + \mu. \) From (4.6) we have \( | S_{1} | = a_{1} a_{2} \mathcal{B} \psi \mod q_{a_{2}} \), also \( (x_{1}, q) = \mathbb{D} \). To complete the proof of the lemma, we have only to show that \( S_{1} \) represents a primitive \( \mathcal{B} \psi \mod q_{a_{2}} \).
Let us assume for a moment that \( D(Y) = \alpha \mod q^2 \), with \( Y \) primitive mod \( q \). Further, by hypothesis, \( \delta[X] = \alpha \mod q \), with \( X \) primitive mod \( q \). It is easy to see that with \( \lambda, \mu \) as defined in (4.1), \( \delta[X + \lambda X + \mu Y] = \alpha \mod q \) and \( \Lambda X + \mu Y \) is primitive mod \( q \). Thus to prove that \( S \) represents a primitive mod \( q \), we have only to show that \( D \) represents a primitive mod \( q \).

Next let us assume that
\[
\sigma_0 y_1 y_1 + y_2 y_2 = \alpha \mod q^2, \quad (y_1, y_2, \alpha_0) = \mathcal{O}.
\]

Then \( D(Y) = \alpha \mod q^2 \) has a primitive solution \( Y = \begin{pmatrix} y_1 \\ y_2 \\ 0 \\ \vdots \end{pmatrix} \).

Thus in order to prove Lemma 6, we have only to prove that (4.7) has a solution. We prove this by induction on \( b \).

Let \( b = 1 \). We have to show, since \( a = 0 \mod q \), that
\[
\sigma_0 y_1 y_1 + y_2 y_2 = 0 \mod q, \quad (y_1, y_2, \alpha_0) = \mathcal{O}.
\]

Now let \( \alpha_0 \) be chosen coprime with \( q \), and then (4.8) will have a solution if \( \alpha_0 = \sigma \mod q \), where
\[
\sigma = \begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix}.
\]

Now let \( b > 1 \) and let
\[
s_0 s_0^2 + s_1^2 = \alpha \mod q^2, \quad (s_0, s_1) = \mathcal{O}.
\]

Let \( \alpha = \sigma_0 \) be an integer satisfying \( (\sigma_0, \sigma_0^2) = \mathcal{O} = (\sigma_0^2, \sigma_0) \). Substituting \( \sigma_1 + \sigma_2 - \alpha \) for \( \sigma_1 \) in (4.9), we have
\[
s_0 s_0^2 + s_0^2 \cdot \sigma_1 + (s_0 + s_0^2 - \alpha) (s_0 + s_0^2 - \alpha) = \sigma_0 s_0^2 + s_0^2 \cdot \sigma_0 + (s_0 s_0^2 + s_0^2 + \alpha) \mod q^2.
\]

So our result would be proved if we can choose \( \sigma_1, \sigma_2 \) to satisfy
\[
\sigma_1 + \sigma_2 = \alpha \mod q.
\]

Since \( (2, \alpha) = \mathcal{O} \), there exists \( \delta \in \mathcal{O} \), such that
\[
(s_0 s_0^2 + s_0^2 - \alpha) \alpha^2 \cdot \delta = \mod q^2.
\]

Consider now the congruence
\[
\sigma_0 s_0^2 + s_0^2 \equiv \delta \mod q.
\]

This is a congruence in \( \sigma_0, s_0 \), with \( (s_0, s_0) = \mathcal{O} \), and therefore has a solution in \( \mathcal{O} \). Passing to the conjugates, the same \( \sigma_0, s_0 \) give a solution of \( s_0 s_0^2 + s_0^2 \equiv \delta \mod q \). Together, then the congruences give us (4.10).

This completes the proof of Lemma 6.

Proof of the theorem.

Remark. For the proof of the theorem, we may, whenever necessary, choose \( \mathcal{D} \) suitably in its equivalence class \( \mathcal{D} \mod q \) or its residue class \( \mathcal{D} \mod q \).

To prove that the conditions (4.1) and (4.2) are necessary, let \( S \in \mathcal{C} \) satisfy \( r(S) = r_1, \delta(S) = s_0, \delta(S) = m, \delta(S) = (u_0, v_0) \), \( E(S) = \mathcal{C} \), and
\[
|S| = |SF| = \mathcal{C} \mod q, \quad (|S|, q) = \mathcal{C}, \quad \mathcal{C} \in E(S) = \mathcal{C}.
\]

By Lemma 4, there exists a matrix \( C \in \mathcal{C} \) such that
\[
S = S_0 S_0 [C], \quad |S_0| = 0, \quad (|S_0|, q) = \mathcal{C}, \quad \mathcal{C} \in E(S_0) = \mathcal{C}.
\]

From (4.11) and (4.12),
\[
S = S_0 (S_0 [C]) \mod q.
\]

Now \( C \mathcal{D} \) is non-singular and \((C \mathcal{D}, \mathcal{D}) = (C, \mathcal{D}) \mod q \). Further, in view of Lemma 4, \( |S_0| (|C|, \mathcal{D}) \) is integral. Let \( \mathcal{D}_1 \mathcal{D}_1 = \mathcal{D} \mathcal{D}_1 \mathcal{D}_1 \mod q \), \( (\mathcal{D}_1, \mathcal{D}_1) = \mathcal{C} \mod q \). Putting \( S_0 = S_0 [|C|] \), \( (|S|, q) = \mathcal{C}, \quad \mathcal{C} \in E(S_0) = \mathcal{C} \), we get
\[
|S| = |S_0| \mathcal{C} \mod q, \quad (|S|, q) = \mathcal{C}.
\]

Let \( \alpha = \sigma_0 \) be defined as in (4.3), then in view of (4.11),
\[
G(\mathcal{Q}, S) = G(\mathcal{Q}, S_0).
\]

Applying Lemma 5 to \( G(\mathcal{Q}, S_0) \), we have, in view of the above equation and properties of \( S_0 \),
\[
G(\mathcal{Q}, S) = \exp \left( \frac{i \pi}{4} \sum_{f \in \mathcal{Q}} \exp \left( \frac{2 \pi i}{q^2} \sum_{x \mod \mathcal{Q}} \sum_{y \mod \mathcal{Q}} \sum_{x^2 + y^2 = x^2 + y^2} \right) \right).
\]

where \( \omega + k \) is such that \( \omega \) is integral and prime to \( q \). Now \( S_0 \) is \( D \) (diagonal) \( \mathcal{Q} \), and \( |S_0| = \mathcal{Q} \), so that the Gauss sum on the right of (4.14) equals \( \frac{|D|}{|D|} \cdot \mathcal{Q} \). Next since \( (\mathcal{Q}, q) = 0, |D| = |q^2 \mod q \) \( \mathcal{Q} \), we see that \( (|D|, q) = 0 \). Substituting in (4.14), we see that (4.2) is satisfied.
We now show that conditions (4.1) and (4.2) are sufficient for the existence of the matrix $S_i$ with given properties. The proof proceeds in several steps.

Step I. We show that it suffices to prove the theorem for the case $u_l > 0$ for $l = 1, \ldots, r$.

Let $|S| = s_0 x^2 \pm q$ where $q \in \mathbb{Q} \cap k$ (in view of (4.1)). Let $S_1 = S + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ where $g_1 \neq 0, g_1 \in \mathbb{Q} \cap k$. Then $|S_1| = s_0 x^2 \pm q + g_1 \delta_1$, where $\delta_1$ is the leading $(m-1)$-subdeterminant of $S$; and we may, without loss of generality, assume $\delta_1 \neq 0$, since $S$ is determined only modulo $q$. Also $g_1 \in \mathbb{Q}$. Let $a \in \mathbb{Z}$ be chosen coprime with $\mathbb{Z} \cap g_1 \mathbb{Z}$, then there exists $b \in \mathbb{Z}$ such that $q + g_1 b \delta_1 = 0 \mod (a)$. Define

$S_a = S + \begin{pmatrix} 0 & 0 \\ 0 & b \delta_1 \end{pmatrix}$

then

$S_a = S \mod q, \quad |S_a| = s_0 x^2 \mod (a), \quad G(q, S_a) = G(q, S)$.

Thus we may start with $S$ such that

$|S| = a \cdot x^2 \mod (a), \quad (x, a) = \mathbb{Z}$

where $a \in \mathbb{Z}$ satisfies $(a, d_0 g_1 \mathbb{Z}) = \mathbb{Z}$. This 'a' may be chosen in such a way that it has any system of signatures, prescribed in advance.

We may assume that $u_l = 0$ for $l = 1, \ldots, p_l < q \in \mathbb{Q}$ (there is nothing to prove if $p_l = 0$). Choose 'a' above satisfying $a^{(l)} < 0, \ldots, a^{(p_l)} < 0$ and $a^{(p_l+1)} > 0, \ldots, a^{(m)} > 0$. Write $sgn(a) = (g_1)$. Consider now the system $m_i = m \cdot f_i, f_i = h_i g_1, \frac{m_i}{f_i} \text{ is positive, } S^* = a S, \quad g_i = a \cdot g_1, \quad q^* = a^m q, \quad \text{where } c = m+1 \text{ or } m+2 \text{ according as } m \text{ is odd or even (so that } c \text{ is always even)}. \quad \text{If } f_i^m = p_i (S_i) \text{ is the product of all } k \text{-prime ideal divisors of } 2 \mathbb{Z} \cap g_1 \mathbb{Z}, \text{ then } \mathbb{Z} \cap g_1 \mathbb{Z} \cdot (a) = \mathbb{Z} \cap g_1 \mathbb{Z} \cdot (a) \text{ if } m > 0, \text{ otherwise } \mathbb{Z} \cap g_1 \mathbb{Z} \cdot (a) = \mathbb{Z} \cap g_1 \mathbb{Z} \cdot (a)$.

i.e. $a^m |S| = a^m a \cdot g_1 \mathbb{Z} \mod a^{m+1} q$, and therefore by Lemma 1 (using the results in case of one variable)

$|S|^* = a^m |S| = s g_1 \mathbb{Z} \mod q, \quad (a, q) = \mathbb{Z}$

so that condition (4.1) is satisfied by the 'system'.

Let now $r = 1$. Define $g^* = a^{-c} g$ with $q$ as in (4.3), so that (since $c$ is even), $sgn(g^*) = (g) = (q)$. Using property (iii) of Gauss sums $\mu_3$, we get

$G(g^*, S^*) = |X(a)|^m G(a g^*, S)$

From (4.3) (since $q \mid a^{m-1} q$)

$G(a g^*, S)$

$= \exp \left( \sum_{l=1}^{r} \frac{\pi i}{g} J_k \right) \cdot \exp \left( \frac{1}{g} \sum_{g_1 \in \mathbb{Z} \cap g_1 \mathbb{Z}} \left( \frac{-a^m q}{g} \right) \right)^{m}$

From (4.16), (4.17) we see that the 'system' satisfies condition (4.2).

Thus the 'system' satisfies the condition of the theorem, and has further the property that $u_l > 0$ for $l = 1, \ldots, r$.

Suppose now that the theorem is proved for the 'system', i.e. there exists an integral $h$-matrix $S_i \sim S^*$ mod $q^*$ satisfying $r(S_i) = m, \text{ind}(S_i) = (f_1), \delta(S_i) = m_0 g_1, K(S_i) = (g)$. Define

$S_0 = a^{-1} S_i$

then $r(S_0) = m_0, \text{ind}(S_0) = (f)$, $\delta(S_0) = m_0 g_1, K(S_0) = (g)$ and

$S_0 \sim S \mod a^{m} q^*$. (4.19)

(4.19) implies $S_0 \sim S \mod q$, since $q \mid a^{m} q^*$. We have only to show that $S_0$ is integral. In view of (4.18) and the assumption that $S_i$ is integral, $S_0$ can have only prime ideal divisors of $(a)$ in the denominator; on the other hand, in view of (4.19), since $S$ is integral and $a \mid a^{m} q^*$, $S_0$ cannot have any prime ideal divisors of $(a)$ in the denominator. Thus $S_0$ is integral. Thus for $m > 2$, it is enough to prove the theorem for the case $u_l > 0, l = 1, \ldots, r$. We make this assumption in the sequel.

Step II. Let $m = 2, r = 1$. We show that it suffices to prove the theorem for the case $(a, q) = (\text{cont } S, q)$, where $\text{cont } S - \text{content of } S = \text{the ideal generated by all the elements of } S$.

We first show that $S$ may be chosen in its class mod $q$ to satisfy $(a, q) = (\text{cont } S, q)$; where $(S)$; $\psi$. We can take $a_0 = 0$, by choosing $S$ properly in its congruence class mod $q$. Let $p_1, \ldots, p_r$ be all the distinct prime ideals that divide $(a, q)$. Let $(\text{cont } S, q) = a = p_0^m \cdot p_i^m, \text{ where } a_0 > 0$. Let $p_i^m = (2), a_i > 0 \text{ for } i = 1, \ldots, t$. We may assume that for $i = 1, \ldots, j-1, p_i^{m+1} = (a_2)$; so that $p_i^m = (a_2)$ if $(p_i, 2) = 0$ for $i = 1, \ldots, j-1$. Let $j-1$ refer to the case when $p_i^{m+1} = (a_2)$ for $i = 1, \ldots, j$. If $j = 1$, there is nothing to prove. Let, therefore, $j-1 < t$. We prove our result by induction on $j$.

The unimodular transformation

$(4.20) \quad a_1 \rightarrow a_1, \quad a_2 \rightarrow b_1 + a_1, \quad p_1 \cdots p_{j-1} | (b), \quad (p_j, b) = 0$
changes the first coefficient to $a_1 + p b_4 a_2 + 2 b_6 a_2$. Consider the following two cases:

First case: $p^{1+e_1+1} \equiv (a_2)$. Choose $b$ in (4.26) in such a way that $p^{1+e_1+1} \equiv (2a_2 + b_6 a_2)$. Then $p^{1+1+1} \equiv (a_2 + b_4 a_2 + 2 b_6 a_2)$ for $i = 1, \ldots, j$.

Second case: $p^{1+1+1} \equiv (a_2)$. Then $p^{1+1} \equiv (a_2)$ and therefore $p^{1+1} \equiv (a_2)$ for $i = 1, \ldots, j$.

Thus we have proved that $S$ may be chosen in its class mod $q$ to satisfy $(a_1, q) = (\text{cont}(S), q) \cdot b$ where $b \mid (2)$.

Remark 1. This transformation holds for any $m$, though we prove it here only for $m = 2$.

Remark 2. If $S$ is chosen to satisfy the above condition, then it follows in view of (4.1) that for any prime ideal $p \mid q$ and for a natural number $b$, $p^b \equiv (a_2)$ implies $p^b \equiv q$.

Now let $D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Let $m^* = m = 2$, $f^* = f_i (i = 1, \ldots, r_j)$. $S^* = S[D]$, $e_2^* = 4 a_2$, $e_3^* = 4 a_2$, $q^* = 4 q$. Clearly $G = p(a_2) = p$, $4 a_2$ mod $q$ if $e_2^* a_3^* = a_2^*$ is coprime with $q^*$ and $\text{sgn}(e_2^*) = (1, -1)^{(m^*)/2}$. Also from (4.1), $e_2^* a_3^* = a_2^* mod e_2^*$, $(a_2^*, q^*) = 0$.

So that the 'system' satisfies condition (4.1). Next let $q^* = \frac{1}{2} q$ with $q$ as in (4.3), then since $\text{den}(q^* S^{-1}) \mid \text{den}(q S^{-1})$ and $S^* = a_2^* a_3^* + q^*$, $q^* \equiv q^*$ (from (4.21)). We have $\text{den}(q S^{-1})$, $2 = 0$. Therefore, by Corollary 1 of Lemma 3, we have

$$G(q^*, S^*) = X[D] \cdot G(q^*, S).$$

Substituting $q^*$ for $q$ in (4.2), observing that $q^*$ satisfies the conditions (4.3), and comparing with (4.2), we see that the 'system' satisfies the Gauss sum condition. Further, $(\text{cont}(S), q^*) = (a_2, 2a_2, 2a_2, a_2) = (a_2, q) = (2a_2, a_2)$ in view of Remark 2 above. Therefore, since $(a_2, q) = (\text{cont}(S), q) \cdot b$ and $b \mid (2)$, we have

$$\text{cont}(S), q^*) = (\text{cont}(S), q) \cdot b, 2 a_2, 2 a_2, 4 a_2 = (a_2, q) \cdot b, 2 a_2, 2 a_2, 4 a_2.$$
Let \( sa_1 - a_z \) be the condition. Then view of the foregoing, \( sa_1^{-1}a_z^2 \) is an integer. This we have shown that we may assume that we started with an \( S \) satisfying

\[
S = \begin{pmatrix}
    sa_1 & 0 \\
    0 & sa_2
\end{pmatrix} = (a_1^{-1}a_z^{-1} a_2)^{-1} \begin{pmatrix} a_2 & 0 \\
0 & a_1
\end{pmatrix}.
\]

Also \( (d_4) = p \), \( (b_2, p_4) = 0 \) (since \( p \) divides \( \epsilon \)) implies \( p \mid q \) in view of (4.1). Finally since \( (p, a_2) = 0 \), we see that \( p \mid (b_2) \).

Thus we have shown that \( S \) may be chosen in its equivalence class mod \( q \) to satisfy conditions (i), (ii), (iii) and (iv) of step III.

We now show that \( \frac{-a_1}{b_2} = \frac{a_2}{b_2} \). Let \( q \) satisfy (4.3) and \( (a_1, p b_2) = 0 \). In view of (4.25),

\[
G(q, S) = G(q, a_1) G(q, a_2).
\]

Now \( (a_1) = p \beta_1 \), \( (b_2, p_4) = 0 \) and \( (a_2) = a_2 \). Define

\[
\beta_2 = (b_2, G)^{-1}.
\]

Then by Lemma 5 (in view of (4.25)),

\[
G(q, S) = \exp \frac{1}{4} \sum_{a_1} \epsilon(a_1 - 1) \left( \text{N}(2a_1q_a^2 - b_2a_2) \times \sum_{a_2 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{-a_1a_2}{q_a^2} \right) \right) \right) 
\]

where \( a_1 \) is integral and prime to \( p b_2 \). And with the same \( \sigma \),

\[
G(q, S) = \exp \left( \frac{1}{4} \sum_{a_1} \epsilon(a_1 - 1) \right) \left( \text{N}(2a_1q_a^2 - b_2a_2) \times \sum_{a_2 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{-a_1a_2}{q_a^2} \right) \right) \right).
\]

From (4.2), (4.26), (4.28) and (4.29), noticing that \( \sigma \) in (4.2) may be chosen to be the same as in (4.28), we have

\[
\left[ \frac{a_1}{a_2} \right] \left( \frac{-a_1}{b_2}, 1 \right)^\frac{1}{4} = \text{N}(b_2^{-1}a_2) \cdot L \cdot M
\]

where \( L \) and \( M \) stand for the Gauss sums on the right of (4.29) and (4.28) respectively. Now \( (p b_2, q) = 0 \). Let \( \text{G}(a_1, p b_2, q) = (a_1), (b_2, p b_2, q) = 0 \), \( \beta_2 = a_2 \sigma(a_1a_2^{-1})^{-1} \). Then by property (iv) of the Gauss sums (§ 3),

\[
M = \left( \sum_{a_1 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) \left( \sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( \frac{-a_1a_2}{q_a^2} \right) \right) \right)
\]

similarly with \( \beta_2 = 4^{-1}a_1^{-1}a_2 \).

\[
L = \left( \sum_{a_1 \text{ mod } p} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) \left( \sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( -\frac{a_1a_2}{q_a^2} \right) \right) \right).
\]

Now

\[
\sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( -\frac{a_1a_2}{q_a^2} \right) \right) = \frac{\sigma}{\epsilon} G(1, 1, 1),
\]

\[
\sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( -\frac{a_1a_2}{q_a^2} \right) \right) = \frac{\sigma}{\epsilon} G(1, 1, 1)
\]

so that since (in view of (4.25)), \( a_1 = a_2, \) (4.30)--(4.33) give,

\[
\left( \sum_{a_1 \text{ mod } p} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) \left( \sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) = \text{N} b_2 ^{\frac{1}{2}}.
\]

Now \( (p, b_2) = 0 \). Let \( b_2 b_2 = (a_1), (b_2, p b_2) = 0 \), \( \beta_2 = a_1^{-1}a_2^{-1} = 4^{-\frac{1}{2}} q_a^2 \). Then by property (iv) of the Gauss sums (§ 3),

\[
\sum_{a_1 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \left( \sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) = \text{N} b_2 ^{\frac{1}{2}}.
\]

Now \( b_2 = b_2 \). The square of an odd ideal, so that

\[
\sum_{a_1 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) = \text{N} b_2 ^{\frac{1}{2}}
\]

and \( \sigma \) is integral. From (4.34), (4.35) and (4.36), therefore,

\[
\left( \sum_{a_1 \text{ mod } p b_2} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) \left( \sum_{a_2 \text{ mod } q} \exp \left( 2\pi i \sigma \left( \frac{a_1a_2}{q_a^2} \right) \right) \right) = \text{N} p
\]

and from property (ii) of the Gauss sums (§ 3), and \( a_1 a_2 = a_2 b_2 \), it follows therefore that the left side of (4.37) is \( \left[ \frac{s_2}{p} \right] \cdot \text{N} p \). This implies that

\[
\left[ \frac{-a_1}{b_2} \right] = -1.
\]

Thus we have shown as a result of steps I, II and III that in case \( m \geq 2 \), it is enough to prove the theorem for \( w_1 > 0 \) (i. e. 1, ..., r) and further
in case $\tau = 1, m = 2$ that we may take $s_{12} \geq 0, (s_{11}) = ap$ where $a = (\text{cont}_S, q)$, $p$ is a prime ideal satisfying $(p, 2a) = 0$,
\[ S = \begin{pmatrix} s_{12} & 0 \\ 0 & s_{11} \end{pmatrix}, \quad p \not| (s_{12}) \quad \text{and} \quad \begin{pmatrix} -s_{12} \\ 0 \end{pmatrix} p = 1. \]

Step IV. Let $m \geq 2$. We show that it suffices to prove the theorem for the case $m > 0$ (i.e., $\tau = 1$) and $s_{12} = 1$.

In case either $m > 2$ or $m = 2$ and $\tau \neq 1$, we may choose $s_{11}$ in its congruence class mod $q$ to satisfy
\[ s_{11} \geq 0 \quad \text{and} \quad (s_{11}, q) = 0. \tag{4.38} \]
This can be achieved by adding to $s_{11}$, a suitable positive rational integer $\epsilon q$, noticing the fact that $(q, q) = 0$. In case $\tau = 1$ and $m = 2$, (4.38) may be assumed satisfied as a result of step III. Define
\[ D = \begin{pmatrix} s_{12} & 0 \\ 0 & s_{11} \end{pmatrix} \]
and $S^*$ by
\[ S^*[D] = s_{11} S, \tag{4.39} \]
and consider $m^* = m, s_{11}^* = s_{11}$ and $s_{12}^* = v_1$ for $l = 1, \ldots, r, q^* = s_{11}^{-1} q$, $\delta^* = s_{11}^{-1} s_{12} = s_{11}^{-1} s_{11}$. Then $w^* = v_1 = 2; 4d_2 q^* | q^*$, where $q^* = p(|s_{11}|)$; $\text{sgn}(s_{11}) = \text{sgn}(s_{11}) = (\epsilon, q^*) = (\epsilon, q^*) = 0.$

Let $(s_{12}) = a_0 b$ where $a_0$ and $b$ are $k$-ideals satisfying $(b, q) = 0$ and $a_0$ is divisible only by such $k$-prime ideals as already divide $q$. In case $m = 2$ and $\tau = 1$, we further have $a_0 = a = (\text{cont}_S, q)$ and $b = 2$-prime ideal $p$ satisfying
\[ \begin{pmatrix} -s_{12} \\ 0 \end{pmatrix} p = 1. \quad \text{Thus by Lemma 6, in view of (4.1) and the fact that $S$ represents $s_{12}$ primitively mod $q$, there corresponds, to a natural number $b$ an $\mathbf{L}$-matrix $S_b = S \bmod q$ such that $S_b$ represents $s_{12}$ primitively mod $qb^2$, that is $S_b$ is equivalent mod $qb^2$ to a matrix with $s_{12}$ as the first element, and}
\]
\[ |S_b| = a_0 b^2 \quad \text{mod $q^2$,} \quad (x, q) = 0. \tag{4.40} \]
Thus we may already assume $S$ to satisfy (4.40). Then by Lemma 1 (using the result in case of one variable),
\[ |S^*| = s_{12} a_0 b^2 \quad \text{mod $q^2$,} \quad (x, q^*) = 0. \tag{4.41} \]
Thus the `system' satisfies the congruence condition (4.41).

Now let $\tau = 1$. Define $\phi^* = s_{11}^{-1} \phi$, where $\phi$ satisfies (4.3) and $(s_{11}, q) = 0$. By Corollary 1 of Lemma 5 and (4.39),
\[ G(\phi^*, s_{11} S) = G(\phi^*, S^*[D]) = N(s_{12}) G(\phi^*, S^*). \tag{4.42} \]

The condition in the corollary viz. \[ |\text{det}(s_{12}^{-1} \phi^* s_{11}^{-1} S^{-1})|, s_{12} \bmod q \] is satisfied in view of (4.41), exactly as in step II. On the other hand
\[ G(\phi^*, s_{11} S) = N(s_{12}) G(s_{12} \phi^*, S). \tag{4.43} \]

From (4.2), (4.42) and (4.43), it follows that the Gauss sum condition is satisfied by the `system'.

Thus the `system' satisfies the conditions of the theorem and we have the additional properties $s_{12}^l > 0$ for $l = 1, \ldots, r$ and $s_{12} = 1$.

Suppose now that the theorem is proved for the `system', i.e. there exists an integral $k$-matrix $S^*$ satisfying
\[ S^*[U] = S^* \bmod q^*, \quad B_{S^*} U = U, \quad U \text{ primitive mod $q^*$}, \quad r(S^*) = m^*, \quad \text{sgn}(S^*) = \langle a_0^*, v_1 \rangle, \quad \delta(S^*) = a_0^*, \quad K(S^*) = \langle s_{11}^* \rangle. \tag{4.44} \]

Then (4.44) and (4.39) give
\[ S^*[UD] = s_{12} S \bmod q^*. \tag{4.45} \]
Now $\delta(U D_i) = (s_{12})$ and $s_{12}^t | q^*$. Thus in view of [8], Lemma 26, there exists an integral matrix $D_i$ satisfying
\[ B_{S^*} D_i = D_i, \quad \delta(D_i) = (s_{12}) \tag{4.46} \]
and
\[ U D = D_i U_1, \quad U_1 \text{ primitive mod $q^*$} \quad \text{and} \quad B_{S^*} U_1 = U_1. \tag{4.47} \]
Define
\[ S_0 = s_{12}^t S^*[D_i]. \tag{4.48} \]
$S_0$ is integral in view of (4.45), (4.47) and (4.48) exactly as in step I. It is easy to see that $S_0$ satisfies all the other requirements.

We have thus proved that for $m \geq 2$, it is enough to prove the theorem for the case $m > 0$ (i.e., $\tau = 1$) and $s_{12} = 1$.

Step V. Completion of the proof by induction.

Let $m = 1$. If $s_{12}$ and $q$ are as defined as in the theorem and if $\mathbf{C}^{-1} = (a_0, b)$, then
\[ S_0 = \begin{pmatrix} s_{12} a_0^* & s_{12} a^* b \\ s_{12} b^* & s_{12} b b^* \end{pmatrix} \tag{4.49} \]
easily be seen to satisfy $r(S_0) = 1, (S_0) = s_{12}$, $K(S_0) = \langle s_{12} \rangle$, $\text{sgn}(s_{12}) = (\epsilon, 1)$. Also $S_0$ is integral. Finally $S_0 \sim S_0 \bmod q$ and (4.1) together imply $S_0 \sim S_0 \bmod q$.

Now let $m \geq 2$, and let us assume the theorem proved for $m - 1$. We will show that it holds for $m$, with $s_{12} = 1$ and $w > 0$ for $l = 1, \ldots, r$. Define
\[ E = \begin{pmatrix} 1 & s_{12} & \ldots & s_{1m} \\ 0 & 0 & \ldots & 0 \end{pmatrix}. \tag{4.50} \]
Then $F$ is unimodular and
\[(4.49) \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \rho \end{pmatrix} [F].\]

Consider $m^* = m - 1$, $u_l = u_l - 1$ and $q_l = q_l$ for $l = 1, \ldots, r$, $a_l \rightarrow s_l$, $s^*_l = s_l$, and $q^* = q$. Then $u_l^* + v_l^* = m^*$, $a_l^* = \mathbb{C}$ and $(C, q^*) \sim C$, $4d^* | q^*$ since $\mathbb{Q} = \mathbb{P}$, and $\text{sgn}(s_l) = (-1)^{q_l}$ since $v_l = v_l$. (4.1) is satisfied by the 'system' in view of the fact that $|S| = |S^*|$ (see (4.49)).

Now let $r = 1$. By property (i) of the Gauss sums and (4.49), we have
\[(4.50) \quad G(q^*, S) \cdot G(q^*, 1)^{-1} = G(q^*, S^*),\]
where $\rho^* = \rho$ satisfies (4.3). Substituting, for $G(q^*, S)$ from (4.2) and for $G(q^*, 1)$ from Lemma 5, in (4.50), we see that the 'system' satisfies the Gauss sum condition.

Thus the 'system' satisfies all the conditions of the theorem and $m^* = m - 1$. Therefore by the induction assumption there exists an integral $l$-matrix $S_l \sim S$ mod $q^*$ such that $r(S_l) = m - 1$, $s_l(S_l) = (u_l - 1, v_l)$, $d(S_l) = s_l$, $E(S_l) = s_l$. Then
\[S = \begin{pmatrix} 1 & 0 \\ 0 & S_l \end{pmatrix}\]
can easily be seen to have all the required properties.

This completes the proof of the theorem.

References


On the diophantine equation $y^2 - k = x^2$

by

W. Ljunggren (Oslo)

1. Let $k$ denote any rational integer. The problem of solving the equation
\[(1) \quad y^2 - k = x^2, \quad k \neq 0\]
in rational integers $x, y$ has been the subject of many papers and has attracted great interest for more than three centuries. However, no general method is known for determining all solutions of a given equation of the form (1). A summary of earlier results is given in a paper by T. Nagell [8] and in two papers by O. Hemer [3], [4]. Cf. L. J. Mordell [6] for the history of this and allied problems.

It is well-known that the solution of (1) can be brought back to the solution in rational integers $u, v$ of a finite number of equations of the type $f(u, v) = 1$, where $f(u, v)$ is a binary cubic form with integral coefficients. By virtue of a famous theorem due to A. Thue [15] the equation (1) has only a finite number of solutions for a given $k$.

These cubic forms have negative or positive discriminants according as $k > 0$ or $k < 0$. In case $k > 0$ one has solved all equations with $k < 100$. An essential tool in obtaining this result is the use of the theorems due to T. Nagell and B. Delaunay [8] concerning cubic forms with negative discriminant. In case $k < 0$ is the problem much more difficult since there are not yet general theorems as to the representations of 1 by binary cubic forms with positive discriminant. Cf. Ljunggren [5].

It was shown by Mordell [7] that the diophantine equation
\[(2) \quad y^2 = 4u^2 - 2g_1 u - g_2,\]
where $g_1$ and $g_2$ are given rational integers, has at most a finite number of rational integral solutions $(u, v)$, when its right-hand side has no squared factor in $u$. He proved that to every integral solution $(u, v)$ of (2) there corresponded a binary quartic with invariants $g_1$ and $g_2$, which represented unity, and conversely.

In (1) we have $g_1 = 0$, $g_2 = -4k$, and the problem is to find all representations of 1 by certain binary, biquadratic forms having