Table des matières du tome XIII, fascicule 4

La revue est consacrée à toutes les branches de *l'Arithmétique* et de la *Théorie des Nombres*, ainsi qu'aux *fonctions ayant de l'importance dans ces domaines*.

Prière d'adresser les textes dactylographiés à l'un des rédacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa 1 (Pologne), ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l'échange de Acta Arithmetica.

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 5 (Pologne), Krakowskie Przedmieście 7.

Prix de ce fascicule 3.00 $.

Les volumes I-III (réédits) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

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, $n \geqslant m$, 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 $M(d, B) = \sum N(A_k, B)$, where the sum is over a set of n-ary forms, A_k, 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 $|B| = q$, he defined $\mathfrak{G}$ to be a set of forms in $n-m$ variables, of determinant dq^{n-m-1}, and having the following properties:

1) no two forms of $\mathfrak{G}$ are equivalent;

2) if $E \in \mathfrak{G}$, there exist integral matrices D and C such that

$$E = qD - C^T(\operatorname{adj} B)C;$$

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* $E_i \in \mathfrak{G}$ *and* $P(d, B, E)$ *denotes the number of essentially distinct solutions* C *of* $E \equiv -X^T(\operatorname{adj} B)X$ (mod q). *If* $q = \pm 1$, $P(d, B, E_i) = 1$.

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 $E \equiv -X^T(\operatorname{adj} B)X$ (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

$$E \equiv -X^T(\operatorname{adj} B)X \pmod{q},$$

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 $(w_1, w_2, \ldots, w_t)$ by $(w)_t$. If a row vector depends on a parameter k, we write $(w_{1k}, w_{2k}, \ldots, w_{tk})$ and denote it by $(w_k)_t$. Accordingly, if a congruence in t indeterminates $x_1, x_2, \ldots, x_t$ has a solution $r_i = x_i$, $1 \leqslant i \leqslant t$, we denote this solution by $(r)_t$. A set of solutions of a congruence modulo v, such that any solution of the congruence is congruent modulo v to precisely one element of the set is called a *solution set* of the congruence. If a solution $(r)_t$ of a congruence modulo v is such that for each i, $r_i \in R(v) = \{0, 1, \ldots, v-1\}$, we say *the solution is in* $R(v)$. Two sets $\{w_1, w_2, \ldots, w_t\}$ and $\{v_1, v_2, \ldots, v_t\}$ are called *order distinct* iff (if and only if) $w_i \neq v_i$, for at least one i, $1 \leqslant i \leqslant t$. *All matrices considered here are understood to have rational integral elements.*

2. Preliminary theorems. If $W = (w_{ij})$ is a square matrix, then, as is customary, W_{ij} is the cofactor of the element w_{ij} in the determinant of W.

THEOREM 2. *If W is any m-square matrix, then $W_{ih}W_{jk} \equiv W_{jh}W_{ik}$ $(\operatorname{mod} |W|)$, where $1 \leqslant h, i, j, k \leqslant m$.*

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, $\mathfrak{M}_{ij}^{hk}$, obtained from adj W be *retaining* 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):

$$\mathfrak{M}_{ij}^{hk} = (-1)^{h+i+j+k}|W|M_{ij}^{hk}.$$

Thus

$$\mathfrak{M}_{ij}^{hk} = W_{ih}W_{jk} - W_{jh}W_{ik} \equiv 0 \pmod{|W|}.$$

THEOREM 3. *Let V be an m-square symmetric matrix with $|V| = t$. If adj V is primitive, then for any prime p such that $p \mid t$, $p \nmid V_{ii}$ for at least one i, $1 \leqslant i \leqslant m$.*

Proof. Assume that $p \mid V_{ii}$ for each i. Since V is symmetric, by Theorem 2, $V_{ii}V_{jj} \equiv V_{ij}^2 \pmod{t}$, for each i and j, $1 \leqslant i, j \leqslant m$. Hence, $p \mid V_{ij}$ for each i and j, which contradicts the primitiveness of adj V.

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

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

Let E_0^* be an arbitrary form belonging to $\mathfrak{G}^*$ and denote its matrix by $E_0^* = (u_{jk})$, $1 \leqslant j, k \leqslant n-m$. Consider

$$E_0^* \equiv -X^T(\operatorname{adj} B)X \pmod{q}. \tag{1}$$

Since $B = (b_{ij})$ is symmetric, $\operatorname{adj} B = (B_{ij})$. Let $X = (x_{rt})$. Thus (1) is equivalent to:

$$-u_{jk} \equiv \sum_{t=1}^{m}\sum_{r=1}^{m} B_{rt}x_{rj}x_{tk} \pmod{q}, \qquad 1 \leqslant j,\ k \leqslant n-m. \tag{2}$$

Let $q = \prod_{i=0}^{s} p_i^{e_i}$, where the p_i are distinct primes, $p_0 = 2$, $e_0 \geqslant 0$, and $e_i > 0$ if $i > 0$. For convenience, we write $p^{e(i)}$ for $p_i^{e_i}$; or, when no confusion will arise, and i is arbitrary but fixed, we write p or p^e, eliminating the i's. For each i, $0 \leqslant i \leqslant s$, we define h_i to be the least positive integer such that $p_i \nmid B_{h_ih_i}$. When no confusion arises, we use h for h_i. By Theorem 3, for each p_i, there exists at least one t, $1 \leqslant t \leqslant m$, such that $p_i \nmid B_{tt}$; hence, $B_{h_ih_i}$ is uniquely determined.

Consider the following:

$kk\boldsymbol{A}$: $$-u_{kk} \equiv \sum_{t=1}^{m}\sum_{r=1}^{m} B_{rt}x_{rk}x_{tk} \pmod{q};$$

$kk\boldsymbol{B}_i$: $$-u_{kk} \equiv \sum_{t=1}^{m}\sum_{r=1}^{m} B_{rt}x_{rk}x_{tk} \pmod{p^{e(i)}};$$

$kk\boldsymbol{C}_i$: $$-B_{hh}u_{kk} \equiv (x_k)^2 \pmod{p^{e(i)}};$$

$kk\boldsymbol{D}_i$: $$-B_{hh}u_{kk} \equiv \Big[\sum_{r=1}^{m} B_{hr}x_{rk}\Big]^2 \pmod{p^{e(i)}};$$

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

Define

$$[kk\boldsymbol{B}] = \{kk\boldsymbol{B}_i \mid 0 \leqslant i \leqslant s\} \quad \text{and} \quad [kk\boldsymbol{D}] = \{kk\boldsymbol{D}_i \mid 0 \leqslant i \leqslant s\}.$$

We now establish several properties of solutions of the above congruences and systems of congruences.

THEOREM 4. *$(d_k)_m$ is a solution of $kk\boldsymbol{A}$ iff it is a solution of $[kk\boldsymbol{D}]$.*

Proof. It is clear $(d_k)_m$ is a solution of $[kk\boldsymbol{B}]$ iff it is a solution of $kk\boldsymbol{A}$. Let $(d_k)_m$ be a solution of $[kk\boldsymbol{B}]$. Thus, for each i, $0 \leqslant i \leqslant s$, $(d_k)_m$ is a solution of $kk\boldsymbol{B}_i$. Let i be arbitrary but fixed, and $p^e = p^{e(i)}$. Since $(B_{hh}, p) = 1$,

$$-u_{kk} \equiv \sum_{t=1}^{m} \sum_{r=1}^{m} B_{rt} d_{rk} d_{tk} \pmod{p^e}$$

iff

$$-B_{hh} u_{kk} \equiv \sum_{r=1}^{m} B_{hh} B_{rr} d_{rk}^2 + 2 \sum_{1 \leqslant t < r \leqslant m} B_{hh} B_{rt} d_{rk} d_{tk} \pmod{p^e}. \tag{3}$$

By Theorem 2, $B_{hh} B_{rt} \equiv B_{rh} B_{ht} \pmod{p^e}$. Hence (3) iff

$$-B_{hh} u_{kk} \equiv \Big[\sum_{r=1}^{m} B_{rh} d_{rk}\Big]^2 \pmod{p^e}$$

iff $(d_k)_m$ is a solution of $kk\boldsymbol{D}_i$; iff $(d_k)_m$ is a solution of $[kk\boldsymbol{D}]$, since i is arbitrary. This completes the proof.

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

THEOREM 5. *There exist $N(kk\boldsymbol{C}_i)p^{(m-1)e(i)}$ solutions of $kk\boldsymbol{D}_i$ in $R(p^{e(i)})$.*

Proof. Let i be arbitrary but fixed. We first show (a): to each solution of $kk\boldsymbol{C}_i$ there correspond $p^{(m-1)e}$ solutions of $kk\boldsymbol{D}_i$ in $R(p^e)$. Let g be a solution of $kk\boldsymbol{C}_i$. Define the congruence, in the m indeterminates x_{rk},

$$g \equiv \sum_{r=1}^{m} B_{rh} x_{rk} \pmod{p^e}. \tag{4}$$

Since $(B_{1h}, B_{2h}, \ldots, B_{mh}, p^e) = 1$, there exist precisely $p^{(m-1)e}$ solutions of (4) in $R(p^e)$. Since g is a solution of $kk\boldsymbol{C}_i$ by definition, (4) implies $kk\boldsymbol{D}_i$; that is:

$$-B_{hh} u_{kk} = \Big[\sum_{r=1}^{m} B_{rh} x_{rk}\Big]^2 \pmod{p^e}.$$

Hence, any solution of (4) is a solution of $kk\boldsymbol{D}_i$; thus (a) is proved.

If g and g' are distinct solutions of $kk\boldsymbol{C}_i$, the corresponding solutions of $kk\boldsymbol{D}_i$ generated by g and g' are distinct.

We next prove (b): each solution of $kk\boldsymbol{D}_i$ corresponds to precisely one solution of $kk\boldsymbol{C}_i$. Let $(d_k)_m$ be a solution of $kk\boldsymbol{D}_i$; that is

$$-B_{hh} u_{kk} \equiv \Big[\sum_{r=1}^{m} B_{rh} d_{rk}\Big]^2 \pmod{p^e}. \tag{5}$$

Now there is precisely one x in $R(p^e)$ such that

$$x \equiv \sum_{r=1}^{m} B_{rh} d_{rk} \pmod{p^e}. \tag{6}$$

Thus by (5) and (6) x is a solution of $kk\boldsymbol{C}_i$. Hence, to each solution, $(d_k)_m$, of $kk\boldsymbol{D}_i$ there corresponds precisely one solution of $kk\boldsymbol{C}_i$ in $R(p^e)$; thus (b) is proved. Consequently, there are $N(kk\boldsymbol{C}_i)p^{(m-1)e}$ solutions of $kk\boldsymbol{D}_i$ in $R(p^e)$ and these occur in $N(kk\boldsymbol{C}_i)$ 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, $(d_k)_m$, of $kk\boldsymbol{D}_i$ there corresponds a unique solution, $g_k^{(i)}$, of $kk\boldsymbol{C}_i$ in $R(p^{e(i)})$ such that*

$$g_k^{(i)} \equiv \sum_{r=1}^{m} B_{rh} d_{rk} \pmod{p^{e(i)}}. \tag{7}$$

COROLLARY B. *To each solution, $g_k^{(i)}$, of $kk\boldsymbol{C}_i$ there correspond $p^{(m-1)e(i)}$ distinct solutions of $kk\boldsymbol{D}_i$ in $R(p^{e(i)})$. If $(d_k)_m$ is one such solution of $kk\boldsymbol{D}_i$, then (7) is satisfied.*

4. Necessary and sufficient conditions for the existence of C-matrices. In the previous section we discussed $kk\boldsymbol{A}$ and related congruences. We now consider

$$jk\boldsymbol{A}: \qquad -u_{jk} \equiv \sum_{t=1}^{m} \sum_{r=1}^{m} B_{rt} x_{rj} x_{tk} \pmod{q};$$

$$jk\boldsymbol{B}_i: \qquad -u_{jk} \equiv \sum_{t=1}^{m} \sum_{r=1}^{m} B_{rt} x_{rj} x_{tk} \pmod{p^{e(i)}};$$

$$jk\boldsymbol{D}_i: \qquad -B_{hh} u_{jk} \equiv \Big[\sum_{r=1}^{m} B_{rh} x_{rj}\Big]\Big[\sum_{t=1}^{m} B_{th} x_{tk}\Big] \pmod{p^{e(i)}};$$

where i, j and k are arbitrary, $0 \leqslant i \leqslant s$, $1 \leqslant j < k \leqslant n-m$. Observe that $jk\boldsymbol{A}$, $jk\boldsymbol{B}_i$ and $jk\boldsymbol{D}_i$ are congruences in the sets of indeterminates $(x_j)_m$ and $(x_k)_m$. Define

$$[jk\boldsymbol{B}] = \{jk\boldsymbol{B}_i \mid 0 \leqslant i \leqslant s\} \quad \text{and} \quad [jk\boldsymbol{D}] = \{jk\boldsymbol{D}_i \mid 0 \leqslant i \leqslant s\}.$$

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 E_0^* iff there exists a set consisting of precisely one $g_k^{(i)}$ for each i and k, such that*

$$g_j^{(i)} g_k^{(i)} \equiv -B_{hh} u_{jk} \pmod{p^{e(i)}} \tag{8}$$

for each i, j and k, $0 \leqslant i \leqslant s$, $1 \leqslant j < k \leqslant n-m$.

Proof. Let (w_{uv}) be a C-matrix associated with E_0^*. By the definition of a C-matrix given in section 3, for each j and k, $1 \leqslant j < k \leqslant n-m$, the row vectors $(w_j)_m$ and $(w_k)_m$ (formed by taking the transpose of the j and kth columns of (w_{uv}), respectively), are a solution of jkA and hence also of jkD_i for each i. Let i, j and k be arbitrary but fixed, with $j < k$. Now $(w_j)_m$ and $(w_k)_m$ are solutions of jjD_i and kkD_i, respectively. Hence, by Corollary A, there exist unique solutions g_j and g_k of jjC_i and kkC_i corresponding to $(w_j)_m$ and $(w_k)_m$ respectively. Thus, by congruence (7) we have:

$$g_j g_k \equiv \Big[\sum_{r=1}^{m} B_{rh} w_{rj}\Big]\Big[\sum_{t=1}^{m} B_{th} w_{tk}\Big] \pmod{p^e}. \tag{9}$$

But $(w_j)_m$, $(w_k)_m$ 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 $g_k^{(i)}$ for each i and k such that property (8) holds. But, by Corollary B, for arbitrary but fixed i, j and k, $0 \leqslant i \leqslant s$, $1 \leqslant j < k \leqslant n-m$,

$$g_j \equiv \sum_{r=1}^{m} B_{rh} d_{rj} \quad \text{and} \quad g_k \equiv \sum_{t=1}^{m} B_{th} d_{tk} \pmod{p^e},$$

where $(d_j)_m$ and $(d_k)_m$ are solutions of jjD_i and kkD_i respectively. From (8) and the above congruences we obtain:

$$g_j g_k \equiv -B_{hh} u_{jk} \equiv \Big[\sum_{r=1}^{m} B_{rh} d_{rj}\Big]\Big[\sum_{t=1}^{m} B_{th} d_{tk}\Big] \pmod{p^e}.$$

Thus $(d_j)_m$, $(d_k)_m$ 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, $0 \leqslant i \leqslant s$, we can obtain a unique solution, say $(D_j)_m$, $(D_k)_m$, for $[jkD]$, and hence also for jkA. Thus the $m \times (n-m)$ matrix (D_{rt}) which has as its kth column $\big((D_k)_m\big)^T$, $1 \leqslant k \leqslant n-m$, is the required C-matrix, and the proof is complete.

Let H be the family of all sets consisting of precisely one $g_k^{(i)}$ for each i and k, and satisfying property (8); that is satisfying

$$g_j^{(i)} g_k^{(i)} \equiv -B_{hh} u_{jk} \pmod{p^{e(i)}},$$

for each i, j and k, $0 \leqslant i \leqslant s$, $1 \leqslant j < k \leqslant n-m$.

We showed in the second part of the proof of Theorem 6, that any element in H generates a C-matrix (D_{rt}) which has for its kth column $\big((D_k)_m\big)^T$, where $(D_k)_m$ is a solution of $[kkD]$. In fact, any element of H generates $q^{(n-m)(m-1)}$ such C-matrices associated with E_0^*; for, in appealing to Corollary B in the above proof, we obtain not only one, but $p^{(m-1)e(i)}$ solutions $(d_j)_m$ of jjD_i corresponding to each solution $g_j^{(i)}$ of jjC_i. Thus, in the above proof, there are actually $q^{(m-1)}$ possible row vectors $(D_j)_m$, and consequently $q^{(m-1)}$ choices for each of the columns $\big((D_j)_m\big)^T$, $1 \leqslant j \leqslant n-m$. Hence, $q^{(n-m)(m-1)}$ choices for the C-matrix (D_{rt}) arise from each member of H.

Thus we have shown that the number of C-matrices associated with E_0^* 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, $N[C\colon E_0^*]$, of sets of C-matrices associated with E_0^*, $q^{(n-m)(m-1)}$ matrices to a set. No two of these matrices are congruent modulo q.*

5. The value of $N[C\colon E_0^*]$. 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 $N[C\colon E_0^*]$ for $n-m = 2$, 3, respectively.

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

LEMMA 1. *If $n-m = 2$, then*

$$N[H] = \prod_{i=0}^{s} N[H_{12}^{(i)}].$$

Proof. Let F be the family of all order distinct sets formed by the union of precisely one element from each $H_{12}^{(i)}$, $0 \leqslant i \leqslant s$. There are $\prod_{i=0}^{s} N[H_{12}^{(i)}]$ elements in F and congruence (8) is satisfied for each i. Hence $F \subseteq H$. Clearly $H \subseteq F$. Thus $N[H] = N[F] = \prod_{i=0}^{s} N[H_{12}^{(i)}]$, 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, $0 \leqslant i \leqslant s$; and let $H_3^{(i)}$ denote the collection of all order distinct sets of the form $\{g_1^{(i)}, g_2^{(i)}, g_3^{(i)}\}$ such that property (8) holds, that is:

$$g_r^{(i)} g_t^{(i)} \equiv -B_{hh} u_{rt} \pmod{p^{e(i)}}, \qquad \text{whenever } 1 \leqslant r < t \leqslant 3.$$

Let $N[H_3^{(i)}]$ denote the number of elements in $H_3^{(i)}$.

LEMMA 2. *If $n-m=3$, then*

$$N[H] = \prod_{i=0}^{s} N[H_3^{(i)}].$$

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 $N[H_{jk}^{(i)}]$, and Brande ([1], pp. 62-84) developed a similar formula for $N[H_3^{(i)}]$. We state, in the notation adopted in this paper, their results as Theorems 8 and 9, respectively.

THEOREM 8. *$N[H_{jk}^{(i)}]$ is zero, or*

$$N[H_{jk}^{(i)}] = \begin{cases} p_i^{2[e_i/2]}, & \text{if } t_i(u_{jj}) \geqslant e_i \text{ and } i \geqslant 0; \\ 2p_i^{2[t_i(u_{jj})/2]}, & \text{if } t_i(u_{jj}) < e_i \text{ and } i > 0; \\ 2^{2[t_i(u_{jj})/2]+M'}, & \text{if } t_i(u_{jj}) < e_i \text{ and } i = 0; \end{cases}$$

where $t_i(u_{jj})$ is defined by: $p_i^{t_i(u_{jj})} \| u_{jj}$, if $u_{jj} \neq 0$, and $t_i(u_{jj}) = e_i$, otherwise; $t_i(u_{jj}) \leqslant t_i(u_{kk})$; and $M' = 0, 1$ or 2 according as $e_0 - 2[t_0(u_{jj})/2] = 1, 2$ or 3, respectively.

THEOREM 9. *$N[H_3^{(i)}]$ is zero, or*

$$N[H_3^{(i)}] = \begin{cases} p_i^{3[e_i/2]}, & \text{if } t_i(u_{11}) \geqslant e_i \text{ and } i \geqslant 0; \\ 2p_i^{3[t_i(u_{11})/2]}, & \text{if } t_i(u_{11}) < e_i \text{ and } i > 0; \\ 2^{3[t_i(u_{11})/2]+M'}, & \text{if } t_i(u_{11}) < e_i \text{ and } i = 0; \end{cases}$$

where $t_i(u_{jj})$ and M' are defined as above with $j=1$; and $t_i(u_{11}) \leqslant t_i(u_{22}) \leqslant t_i(u_{33})$.

Let $\theta(i, E_0^*) = \min([e_i/2], [t_i(u_{11})/2])$; $\xi(E_0^*)$ be the number of odd primes, p_i, for which $e_i > t_i(u_{11})$; and

$$M(E_0^*) = \begin{cases} 1, & \text{if } e_0 - 2\theta(i, E_0^*) = 2; \\ 2, & \text{if } e_0 - 2\theta(i, E_0^*) \geqslant 3; \\ 0, & \text{otherwise}. \end{cases}$$

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 $E_0^* \in \mathfrak{G}^*$, then $N[C\colon E_0^*]$ is zero, or*

$$N[C\colon E_0^*] = 2^{M(E_0^*)+\xi(E_0^*)} \prod_{i=0}^{s} p_i^{(n-m)\theta(i, E_0^*)}.$$

6. Conditions for essential equality of C-matrices. Assume $\mathfrak{G}$ is non-empty, $n-m = 2, 3$ and let $E \in \mathfrak{G}$.

LEMMA 3. *Two C-matrices, C_1 and C_2, associated with $E \in \mathfrak{G}$, are essentially equal iff there exists an automorph Q_E of E such that*

$$(\operatorname{adj} B)(C_2 - C_1 Q_E) \equiv (0) \pmod{q}, \tag{10}$$

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 ([4], p. 888), there is an integral matrix R and an automorph Q_E of E such that

$$C_2 = BR + C_1 Q_E. \tag{11}$$

Since B is non-singular, $B^{-1} = (\operatorname{adj} B)/q$ exists, and hence (11) implies (10).

Conversely, if there exists an automorph Q_E' of E such that (10) is satisfied, then there exists an integral matrix $R' = B^{-1}(C_2 - C_1 Q_E')$ 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, $0 \leqslant i \leqslant s$, (z_{wv}) be an arbitrary $m \times (n-m)$ matrix, and t be such that $1 \leqslant t \leqslant n-m$. Then*

$$\sum_{w=1}^{m} B_{hw} z_{wt} \equiv 0 \pmod{p^e}$$

iff for each r, $1 \leqslant r \leqslant m$,

$$\sum_{w=1}^{m} B_{rw} z_{wt} \equiv 0 \pmod{p^e}.$$

Proof. Assume

$$\sum_{w=1}^{m} B_{hw} z_{wt} \equiv 0 \pmod{p^e}. \tag{12}$$

Let r be arbitrary, $1 \leqslant r \leqslant m$. Multiplying (12) by B_{rh}, applying Theorem 2, and recalling that $(B_{hh}, p_i) = 1$, (12) implies:

$$\sum_{w=1}^{m} B_{rw} z_{wt} \equiv 0 \pmod{p^e}.$$

Since r is arbitrary, the sufficiency is proved. The necessity is obvious.

Let the C-matrices $C_1 = (d_{rt})$ and $C_2 = (d'_{rt})$ belong to the same one of the $N[C\colon E]$ sets of C-matrices associated with E. Then for each t, $1 \leqslant t \leqslant n-m$, $(d_t)_m$ and $(d'_t)_m$ are solutions of $[tt\boldsymbol{D}]$. Then, by Corollary A to Theorem 5, for each i, there is precisely one $g_t^{(i)}$ and one $g_t'^{(i)}$ corresponding to $(d_t)_m$ and $(d'_t)_m$, respectively, such that

$$(13) \qquad g_t^{(i)} \equiv \sum_{w=1}^{m} B_{wh} d_{wt} \quad \text{and} \quad g_t'^{(i)} \equiv \sum_{w=1}^{m} B_{wh} d'_{wt} \pmod{p^{e(i)}}.$$

But, C_1 and C_2 belong to the same one of the $N[C\colon E]$ sets of C-matrices, hence they are generated by the same element of H, as is clear from the proof of Theorem 7. Thus, we must have $g_t^{(i)} = g_t'^{(i)}$ for each t and each i. Hence from (13) we obtain

$$(14) \qquad \sum_{w=1}^{m} B_{wh}[d'_{wt} - d_{wt}] \equiv 0 \pmod{p^{e(i)}},$$

for each i and t.

Now the $(n-m)\times(n-m)$ identity matrix, I, is an automorph of every form in $\mathfrak{G}$, hence let $Q_E = (V_{jk}) = I$. Thus, for each t, $1 \leqslant t \leqslant n-m$, $d_{wt} = \sum_{j=1}^{m} d_{wj} V_{jt}$. Hence (14) is equivalent to

$$(15) \qquad \sum_{w=1}^{m} B_{hw}\Big[d'_{wt} - \sum_{j=1}^{n-m} d_{wj} V_{jt}\Big] \equiv 0 \pmod{p^{e(i)}},$$

for each i and t. For each w and t, let Z_{wt} equal the expression in brackets in (15). Thus the $m\times(n-m)$ matrix $(Z_{wt}) = (C_2 - C_1 Q_E)$, and (15) is equivalent to

$$(16) \qquad \sum_{w=1}^{m} B_{hw} Z_{wt} \equiv 0 \pmod{p^{e(i)}}, \quad \text{for each } i \text{ and } t.$$

By Lemma 4, (16) is equivalent to

$$\sum_{w=1}^{m} B_{rw} Z_{wt} \equiv 0 \pmod{p^{e(i)}},$$

for each r, $1 \leqslant r \leqslant m$, and for each i and t. Since the p_i are distinct primes, it follows that

$$\sum_{w=1}^{m} B_{rw} Z_{wt} \equiv 0 \pmod{q}, \quad \text{for each } r \text{ and } t.$$

Hence, by (10), C_1 and C_2 are essentially equal. Thus we have proved

THEOREM 11. *If C_1 and C_2 are C-matrices which belong to the same one of the $N[C\colon E]$ sets of C-matrices, then C_1 and C_2 are essentially equal.*

7. An upper bound for $M(d, B)$. 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 $B = \operatorname{diag}(1, 1, 2, 3)$. Thus $\operatorname{adj} B$ is primitive, and $\mathfrak{G}^*$ may be chosen as the set of all binary reduced forms whose discriminant is -24.

Clearly, $E = (1, 0, 6) \in \mathfrak{G}^*$. Thus $B_{h_0h_0} = B_{33} = 3$, and $B_{h_1h_1} = B_{44} = 2$. A simple calculation shows that $g_1^{(0)} = 1$; $g_2^{(0)} = 0$; $g_1^{(1)} = 1$ and $g_1'^{(1)} = 2$; and $g_2^{(1)} = 0$. For $i = 0$, (8) is satisfied by $\{g_1^{(0)}, g_2^{(0)}\} = (1, 0)$; and for $i = 1$, (8) is satisfied by $\{g_1^{(1)}, g_2^{(1)}\} = (1, 0)$ and by $\{g_1'^{(1)}, g_2^{(1)}\} = (2, 0)$. 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 2×2 identity matrix, we find:

$$(\operatorname{adj} B)(C_2 - C_1 Q_E) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 6 & 0 \\ 6 & 0 \end{bmatrix} \equiv (0) \pmod{6}.$$

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 $N[C\colon E]$ sets of C-matrices associated with E. Therefore, the converse of Theorem 11 is not true in general.

By Theorem 10, for $n-m = 2, 3$, and $E \in \mathfrak{G}$, we can evaluate $N[C\colon E]$. Theorem 11 and the above example show that belonging to the same one of the $N[C\colon E]$ sets of C-matrices is a sufficient, but not a necessary condition for the essential equality of C-matrices. Thus, $P(d, B, E) \leqslant N[C\colon E]$, 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 12. *If B has primitive adjoint and $n-m = 2, 3$, then*

$$M(d, B) \leqslant \sum N[C\colon E_j] = \sum 2^{M(E_j)+\xi(E_j)} \prod_{i=0}^{s} p_i^{(n-m)\theta(i,E_j)},$$

where the sum is over all forms E_j defined by $\mathfrak{G}$.

References

[1] E. W. Brande, *The Representations of Binary Quadratic Forms by Quinary Quadratic Forms*, Ph. D. Dissertation, Saint Louis University, 1961.

[2] J. E. Fischer, *Quaternary-Binary Representations in Quadratic Forms*, Ph. D. Dissertation, Saint Louis University, 1954.

[3] W. V. D. Hodge and D. Pedoe, *Methods of Algebraic Geometry*, 3 vols., Cambridge 1953.

[4] B. W. Jones, *Representations by Quadratic Forms*, Ann. of Math. (2) 50 (1949), pp. 884-899.

SAINT LOUIS UNIVERSITY, SAINT LOUIS, MISSOURI
SAINT JOSEPH COLLEGE, EMMITSBURG, MARYLAND

Reçu par la Rédaction le 10. 8. 1966

ACTA ARITHMETICA
XIII (1968)

On the coefficients of the zeta function of an imaginary quadratic field*

by

RAYMOND G. AYOUB (University Park, Pa)

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

Let

$$\zeta_K(s) = \sum \frac{1}{N(\mathfrak{A})^s} = \sum_{n=1}^{\infty} \frac{F(n)}{n^s} \tag{1}$$

be the Dedekind zeta function of K where

$$F(n) = \sum_{N(\mathfrak{A})=n} 1. \tag{2}$$

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

$$\zeta_K(s) = \zeta(s) L(s, \chi_d) \tag{3}$$

and that

$$F(n) = \sum_{l|n} \chi_d(l)$$

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

Let

$$H(x) = \sum_{n\leqslant x} F(n). \tag{4}$$

It is known [3] that

$$H(x) = ax + \Delta_k(x) \tag{5}$$

where a is the residue of $\zeta_K(s)$ at $s = 1$ and where $\Delta_k(x) = O(x^{1/3})$ with the constant implied by the O depending on k.

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