REPRESENTATION BY QUADRATIC FORMS

GORDON PALL

1. Introduction. The elementary portions of the theory of integral representation of numbers or forms by quadratic forms will be somewhat simplified and generalized in this article. This indicates certain directions in which new applications can be made. The applications made here will be largely to the representation of numbers or binary quadratic forms by ternary quadratic forms. Particularly, we shall obtain the correct estimate (Theorem 10) needed to fill a lacuna in certain work of U. V. Linnik [1] on the representation of large numbers by ternary quadratic forms. Since Linnik applied his theorem on ternaries to prove [9] that every large number is a sum of at most seven positive cubes, a lacuna in this proof can now be regarded as filled.

While a genus, consisting of a finite number of classes of forms, is *regular* in the sense that one or other of its classes represents any number not trivially excluded by the generic conditions, it is difficult to prove anything general about the numbers representable separately by a single class. Thus, for example, $x^2+y^2+7z^2$ and $x^2+2y^2-2yz+4z^2$ are representative forms (one from each class) of the two classes of a certain genus, and represent between them all (and only) the positive integers not of the forms $7^{2k+1}(7n+r)$, $(r=3, 5, 6)$. But a given number (e.g. 3) not of the excluded forms may happen to be represented by one class but not the other. In this example it can be proved that each class represents all positive integers congruent to 0 or 1 mod 4 and not of the excluded type $7^{2k+1}(7n+r)$, and there is some reason to believe that all "large" numbers represented by either form are represented by the other. Although general theorems stating that single classes are regular for large numbers have been proved (Kloosterman [2], Tartakowsky [3], Ross and Pall [4]) for forms in four and more variables, the situation is more complicated in the case of positive ternary quadratic forms.

Examples illustrating this were published by the author in 1939 [5]. Thus, the forms $f=x^2+y^2+16z^2$ and $g=2x^2+2y^2+5z^2-2xz-2yz$ represent the two classes of a certain genus of determinant 16. It was proved that g represents no square m^2 such that all the prime factors of m are congruent to 1 mod 4. Since f obviously represents all squares, it is clear that g does not represent all the large numbers represented by its genus. The example shows also that, in general, a class may not represent the numbers consistent with its genus and divisible by a large square factor.

It may be of interest to state another property of f and g, that by combining classical results of Glaisher [6] with results on the representation of numbers

Received September 1, 1948.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

$8n+1$ in the Jones-Pall article mentioned earlier, one obtains precise formulae for the number of representations $f(n)$ and $g(n)$ of an arbitrary integer n by f and g. This is believed to be the first known example among genera of forms in more than two variables. If $r_0(n)$ denotes the number of representations of n as a sum of three squares (for which there are well-known expressions), then

$$\begin{aligned}
f(n) &= g(n) = r_0(n)/3 \text{ if } n \equiv 2 \text{ or } 5 \bmod 8;\\
f(n) &= g(n) = 0 \qquad \text{if } n \equiv 3,\, 6, \text{ or } 7 \bmod 8;\\
f(n) &= g(n) = (1-j/3)r_0(n) \text{ if } n = 4(4k+j),\, j = 0, 1, 2, 3;\\
f(n) &- g(n) = 0 \qquad \text{if } n \equiv 1 \bmod 8,\ n \text{ not square,}\\
&= (-1)^{\frac{1}{2}(s-1)}4s \quad \text{if } n = s^2,\ s \text{ odd and positive;}\\
f(n) &+ g(n) = 2r_0(n)/3 \text{ if } n \equiv 1 \bmod 8.
\end{aligned}$$

Linnik [1] obtained, by means of generalized quaternions, a theorem stating that under certain conditions (which are not satisfied by the preceding example) a class of positive-definite, ternary quadratic forms represents the sufficiently large odd numbers prime to the determinant which its genus represents. At a certain stage of his proof, he reduces the problem to that of representing a binary quadratic form $\phi = k\phi_1$(ϕ_1 properly or improperly primitive) as the sum of squares of three linear forms

$$(a_1x+b_1y)^2+(a_2x+b_2y)^2+(a_3x+b_3y)^2$$

such that the g.c.d. of the numbers $a_2b_3-a_3b_2$, $a_3b_1-a_1b_3$, $a_1b_2-a_2b_1$ is equal to the divisor k of ϕ. Later, ϕ is thus represented by a more general ternary quadratic form. He states that if D denotes the determinant of ϕ then for every positive ϵ, the number of such representations of ϕ is of the order $0(D^\epsilon)$; and that "this can be proved by methods similar to those of Gauss." Classical treatments (e.g. in [7]) seem, however, to have been restricted to the case where the divisor k of ϕ is squarefree; and Linnik's statement is in fact not true in general. The true estimate is given in Theorems 4 and 5, and involves the factor h, where h^2 is the largest square factor common to k and $ab-t^2$, where $\phi_1 = ax^2+2txy+by^2$; thus h can be as large as $D^{1/6}$.

Fortunately, the forms in which h is large can be counted differently, and hence Linnik's applications can be carried through successfully. This was indicated by the author [8] in 1941 for the special case of ordinary quaternions and a sum of three squares.

Notations. Unless otherwise indicated, capital letters $A,\ldots,Z$ denote matrices. The symbol $T_1^{(n,k)}$ indicates that T_1 has n rows and k columns. $A,\ldots,G$ are symmetric. German letters $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{t}$ designate column vectors. T^{T} denotes the transpose of T. I is an identity matrix; a zero matrix is denoted by 0; p is a prime. The determinant of a quadratic form $f = \mathfrak{x}'A\mathfrak{x}$ is denoted by $|f|$ or $|A|$. The form $\phi_1 = ax^2+2txy+by^2$ is properly primitive ($p.p.$) if a, $2t$, and b are relatively prime (a, t, b integers); improperly primitive ($i.p.$) if a, t, b are relatively prime and a, b are even. The terms *unimodular* and *unit-modular* designate integral square matrices of respective determinants 1 and ± 1.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

2. Integral and primitive representations. Let $A^{(n,n)}$ and $B_1^{(k,k)}$ be non-singular, symmetric, real matrices, $1 \leq k \leq n$. We say that A *represents* B_1 if there exists an integral matrix $T_1^{(n,k)}$ such that

$$T^{\mathsf{T}}{}_1 A T_1 = B_1; \tag{1}$$

and we call T_1 a *representation* of B_1 *by* A. Also, T_1, or $\mathfrak{x} = T_1\mathfrak{y}$, is called a representation of the quadratic form $\mathfrak{y}^{\mathsf{T}}B_1\mathfrak{y}$ by the quadratic form $\mathfrak{x}^{\mathsf{T}}A\mathfrak{x}$. Note that since a representation is a matrix, two representations are considered as equal only if corresponding components are equal. Thus the solution $x = 7$, $y = 4$ of $x^2 + y^2 = 65$ gives rise under permutations and sign-changes to eight representations of 65 by the form $x^2 + y^2$, or by its matrix I.

In a similar manner, since $T^{\mathsf{T}}{}_1(W^{\mathsf{T}}AW)T_1 = (WT_1)^{\mathsf{T}}A(WT_1)$, where W is any unimodular automorph of A, the matrix WT_1 is a representation of B_1 by A, with T_1. As W ranges over all the unimodular automorphs of A, the set of matrices WT_1 will be called a *set of representations*, and denoted by (WT_1).

If the g.c.d. μ of the minor determinants of order k in T_1 is 1, the representation is termed *primitive*. If A and B_1 are integral, the problem of finding the representations of B_1 by A can be reduced to that of finding the primitive representations of a certain finite set of matrices by A. We use for this purpose the following lemma.

LEMMA 1. *Let $T_1^{(n,k)}$ be an integral matrix of g.c.d. μ, $1 \leq k \leq n$. Then T_1 can be expressed in one and only one way in the form*

$$T_1 = R_1 M, \tag{2}$$

where $R_1^{(n,k)}$ is primitive, $M^{(k,k)}$ is integral, $|M| = \mu$, and M has the form

$$\begin{bmatrix} \mu_1 & \mu_{12}, & \ldots, & \mu_{1k} \\ 0 & \mu_2, & \ldots, & \mu_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0, & \ldots, & \mu_k \end{bmatrix}, \qquad \begin{array}{l} \mu_1, \ldots, u_k = \mu, \\ 0 \leqq \mu_{ji} < \mu_i \; (i = 2, \ldots, k; j < i), \end{array} \tag{3}$$

where the elements $\mu_1, \ldots, \mu_k$ are positive integers, the elements μ_{ji} above each μ_i, are integers reduced modulo μ_i, and those below the principal diagonal are 0.

Proof. By Lemma 3 below, we can obtain (2) with R_1 primitive, and M merely integral and of determinant μ, but have the possibility of replacing R_1 by R_1V^{-1} and M by VM, with V unimodular. Hence the lemma is a consequence of the following result, first given for a general k by C. Hermite [11].

LEMMA 2. *If $M^{(k,k)}$ is integral, and $|M| = \mu > 0$, then by choice of a unimodular matrix V, VM can be made equal to one and only one Hermite-matrix* (3).

If we substitute $T_1 = R_1 M$ in (1), we have

$$R^{\mathsf{T}}{}_1 A R_1 = B'_1, \textit{ where } B'_1 = (M^{\mathsf{T}})^{-1} B_1 M^{-1}, \tag{4}$$

and the left member is an integral, symmetric matrix. Hence

$$B_1 = M^{\mathsf{T}} B'_1 M, \tag{5}$$

where B'_1 is integral. Thus μ^2 is restricted to be one of the finitely many square factors of $|B_1|$, and hence the Hermite-matrix M has only a finite number

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

of possible values. *All the representations of B_1 by A are found, without duplication, in the formula $T_1 = R_1 M$, where M ranges over the Hermite-matrices* (3) *such that $(M^{\mathsf{T}})^{-1} B_1 M^{-1}$ is an integral matrix and R_1 runs over the primitive representations of every such matrix by A.*

If $k = 1$, this amounts to the observation that all integral solutions t of $f(t_1, \ldots, t_n) = b_1$ are given by $\mathfrak{t} = \mu \mathfrak{x}$, where μ^2 is a square factor of b_1 and $\mathfrak{x}$ is a primitive solution of $f(x_1, \ldots, x_n) = b_1/\mu^2$.

It should be noted that, in finding or enumerating the representations of B_1 by A, either can be replaced by an equivalent matrix. If A is replaced by $P^{\mathsf{T}} A P$ and B_1 by $V^{\mathsf{T}} B_1 V$ where P and V are unimodular, then the representation T_1 is replaced by the corresponding representation $P^{-1} T_1 V$ of $V^{\mathsf{T}} B_1 V$ by $P^{\mathsf{T}} A P$.

It can be proved that the integral matrix T_1 has a *greatest right divisor* M, namely an integral non-singular matrix $M^{(k,k)}$ such that (a) $T_1 = R_1 M$ for some integral matrix R_1, and (b) if $N^{(k,k)}$ is any integral matrix such that $T_1 N^{-1}$ is integral, then MN^{-1} is integral. More generally, the following result holds.

LEMMA 3. *Let $T_1^{(n,k)}$ be an integral matrix of rank k, and denote the g.c.d. of the minor determinants of order k in T_1 by μ. Assume $1 \leq k < n$. Then,* (i) *T_1 has a greatest right divisor M,* (ii) $|M| = \pm \mu$, (iii) *every greatest right divisor* of T_1 *is given by VM, where $V^{(k,k)}$ is unit-modular,* (iv) *there exists an integral matrix $T_2^{(n,n-k)}$, called a (right) complement of T_1, such that $(T_1 \ T_2)$ has determinant μ,* (v) *if T_2 is a particular complement of T_1, then every complement T^*_2 of T_1 is given by*

$$T^*_2 = T_1 H + T_2 U, \tag{6}$$

where $U^{(n-k,n-k)}$ is an arbitrary unimodular matrix and $H^{(k,n-k)}$ is any rational matrix such that $T_1 H$ (or MH) is integral.

It should be remarked that (i), (ii), and (iii) hold also when $k = n$. For the proof we refer to Siegel [10]. However, a proof of (v) for the primitive case will be useful later:

LEMMA 4. *If T_1 is primitive, and T_2 is one matrix such that $(T_1 T_2)$ is unimodular, then the most general such complement T^*_2 is given by* (6) *with U any $(n-k, n-k)$ unimodular matrix and H any $(k, n-k)$ integral matrix.*

Proof. Let $(S_1 S_2)^{\mathsf{T}}$, with $S_1^{(n,k)}$ and $S_2^{(n,n-k)}$, denote $(T_1 T_2)^{-1}$. Then

$$S^{\mathsf{T}}_1 T_1 = I_1, \quad S^{\mathsf{T}}_1 T_2 = 0, \quad S^{\mathsf{T}}_2 T_1 = 0, \quad S^{\mathsf{T}}_2 T_2 = I_2, \tag{7}$$

where I_1 and I_2 denote identity matrices, of orders k and $n - k$. Hence, if T^*_2 is any complement of T_1,

$$\begin{bmatrix} S^{\mathsf{T}}_1 \\ S^{\mathsf{T}}_2 \end{bmatrix} (T_1 T^*_2) = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}, \tag{8}$$

where $H = S^{\mathsf{T}}_1 T^*_2$ and $U = S^{\mathsf{T}}_2 T^*_2$. Evidently, H is integral and (comparing determinants) U is unimodular. Multiplying on the left by $(T_1 T_2)$, we have

$$(T_1 T^*_2) = (T_1 T_2) R, \text{ where } R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}, \tag{9}$$

and hence (6).

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

3. The basic algorithm. Let T_1 be a primitive representation of B_1 by A, $1 \leq k < n$. Choose a particular complement T_2 of T_1, so that $T = (T_1\, T_2)$ is unimodular, and construct the matrix equivalent to A,

$$B = T^{\mathsf{T}} AT = \begin{bmatrix} T^{\mathsf{T}}{}_1 AT_1 & T^{\mathsf{T}}{}_1 AT_2 \\ T^{\mathsf{T}}{}_2 AT_1 & T^{\mathsf{T}}{}_2 AT_2 \end{bmatrix} = \begin{bmatrix} B_1 & K^{\mathsf{T}} \\ K & B_2 \end{bmatrix}, \tag{10}$$

K and B_2 being defined by the last equation. Construct also $S^{\mathsf{T}} = T^{-1}$, $S = (S_1\, S_2)$, where $S_1^{(n,k)}$ and $S_2^{(n,n-k)}$, denote adj A by C, and construct

$$D = \operatorname{adj} B = S^{\mathsf{T}} CS = \begin{bmatrix} S^{\mathsf{T}}{}_1 CS_1 & S^{\mathsf{T}}{}_1 CS_2 \\ S^{\mathsf{T}}{}_2 CS_1 & S^{\mathsf{T}}{}_2 CS_2 \end{bmatrix} = \begin{bmatrix} D_1 & L^{\mathsf{T}} \\ L & D_2 \end{bmatrix}. \tag{11}$$

The algorithm is based on a consideration of what happens to B (or D) when T_2 is replaced by other complements $T_1H + T_2U$ (H integral, U unimodular) of T_1.

Denote $|B_1|$ and $|D_2|$, respectively, by b_1 and d_2. It will be convenient to record here the result of "completing squares" relative to B_1 and D_2, in B and D. To complete squares, we replace B by $P^{\mathsf{T}}BP$ and D by $Q^{\mathsf{T}}DQ$, where

$$P = \begin{bmatrix} I_1 & -B_1^{-1}K^{\mathsf{T}} \\ 0 & I_2 \end{bmatrix}, \; Q = \begin{bmatrix} I_1 & 0 \\ -D_2^{-1}L & I_2 \end{bmatrix}, \; PQ^{\mathsf{T}} = Q^{\mathsf{T}}P = I;$$

and so obtain

$$P^{\mathsf{T}}BP = \begin{bmatrix} B_1 & 0^{\mathsf{T}} \\ 0 & b_1^{-1}G \end{bmatrix}, \; Q^{\mathsf{T}}DQ = \begin{bmatrix} d_2^{-1}E & 0^{\mathsf{T}} \\ 0 & D_2 \end{bmatrix}, \tag{12}$$

where

$$G = b_1B_2 - K(\operatorname{adj} B_1)K^{\mathsf{T}},\; E = d_2D_1 - L^{\mathsf{T}}(\operatorname{adj} D_2)L. \tag{13}$$

If $a = |A|$, then $|D| = a^{n-1}$, and it will be found that, since $BD = aI$,

$$L^{\mathsf{T}} = -B_1^{-1}K^{\mathsf{T}} D_2,\; GD_2 = ab_1I_2,\; B_1E = ad_2I_1,\; d_2 = b_1a^{n-k-1}, \tag{14}$$
$$|G| = ab_1^{n-k-1},\; \operatorname{adj} G = b_1^{n-k-2}D_2,\; E = a^{n-k} \operatorname{adj} B_1.$$

If T_2 is replaced by $T_1H + T_2U$, then T is replaced by TR, where

$$R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix} = \begin{bmatrix} I_1 & 0 \\ 0 & U \end{bmatrix}\begin{bmatrix} I_1 & H \\ 0 & I_2 \end{bmatrix}. \tag{15}$$

Thus, the effect on the quadratic form $\mathfrak{x}^{\mathsf{T}} B\mathfrak{x}$, of replacing T_2 by $T_1H + T_2U$, is to apply the unimodular transformation U to the variables $x_{k+1}, \ldots, x_n$, and then the translation

$$x_i = y_i + \sum_{j=k+1}^{n} h_{ij}x_j (i = 1, \ldots, k),\;\; x_j = y_j (j = k+1, \ldots, n) \tag{16}$$

where $H = (h_{ij})$. The matrix G obtained by completing squares is evidently not affected by the translation (16). We thus have the following theorem.

THEOREM 1. *With any primitive representation T_1 of B_1 by A is associated an aggregate of pairs of matrices*:

$$U^{\mathsf{T}} GU \text{ and } U^{\mathsf{T}} K + H^{\mathsf{T}} B_1, \tag{17}$$

the aggregate being derivable from any one pair G and K by use of an arbitrary unimodular U and integral H. Here G is the matrix obtained on "completing squares" with respect to B_1, in the matrix $B = T^{\mathsf{T}} AT$, where T is a unimodular matrix having T_1 as its first k columns. The same matrices G and K are associated with WT_1, where W is any unimodular automorph of A.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

The last statement is evident, since, if T is replaced by WT, the same matrices B and hence the same matrices G and K are obtained.

The important case $k = 1$ is worth formulating separately.

THEOREM 2. *Let* $\mathfrak{t}$ *be a primitive representation of a non-zero number* m *by a real non-singular quadratic form* f. *All forms* $g = mx_1^2 + \ldots$ *obtained from* f *by unimodular transformations whose first column is* $\mathfrak{t}$, *are obtainable from any particular one of them,*

(18) $$g_1 = m(x_1 + \ldots)^2 + \phi(x_2, \ldots, x_n),$$

of which the form after completing squares is here displayed, by applying an arbitrary unimodular transformation to ϕ, *and then replacing* x_1 *by* $x_1 + h_2x_2 + \ldots + h_nx_n$ *with integers* $h_2, \ldots, h_n$. *The same forms g are obtained if* $\mathfrak{t}$ *is replaced by* $W\mathfrak{t}$, *where* W *is a unimodular automorph of* f.

The invariance of the class of ϕ for a given primitive set of representations of m has important consequences in the theory of reduction of n-ary quadratic forms. It may be remarked also that there are applications in cosmogony of results of the sort that there is only one set of representations of certain numbers m, as for example [15] of 1 by $x^2 - y^2 - z^2 - t^2$; and this is connected (as will be clear from the following) with the fact that only one class of forms ϕ may appear on completing squares.

Conversely, for given B_1, G, and K, we can set

(19) $$G + K(\operatorname{adj} B_1)K^{\mathsf{T}} = b_1B_2, \quad B = \begin{bmatrix} B_1 & K^{\mathsf{T}} \\ K & B_2 \end{bmatrix}.$$

Observe that if G and K are replaced by $U^{\mathsf{T}}GU$ and $U^{\mathsf{T}}K + H^{\mathsf{T}}B_1$, then B is replaced by $R^{\mathsf{T}}BR$ with R as displayed in (9). If it *happens* that $A \sim B$, let T be a unimodular transformation of A into B. Then, as is well known, the most general such transformation is WT, where W ranges over the unimodular automorphs of A. Hence the matrices WT_1, where T_1 consists of the first k columns of T, constitute a set (WT_1) of primitive representations of B_1 by A associated with the pair G and K.

By confining attention to integral matrices A and B_1, some limitation is obtained on the possible matrices G and K. Then K and G are integral matrices such that

(20) $$K(\operatorname{adj} B_1)K^{\mathsf{T}} \equiv -G \pmod{b_1}, \qquad (b_1 = |B_1|).$$

Since $B_1(\operatorname{adj} B_1) = b_1I_1$, evidently if K satisfies (20), all the matrices $K + H^{\mathsf{T}}B_1$ with $H^{(k,n-k)}$ an integral matrix, are also solutions. These matrices are said to form a *right-sided residue class modulo* B_1, and two matrices in the same right-sided residue class will be termed *congruent modulo* B_1 (or *right-congruent*, to avoid ambiguity).

If a matrix G is chosen in the class of equivalent matrices $U^{\mathsf{T}}GU$, then U is restricted to be a unimodular automorph of G, and the associated matrices K satisfying (20) constitute a *complex of solutions of* (20), in accordance with the following definition. Two integral matrices K and K' are said to be in the same complex of solutions of (20) if, for some unimodular automorph U of G, $U^{\mathsf{T}}K$ and K' are congruent modulo B_1.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

Thus, every set (WT_1) of primitive representations of B_1 by A is uniquely associated with a certain class of matrices G, and if we select a matrix G of the class, with a unique complex of solutions K of (20). Conversely, any symmetric matrix G and associated complex of solutions of (20) is connected with a set of primitive representations of B_1 by some matrix A'.

In some cases, a set of nonequivalent matrices $A', \ldots, A^{(h)}$ and a set of nonequivalent matrices $G', \ldots, G^{(s)}$, each $G^{(j)}$ $(j = 1, \ldots, s)$ being accompanied by one or more complexes of solutions K of (20) with $G = G^{(j)}$, can be associated by our algorithm. For example, if $A', \ldots, A^{(h)}$ consist of representatives (one from each class) of a given determinant a, then (cf. (14)) $G', \ldots, G^{(s)}$ will be matrices of determinant ab_1^{n-k-1}; and if K is a solution of (20) with G one of the $G^{(j)}$, then the matrix B constructed as in (19) will have determinant a, and hence must be equivalent to one of $A', \ldots, A^{(h)}$. Examples will show that the matrices $G', \ldots, G^{(s)}$ may not comprehend all classes of determinant ab_1^{n-k-1}, since (20) may not be solvable for some of these. An important case is that where $A', \ldots, A^{(h)}$ are representatives of the classes of a genus. Then $G', \ldots, G^{(s)}$ can be shown to consist of the classes of one or more genera. In general, not every complex of solutions of K of (20) with $G = G^{(j)}$ will be such that the matrices B constructed therefrom as in (19) are in a prescribed genus, and it becomes necessary to specify those solutions.

It should be noted that, if $k = n - 1$, G is a matrix of one element, namely $ab_1^{n-k-1} = a = |A|$. The only unimodular automorph of G is $U = [1]$. Congruence (20) is then a single quadratic congruence

$$\sum_{i,j=1}^{n-1} c_{ij} k_i k_j \equiv -a \pmod{b_1}, \tag{21}$$

where adj $B_1 = (c_{ij})$ and $K = [k_1, k_2, \ldots, k_{n-1}]$. Accordingly, all the primitive representations of an $(n - 1)$-ary quadratic form by an n-ary quadratic form f can be found by solving (21), constructing from these solutions quadratic forms g with matrix B as in (19), and determining whether f is equivalent to such forms g.

This process is somewhat simpler than that of Gauss, Smith, and Minkowski, who preferred to work with the adjoint form (11), as will be briefly indicated in § 9. If the matrices G are known, the process can be used for $n - k > 1$.

4. A fundamental quantitative relation. The preceding association can be put on a more quantitative basis by use of the following theorem.

THEOREM 3. *Let A, T_1, B_1, G, and K be associated as in the preceding algorithm. Let $\Gamma_1(A, T_1)$ denote the subgroup of unimodular automorphs W of A such that $WT_1 = T_1$, and $\Gamma_2(G, K)$ the subgroup of unimodular automorphs U of G such that $U^{\mathsf{T}} K$ and K are congruent modulo B_1. The two subgroups are isomorphic.*

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

Proof. If T is unimodular and T_1 is the matrix of its first k columns, and $B = T^{\mathsf{T}} AT$, then the most general unimodular transformation of A into B with T_1 the matrix of its first k columns is given by WT with W in $\Gamma_1(A, T_1)$. For every such W, $T^{-1}WT$ is an automorph of B of the special form

$$T^{-1}WT = T^{-1}(T_1 \quad WT_2) = R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}. \tag{22}$$

The condition $R^{\mathsf{T}} BR = B$ expands into

$$K = U^{\mathsf{T}} K + H^{\mathsf{T}} B_1, \quad U^{\mathsf{T}} GU = G. \tag{23}$$

Hence U belongs to $\Gamma_2(G, K)$. Conversely, if U is in $\Gamma_2(G, K)$, and H is defined by (23_1), then $R^{\mathsf{T}} BR = B$ for the R displayed in (22), and $W = TRT^{-1}$ is an automorph of A such that $WT_1 = TR(I_1\, 0)^{\mathsf{T}} = (T_1\, T_2)(I_1\, 0)^{\mathsf{T}} = T_1$. This sets up a one-one correspondence between the two subgroups, and is it easily verified that this correspondence is preserved under multiplication.

Corollary. *If $k = n - 1$, the representations WT_1 of a set are different for different automorphs W, and the only automorph W of A such that $WT_1 = T_1$ is* $W = I$.

Proof. The matrix G is unary and the only U is [1]. Note the assumption here that A and B_1 are non-singular.

The number ν of elements in $\Gamma_2(G, K)$ may be finite or infinite, but the index denoted by γ, of $\Gamma_2(G, K)$ within the group $\Gamma_2(G)$ of all unimodular automorphs U of G, is finite. Indeed, if the elements of $\Gamma_2(G, K)$ are denoted by U', U'', . . . , then each coset $U'V$, $U''V$, . . . is characterized by the property that the products $V^{\mathsf{T}}\, U'^{\mathsf{T}}\, K$, $V^{\mathsf{T}}\, U''^{\mathsf{T}}\, K$, . . . , are congruent modulo B_1; and the number of incongruent residues modulo B_1 is finite. Thus γ is equal to the number of incongruent elements K modulo B_1 in a complex of solutions of (20). If the number u of automorphs U of G is finite, $u = \nu\gamma$. Hence, by Theorem 3, if also the number w of automorphs W of A is finite,

$$\frac{1}{\nu} = \frac{\textit{number of distinct representations } WT_1}{w} = \frac{\gamma}{u}. \tag{24}$$

If w is finite, the *weight of a representation* T_1 (*by* A) is defined to be $1/w$. By (24), the sum of the weights of the representations in a set (WT_1) is $1/\nu$. Now ν is finite when u is finite, even though w may be infinite. It is consistent and natural to define the *weight of a set of representations* (WT_1) to be $1/\nu$, if ν is finite.

The association of § 3 can therefore be given the following quantitative form. Let the numbers u_j of unimodular automorphs of $G^{(j)}$ be assumed finite, ($j = 1, \ldots, s$). Denote by $A^{(i)}(B_1)$ the sum of the weights of all sets of primitive representations of B_1 by $A^{(i)}$; and let $\rho(G^{(j)})$ denote the number of solutions K of (20) (with $G = G^{(j)}$) which are incongruent modulo B_1 and are such that the corresponding matrix B in (19) is equivalent to one of the $A^{(i)}$. Then

$$\sum_{i=1}^{h} A^{(i)}(B_1) = \sum_{j=1}^{s} \rho(G^{(j)})/u_j. \tag{25}$$

Note that if $A^{(i)}[B_1]$ denotes the number of primitive representations of B_1 by

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

$A^{(i)}$, and the numbers $w_1, \ldots, w_h$ of unimodular automorphs of $A', \ldots, A^{(h)}$ are finite, the left member of (25) has the form $\Sigma A^{(i)}[B_1]/w_i$.

The *weight of a matrix*, or class, is the reciprocal of the number of its unimodular automorphs. Hence the right member of (25) is the sum of the weights of the matrices $G^{(j)}$ multiplied by $\rho(G^{(j)})$. Since matrices of a given genus can be supposed congruent to any modulus, $\rho(G^{(j)})$ depends only on the genus of $G^{(j)}$. Hence, if the matrices $G^{(j)}$ include the classes of a genus τ, and $\rho(\tau)$ denotes the value of $\rho(G)$ for G in τ, the corresponding terms in (25) unite into $\rho(\tau)w(\tau)$ where $w(\tau)$ denotes the weight of the genus, *i.e.* the sum of weights of its classes.

5. An example: representation by binary quadratic forms, $n = 2$, $k = 1$. The reader may find it of interest to review this classical case as an instance of the preceding methods. Let $f = [a, b, c]$ denote an integral binary quadratic form of non-zero discriminant $d = b^2 - 4ac$. It is desired to find the primitive representations $\mathfrak{x}$ of a given non-zero integer m by f, *i.e.* the coprime solutions x_1, x_2 of

(a) $$ax_1^2 + bx_1x_2 + cx_2^2 = m.$$

If $\mathfrak{x}$ is a primitive solution of (a), there exist integers y_1, y_2 such that $x_1y_2 - x_2y_1 = 1$; and it is easily seen that the general formula for such integers is given in terms of a particular pair by $y_1 + hx_1$, $y_2 + hx_2$, with h an arbitrary integer. The unimodular $T = [\mathfrak{x}\ \mathfrak{y}]$ replaces f by $g = [m, n, q]$ where

(b) $$n = 2ax_1y_1 + b(x_1y_2 + x_2y_1) + 2cx_2y_2,$$

m is given by (a), and q is then fixed by the discriminant $d = n^2 - 4mq$. If y_1 and y_2 are replaced by $y_1 + hx_1$ and $y_2 + hx_2$, g is replaced by the equivalent form $[m, n + 2hm, q']$. Thus, every primitive representation $\mathfrak{x}$ of m by f is associated with a solution $z = n$ of

(c) $$z^2 \equiv d (\mathrm{mod}\ 4m), \quad 0 \leq z < |2m|.$$

For any unimodular automorph W of f, WT replaces f by the same g, and the set of primitive representations $W\mathfrak{x}$ is associated with the same root z of (c).

Conversely, for every solution z of (c), consider the integral form

(d) $$g_z = [m, z, (z^2 - d)/(4m)], \text{ of discriminant } d.$$

If f is not equivalent to g_z, then no primitive representations of m by f are associated with z. If $f \sim g_z$, and T is a unimodular transformation of f into g_z, the most general such transformation is WT, W ranging over the unimodular automorphs of f. The first columns $W\mathfrak{x}$ of WT constitute a set of primitive representations of m by f associated with z. Hence we have two theorems:

THEOREM A (Gauss). *Let $f = [a, b, c]$ be an integral binary quadratic form of non-zero discriminant d, m be a non-zero integer. The number $f'(m)$ of primitive sets of representations of m by f is equal to the number of solutions z of* (c) *such that $f \sim [m, z, (z^2 - d)/(4m)]$.*

THEOREM B (Dirichlet). *Let $f_1, \ldots, f_h$ be representative forms, one from each class, of integral binary quadratic forms of a given non-zero discriminant d, m be*

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

a non-zero integer. Let $R'(m, d)$ denote the number $f'_1(m)+\ldots+f'_h(m)$ of sets of primitive representations of m by the system of forms $f_1, \ldots, f_h$. Then $R'(m, d)$ equals the number of solutions z of (c).

If we desired the number of sets of primitive representations of m by the system of *primitive* classes of discriminant d, we would merely restrict z to be a solution of (c) such that g_z is primitive. Or, if we wished the classes to be those of a given genus, we could express the condition that g_z is in that genus. It is readily shown that if m is divisible by no prime p such that d/p^2 is an integer of the form $4k+0$ or 1, then m is represented in at most one genus of discriminant d, and that g_z is necessarily primitive,—so that both the preceding conditions are somewhat trivial in the binary case.

6. The primitive representation of a binary quadratic form as a sum of three squares. As a preliminary to its extension in § 8, we consider by the preceding methods the classic problem of finding the number N of primitive representations of a positive-definite classic binary quadratic form $\phi = [a', 2t', b']$ by $x^2+y^2+z^2$, that is the number of solutions of the identity

$$a'x^2+2t'xy+b'y^2=(\alpha_1 x+\beta_1 y)^2+(\alpha_2 x+\beta_2 y)^2+(\alpha_3 x+\beta_3 y)^2$$

in integers $\alpha_1, \ldots, \beta_3$ such that $\alpha_2\beta_3-\alpha_3\beta_2$, $\alpha_1\beta_2-\alpha_2\beta_1$, $\alpha_3\beta_1-\alpha_1\beta_3$ are relatively prime. Here $A = I^{(3,3)}$, B_1 is the matrix of ϕ, $b_1=a'b'-t'^2>0$, and (21) reduces to

$$b'k_1^2-2t'k_1k_2+a'k_2^2 \equiv -1 \pmod{b_1}, \tag{26}$$

with $K=[k_1, k_2]$. For any integral solution K of (26), the matrix

$$B = \begin{bmatrix} B_1 & K^{\mathsf{T}} \\ K & B_2 \end{bmatrix}, \text{ where } B_2=(1+b'k_1^2-2t'k_1k_2+a'k_2^2)/b_1,$$

is a classic, positive-definite matrix of determinant 1, and hence (since there is only one class of such matrices) is equivalent to A. Since A has 24 unimodular automorphs and $G=[1]$, $N=24\lambda$, where λ is the number of solutions K modulo B_1 of (26). The computation of λ is reduced to that of the number μ of solutions K modulo b_1, by the following lemma.

LEMMA 5. *Let $B_1^{(k,k)}$ be assumed merely integral and of non-zero determinant $\pm\beta$, $\beta>0$. Set $H^{\mathsf{T}}=[h_1, \ldots, h_k]$. As $h_1, \ldots, h_k$ run through all integers, $H^{\mathsf{T}} B_1$ gives rise to exactly β^{k-1} incongruent matrix residues modulo β.*

Proof. The property in question is unaltered if B_1 is multiplied on both sides by unit-modular matrices. Hence B_1 can be replaced by a diagonal matrix $\{e_1, \ldots, e_k\}$, where the e's are positive integers and their product equals β. Then $H^{\mathsf{T}} B_1$ is the diagonal matrix $\{h_1e_1, \ldots, h_ke_k\}$, and the elements have, independently, $\beta/e_1, \ldots, \beta/e_k$ residues modulo β.

Now μ/λ is equal to the number of incongruent residues modulo b_1 which are obtained, for given K, from $K+H^{\mathsf{T}} B_1$ as $H^{\mathsf{T}}=[h_1, h_2]$ ranges over all integral vectors. By Lemma 5, $\mu/\lambda=b_1$. Hence $N=24\,\mu/b_1$.

The conditions for (26) to be solvable (and hence for ϕ to be primitively representable as a sum of three squares) will now be examined. No odd prime p can divide all three numbers a', t', and b', since such a prime would divide the

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

modulus b_1 and does not divide the right member -1. Similarly, if a' and b' are even, then t' must be odd, hence $b_1 \equiv 3 \bmod 4$. Since, by (26), ϕ represents $-1 \bmod p$, the generic character $(\phi|p)$ must have the value $(-1|p)$ for every odd prime p dividing b_1. Now, if ϕ_1 is any primitive non-negative binary quadratic form of discriminant d $(= -2^q e,\ e$ odd, $q \geq 0)$, then the generic characters of ϕ_1 are known to satisfy

$$(27) \qquad (2|m)^q(-1|m)^{\frac{1}{2}(e+1)} \prod_{i=1}^{s} (m|p_i) = 1,$$

where $|e| = p_1 p_2 \ldots p_s$ expresses $|e|$ as a product of primes, and m denotes any integer prime to d and represented by ϕ_1. If $b_1 \equiv 4$ or $0 \bmod 8$, the residue mod 4 or 8 of the odd numbers represented by ϕ is invariant, and by (26) this residue has to be that of -1; however, if we substitute -1 for m in (27), it reduces to the impossibility $(-1)^{\frac{1}{2}(e+1)}\ (-1)^{\frac{1}{2}(e-1)} = 1$. Hence $b_1 \not\equiv 0 \bmod 4$. The same contradiction is found if ϕ is properly primitive and $e = b_1 \equiv 3 \bmod 4$. Finally, if ϕ is improperly primitive (hence $b_1 \equiv 3 \bmod 4$), then the application of (27) to $\phi_1 = \frac{1}{2}\phi$, for which $(\phi_1|p) = (-2|p)$, shows that $(2|b_1) = -1$, *i.e.* $b_1 \equiv 3 \bmod 8$. Hence, *a positive definite classic binary quadratic form is primitively representable as a sum of three squares if and only if* ϕ *is p.p. and* $|\phi| \equiv 1$ *or* $2 \bmod 4$, *or* ϕ *is i.p. and* $|\phi| \equiv 3 \bmod 8$, *and* ϕ *represents* $-1 \bmod |\phi|$.

Now a form equivalent to ϕ can be given the residue $ax^2 + hb_1y^2 \bmod b_1$, where $a \equiv -1 \equiv h \bmod b_1$. Hence (26) has $2^\nu b_1$ solutions, and $N = 24.2^\nu$, where ν denotes the number of distinct odd primes dividing b_1.

To obtain the number of primitive representations of a positive integer b_1 $(\equiv 1$ or $2 \bmod 4$, or $3 \bmod 8)$ as a sum of three squares, we may take $n = 3$, $k = 1$, $A' = I$, $h = 1$, $B_1 = b_1$ in (25). Then $G', \ldots, G^{(s)}$ are representative matrices (one from each class) of the particular genus of binary quadratic forms of determinant b_1 which are primitively representable by adj I $(= I)$. Using the residue $-x^2 - b_1y^2 \bmod b_1$ for any of the $G^{(i)}$, (20) becomes

$$\begin{bmatrix} k_1^2 & k_1k_2 \\ k_2k_1 & k_2^2 \end{bmatrix} \equiv - \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix} \pmod{b_1},$$

which has 2^ν solutions k_1, $k_2 \bmod b_1$. Hence, the number of primitive representations of b_1 as a sum of three squares is equal to $24.2^\nu\ s/u$, where s denotes the number of classes of the genus described above, and u is the number of unimodular automorphs of any form in that genus ($u = 4$ if $b_1 = 1$, $u = 6$ if $b_1 = 3$, $u = 2$ otherwise.)

7. Properties of Hermite-matrices. To obtain all representations, primitive or imprimitive, of B_1 by A, we have to consider the Hermite-matrices M such that $M^{\mathsf{T}^{-1}}\ B_1 M^{-1}$ is in a genus capable of primitive representation by A. The discussion will be simplified by reduction to the case where $|M|$ is a power of a prime.

LEMMA 6. (i) *Let* m_1, m_2 *be coprime integers. An integral matrix* Q *of determinant* m_1m_2 *has a unique Hermite-matrix of determinant* m_2 *as a right-divisor.* (ii) *If* $m_1, m_2, \ldots, m_s$ *are coprime in pairs, a matrix* Q *of determinant*

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

$m_1m_2 \dots m_s$ can be expressed in one and only one way in the form $UM'_1M'_2, \dots, M'_s$, where U is unimodular and $M'_1, \dots, M'_s$ are Hermite-matrices of respective determinants $m_1, \dots, m_s$. (iii) *If $M_1, \dots, M_s$ are Hermite-matrices of determinants $m_1, \dots, m_s$, coprime in pairs, then the matrix Q of determinant $m_1m_2 \dots m_s$ having M_i as its right-divisor of determinant m_i $(i = 1, \dots, s)$ is uniquely determined up to a left-unimodular factor. Hence, if Q is a Hermite-matrix, it is unique.*

Proof. (i) We can express U_1QU_2 as a diagonal matrix D, which can evidently be factored as D_1D_2 with $|D_1| = m_1$ and $|D_2| = m_2$. The existence of a right-divisor of Q, with determinant m_2 follows. This divisor can be supposed to be an Hermite-matrix. To establish its uniqueness, consider $N_1M_1 = N'_1M'_1$, where $|N_1| = |N'_1| = m_1$, and $|M'_2| = |M_2| = m_2$. Hence $(N'_1)^{-1}N_1 = (M'_2M_2^{-1})$, and both sides are integral since their respective possible denominators are coprime. Hence $M'_2 = UM_2$ with U unimodular, and $U = I$ by Lemma 2.

(ii) Obvious by repeated applications of (i).

(iii) Let $Q = Q_1M_1$. We will prove that the Hermite right-divisors of Q_1 with the determinants $m_2, \dots, m_s$ are uniquely determined, and hence (iii) will follow by induction. Thus, suppose $Q_2M'_2M_1 = Q_3N_1M_2$ and $Q_4M''_2M_1 = Q_5N'_1M_2$, where the Q's have determinants $m_3, \dots, m_s$ and the other matrices have determinants m_1 or m_2 according to their subscripts. The argument used in (i) shows that $M'_2M_1 = UN_1M_2$ and $M''_2M_1 = U'N'_1M_2$. Hence $(UN_1)^{-1}M'_2 = (U'N'_1)^{-1}M''_2$, $(UN_1)(U'N'_1)^{-1}$ must be integral and hence unimodular, $M'_2 = U''M''_2$, $M'_2 = M''_2$.

Two quadratic forms are in the same genus if they have the same index and and determinant, and are in the same class w.r.t. p (defined by residues modulo p^r with r large) for every prime p dividing the determinant and for the prime 2. The class w.r.t. p is unchanged by the application to the quadratic form of integral transformations of determinants prime to p, or of rational transformations of determinants prime to p and with coefficients whose denominators are prime to p. It follows that the class w.r.t. p of $B''_1 = (M^{\mathsf{T}})^{-1}B_1M^{-1}$ is the same as that of $(M^{\mathsf{T}}_1)^{-1}B_1M_1^{-1}$, where M_1 is the Hermite right-divisor of M whose determinant is the highest power of p dividing $|M|$. Also, by (iii) of Lemma 6, the number of Hermite-matrices of determinant $m_1m_2 \dots m_s$ (where the m_i are powers of distinct primes p_i, $i = 1, \dots, s$) for which $(M^{\mathsf{T}})^{-1}B_1M^{-1}$ is in a given genus, is the product of the numbers of Hermite-matrices M_i of determinant m_i for which $(M^{\mathsf{T}}_i)^{-1}B_1M_i^{-1}$ is in the class w.r.t. p_i determined by that genus.

Let B_1 be an integral, positive-definite 2 by 2 matrix of determinant b_1, and let ν denote the number of distinct odd primes dividing b_1. Let $\chi(p)$ denote the number of Hermite-matrices

$$M_1 = \begin{bmatrix} p^r & q \\ 0 & p^s \end{bmatrix}, \; q, r, \textit{ and } s \textit{ non-negative integers}, \; q < p^s, \tag{28}$$

such that $B'_1 = (M^T{}_1)^{-1} B_1 M_1^{-1}$ is an integral matrix satisfying the conditions of primitive representation by $x^2 + y^2 + z^2$ relating to the prime p, but if $p > 2$ count every system q, r, s for which $|B'_1|$ is prime to p as worth only $\frac{1}{2}$. The reason for counting the latter systems as worth $\frac{1}{2}$ is that in applying the formula 24.2^ν for the number of primitive representations of B'_1 (or rather of B''_1) by I, the value of ν is diminished by one, from the value as defined for B_1. Accordingly, the number of all representations of B_1 by $I^{(3,3)}$ will be

$$24.2^\nu \prod_p \chi(p),$$

where p runs over the primes such that $p^2 | 4b_1$.

8. The factors $\chi(p)$. First consider $p > 2$. The form ϕ can be given the residue $p^{u_1} m_1 x_1^2 + p^{u_2} m_2 x_2^2 \pmod{p^\tau}$ (τ sufficiently large), where m_1 and m_2 are prime to p, and $0 \leq u_1 \leq u_2$. On applying to ϕ the inverse of (28), we obtain the form

$$\text{(29)} \quad \phi' = a_1 x_1^2 + 2b_1 x_1 x_2 + c_1 x_2^2, \; a_1 = p^{u_1 - 2r} m_1, \; b_1 = -q p^{u_1 - 2r - s} m_1,$$
$$c_1 = p^{-2r-2s}(q^2 p^{u_1} m_1 + p^{2r+u_2} m_2).$$

The conditions on ϕ' for primitive representability by $x^2 + y^2 + z^2$ are that one of a_1, b_1, c_1 be prime to p, and that if p divides $|\phi'|$ then ϕ' must represent $-1 \bmod p$. It will be convenient to consider instead the slightly more general condition that ϕ' shall represent $-d \bmod p$, where d is a given integer prime to p.

The solutions with a_1 prime to p require

$$\text{(30)} \qquad r = \tfrac{1}{2}u_1, \; q = 0, \; s \leq \tfrac{1}{2}u_2,$$

since b_1 and c_1 must be integers and $q < p^s$. With $q = 0$, we may have also

$$\text{(31)} \qquad r < \tfrac{1}{2}u_1, \; q = 0, \; s = \tfrac{1}{2}u_2,$$

since c_1 must be prime to p when p divides a_1 and b_1. For the remaining cases, with q not zero, we set $q = p^t q_1$, $0 \leq t < s$, q_1 prime to p.

If $p | a_1$ but not b_1, then $u_1 + t = 2r + s$, hence (c_1 being integral), $u_1 + 2t < 2r + 2s$, $u_1 + 2t = 2r + u_2$. From these readily follow $u_2 = t + s$, $\frac{1}{2}(u_2 - u_1) \leq t = u_2 - s$, and hence

$$\text{(32)} \qquad \tfrac{1}{2}u_2 < s \leq \tfrac{1}{2}(u_1 + u_2), \; t = u_2 - s, \; r = t - \tfrac{1}{2}(u_2 - u_1).$$

Also, q_1 has $2e_3$ values mod $p^{2s-u_2} = p^{s-t}$, where $e_3 = \frac{1}{2}\{1 + (-m_1 m_2 | p)\}$; and hence q has $2e_3$ values mod p^s for each complex of values s, t, r. Note that in the present case $|\phi'|$ is prime to p.

There remain to be considered the cases satisfying

(33) $2r < u_1$, $2r + s < u_1 + t$, p^{2r+2s} *precisely divides* $p^{u_1+2t} q_1^2 m_1 + p^{2r+u_2} m_2$.

It will be convenient to subdivide these cases into three parts, as follows:

(a) $2s = u_2$, $\frac{1}{2}(u_2 - u_1) < t < \frac{1}{2}u_2$, $r < t - \frac{1}{2}(u_2 - u_1)$;

(b) $\frac{1}{2}u_2 \leq s < \frac{1}{2}(u_1 + u_2)$, $\frac{1}{2}(u_2 - u_1) \leq t < u_2 - s$, $r = t - \frac{1}{2}(u_2 - u_1)$, *while* q_1 mod p^{s-t} *is such that* $(q_1^2 m_1 + m_2)/p^{2s-u_2}$ *is prime to* p;

(c) $r < \frac{1}{2}u_1$, $t < r + \frac{1}{2}(u_2 - u_1)$, $s = t + \frac{1}{2}u_1 - r$, q_1 *arbitrary prime to* p.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

Thus (a) can be verified as embodying the conditions to be satisfied when $2r + 2s = 2r + u_2 < 2t + u_1$, whence (as $r \geq 0$) $\frac{1}{2}(u_2 - u_1) < t < s$. Again, (b) corresponds to $u_1 + 2t = u_2 + 2r \leq 2r + 2s$, whence (by (33_2)) $t < u_2 - s \leq \frac{1}{2}u_2$. Note here, for use in the case where $2s = u_2$, that it can be proved that $q_1^2m_1 + m_2$ has the quadratic character of $-d$ modulo p for precisely θ values q_1 modulo p, where

(34) $$\theta = \tfrac{1}{2}\{p - 2 - (-dm_1|p) - (-dm_2|p) - (-m_1m_2|p)\}.$$

Note also that if $2s > u_2$, $(-m_1m_2|p) = 1$, and $q_1^2m_1 + m_2 = p^{2s-u_2}q'$, then

$$(q_1 + hp^{2s-u_2})^2m_1 + m_2 = p^{2s-u_2}(q' + 2q_1m_1h + p^{2s-u_2}h^2m_1),$$

and the last factor has the quadratic character modulo p of $-d$ for $\frac{1}{2}(p-1)$ residues h modulo p; consequently, $(q_1^2m_1 + m_2)/p^{2s-u_2}$ has the quadratic character of $-d$ for $p-1$ residues q_1 modulo p^{2s-u_2+1}. Finally, (c) occurs if $u_1 + 2t = 2r + 2s < 2r + u_2$ (whence $t < s$ is equivalent to $r < \frac{1}{2}u_1$).

We will use the abbreviations $\epsilon_1, \epsilon_2, \epsilon_3 = 0$ or 1 according as (respectively) $u_1, u_2, u_2 - u_1$ are odd or even; and $\eta_i = \frac{1}{2}\{1 + (-dm_i|p)\}$, $\delta_i = \{\frac{1}{2}(u_i + 1)\}$, $(i = 1, 2)$; $\eta_3 = \frac{1}{2}\{1 + (-m_1m_2|p)\}$.

For odd p, $\chi(p)$ will be a sum of terms due to each of the cases (30) to (33)(c), and determined as follows.

If $2s < u_2$ in (30), m_1 must have the quadratic character of $-d$. Hence the terms $\chi(p)$ corresponding to (30) and (31) are, respectively,

(35) $$\epsilon_1\delta_2\eta_1 + \tfrac{1}{2}\epsilon_1\epsilon_2, \text{ and } \epsilon_2\delta_1\eta_2,$$

the $\frac{1}{2}$ being due to the circumstance that $|\phi'|$ is prime to p if $s = \frac{1}{2}u_2$ in (30). The term of $\chi(p)$ arising from (32) is evidently

(36) $$\epsilon_3\eta_3\delta_1.$$

In case (33)(a), for each value $t = \frac{1}{2}u_2 - i$ $(i = 1, 2, \ldots, \delta_1 - 1)$, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{i-1}$ values modulo p^{s-t}, and r has $\delta_1 - i$ values. The corresponding part of $\chi(p)$ is therefore

(37) $$\epsilon_2\eta_2 \sum_{i=1}^{\delta_1-1} (p-1)p^{i-1}(\delta_1 - 1) = \epsilon_2\eta_2\{(p^{\delta_1} - 1)/(p-1) - \delta_1\}.$$

If $2s = u_2$ in (33)(b), we can set $t = s - j$ $(j = 1, 2, \ldots, \frac{1}{2}u_1)$. Then q_1 has θp^{j-1} values modulo p^{s-t}, and the corresponding part of $\chi(p)$ is

(38) $$\theta\epsilon_2\epsilon_3 \sum_j p^{j-1} = \tfrac{1}{2}\epsilon_2\epsilon_3(p^{\delta_1} - 1) - \zeta\epsilon_2\epsilon_3(p^{\delta_1} - 1)/(p-1),$$

where $\zeta = \frac{1}{2}\{1 + (-dm_1|p) + (-dm_2|p) + (-m_1m_2|p)\} = \eta_1 + \eta_2 + \eta_3 - 1$. If $2s > u_2$ in (33)(b), we can set $s = \frac{1}{2}(u_1 + u_2) - i$ $(i = 1, \ldots, \delta_1 - 1)$ and $t = \frac{1}{2}(u_2 - u_1) + j$ $(j = 0, 1, \ldots, i-1)$, and have for the corresponding term of $\chi(p)$,

(39) $$\epsilon_3\eta_3 \sum_i \sum_j (p-1)p^{i-j-1} = \epsilon_3\eta_3\{(p^{\delta_1} - 1)/(p-1) - \delta_1\}.$$

Finally, in (33)(c), u_1 is even, and for given r, t, and s, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{\delta_1-r-1}$ residues mod p^{s-t}, and the corresponding term of $\chi(p)$ is

(40) $$\eta_1\epsilon_1 \sum_{r=0}^{\delta_1-1} (r - \delta_1 + \delta_2)(p-1)p^{\delta_1-r-1} = \eta_1\epsilon_1\{(\delta_2 - \delta_1)p^{\delta_1} + (p^{\delta_1} - 1)(/(p-1) - \delta_1\}.$$

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

The sum of the terms in (35)-(40) will be found to be

(41) $$\chi(p) = \kappa_1(p^{\delta_1} - 1)/(p-1) + \kappa_2 p^{\delta_1},$$

where $\kappa_1 = \epsilon_1\eta_1 + \epsilon_2\eta_2 + \epsilon_3\eta_3 - (\eta_1 + \eta_2 + \eta_3 - 1)\epsilon_1\epsilon_2$, $\kappa_2 = \frac{1}{2}\epsilon_1\epsilon_2 + \epsilon_1\eta_1(\delta_2 - \delta_1)$. Thus the values of κ_1 and κ_2 may be tabulated as follows:

	κ_1	κ_2
Case u_1 even, u_2 even.	1	$\frac{1}{2} + \frac{1}{2}\{1 + (-dm_1\|p)\}(u_2 - u_1)/2$
u_1 even, u_2 odd.	$\frac{1}{2}\{1 + (-dm_1\|p)\}$	$\frac{1}{2}\{1 + (-dm_1\|p)\}u_2 + 1 - u_1)/2$
u_1 odd, u_2 even.	$\frac{1}{2}\{1 + (-dm_2\|p)\}$	0
u_1 odd, u_2 odd.	$\frac{1}{2}\{1 + (-m_1m_2\|p)\}$	0

The value of $2\chi(p)$ thus obtained agrees with that for the case $d = 1$ given by the author [8] without details of proof; the method then used was quite different and based on a formula of Siegel. To express the value of $\chi(p)$ in terms of generic characters of ϕ, we may write $\phi = k\phi_1$, where ϕ_1 is either p.p. or i.p., and k is a positive integer. For each odd prime p, we may set $k = p^{u_1}k_1$, and $|\phi_1| = p^{u_2 - u_1}t_1$, where k_1 and t_1 are prime to p. Then u_1 and u_2 coincide with their values in the associated form-residue $p^{u_1}m_1x_1^2 + p^{u_2}m_2x_2^2$, $(m_1|p) = (k_1|p)(\phi_1|p)$, $(m_1m_2|p) = (t_1|p)$.

Before discussing $\chi(2)$, we will compute the modified value $\chi_1(p)$ for Linnik's problem, in which the number of representations is desired in which the divisor k of the binary form is equal to the divisor of the representations. This now means that $u_1 = r + s$.

In (30) this gives $r = s = \frac{1}{2}u_1$, and contributes to $\chi_1(p)$ the term $\epsilon_1\eta_1$ if $u_1 < u_2$, $\frac{1}{2}\epsilon_1\epsilon_2$ if $u_1 = u_2$. The contribution due to (31) is 0 unless $\frac{1}{2}u_2 \le u_1 < u_2$, and then is $\epsilon_2\eta_2$. In (32), we need $u_1 = u_2$, and then get $\eta_3\delta_1$ values r, s, t. So far the contribution is small. However, in case (33)(a), if $r + s = u_1$, then $r = u_1 - \frac{1}{2}u_2 < t - \frac{1}{2}(u_2 - u_1), t > \frac{1}{2}u_1$. Thus (33) (a) requires that $\frac{1}{2}u_2 \le u_1 < u_2$, and the conditions to be satisfied are

$$\tfrac{1}{2}u_1 < t < \tfrac{1}{2}u_2,\ 2s = u_2,\ r = u_1 - s,\ q_1 \text{ prime to } p.$$

Thus we may set $t = \frac{1}{2}u_2 - i$, $(i = 1, 2, \ldots, v)$, where $v = [\frac{1}{2}(u_2 - u_1 - 1)]$, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{i-1}$ values modulo p^{s-t}, r now has one value, and the corresponding part of $\chi_1(p)$ is

$$\epsilon_2\eta_2 \sum_i (p-1)p^{i-1} = \epsilon_2\eta_2(p^v - 1).$$

Case (33) (b) is found to require $\frac{1}{2}u_2 \le u_1 < u_2$, and then to specify

$$\tfrac{1}{2}(u_2 - u_1) \le t \le \tfrac{1}{2}u_1,\ r = t - \tfrac{1}{2}(u_2 - u_1),\ s = \tfrac{1}{2}(u_1 + u_2) - t.$$

The subcase $2s = u_2$ implies $u_1 = 2t$ and gives the contribution $\theta\epsilon_1\epsilon_2 p^{\frac{1}{2}(u_2 - u_1) - 1}$. Also, $2s > u_2$ implies $t < \frac{1}{2}u_1$, we can set $t = \frac{1}{2}(u_2 - u_1) + j$ $(j = 0, 1, \ldots, u_1 - 1 - [\frac{1}{2}u_2])$, and find the contribution $\epsilon_3\eta_3(u_1 - [\frac{1}{2}u_2])(p-1)p^{\frac{1}{2}(u_2 - u_1) - 1}$. Finally, (33) (c) is equivalent to

$$\tfrac{1}{2}u_1 < s < \tfrac{1}{2}u_2,\ \ 0 \le r = u_1 - s,\ t = \tfrac{1}{2}u_1.$$

Hence the contribution to $\chi_1(p)$ is

$$\eta_1\epsilon_1 \sum_{s=\frac{1}{2}u_1+1}^{u_1} (p-1)p^{s-\frac{1}{2}u_1-1} = \eta_1\epsilon_1(p^{\frac{1}{2}u_1} - 1) \text{ or } \eta_1\epsilon_1 \sum_{s=\frac{1}{2}u_1+1}^{[\frac{1}{2}(u_2-1)]} (p-1)p^{s-\frac{1}{2}u_1-1} = \eta_1\epsilon_1(p^v - 1),$$

according as $u_1 < \frac{1}{2}u_2$ or $\frac{1}{2}u_2 \le u_1 < u_2$.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

Summing up, the value of $\chi_1(p)$ for odd primes p is given by

$$(42)\qquad \begin{gathered} 1, \text{ if } u_1 = u_2 = 0; \\ \tfrac{1}{2}\epsilon_1\epsilon_2 + \eta_3\delta_1, \text{ if } u_1 = u_2 > 0; \\ \eta_1\epsilon_1 p^{u_1/2}, \text{ if } u_1 < \tfrac{1}{2}u_2; \end{gathered}$$

$p^v\rho$, if $\frac{1}{2}u_2 \leq u_1 < u_2$, where $\rho = \epsilon_1\eta_1 + \epsilon_2\eta_2 + \theta\epsilon_1\epsilon_2 + \epsilon_3\eta_3(u_1 - [\frac{1}{2}u_2])(p-1)$. Here $v = [\frac{1}{2}(u_2 - u_1 - 1)]$. Note that the order of size of this factor is that of the power of p dividing h, where h^2 is the largest square factor common to k and $|\phi_1|$.

Except for the values of $\chi(2)$ and $\chi_1(2)$, we have the following theorem.

THEOREM 4. *Let k be a positive integer, ϕ_1 be a positive-definite integral binary quadratic form, either properly or improperly primitive, $\Delta = |\phi_1| \neq 0$, $\phi = k\phi_1$. The number of all representations of ϕ by $x^2 + y^2 + z^2$ is given by*

$$(43)\qquad 24.2^{\nu} \prod_{p|2k\Delta} \chi(p).$$

Here ν denotes the number of distinct odd primes dividing $k\Delta$, and $\chi(p)$ is given for odd primes p by (41) *with $d = 1$ and in accordance with the following notations. For any prime p, set $k = p^{u_1}k_1$, $\Delta = p^{u_2 - u_1}t_1$, k_1 and t_1 prime to p. If $p > 2$, define $(m_1|p) = (k_1|p)(\phi_1|p)$ and $(m_2|p) = (m_1t_1|p)$, $\delta_1 = [(u_1+1)/2]$. If $p = 2$, then $\chi(2) = 0$, except that $\chi(2) = 1$ in the following cases:*

(44) *$u_1 + u_2$ odd; u_1 and u_2 even, $t_1 \equiv 1 \bmod 4$; u_1 even, ϕ_1 i.p., $t_1 \equiv 3 \bmod 8$; u_1 and u_2 odd, ϕ_1 p.p., $t_1 \equiv 1, 3,$ or $5 \bmod 8$.*

The number of representations in which the divisor of the representations is equal to the divisor k of ϕ is given by

$$(45)\qquad 24.2^{\nu} \prod_{p|2k\Delta} \chi_1(p),$$

where $\chi_1(p)$ is given for odd primes p by (42), *and $\chi_1(2) = 0$ except that $\chi_1(2) = 1$ in the following cases:*

(46) *$u_1 = u_2 - 1$; $u_1 = u_2$ in all but the first case of* (44).

If $m = k^2\Delta$ and h^2 denotes the largest odd square factor common to k and Δ, then the expression in (45) *has for large m the order of size $h.0(m^\epsilon)$, for any preassigned positive ϵ.*

Proof. It remains only to verify the values of $\chi(2)$ and $\chi_1(2)$. The form ϕ is equivalent to a form having to modulus a sufficiently high power of 2, either the residue

$$2^{u_1}m_1x_1^2 + 2^{u_2}m_2x_2^2, \text{ with } m_1m_2 \text{ odd and } 0 \leq u_1 \leq u_2,$$

if ϕ_1 is p.p., or the residue $2^{u_1}(2x_1^2 + 2x_1x_2 + 2jx_2^2)$, with j an integer, $u_1 \leq 0$, if ϕ_1 is i.p.

In the former case, the notations in (29) can be used with $p = 2$. The conditions that ϕ' must satisfy are that a_1, b_1, c_1 are integers such that either a_1 or c_1 is odd and $a_1c_1 - b_1^2 \equiv 1$ or $2 \bmod 4$, or a_1 and c_1 are even but b_1 is odd and $a_1c_1 - b_1^2 \equiv 3 \bmod 8$. Hence a_1 cannot be divisible by 4, therefore $u_1 = 2r + 1$ or $2r$.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

If $u_1 = 2r + 1$, then since b_1 is integral, $q = 0$ or 2^{s-1}. If $q = 0$, then c_1 must now be odd, $u_2 = 2s$. If $q = 2^{s-1}$, then $c_1 = \frac{1}{2}m_1 + 2^{u_2-2s}m_2$ must be odd or double of an odd, hence $u_2 = 2s - 1$ and $m_1m_2 \equiv 1, 5$, or $3 \bmod 8$.

If $u_1 = 2r$, then $q = 0$, $c_1 = 2^{u_2-2s}m_2$, hence either $u_2 = 2s + 1$, or $u_2 = 2s$ and $m_1m_2 \equiv 1 \bmod 4$.

In the latter case (with ϕ_1 i.p.), ϕ' is given by

(47) $a_1 = 2^{u_1+1-2r}$, $b_1 = +2^{u_1-2r-s}(2^r - 2q)$, $c_1 = 2^{u_1+1-2r-2s}(q^2 - 2^rq + 2^{2r}j)$.

Since $4|a_1$ is excluded as before, $u_1 = 2r$ or $2r - 1$.

If $u_1 = 2r - 1$, then $a_1 = 1$, $b_1 = 2^{-s}(2^{r-1} - q)$, hence $q = 2^{r-1}$ if $r - 1 < s$, $q = 0$ if $r - 1 \geq s$. If $q = 0$, then $c_1 = 2^{2r-2s}j \equiv 0 \bmod 4$, and the condition that $a_1c_1 - b_1^2 \equiv 1$ or $2 \bmod 4$ is contradicted. If $q = 2^{r-1}$, then $c_1 = 2^{2r-2-2s}(4j - 1)$, which is not integral since $r - 1 < s$, a contradiction.

There remains $u_1 = 2r$, $a_1 = 2$. If $s = 0$, then $q = 0$, $b_1 = 2^r$, $c_1 = 2^{2r+1}j$, hence $r = 0$ and j must be odd. If $s = 1$, then $r \geq 1$ since b_1 is integral, $q = 0$ since c_1 is integral, hence $r = 1$ and j must be odd since ϕ' can only be i.p. Let $s \geq 2$. Then $r \geq 2$ and q is even since b_1 and c_1 are integral. If $r \geq s$, we may set $q = 2^{s-1}k$ ($k = 0$ or 1), have $c_1 = 2^{1-2s}(2^{2s-2}k^2 - 2^{r+s-1}k + 2^{2r}j)$, k even, $k = 0$, $r = s$ and $j = 1$. If $r < s$, we may set $q = 2^{r-1} + 2^{s-1}k$ ($k = 0$ or 1), $c_1 = \frac{1}{2}\{k^2 + (4j - 1)2^{2r-2s}\}$ which cannot be an integer. Thus there are no solutions in the case with ϕ_1 i.p. unless u_1 is even and j is odd, and then q, r, and s are uniquely determined.

From this, (44) readily follows, and then by taking $r + s = u_1$, also (46).

In Linnik's application to proving that (under certain conditions) a large number is represented by each class of a ternary genus, it was assumed that m is prime to the determinant d of the genus. The determinant of the binary quadratic form $\phi = k\phi_1$, which is to be represented by a ternary form of determinant d^2 happens to be of the form $b_1 = m - q_1k$, where q_1 is an integer and k is the divisor of ϕ. Hence the assumption that m is prime to d implies that k is prime to d. To fill the gap in Linnik's proof it therefore suffices to prove the following theorem.

THEOREM 5. *Consider a representative set of forms $f_1, \ldots, f_s$ with integral matrices of a given non-zero determinant d, and an integral binary quadratic form $\phi = k\phi_1$ (ϕ_1 p.p. or i.p.) of determinant $b_1 = k^2\Delta$, where k is prime to d. Let h^2 denote the largest square factor common to k and Δ. Let ρ denote the number of sets of representations of ϕ by $f_1, \ldots, f_s$ such that the divisor of the representations is k. Then for any positive ϵ, there exists a constant q, depending on ϵ and d, but independent of b_1 and ϕ, such that*

$$\rho < qh(b_1)^\epsilon. \tag{48}$$

Proof. The condition of primitive representation is, as in (26),

$$b'k_1^2 - 2t'k_1k_2 + a'k_2^2 \equiv -d \pmod{b_1}. \tag{49}$$

Hence the divisor k of $\phi = a'x^2 + 2t'xy + b'y^2$ must divide d. If k is prime to d this implies that $k = 1$. Accordingly, the representations of divisor k of the form $\phi = k\phi_1$ by ternaries of determinant d are associated with primitive

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

representations of forms which are properly or improperly primitive, and which represent $-d$ modulo Δ, where $\Delta = |\phi_1|$. The theorem is therefore a consequence of the following three lemmas.

LEMMA 7. *Let* $b_1 = \prod_{i=1}^{v} p_i^{\beta_i}$ *express* b_i *as a product of powers of distinct primes. Then the number of divisors of* b_1, *namely* $\prod(\beta_i + 1)$, *is* $0\ (b_1^{\epsilon})$ *for every positive* ϵ. *Hence,* $2^v = 0(b_1^{\epsilon})$ *and* $5^v = 0(b_1^{\epsilon})$.

Proof. See [14].

LEMMA 8. *If* a', t', *and* b' *are relative prime, the number of solutions* K *modulo* B_1 *of* (49) *does not exceed* $4d.2^v$, *where* v *denotes the number of distinct odd primes dividing* b_1.

Proof. If $[a', 2t', b']$ is i.p., then $b_1 = a'b' - t'^2$ is odd, and the prime 2 does not affect the result. Hence for any prime p dividing b_1, ϕ can be given the residue $m_1x_1^2 + p^{u_2}m_2x_2^2$ (mod p^s), where m_1 and m_2 are prime to p and p^s is the precise power of p dividing b_1. Then (49) becomes $p^s m_2 k_1^2 + m_1 k_2^2 \equiv -d$ (mod p^s), for each p^s. Hence k_1 has p^s values modulo p^s, or b_1 values modulo b_1, and this is cancelled by the factor b_1 due to Lemma 5. Also k_2 can have at most $4p^{\delta}$ residues modulo p^s if $p^{2\delta}|d$ and $p^{2\delta+2}$ does not divide d, and $p^{2\delta}|p^s$; and at most $p^{[\frac{1}{2}s]}$ residues modulo p^s if $p^s|d$.

LEMMA 9. *The number of systems of values* r, s, q *for which the form* ϕ' *in* (29) *is primitive modulo* p, *but such that* $r + s = u_1$, *does not exceed* $5(u_1 + 2)p^{\sigma}$, *where* p^{σ} *denotes the precise power of* p *dividing* h (*cf. last statement of Theorem* 4). *This holds true for* $p = 2$, *with* ϕ' *given either by* (29) *or* (47).

Proof. We follow the steps in § 8, dropping the condition that ϕ' represent $-d$ mod p, and noticing whether the statements are valid also for $p = 2$. The number of systems r, s, q satisfying $r + s = u_1$ and (30), or (31), is at most 1. From (32) are derived if p is odd less than $2(u_1 + 1)$ values r, s, q, indeed $2\delta_1$ values if $u_1 = u_2$, none if $u_1 < u_2$. If $p = 2$, (32) gives at most four values q_1 mod p^{s-t}, hence at most $2(u_1 + 1)$ values r, s, q. We have (33) (a) as before, with at most $p^{\sigma} - 1$ systems r, s, q if $\frac{1}{2}u_2 \leq u_1 < u_2$, zero otherwise. In (33) (b), if $2s = u_2$, we replace θ by $p - 1$ (taking q_1 arbitrary), and thus obtain at most $(p - 1)p^{\sigma-1}$ systems, r, s, q. If $2s > u_2$, the number of systems obtained is at most twice that obtained earlier, hence at most $2(u_1 + 1)(p - 1)p^{\sigma-1}$. In (33) (c) we may replace η_1 by 1 and have at most $p^{\frac{1}{2}u_1} - 1$ if $u_1 < \frac{1}{2}u_2$, $p^v - 1$ if $\frac{1}{2}u_2 \leq u_1 < u_2$, —in both cases $p^{\sigma} - 1$. The sum total does not exceed $2(u_1 + 3)\ p^{\sigma}$.

The factor for $p = 2$ due to case (47) remains to be considered. The possibility a_1 and b_1 even, c_1 odd, with $r + s = u_1$, is easily seen to be contradictory. If a_1 is odd, then $r = \frac{1}{2}(u_1 + 1)$, $s = u_1 - r$, and since b_1 is an integer, q has 2 residues modulo 2^s. Finally, consider a_1 even, b_1 odd. Since $r + s = u_1$, $1 - 2^{1-r}q$ is odd. There are $1 + [u_1/2]$ values q, r, s with $q = 0$. If $q \neq 0$, we may set $q = 2^t q_1$, must have $s > t \geq r$, while

$$c_1 = \left\{(2^{t-r+1}q - 1)^2 + 4j - 1\right\}/2^{s-r+1}.$$

Thus $2^{t-r+1}q_1 - 1$ has at most two residues mod 2^{s-r}, and hence q has at most

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

four residues mod 2^s. Thus there are at most $4(u_1+1)$ complexes q, r, s. The total due to (47) does not exceed $5(u_1+2)$.

9. Adjoint representations. Gauss, Smith, and Minkowski used a somewhat different algorithm from that which we have described in the preceding. They made use of the case $k = 1$ or $n - 1$ of a correspondence (which will here be simplified and generalized) between the primitive representations of a form ϕ in k variables by a form f in n variables, and the primitive representations of a certain related form ψ in $n - k$ variables by the adjoint of f.

Certain aspects of their treatments are superfluous, as for example the insistence upon dealing with integral forms, and this fact hides the essential simplicity of the correspondence. Indeed, the forms ϕ and ψ, f and adj f, are also in a certain measure superfluous, and the correspondence is basically one between *adjoint representations* described as follows.

Consider $(S_1\ S_2)^{\mathsf{T}} = (T_1\ T_2)^{-1}$, where $(T_1\ T_2)$ is unimodular. If T_2 is replaced by any complement $T_1H + T_2U$ of T, then T^{-1} is replaced by

$$(50)\qquad \left((T_1\ T_2)\begin{bmatrix} I_1 & H \\ 0 & U\end{bmatrix}\right)^{-1} = \begin{bmatrix} I_1 & -HU^{-1} \\ 0 & U^{-1}\end{bmatrix}\begin{bmatrix} S^{\mathsf{T}}{}_1 \\ S^{\mathsf{T}}{}_2\end{bmatrix} = \begin{bmatrix} S^{\mathsf{T}}{}_1 - HU^{-1}S^{\mathsf{T}}{}_2 \\ U^{-1}S^{\mathsf{T}}{}_2\end{bmatrix}$$

and hence S_2 is replaced by $S_2(U^{\mathsf{T}})^{-1}$. Similarly, if S_1 is replaced by any left complement $S_1V + S_2J$ (V unimodular, J integral) of S_2, then T_1 is replaced by $T_1(V^{\mathsf{T}})^{-1}$. Thus the two *aggregates* of representations T_1V and S_2U, where $V^{(k,k)}$ and $U^{(n-k,n-k)}$ are arbitrary unimodular matrices, are *adjoint* to one another in the following sense. For any U and V, T_1V has a right complement T_2, and S_2U has a left complement S_1 such that $(S_1S_2U)^{-1} = (T_1V\ T_2)^{\mathsf{T}}$. Only the matrices T_1V and S_2U arise from one another in this manner.

Consider now (10) and (11). If T_2 is replaced by any complement $T_1H + T_2U$ of T_1, D_2 is replaced by the equivalent matrix $U^{-1}D_2(U^{\mathsf{T}})^{-1}$. This coincides with D_2 if and only if U^{T} is a unimodular automorph of D_2. Similarly, if S_1 is replaced by other complements, T_1 is replaced by $T_1(V^{\mathsf{T}})^{-1}$, and this is a representation of B_1 by A if and only if V^{T} is a unimodular automorph of B_1.

It follows that there is associated, with the *ensemble* of primitive representations (T_1V) of B_1 by A (where V runs through all unimodular automorphs of B_1), in a unique manner an ensemble of primitive representations (S_2U) of D_2 by adj A (where U ranges over the unimodular automorphs of D_2); and conversely.

Representations of non-equivalent matrices B_1 and B'_1 by A cannot be associated with the same ensemble of primitive representations of D_2 by C, since the replacement of S_1 by other complements of S_2U replaces B_1 by an equivalent matrix.

If B_1 is replaced by an equivalent matrix $Z^{\mathsf{T}}B_1Z$ (Z unimodular), and T_1 by T_1Z, the matrices S_2U are unaltered. Thus, corresponding primitive representations of $Z^{\mathsf{T}}B_1Z$ by A are associated with the same representations of D_2 by C as are those of B_1 itself.

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

Since at least one minor determinant of order k in T_1 is not zero, $T_1V = T_1V'$ implies $V = V'$. Hence as V ranges over the unimodular automorphs of B_1, the matrices T_1V are distinct; and similarly for S_2U.

If $k = n - 1$, and A and B_1 are integral, then D_2 is an integer d_2, and B_1 is an integral $(n-1)$-ary matrix of determinant d_2. Hence all the primitive representations of d_2 by C can be obtained by choosing one matrix B_1 from each of the finite number of classes of determinant d_2, and constructing the primitive representations of T_1 of each such B_1 by A. The number of ensembles of primitive representations (T_1V) will now be exactly equal to the number of primitive representations of d_2 by C, since a unary D_2 has only one unimodular automorph.

Gauss, Smith, and Minkowski made use of this correspondence to reduce the problem of representing numbers to that of representing $(n-1)$-ary forms.

It should be observed, finally, that in general, for a given A, a correspondence can be set up between ensembles of primitive representations of a set of non-equivalent matrices $B_1^{(i)}$ $(i = 1, \ldots, h_1)$ by A, and a set of non-equivalent matrices $D_2^{(j)}$ $(j = 1, \ldots, h_2)$ by adj A. As noted in (14), the determinants satisfy $d_2 = b_1 a^{n-k-1}$; and the matrices D_2 satisfy adj $G = b_1^{n-k-2}D_2$, with B_1 one of the $B_1^{(i)}$, and $b_1^{-1}G$ the matrix obtained by completing squares with reference to B_1 in B. The corresponding sets of matrices can be determined precisely in particular cases.

Thus, for example, if $n = 3$, $A = C = I$, $k = 1$, and b_1 is a positive integer, the matrices $D_2^{(j)}$ are representatives of the s classes of the genus described in § 6, and each such matrix has $24.2^{\nu}/u$ ensembles of primitive representations by adj A, if we assume that $b_1 \not\equiv 0, 4, 7 \bmod 8$. Hence, as before, the number of primitive representations of b_1 by $x^2 + y^2 + z^2$ is equal to $s\ 24\ 2^{\nu}/u$. Thus, the representations of $2x_1^2 + 2x_1x_2 + 2x_2^2$ as $(a_1x_1 + b_1x_2)^2 + (a_2x_1 + b_2x_2)^2 + (a_3x_1 + b_3x_2)^2$ will be found by trial to be 48 in number, and since this binary form has six unimodular automorphs they comprehend 8 ensembles,—corresponding to the 8 representations of 3 as a sum of three squares. Similarly, it may be verified that $2x_1^2 + 2x_1x_2 + 2x_2^2$ has 48 representations by $x^2 + y^2 + z^2 + 2w^2$, comprehending $48/6 = 8$ ensembles; and that these are associated with 16 representations of $x_1^2 + 6x_2^2$ by $2x^2 + 2y^2 + 2z^2 + w^2$, hence $16/2 = 8$ ensembles.

10. The alternative algorithm based on the adjoint form. The method used by Gauss, Smith, and Minkowski differed from ours in one further respect. What they did (in the case $k = n - 1$) was, essentially, to construct the adjoint matrix D in (11) rather than B.

If T_2 is replaced by any complement $T_1H + T_2U$, D is transformed by

$$\left(\begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}^{-1}\right)^{\mathsf{T}} = \begin{bmatrix} I_1 & 0 \\ -(U^{\mathsf{T}})^{-1}H^{\mathsf{T}} & U^{\mathsf{T}-1} \end{bmatrix},$$

and hence D_2 is replaced by $U^{-1}D_2(U^{\mathsf{T}})^{-1}$ and L by $U^{-1}L - U^{-1}D_2(U^{\mathsf{T}})^{-1}H^{\mathsf{T}}$. If we choose a particular matrix D_2 in its class, $(U^{\mathsf{T}})^{-1}$ (and also U^{T}) is re-

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press

stricted to be a unimodular automorph of D_2, and L is replaced by $U^{-1}L - D_2H^{\mathsf{T}}$. Thus the set of primitive representations (WT_1) of B_1 by A is associated with a matrix D_2 and a *complex of solutions* L of the congruence

$$L^{\mathsf{T}}(\text{adj } D_2)L \equiv -a^{n-k} \text{ adj } B_1 \pmod{d_2}. \tag{51}$$

Here, two matrices L and L' are defined to be in the same complex of solutions of (51) if there exists a unimodular automorph U^{T} of D_2 such that $U^{-1}L$ and L' are in the same left-sided residue class modulo D_2. An equation similar to (25) can be formulated, it being necessary to confine attention to solutions L of (51) such that if D_1 is defined by

$$L^{\mathsf{T}}(\text{adj } D_2)L + a^{n-k} \text{ adj } B_1 = d_2D_1, \tag{52}$$

then the matrix D (formed as in the last member of (11)) is equivalent to one of adj $A', \ldots,$ adj $A^{(h)}$.

The case $k = n - 1$ is particularly simple. Then $D_2 = d_2 = b_1$, adj $D_2 = 1$, and the only automorph U^{T} of D_2 is 1. Congruence (51) becomes

$$L^{\mathsf{T}}L \equiv -a \text{ adj } B_1 \pmod{b_1}, \tag{53}$$

and two matrices L and L' are in the same complex if and only if $L \equiv L'$ mod b_1. Accordingly, there is a 1-1 correspondence between the solutions L mod b_1 of (51), such that the resulting matrices D are equivalent to one of the adj $A^{(i)}$, and the sets (WT_1) of primitive representations of B_1 by the system of matrices $A^{(i)}$.

References

[1] U. V. Linnik, "On the Representation of Large Numbers by Positive Ternary Quadratic Forms," *Bull. Acad. Sci. USSR, math. ser.*, vol. 4 (1940), 363-402.

[2] H. D. Kloosterman, *Acta Math.*, vol. 49 (1926), 407-464.

[3] W. Tartakowsky, *Bull. Acad. Sci. Leningrad* (7) 2 (1929), 111-122 and 165-196.

[4] G. Pall, *Amer. J. Math.*, vol. 68 (1946), 47-58; A. E. Ross and G. Pall, *Amer. J. Math.*, vol. 68 (1946), 59-65.

[5] B. W. Jones and G. Pall, *Acta Math.*, vol. 70 (1939), 165-191.

[6] J. W. L. Glaisher, *Quart. J. Math.*, vol. 20 (1885), 94.

[7] B. A. Venkov, *Elementary Theory of Numbers* (Russian), 1937.

[8] G. Pall, *Amer. J. Math.*, vol. 64 (1942), 503-513.

[9] U. V. Linnik, *Rec. Math.* [*Mat. Sbornik*] N.S., vol. 12 (54), (1943), 218-224.

[10] C. L. Siegel, *Ann. of Math.*, vol. 36 (1935), 527-606.

[11] C. Hermite, *J. für Mathematik*, vol. 47 (1850), 192.

[12] H. J. S. Smith, *Collected Mathematical Papers* (Oxford, 1894).

[13] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801, Arts. 278-283.

[14] G. H. Hardy and E. M. Wright, *The Theory of Numbers* (Clarendon Press, 1938), p. 259.

[15] A. Schild, *Can. J. Math.*, vol. 1 (1949), 47.

Illinois Institute of Technology
Chicago

https://doi.org/10.4153/CJM-1949-032-9 Published online by Cambridge University Press