Table des matières du tome XIII, fascicule 4

S. J. P. Gilman, A bound on the number of representations of quadratic forms
R. J. Ayoub, On the coefficients of the zeta function of an imaginary quadratic field
Ch. F. Osgood, A method in diophantine approximation (II)
H. Halberstam and A. Rothkiewicz, A gap theorem for pseudoprimes in arithmetic progressions
P. G. Schmid, Zur Anzahl Abelcher Gruppen gegebener Ordnung II
F. Schweiger, Induzierte Maße und Jacobische Algorithmen
B. Novák, Verallgemeinerung eines Peterssonchen Satzes und Gitterpunkte mit Gewichten
M. M. Arzhanov, О некоторых возможностях ображения малых теорем

ACTA ARITHMETICA
XIII (1968)

A bound on the number of representations of quadratic forms

by

S. J. F. Gilman (Saint Louis)

1. Introduction. Let $f$ and $g$ be quadratic forms in $n$ and $m$ variables respectively, $n \geq m$, and such that their respective matrices, $A$ and $B$, are non-singular. B. W. Jones [4] denoted by $N(A, B)$ the number of essentially distinct primitive representations of $B$ by $A$, and defined the representations function $M(d, B) = \sum N(A_d, B)$, where the sum is over a set of $n$-ary forms $A_d$ of determinant $d$ and such that the set consists of one and only one form from each of the classes of determinant $d$. For $n > m$, $|A| = d$ and $|B| = g$, he defined $\mathcal{O}$ to be a set of forms in $n - m$ variables, of determinant $dg^{n-m-1}$, and having the following properties:

1) no two forms of $\mathcal{O}$ are equivalent;
2) if $E \in \mathcal{O}$, there exist integral matrices $D$ and $C$ such that

$$E = qD - \omega^T(\text{adj} B)C$$

3) there is no larger set having properties 1) and 2).

Jones then proved the important

Theorem 1 ([4], Theorem 1a, p. 889). The function $M(d, B) = \sum P(d, B, E_i)$, where the sum is over all forms $E_i \in \mathcal{O}$ and $P(d, B, E)$ denotes the number of essentially distinct solutions $C$ of $E = -X^T(\text{adj} B)X$ (mod $q$). If $g = \pm 1$, $P(d, B, E) = 1$.

Jones was able to evaluate $M(d, B)$ only for the cases: $n - m = 1; m = 1$; and $n = 3, m = 1$, with $(q, 2d) = 1$. J. E. Fischer [2] developed a formula for the number of solutions of $E = -X^T(\text{adj} B)X$ (mod $q$), when $n = 4, m = 2$, and $B$ is primitive. (A square matrix $W = (w_{ij})$ is said to be primitive if the g.c.d. of the $w_{ij}$ is 1.) E. W. Brande [1] extended the results of Fischer and formulated an upper bound for the number of essentially distinct primitive representations of a primitive binary quadratic form by an $n$-ary quadratic form for $n = 4, 5$.

* This paper is based on the author's Saint Louis University Ph. D. dissertation.
We extend the results of Jones, Fischer and Brande, and give an upper bound for $M(d, B)$ when $n = m = 2, 3$ and $B$ has primitive adjoint. In order to do this, we consider, in section 2, some general theorems which not only have important applications to our problem, but also are of interest in themselves. In sections 3 and 4 we discuss a series of congruences related to

$$E = -X^T(\text{adj} B)X \pmod{g},$$

in order to establish necessary and sufficient conditions for the existence of solutions of this congruence. These results enable us, in section 5, to count the number of solutions of the above congruence, and finally, in sections 6 and 7, to obtain the principal result, namely, an upper bound for the number of essentially distinct such solutions.

Throughout, we have adopted the terminology and notation of Jones in [4]. In addition, we make the following conventions:

We denote any row vector $(w_1, w_2, \ldots, w_k)$ by $(w)$, where $w_k$ depends on a parameter $k$, we write $(w_{lab}, w_{lak}, \ldots, w_{lak})$ and denote it by $(w_{lab})$. Accordingly, if a congruence in $t$ indeterminates $x_1, x_2, \ldots, x_t$ has a solution $r = x_i, 1 \leq i \leq t$, we denote this solution by $(r)$. A set of solutions of a congruence modulo $v_0$ such that any solution of the congruence is congruent to one element of the set is called a solution set of the congruence. If a solution $(r)$ of a congruence modulo $v_0$ is such that for each $i, r_{(i)}(v_0) = \{0, 1, \ldots, v_0 - 1\}$, we say the solution is in $R(v_0)$. Two sets $(w_1, w_2, \ldots, w_k)$ and $(v_1, v_2, \ldots, v_k)$ are called order distinct iff (if and only if) $w_i \equiv v_i \pmod{v_0}$ for at least one $i, 1 \leq i \leq t$. All matrices considered here are understood to have rational integral elements.

2. Preliminary theorems. If $W = (w_0)$ is a square matrix, then $W_d$ is the cofactor of the element $w_{i0}$ in the determinant of $W$.

Theorem 2. If $W$ is any $m$-square matrix, then $W_d Ad W_a = W_d W_a \pmod{|W|}$, where $1 \leq i, j, k \leq m$.

Proof. Let $h, i, j$, and $k$ be fixed. If $i = j$ or $h = k$, the proof is trivial. Let $i \neq j$ and $h \neq k$, and consider the minor $M_{ij}^{hk}$, obtained from $Ad W$ by removing rows $h$ and $k$, and columns $i$ and $j$. Let $M_{ij}^{hk}$ be the minor obtained from $W$ by deleting rows $h$ and $k$, and columns $i$ and $j$. By a theorem of Jacobi ([3]), vol. 1, pp. 82–83:

$$\sum_{i=1}^{m} \sum_{j=1}^{m} B_{ij} x_i x_j \pmod{g},$$

Thus

$$\sum_{i=1}^{m} \sum_{j=1}^{m} B_{ij} x_i x_j \equiv 0 \pmod{|W|}.$$

Theorem 3. Let $V$ be an $m$-square symmetric matrix with $|V| = 1$. If $Ad V$ is primitive, then for any prime $p$ such that $p|V$, $p|V_d$ for at least one $i, 1 \leq i \leq m$.

Proof. Assume that $p|V_i$, for each $i$. Since $V$ is symmetric, by Theorem 2, $V_d V_{ii} = V_{ii} \pmod{p}$, for each $i$ and $j$, $1 \leq i, j \leq m$. Hence, $p|V_i$ for each $i$ and $j$, which contradicts the primitiveness of $Ad V$.

A contrapositive argument readily shows that if $V_i$ is primitive, $V_i$ also is primitive. The converse is not in general true for $m > 2$.

3. Relations among the solutions of certain congruences. Consider a set $G$ consisting of exactly one form from each of the classes of forms in $n - m$ variables and of determinant $d^{n-m-1}$. A form $E$ of $G$ belongs to $G$ if there exists an $m \times (n - m)$ matrix $C$ which satisfies $E = -X^T(\text{adj} B)X \pmod{g}$. We call such a matrix a $C$-matrix associated with $E$, or briefly a $C$-matrix, and denote it by $C, C_1, C_2$.

Let $E^*_1$ be an arbitrary form belonging to $G$ and denote its matrix by $E^*_1 = (w_{ab}), 1 \leq j, k \leq n - m$. Consider

$$E^*_1 = -X^T(\text{adj} B)X \pmod{g}.$$

Since $B = (b_{ij})$ is symmetric, $\text{adj} B = (b_{ij})$. Let $X = (w_{ij})$. Thus (1) is equivalent to:

$$-w_{ab} = \sum_{i=1}^{m} \sum_{j=1}^{m} B_{ab} w_{ai} w_{aj} \pmod{g}, 1 \leq j, k \leq n - m.$$

Let $g = \text{lcm}(p_i)$, where the $p_i$ are distinct primes, $p_1 = 2, p_2 > 0$, and $p_2 > 0$ if $t > 0$. For convenience, we write $p_{00}$ for $p$; or, when no confusion will arise, and $i$ is arbitrary but fixed, we write $p_{i}$ for $p_i$, eliminating the $i$'s. For each $i, 0 < i < s$, we define $k_i$ to be the least positive integer such that $p_i|B_{ai}$. When no confusion arises, we use $k$ for $k_i$. By Theorem 3, for each $p_i$, there exists at least one $i, 1 \leq i \leq m$, such that $p_i|B_{ai}$; hence, $B_{ai}$ is uniquely determined.

Consider the following:

$kA$:

$$-w_{ab} = \sum_{i=1}^{m} \sum_{j=1}^{m} B_{ab} x_i x_j \pmod{g};$$

$kB$:

$$-w_{ab} = \sum_{i=1}^{m} \sum_{j=1}^{m} B_{ab} x_i x_j \pmod{p_{00}};$$

$C$:

$$B_{ab} = (a_{ik}) \pmod{p_{00}};$$

$D$:

$$B_{ab} = (a_{ik}) \pmod{p_{00}};$$

where $i$ and $k$ are arbitrary, $0 < i < s$, $1 < k < n - m$.

Define

$$[kB] \in C_{i} \ (0 < i < s) \quad \text{and} \quad [kD] \in C_{i} \ (0 < i < s).$$
We now establish several properties of solutions of the above congruences and systems of congruences.

**Theorem 4.** \((d_{ls})_m\) is a solution of \(hkA\) iff it is a solution of \([kkD]\).

**Proof.** It is clear \((d_{ls})_m\) is a solution of \([kkB]\) iff it is a solution of \(kkA\). Let \((d_{ls})_m\) be a solution of \([kkB]\). Thus, for each \(i\), \(0 < s < l < s\), \((d_{ls})_m\) is a solution of \(kkB_l\). Let \(i\) be arbitrary but fixed, and \(p^l = p^g\). Since \((B_{ls}, p) = 1\),

\[-u_{ls} = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l) \]

iff

\[-B_{ls} u_{ls} = \sum_{i=1}^{m} B_{ls} B_{ls} x_{ls} + 2 \sum_{1 < s < l < m} B_{ls} B_{ls} x_{ls} (mod p^l). \]

By Theorem 2, \(B_{ls} B_{ls} = B_{ls} B_{ls} (mod p^l)\). Hence (3) iff

\[-B_{ls} u_{ls} = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l) \]

iff \((d_{ls})_m\) is a solution of \([kkD]\); iff \((d_{ls})_m\) is a solution of \([kkD]\), since \(i\) is arbitrary. This completes the proof.

Let \(N(kkC_1)\) be the number of solutions of \(kkC_1\) in \(R(p^{l-1})\). If, for each \(i\) and \(k\), \(0 < s < l < s\), \(1 < k < n - m\), \(N(kkC_1) > 0\), let \(g_{0}^{(k)}\) denote an arbitrarily chosen solution of \(kkC_1\) in \(R(p^{l-1})\); otherwise, no \(g_{0}^{(k)}\) is defined. When no confusion arises, we write \(g\) or \(g_{0}\), for \(g_{0}^{(k)}\).

**Theorem 5.** There exist \(N(kkC_1)p^{(n-1)l}N(kkD_l)\) solutions of \(kkD_l\) in \(R(p^{l-1})\).

**Proof.** Let \(i\) be arbitrary but fixed. First we show (a): to each solution of \(kkC_1\), there correspond \(p^{(n-1)l}\) solutions of \(kkD_l\) in \(R(p^l)\). Let \(g\) be a solution of \(kkC_1\). Define the congruence, in the \(m\) indeterminates \(x_{ls},

\[g = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l)\]

Since \((B_{ls}, B_{ls}, \ldots, B_{ls}, p^l) = 1\), there exist precisely \(p^{(n-1)l}\) solutions of (4) in \(R(p^l)\). Since \(g\) is a solution of \(kkC_1\) by definition, (4) implies \(kkD_l\); that is,

\[-B_{ls} u_{ls} = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l)\]

Hence, any solution of (4) is a solution of \(kkD_l\); thus (a) is proved.

If \(g\) and \(g'\) are distinct solutions of \(kkC_1\), the corresponding solutions of \(kkD_l\), generated by \(g\) and \(g'\) are distinct.

We next prove (b): each solution of \(kkD_l\) corresponds to precisely one solution of \(kkC_1\). Let \((d_{ls})_m\) be a solution of \(kkD_l\); that is

\[-B_{ls} u_{ls} = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l)\]

Now there is precisely one \(x\) in \(R(p^l)\) such that

\[x = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^l).\]

Thus by (5) and (6) \(x\) is a solution of \(kkC_1\). Hence, to each solution, \((d_{ls})_m\) of \(kkD_l\), there corresponds precisely one solution of \(kkC_1\) in \(R(p^l)\); thus (b) is proved. Consequently, there are \(N(kkC_1)p^{(n-1)l}\) solutions of \(kkD_l\) in \(R(p^l)\) and these occur in \(N(kkC_1)\) disjoint sets. This completes the proof.

The following results are immediate consequences of the above proof.

We state them as corollaries for later use.

**Corollary A.** To each solution, \((d_{ls})_m\), of \(kkD_l\), there corresponds a unique solution, \(g_{0}^{(k)}\), of \(kkC_1\) in \(R(p^{l-1})\) such that

\[g_{0}^{(k)} = \sum_{i=1}^{m} B_{ls} x_{ls} (mod p^{l-1})\]

**Corollary B.** To each solution, \(g_{0}^{(k)}\), of \(kkC_1\), there correspond \(p^{(n-1)l}\) distinct solutions of \(kkD_l\) in \(R(p^{l-1})\). If \((d_{ls})_m\) is one such solution of \(kkD_l\), then (7) is satisfied.

4. Necessary and sufficient conditions for the existence of \(C\)-matrices. In the previous section we discussed \(kkA\) and related congruences. We now consider

\[jkA\]:

\[ -u_{jk} = \sum_{i=1}^{m} B_{jk} x_{jk} (mod p^g)\]

\[jkB\]:

\[ -u_{jk} = \sum_{i=1}^{m} B_{jk} x_{jk} (mod p^{l-1})\]

\[jkD\]:

\[-B_{jk} u_{jk} = \sum_{i=1}^{m} B_{jk} x_{jk} (mod p^l)\]

where \(i, j, k, l\) are arbitrary, \(0 < i < s, \ 1 < j < k < n - m\). Observe that \[jkA, \ jkB, \ jkD\] are congruences in the sets of indeterminates \((x_{jk})_m\) and \(x_{jk}\). Define

\[\{jkB\} = \{jkB\} \ 0 < i < s\ \ \text{and} \ \{jkD\} = \{jkD\} \ 0 < i < s\]
It is clear that \( jkA \) and \( jkB \) are equivalent, that is they have the same solution set. By a proof similar to the proof of Theorem 4, it follows that for arbitrary but fixed \( i \), \( jkB_i \) and \( jkD_i \) are equivalent. Consequently, \( jkA, jkB, \) and \( jkD \) are equivalent.

We are now ready to give a necessary and sufficient condition for the existence of a \( C \)-matrix.

**Theorem 6.** There exists a \( C \)-matrix associated with \( \Delta_+^s \) if and only if there exists a set consisting of precisely one \( g_i^0 \) for each \( i \) and \( k \), such that

\[
g_i^0 g_j^0 = -B_{ik} w_{jk} \pmod{p^m}
\]

for each \( i, j \) and \( k \), \( 0 \leq i < s, 1 \leq j < k < n - m \).

**Proof.** Let \( (w_{ik}) \) be a \( C \)-matrix associated with \( \Delta_+^s \). By the definition of a \( C \)-matrix given in Section 3, for each \( j \) and \( k \), \( 1 \leq j < k < n - m \), the row vectors \( (w_{ik}) \) (formed by taking the transpose of the \( j \) and \( k \)th columns of \( (w_{ik}) \), respectively) are a solution of \( jkB \) and hence also of \( jkD_i \) for each \( i \). Let \( i, j \) and \( k \) be arbitrary but fixed, with \( j < k \). Now \( (w_{ik}) \) and \( (w_{ik}) \) are solutions of \( jkD_i \) and \( \Delta_{ik} \), respectively. Hence, by Corollary A, there exist unique solutions \( g_i \) and \( g_k \) of \( jkD_i \) and \( \Delta_{ik} \) corresponding to \( (w_{ik}) \) and \( (w_{ik}) \), respectively. Thus, by congruence (7) we have,

\[
g_i g_k = \sum_{i=1}^{m} B_{ik} d_{ik} \pmod{p^m}
\]

But \( (w_{ik}) \) and \( (w_{ik}) \) are a solution of \( jkD_i \) for each \( i \). Thus for each \( i, j, \) and \( k \), (9) implies (8).

Conversely, assume there exists a set consisting of precisely one \( g_i^0 \) for each \( i \) and \( k \) such that property (8) holds. But, by Corollary C, for arbitrary but fixed \( i \), \( j \) and \( k \), \( 0 \leq i < s, 1 \leq j < k < n - m \),

\[
g_j = \sum_{i=1}^{m} B_{ik} d_{ik} \quad \text{and} \quad g_k = \sum_{i=1}^{m} B_{ik} d_{ik} \pmod{p^m},
\]

where \( (d_{ik}) \) and \( (d_{ik}) \) are solutions of \( jkD_i \) and \( \Delta_{ik} \), respectively. From (8) and the above congruences we obtain:

\[
g_i g_k = -B_{ik} w_{jk} \pmod{p^m}
\]

Thus \( (d_{ik}) \) and \( (d_{ik}) \) are a solution of \( jkD_i \). For fixed \( j < k \), by the Chinese Remainder Theorem, from a set of such solutions of \( jkD_i \), one for each \( i \), \( 0 \leq i < s \), we can obtain a unique solution, say \( (D_{ik}) \), \( (D_{ik}) \), for \( jkD \), and hence also for \( jkA \). Thus the \( m \times (n - m) \) matrix \( (D_{ik}) \) which has as its \( k \)th column \( (D_{ik}) \), \( 1 \leq k < n - m \), is the required \( C \)-matrix, and the proof is complete.

Let \( H \) be the family of all sets consisting of precisely one \( g_i^0 \) for each \( i \) and \( k \), and satisfying property (8); that is satisfying

\[
g_i^0 g_j^0 = -B_{ik} w_{jk} \pmod{p^m},
\]

for each \( i, j \) and \( k \), \( 0 \leq i < s, 1 \leq j < k < n - m \).

We showed in the second part of the proof of Theorem 6, that any element in \( H \) generates a \( C \)-matrix \( (D_{ik}) \) which has for its \( k \)th column \( (D_{ik}) \), where \( (D_{ik}) \) is a solution of \( (kD_i) \). In fact, any element of \( H \) generates \( q^{m(n-m)} \) such \( C \)-matrices associated with \( \Delta_{ik} \), for, in appealing to Corollary B in the above proof, we obtain not only one, but \( q^{m(n-m)} \) solutions \( (d_{ik}) \) of \( jkD_i \) corresponding to each solution \( g_i^0 \) of \( jkC_i \). Thus, in the above proof, there are actually \( q^{m(n-m)} \) possible row vectors \( (D_{ik}) \), and consequently \( q^{m(n-m)} \) choices for each of the columns \( (D_{ik}) \), \( 1 \leq j < k < n - m \). Hence, \( q^{m(n-m)} \) choices for the \( C \)-matrix \( (D_{ik}) \) arises from each member of \( H \).

Thus we have shown that the number of \( C \)-matrices associated with \( \Delta_+^s \) depends on the number of elements in \( H \). We state the precise relationship in the following

**Theorem 7.** The number \( N[H] \), of elements of \( H \) is the number \( N\{C: E_1^s\} \), of sets of \( C \)-matrices associated with \( \Delta_+^s \), \( q^{m(n-m)} \) \( (n-m) \)-matrices to a set. No two of these matrices are congruent modulo \( q \).

5. The value of \( N[C: E_1^s] \): We first prove two lemmas, and then use results obtained by J. E. Fischer in [2] and by E. W. Brande in [1] in order to evaluate \( N[C: E_1^s] \) for \( n - m = 2, 3 \), respectively.

Let \( i, j \) and \( k \) be arbitrary but fixed, \( 0 \leq i < s, 1 \leq j < k < n - m \). Consider the family of all order distinct sets of the form \( (g_i^0, g_j^0) \). Let \( H_{ij}^k \) denote the family of all such sets satisfying property (8) for the given \( j \) and \( k \). Let \( N[H_{ij}^k] \) denote the number of elements in \( H_{ij}^k \).

**Lemma 1.** If \( n - m = 2 \), then

\[
N[H] = \sum_{i} N[H_{ij}^k].
\]

**Proof.** Let \( F \) be the family of all order distinct sets formed by the union of precisely one element from each \( H_{ij}^k \), \( 0 \leq i < s \). There are \( \sum_{i} N[H_{ij}^k] \) elements in \( F \) and congruence (8) is satisfied for each \( i \). Hence \( F \bigcap H \). Clearly \( H \subset F \). Thus \( N[H] = N[F] = \sum_{i} N[H_{ij}^k] \), where \( N[F] \) is the number of elements in \( F \). This proves the lemma.
Next, consider the case: \( n - m = 3 \). Let \( i \) be arbitrary but fixed, \( 0 \leq i \leq n \); and let \( H_{[i]}^{[1]} \) denote the collection of all order \( d \) distinct sets of the form \( \{ g_1^{[1]}, g_2^{[1]}, g_3^{[1]} \} \) such that property (8) holds, that is:
\[
g_1^{[1]} g_2^{[1]} = B_{AB} u_{ij} (\text{mod } p^{(0)}) \quad \text{whenever } 1 \leq r < t < 3.
\]
Let \( N[H_{[i]}^{[1]}] \) denote the number of elements in \( H_{[i]}^{[1]} \).

**Lemma 2.** If \( n - m = 3 \), then
\[
N[H] = \prod_{i=1}^{n} N[H_{[i]}^{[1]}].
\]

We omit the proof since it is essentially the same as that of Lemma 1. Fischer [2, pp. 35-59] developed a formula for the value of \( N[H_{[i]}^{[1]}] \), and Brande [1], pp. 62-84 developed a similar formula for \( N[H_{[i]}^{[1]}] \).

We state, in the notation adopted in this paper, their results as Theorems 8 and 9, respectively.

**Theorem 8.** \( N[H_{[i]}^{[1]}] \) is zero, or
\[
N[H_{[i]}^{[1]}] = \begin{cases}
\begin{align*}
p^{(0)} & , \quad \text{if } t_i(u_{ij}) > e_i \text{ and } i \not\equiv 0; \\
2p^{(0)}(e_i)(r_1) & , \quad \text{if } t_i(u_{ij}) < e_i \text{ and } i \equiv 0; \\
2^{(0)}(e_i)(r_1 + e_i^*) & , \quad \text{if } t_i(u_{ij}) < e_i \text{ and } i \equiv 0;
\end{align*}
\end{cases}
\]
where \( t_i(u_{ij}) \) is defined by: \( p^{(0)}(e_i)(u_{ij}) = \frac{t_i(u_{ij})}{e_i} \), if \( u_{ij} \neq 0 \), and \( t_i(u_{ij}) = e_i \), otherwise; \( t_i(u_{ij}) \leq t_i(u_{i}) \); and \( M' = 0, 1 \text{ or } 2 \) according as \( e_i - 2(t_i(u_{ij})/2) = 1, 2 \) or 3, respectively.

**Theorem 9.** \( N[H_{[i]}^{[1]}] \) is zero, or
\[
N[H_{[i]}^{[1]}] = \begin{cases}
\begin{align*}
p^{(0)} & , \quad \text{if } t_i(u_{ij}) > e_i \text{ and } i \not\equiv 0; \\
2p^{(0)}(e_i)(r_1) & , \quad \text{if } t_i(u_{ij}) < e_i \text{ and } i \equiv 0; \\
2^{(0)}(e_i)(r_1 + e_i^*) & , \quad \text{if } t_i(u_{ij}) < e_i \text{ and } i \equiv 0;
\end{align*}
\end{cases}
\]
where \( t_i(u_{ij}) \) and \( M' \) are defined as above with \( j = 1 \); and \( t_i(u_{ij}) \leq t_i(u_{i}) \).

Let \( \theta(i, E_i) = \min\{e_i/2, t_i(u_{ij})/2\} \); \( \ell(E_i) \) be the number of odd primes, \( p_0 \), for which \( e_i > t_i(u_{ij}) \); and
\[
M(E_i) = \begin{cases}
1, & \text{if } e_i - 2\theta(i, E_i) = 0; \\
2, & \text{if } e_i - 2\theta(i, E_i) \geq 3; \\
0, & \text{otherwise}.
\end{cases}
\]

Using this notation, and appealing to Theorems 7, 8, and 9, and to Lemmas 1 and 2, we have proved

**Theorem 10.** If \( n - m = 2, 3 \) and \( E_i \not\equiv 0 \), then \( N[C; E_i] \) is zero, or
\[
N[C; E_i] = 2^{\ell(E_i) + n - t + 1} \prod_{p \in p_0} \left( 1 - \frac{1}{p^{e_i}} \right).
\]

**6. Conditions for essential equality of \( C \)-matrices.** Assume \( \Theta \) is non-empty, \( n - m = 2, 3 \) and let \( E \not\equiv 0 \).

**Lemma 3.** Two \( C \)-matrices, \( C_1 \) and \( C_2 \), associated with \( E \not\equiv 0 \), are essentially equal iff there exists an automorphism \( Q_{E} \) of \( E \) such that
\[
(\text{adj } B)(C_1 - C_2 Q_{E}) = 0 \quad (\text{mod } q),
\]
where \( 0 \) is the \( m \times (n - m) \) zero matrix.

**Proof.** If \( C_1 \) and \( C_2 \) are essentially equal \( C \)-matrices, then by definition (14, p. 888), there is an integral matrix \( B \) and an automorphism \( Q_{E} \) of \( E \) such that
\[
C_1 = BR + C_2 Q_{E}.
\]
Since \( R \) is non-singular, \( B^{-1} = (\text{adj } B)/q \) exists, and hence (11) implies (10).

Conversely, if there exists an automorphism \( Q_{E} \) of \( E \) such that (10) is satisfied, then there exists an integral matrix \( E' = B^{-1}C_2 - C_2 Q_{E} \) such that (11) is satisfied. Thus, \( C_1 \) and \( C_2 \) are essentially equal and the proof is complete.

**Lemma 4.** Let \( i \) be arbitrary, \( 0 \leq i \leq n \), \( (e_{ni}) \) be an arbitrary \( m \times (n - m) \) matrix, and \( t \) be such that \( 1 \leq t \leq n - m \). Then
\[
\sum_{i=1}^{m} B_{ni} e_{ni} = 0 \quad (\text{mod } p^{t})
\]
iff for each \( r, 1 \leq r \leq m \),
\[
\sum_{i=1}^{m} B_{ni} e_{ni} = 0 \quad (\text{mod } p^{r}).
\]

**Proof.** Assume
\[
\sum_{i=1}^{m} B_{ni} e_{ni} = 0 \quad (\text{mod } p^{r}).
\]
Let \( r \) be arbitrary, \( 1 \leq r \leq m \). Multiplying (12) by \( B_{ni} \), applying Theorem 2, and recalling that \( (B_{ni}, p_i) = 1 \), (12) implies:
\[
\sum_{i=1}^{m} B_{ni} e_{ni} = 0 \quad (\text{mod } p^{r}).
\]
Since \( r \) is arbitrary, the sufficiency is proved. The necessity is obvious.
7. An upper bound for \( M(d, E) \). We show, by an example, that the converse of Theorem 11 is not true in general.

Let \( A \) be the 6-ary identity matrix, and let \( B \) be the 4-ary diagonal matrix \( B = \text{diag}(1, 1, 2, 3) \). Thus \( \text{adj} B \) is primitive, and \( \mathcal{C}^* \) may be chosen as the set of all binary reduced forms whose discriminant is \(-24\).

Clearly, \( B = (1, 0, 0, 0) \in \mathcal{C}^* \). Thus \( B_{1,2} = B_{3,3} = 3 \), and \( B_{1,1} = B_{4,4} = 2 \). A simple calculation shows that \( g_0^{(0)} = 1; g_0^{(0)} = 0; g_0^{(0)} = 1 \) and \( g_0^{(0)} = 2; g_0^{(0)} = 0 \). For \( i = 0 \), \( (8) \) is satisfied by \( (g_0^{(0)}, g_0^{(0)}) = (1, 0) \); and for \( i = 1 \), \( (8) \) is satisfied by \( (g_0^{(0)}, g_0^{(0)}) = (1, 0) \) and \( (g_0^{(0)}, g_0^{(0)}) = (2, 0) \). Thus, each of the sets \((1, 0; 1, 0)\) and \((1, 0; 2, 0)\) yields a set of \( C \)-matrices.

It is easy to show that \((1, 0; 1, 0)\) and \((1, 0; 2, 0)\) yield the \( C \)-matrices

\[
C_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 2 & 0 \end{bmatrix} \quad \text{and} \quad C_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix}
\]

respectively. Using \( Q_E = -I \), where \( I \) is the \( 2 \times 2 \) identity matrix, we find:

\[
(\text{adj} B)(C_1 - CQ_E) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 6 & 0 \\ 6 & 0 \end{bmatrix} = (0) \mod(6).
\]

Hence, by Lemma 3, \( C_1 \) and \( C_2 \) are essentially equal \( C \)-matrices associated with the same form \( E = (1, 0, 6) \), but with order distinct elements of \( H \), and hence belong to different ones of the \( N[C; E] \) sets of \( C \)-matrices associated with \( E \). Therefore, the converse of Theorem 11 is not true in general.

By Theorem 10, for \( n - m = 2 \) and \( E \in \mathcal{C} \), we can evaluate \( N[C; E] \).

Theorem 11 and the above example show that belonging to the same one of the \( N[C; E] \) sets of \( C \)-matrices is a sufficient, but not a necessary condition for the essential equality of \( C \)-matrices. Thus, \( P(d, B, E) \leq \mathcal{N}[C; E] \), where we recall \( P(d, B, E) \) is the number of essentially distinct \( C \)-matrices associated with \( E \). Combining these results with Theorem 1, we have proved our principal result, namely

**Theorem 11.** If \( C_1 \) and \( C_2 \) are \( C \)-matrices which belong to the same one of the \( N[C; E] \) sets of \( C \)-matrices, then \( C_1 \) and \( C_2 \) are essentially equal.
On the coefficients of the zeta function of an imaginary quadratic field*

by

RAYMOND G. AYOUR (University Park, Pa)

§ 1. Introduction. Let $K = \mathbb{Q}(\sqrt{D})$, $D < 0$ be an imaginary quadratic field of discriminant $d$ and let $|d| = k$.

Let

$$
\zeta_K(s) = \sum \frac{1}{n^{s}} = \sum_{m=1}^{\infty} \frac{P(n)}{n^s}
$$

be the Dedekind zeta function of $K$ where

$$
P(n) = \sum_{N|E=n} 1.
$$

It is known (see e.g. [1], Chap. V) that

$$
\zeta_K(s) = \zeta(s) L(s, \chi_d)
$$

and that

$$
P(n) = \sum \chi_d(l)
$$

where $\chi_d(n) = \left( \frac{d}{n} \right) = $ Kronecker symbol.

Let

$$
H(x) = \sum_{n \leq x} P(n).
$$

It is known [3] that

$$
H(n) = \alpha x + A_d(x)
$$

where $\alpha$ is the residue of $\zeta_K(s)$ at $s = 1$ and where $A_d(x) = O(x^\theta)$ with the constant implied by the $O$ depending on $k$.

* This research was supported by the N. S. F. under grant GP-5593.