THE ARITHMETICAL INVARIANTS OF QUADRATIC FORMS

GORDON PALL

1. Introduction. Anyone who has tried to read the developments by H. J. S. Smith [9][1] or H. Minkowski [6] of the systems of invariants (for a general positive integer n) associated with a genus of integral n-ary quadratic forms must be discouraged by their complexity. Further, from the standpoint of practical computation for a given form, these invariants are quite tedious to obtain, requiring as a first step the determination of a very special "characteristic form."

These complications are perhaps due essentially to the insistence on integral coefficients at all stages of the theory of integral forms. It is remarkable that, although Gauss began the systematic development of the theory of integral quadratic forms about the year 1800, it was not until over a hundred years later (in Hensel's work on p-adic numbers) that it was realized that there might be a considerable advantage in studying quadratic forms first in the field of rationals, and applying results thus obtained to the more difficult problems in the ring of integers. It turns out in fact that the complicated "simultaneous characters" of Smith and Minkowski are closely related to certain easily computed invariants under rational, linear transformations, and this fact enormously simplifies their use.

Our main purpose in this lecture will be to set forth a complete and easily computable system of invariants for a genus of integral n-ary quadratic forms. By our methods, anyone used to working with Legendre-Jacobi symbols should be able to obtain in less than fifteen minutes a complete system of invariants of a given integral form in (say) six variables, provided the coefficients are not unreasonably large. One has little more to do than "complete squares" by the method of elementary algebra, and then to read off the values of the invariants.

In an article scheduled to appear in the Duke Mathematical Journal, B. W. Jones shows how to reduce any integral quadratic form to a unique canonical form modulo 2^r (r large), and so embodies a complete set of invariants in a form which is in some respects equivalent but not quite so handy as ours.

Before describing these invariants, we shall recall some of the general properties of a genus of integral quadratic forms.

An address delivered at the invitation of the Program Committee before the New York meeting of the Society on October 28, 1944; received by the editors November 18, 1944.

[1] Numbers in brackets refer to the references cited at the end of the paper.

2. **Properties of a genus.** A quadratic form $f=x'Ax=\sum a_{ij}x_ix_j$ is called *integral* if its *coefficients* a_{ii} and $2a_{ij}$ $(i, j=1, \cdots, n)$ are integers. We shall assume that the determinant, $|f|$ or $|A|$, of f is not zero.

The linear transformation $x=Ty$ replaces f by the form g of matrix $T'AT$. We shall single out the cases where the elements of the matrix T are (a) real, (b) rational, (c) rational but with denominators prime to a given integer k, (d) integral with $|T|$ prime to k, (e) integral with $|T|=\pm 1$, (f) integral with $|T|=1$. In each case we assume $|T|\neq 0$. In cases (e) and (f) we shall call T respectively *unit-modular* and *unimodular.*

If f is replaced by $\sum b_iy_i^2$, by a real transformation, the number of negative coefficients b_i is invariant (under real transformations), will be denoted here by ι, and called the *index* of f. We learn in algebra that n and ι comprise a complete invariant system under real transformations.

Gauss called f and g *equivalent* if T is unimodular. All forms equivalent to a given one constitute a *class.* Some recent writers have defined class by means of what we have named unit-modular transformations. There is no essential difference, and any statement about one kind of class can be immediately interpreted in terms of the other kind.

A genus will consist of a finite number of classes, and can be defined in several ways. Since we shall have a later use for the result, we shall recall Gauss's original definition of genus for binary quadratic forms, or rather a slight modification of his definition. Any integral b.q.f. can be written as $f=d_1(ax_1^2+bx_1x_2+cx_2^2)=d_1f_1$, where d_1 is a positive integer, and a, b, c are coprime integers. The quantities d_1, $D=b^2-4ac$, and index ι, are invariants of f under unit-modular transformations. These quantities satisfy the conditions $(-1)^\iota D<0$; $D\equiv 0$ or 1 mod 4; $\iota=0$, 1, or 2. Besides these, the following quantities, called *generic characters*, are invariant:

$$(1)\qquad \begin{array}{ll} (f_1\,|\,p) & \text{for each odd prime } p \text{ in } D, \\ (-1\,|\,f_1) & \text{if } \omega \geqq 4, \text{ or if } \omega = 2 \text{ and } \rho = 1, \\ (-2\rho\,|\,f_1) & \text{if } \omega \geqq 5, \text{ or if } \omega = 3. \end{array}$$

Here $-D=2^\omega e$, where e is odd, and ρ stands for $(-1\,|\,e)$. (What we mean is that if f_1 is replaced in the character $(f_1|p)$ by any number n represented by f_1 and prime to p, the value of the Legendre symbol $(n|p)$ is always the same; similarly if $p=2$, n being odd and represented by f_1.) The preceding invariants are not (unless D is a square) independent, but are easily shown to satisfy the single relation

$$(2 \mid f_1)^{\omega}(-1 \mid f_1)^{(e+1)/2} = (-1)^{[\iota/2]}(f_1 \mid e_1), \tag{2}$$

where $e_1 = |e|$. This complicated relation will be given a more elegant form in §7.

Gauss defined two binary forms f and g as in the same *genus* if they have the same values for their invariants d_1, D, ι, and (1). This definition has the merit that the invariants are easily computable, and so one can tell in a jiffy whether two given forms are, or are not, in the same genus. Then Gauss proved, for binaries, two simple properties which were later extended to three, and then to n, variables, by Smith, Minkowski, and Siegel:

THEOREM 2.1. *Call two n-ary forms f and g equivalent modulo k, if f can be transformed by an integral transformation of determinant prime to k into a form congruent (coefficient for coefficient) modulo k to g. Then f and g are in the same genus if and only if they have the same index ι, and are equivalent modulo k, for every positive integer k.*

THEOREM 2.2. *Two n-ary forms f and g are in the same genus if and only if, for every positive integer k, each can be transformed into the other by a rational transformation with denominators prime to k.*

Minkowski [6, p. 71] in effect *defined* a genus by means of the property in Theorem 2.1. He then used the obvious fact that the numbers of solutions of $f \equiv n \bmod k$ and $g \equiv n \bmod k$ must be the same for every n and k, to obtain a complete (but complicated) system of invariants, which he showed would imply the equivalence mod k of f and g for every k. Eisenstein [2] (for ternaries of odd determinant) and Smith (for n-aries) had previously carried on in the Gauss tradition, and defined a genus by means of directly computable invariants. Smith no doubt obtained these invariants by studying the number of solutions of the congruences $f \equiv n \bmod p^r$, for any prime p. He knew the truth of both Theorems 2.1 and 2.2, although he published complete proofs only for $n=3$. Siegel [8] was the first to prove Theorem 2.2 for a general n.

Both the properties in the above theorems imply that f and g have the same determinant d. If we assume they have the same determinant d, both statements can be improved. Thus, two forms of integral matrix are in the same genus if they have the same determinant d, index ι, n, and are equivalent modulo $8d$; or again, if they have the same determinant d, and one can be transformed into the other by a rational transformation with denominators prime to $2d$.

Hel Braun [1] considered the complete system of generic invariants given by n, ι, a determinant d such that $(-1)\,d>0$, $q_0 = 8d^3$, and a matrix-residue S mod q_0; and showed that such a system corresponds to an actually existing form, if and only if there exists an integer x_1 prime to q_0 such that $|S| \equiv x_1^2 d$ mod q, and

$$\sum_{x \bmod q_0} \exp 2\pi i x'Sx/q_0 = \exp \frac{\pi i}{4}(n - 2\iota)\cdot(2q_0)^{n/2}\cdot d^{1/2}.$$

The latter condition was obtained by applying the reciprocity law for Gauss sums, and it is not surprising therefore that we can replace it by condition (7) of §5, which is closely related to the quadratic reciprocity law.

3. **The essentials of p-adic numbers and Hilbert norm-residue symbols obtained by an independent method.** There are at least three interesting points in which our treatment differs from that of Hensel [4, chap. 12] and Hasse [3]. First, we shall define a symbol, which, although essentially equal to Hilbert's norm-residue symbol, is defined more simply and symmetrically. Second we shall not use p-adic numbers as such, but shall replace them by rational congruences. Third, we can get all the results of Hasse (on rational quadratic forms) by strictly elementary methods (cf. §6).

Let p be a given prime. Two nonzero rational numbers a and b will be said to be in the same *p-adic class* if, for each positive integer r, there exists a rational number x such that

$$ax^2 \equiv b \bmod p^r. \tag{1}$$

By (1) we mean that $(ax^2-b)/p^r$ is a rational number whose denominator is prime to p, that is, an integer modulo p. It is easily shown that if p is odd there are exactly four p-adic classes, containing the respective numbers (called p-adic kernels)

$$1,\ p,\ \nu,\ p\nu, \tag{2}$$

where ν denotes any given quadratic non-residue mod p; and if $p=2$, there are exactly eight p-adic classes, with the p-adic kernels

$$1,\ 3,\ -1,\ -3,\ 2,\ 6,\ -2,\ -6. \tag{3}$$

To find the p-adic class of any nonzero rational number we need only write it in the form $s^2p^\alpha k$, where s is a rational number, $\alpha=0$ or 1, and k is an integer prime to p; and replace k by a number of the same quadratic character, 1 or ν if $p>2$, ± 1 or ± 3 if $p=2$.

It is useful to introduce a conventional "prime" p, called the prime ∞ or p_∞; and for this to understand that the solvability of (1) for every r means the solvability of

$$ax^2 = b \tag{4}$$

with x real. For the prime p_∞ it is evident that there are two p-adic classes, one consisting of all positive, the other of all negative rationals.

Example. 2 and $-7/2$ are in the same p-adic class for $p=2, 11$; in different p-adic classes if $p=\infty, 3, 5, 7$.

If a and b are any nonzero rational numbers, we define the symbol $(a, b)_p$ to have the value $+1$ or -1 according as the congruence

$$ax^2 + by^2 \equiv 1 \bmod p^r \tag{5}$$

has or has not, for each r, rational solutions x_r and y_r.

Two remarks should be made. First, our symbol $(a, b)_p$ has the same value as Hilbert's symbol $\left(\frac{a,\,b}{p}\right)$ in those cases in which Hilbert's symbol is defined. Second, in strict analogy to the Hensel p-adic background, which we are here replacing by rational congruences, we might have supposed that it would be necessary to restrict the solution numbers x_r and y_r in (5) to have the power of p in their denominators bounded independently of r. It is of interest to note in passing that this restriction is unnecessary, not only in the case of (5), but in the more general case of representation of forms by forms.

It follows at once from (5) that

$$(a, b)_p = (a', b')_p \tag{6}$$

if a' and b' are in the p-adic classes of a and b respectively. Hence $(a, b)_p$ can be evaluated by considering only a few cases, and we now give the final results:

$$(a, b)_\infty = -1 \text{ if and only if } a \text{ and } b \text{ are negative;} \tag{7}$$

$$(p^\alpha m, p^{\alpha'}m')_p = (-1 \mid p)^{\alpha\alpha'}(m \mid p)^{\alpha'}(m' \mid p)^{\alpha} \quad \text{if} \quad p > 2; \tag{8}$$

$$(2^\alpha m, 2^{\alpha'}m')_2 = (2 \mid m)^{\alpha'}(2 \mid m')^{\alpha}(-1)^{(m-1)(m'-1)/4} \qquad \text{if} \quad p = 2. \tag{9}$$

Here m and m' denote integers prime to p; α and α' are 0 or 1.

Example. $(2, -5/2)_p$ has the value -1 if $p=5$; $(+1)(-1)(+1) = -1$ if $p=2$; $+1$ for all other primes p.

The following properties of the symbol $(a, b)_p$, valid for all primes p, are easily verified by use of (7)–(9), or can be proved independently:

$$(a, b)_p = (b, a)_p; \tag{10}$$

$$(a, b)_p = 1 \text{ if } a, b, \text{ or } a + b \text{ is in the } p\text{-adic class of } 1; \tag{11}$$

$$(a, -a)_p = 1, \qquad (a, a)_p = (a, -1)_p; \tag{12}$$

$$(13) \quad (a, b_1b_2)_p = (a, b_1)_p(a, b_2)_p, \qquad (a_1a_2, b)_p = (a_1, b)_p(a_2, b)_p.$$

For any odd prime p, $(a, b)_p$ is evidently $+1$ unless p actually appears in a or b. One easily sees that for given a and b, $(a, b)_p$ is -1 for only a finite even number (possibly zero) of primes p (counting in p_∞). This fact is usually written in the simple form

$$(14) \qquad \prod_p (a, b)_p = +1,$$

and will be found to be equivalent to various cases of the quadratic reciprocity law.

4. **The invariants of a rational quadratic form under rational transformations.** Minkowski [6, pp. 219–239] obtained a complete system of such invariants, in 1890, on the basis of his theory for integral forms. The system which we shall now describe is essentially that of Hasse (1923), the binary and ternary case having been due to Hensel. Hasse gave many beautiful applications, and to appreciate the following developments properly, one should read his work. An exposition containing a number of novel features will be given in a forthcoming book by the author; proofs will be found there of all results stated here without proof. The following remarks should be sufficient for the applications made in §6 to integral forms.

Besides applying rational linear transformations T to f, we are interested in the effect of multiplying f by a nonzero rational number. If $t=|T|$, evidently $|f|$ is multiplied by t^2. Also, $|\lambda f| = \lambda^n|f|$. This proves the following theorem.

THEOREM 4.1. *The squarefree integer part d of the determinant D_n of an n-ary form f is invariant under nonsingular linear transformations with rational coefficients. If n is even, d is also invariant under multiplication by rational constants.*

To obtain further invariants under rational transformations, Hasse wrote f in the form $\sum a_i x_i^2$, and showed that the product of the $n(n+1)/2$ Hilbert symbols $(a_i, a_j)_p$ $(i \leqq j;\ i, j=1, \cdots, n)$ is an invariant of f under rational transformations. The restricted form of f made his proof [3, pp. 209–216] unnecessarily complicated. Instead, it is easy to prove, for any form $f=\sum a_{ij}x_ix_j$, that if D_i $(i=1, \cdots, n)$ denotes the leading principal minor determinant of order i in the matrix (a_{ij}) of f, then if none of the D_i vanishes, the quantity

$$(1) \qquad c_p = c_p(f) = (-1, -D_n)_p \prod_{i=1}^{n-1} (D_i, -D_{i+1})_p$$

is invariant under rational transformations. Indeed this remains true, when properly interpreted, even if some of the D_i other than D_n vanish, provided no two consecutive D_i vanish; for then, if we interpret any product such as $(D_{j-1}, -0)_p(0, -D_{j+1})_p$ as though it were $(D_{j-1}, -h)_p(h, -D_{j+1})_p$ with any value h not zero, we obtain the correct value of $c_p(f)$.

Theorem 4.2. *Two forms f and g are rationally equivalent if and only if they have the same values for their invariants*

$$n,\ i,\ d,\ c_p \text{ for every } p. \tag{2}$$

These invariants are not independent of one another, and it is easily seen that they satisfy the relations

$$0 \leqq \iota \leqq n, \quad (-1)^\iota d > 0, \quad c_\infty = (-1)^{[(\iota-1)/2]}, \quad \prod_p c_p = +1; \tag{3}$$

$$\text{if } n = 1, \quad c_p = (-1, -d)_p \text{ for every } p; \tag{4}$$

$$\text{if } n = 2, \quad c_p = 1 \text{ if } p \text{ satisfies } (-d \mid p) = 1. \tag{5}$$

Conversely, Hasse obtains many applications of the existence theorem that if n, ι, and d are integers, d squarefree, and (c_p) is a complex of signs satisfying (3)–(5), then there exists a form f with these assigned values for its invariants.

Besides (3_4) it should be noted that if f is integral and p is an odd prime not dividing $|f|$, then $c_p(f) = +1$.

The following formulae are easily proved, and show how easily the invariants c_p can be handled in applications. If λ is any nonzero rational number, then

$$c_p(\lambda f) = \begin{cases} (\lambda, (-1)^{(n+1)/2})_p c_p(f) & \text{if } n \text{ is odd,} \\ (\lambda, (-1)^{n/2}D_n)_p c_p(f) & \text{if } n \text{ is even.} \end{cases} \tag{6}$$

If $f = f_1(x_1, \cdots, x_r) + f_2(x_{r+1}, \cdots, x_n)$, where the variables do not overlap, and $d_1 = |f_1|$, $d_2 = |f_2|$, then

$$c_p(f) = c_p(f_1)c_p(f_2)\cdot(-1, -1)_p(d_1, d_2)_p. \tag{7}$$

In particular, if $f = a_1x_1^2 + \phi(x_2, \cdots, x_n)$, and $d = |f|$,

$$c_p(f) = (a_1, d)_p c_p(\phi). \tag{8}$$

5. The invariants of a genus of integral quadratic forms.

Lemma 5.1. *Let p be any finite prime. Every integral n-ary quadratic form f can be expressed (by means of a rational transformation which is integral modulo p and has determinant 1) in the form*

$$p^{e_1}\phi_1 + p^{e_2}\phi_2 + \cdots + p^{e_s}\phi_s, \qquad e_1 < e_2 < \cdots < e_s, \tag{1}$$

where each ϕ_i denotes a form with integral coefficients modulo p, the variables in different ϕ_i do not overlap, $|\phi_i|$ is prime to p $(i=1, \cdots, s)$, and the e_i are integers. Also, $e_1 \geqq 0$, except that $e_1=-1$ if $p=2$ and f has any odd cross-product coefficient. If n_i denotes the number of variables in ϕ_i, $\sum n_i = n$, and $\sum e_i n_i$ is the exponent to which p appears in $|f|$.

We give the proof (cf. [7, p. 38; 6, pp. 22 seq.]), since it is part of the technique of computing the generic invariants. It amounts to little more than judiciously completing squares. We can write $f=p^{e_1}f_1$, where the matrix (a_{ij}) of f_1 is integral, but that of f_1/p is not. If $p>2$ and any a_{ii} is prime to p, we can suppose it to be a_{11}; if every a_{ii} is divisible by p, then some $2a_{ij}$ is prime to p, and we can suppose this true of $2a_{12}$; we replace x_2 by x_1+x_2, and secure a_{11} to be prime to p. If $p=2$, and any a_{ii} is odd, we take it to be a_{11}; but if every a_{ii} is even we can suppose a_{12} odd, and that $a_{11}\neq 0$.

Thus the matrix of f_1 is of the form

$$\begin{bmatrix} A & B \\ B' & C \end{bmatrix}, \text{ where } A = [a_{11}] \text{ or } \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad |A| \text{ prime to } p,$$

the latter case occurring only if $p=2$. Then the transformation

$$\begin{bmatrix} I & -A^{-1}B \\ 0 & I \end{bmatrix} \text{ replaces } f_1 \text{ by the form of matrix } \begin{bmatrix} A & 0 \\ 0 & C-B'A^{-1}B \end{bmatrix},$$

and this transformation is integral modulo p.

In the first case, where $A=(a_{11})$, this process is tantamount to completing squares by the identity of elementary algebra:

$$\sum a_{ij}x_ix_j = a_{11}\left(x_1 + \sum_2^n a_{11}^{-1}a_{1j}x_j\right)^2 + a_{11}^{-1}\sum_{j,k=2}^n (a_{11}a_{jk} - a_{1k}a_{j1})x_jx_k,$$

absorbing into a square the terms involving x_1. In the second case, it is not difficult to show that one arrives at the same form (of matrix $C-B'A^{-1}B$) by merely completing squares twice, once for the variable x_1, then for the variable x_2; the denominators 2 which appear in the partial linear transformations disappear in their product. For example, we have

$$\begin{aligned} f &= 2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 \\ &= 2(x_1 + x_2/2 + x_3/2)^2 + \phi/2, \end{aligned}$$

where

$$\phi = 3x_2^2 + 2x_2x_3 + 3x_3^2 = 3(x_2 + x_3/3)^2 + (8/3)x_3^2,$$

and can assert that f is transformed into $2y_1^2+2y_1y_2+2y_2^2+(4/3)y_3^2$ by a linear transformation which is *integral* modulo 2 and has determinant 1.

By repeated applications of the preceding process, we evidently arrive at a form (1), where each ϕ_i is either a sum of binary quadratic forms

$$2(ax^2 + bxy + cy^2),\ b \text{ odd, the determinant } 4ac - b^2 \text{ odd,}$$

or contains at least one term ax^2, a odd. In these respective cases we shall term ϕ_i of *type B or A*. We can now read off from f the complete system of its generic invariants:

THEOREM 5.2. *Let $p>2$. In the form* (1), *the quantities*

$$s,\ e_1,\ \cdots,\ e_s,\ n_1,\ \cdots,\ n_s,\ \left(\frac{|\phi_i|}{p}\right) \qquad (i = 1, \cdots, s) \tag{2}$$

constitute a complete system of invariants of f, under integral transformations of determinant prime to p.

That is, two forms f and g with the same values for their invariants (2) are equivalent modulo p^r, r arbitrarily large.

THEOREM 5.3. *If $p=2$, the following quantities are invariant, in the form $2^{e_1}\phi_1+ \cdots +2^{e_s}\phi_s$, under integral transformations of odd determinant*:

(3) $s,\ e_1,\ \cdots,\ e_s,\ n_1,\ \cdots,\ n_s,$ *the type A or B of each ϕ_i*;

(4) *the residue* mod 8 *of Δ_{1k} if ϕ_k is followed by a rise of* 8;

(5) *the residue* mod 4 *of Δ_{1k} if ϕ_k is followed by a rise of* 4;

(6) *the quantity* $\left(\frac{2}{\Delta_{1k}}\right)^{l-1}\left(\frac{2}{\Delta}\right)^{\nu} c_2(\psi)$

for every block

$$\psi = \phi_k + 2\phi_{k+1} + 2^2\phi_{k+2} + \cdots + 2^{l-1}\phi_{k+l-1}$$

or

$$\phi_{k-1}/2 + \phi_k + 2\phi_{k+1} + \cdots + 2^{l-1}\phi_{k+l-1},$$

where $\phi_k, \phi_{k+1}, \cdots, \phi_{k+l-1}$ are all of type A and $l \geqq 1$, and in the second case ϕ_{k-1} is of type B; and the block cannot be enlarged into another block of the same type. Here Δ_{1k} denotes the product of the odd determinants $|\phi_1| \cdots |\phi_k|$; a "rise of 8" means that either $k=s$, or ϕ_k is of type A and $8 \mid 2^{e_{k+1}-e_k}\phi_{k+1}$, or ϕ_k is of type B (so that $\phi_k/2$ is integral) and $4 \mid 2^{e_{k+1}-e_k}\phi_{k+1}$; a "rise of 4" means that ϕ_k is of type B or that ϕ_k is *of type A and* $4 \mid 2^{e_{k+1}-e_k}\phi_{k+1}$. *In* (6), Δ *and* ν *are defined by* $|\psi| = 2^\nu\Delta$, *where Δ is odd; and clearly* $\nu \equiv \sum n_{k+1}$ (*i odd*, $1 \leqq i \leqq l-1$) mod 2. *Two forms with the same invariants listed here are equivalent* mod 2^r, *r arbitrarily large.*

THEOREM 5.4. *Two integral n-ary forms with the same index and determinant are in the same genus if and only if they have the same values for the invariants listed in the preceding two theorems for the prime 2 and for each odd prime in their determinant.*

THEOREM 5.5. *Let n, ι, d be given integers,* $0 \leqq \iota \leqq n$, $(-1)^\iota d > 0$. *For each prime p in d, assign a form-residue* $p^{e_1}\phi_1 + \cdots + p^{e_s}\phi_s$, *where* $\sum e_i n_i$ *is the exponent of p in d, and assign values to the invariants listed in Theorems* 5.2 *and* 5.3, *subject to the restriction that* $|\phi_1|\,|\phi_2| \cdots |\phi_s|$ *has the same quadratic character as* $d/p^{e_1n_1+\cdots+e_sn_s}$. *Then there exists an integral form with the invariants so assigned, if and only if*

$$\prod_p c_p(f) = +1. \tag{7}$$

This should be compared with Hel Braun's result mentioned in §2.

As an example of the computation of the invariants of a genus, consider the form $f = 5x_0^2+4x_1^2+4x_2^2+4x_3^2+2x_0x_1-4x_0x_2+4x_0x_3+4x_1x_3 = 5(x_0+x_1/5-2x_2/5+2x_3/5)^2+(19x_1^2+16x_2^2+16x_3^2+4x_1x_2+16x_1x_3+8x_2x_3)/5 = 5y_0^2+\phi/5$, where $\phi = 19(x_1+2x_2/19+8x_3/19)^2+60\psi/19$, where $\psi = 4x_3^2+2x_3x_2+5x_2^2 = 5(x_2+x_3/5)^2+(19/5)x_3^2$. The determinant is therefore $5(1/5)\cdot(19)(60/19)^2(5)(19/5) = 144$. Hence the only primes that need be considered are 2 and 3, and since the fractional coefficients above happen to be integral modulo 2 and 3, we can read off without further work the forms $5y_0^2+(19/5)y_1^2+(60/19)y_2^2+(12/5)y_3^2$, or what is essentially equivalent,

$$5z_0^2 + 7z_1^2 + 4(5z_2^2 + 7z_3^2) \bmod 2^r,$$

and

$$2z_0^2 + 2z_1^2 + 3(2z_2^2 + 2z_3^2) \bmod 3^r.$$

The invariants (2) relating to the prime 3 are therefore $s=2$, $e_1=0$, $e_2=1$, $n_1=n_2=2$, $(4|3)=1$, $(4|3)=1$. The invariants (3)–(6) relating to the prime 2 are $s=2$, $e_1=0$, $e_2=2$, $n_1=n_2=2$, both ϕ_1 and ϕ_2 of type A, the residue mod 8 of $|\phi_1|\,|\phi_2|$ is 1, the residue mod 4 of $|\phi_1|$ is 3, $c_2(\phi_1) = (-5, -7)_2 = +1$, $c_2(\phi_2) = +1$. The form f is thus seen to be in the same genus as $x_0^2+3x_1^2+4x_2^2+12x_3^2$. It may be remarked that f occurred, along with many more complicated forms, in an investigation of all systems of generalized quaternions permitting unrestricted factorization, and that there are exactly 39 such systems in which the norm-form (a quaternary quadratic form) is positive definite and in a genus of one class.

6. **Some remarks on the methods of proof.** Certain quantitative results concerning genera of quadratic forms, such as the weight formulae of Smith, Minkowski, and Siegel, have never been proved by strictly elementary methods. It may however be conjectured that any qualitative properties can be so proved. For example, the author has proved all the results of this article by elementary means, without using (for example) Dirichlet's theorem on the existence of primes in an arithmetical progression. This theorem seems to have evaded all efforts to find an elementary proof. Many writers have used Dirichlet's theorem in work on quadratic forms, when they might instead have used the following theorem of Gauss, on the existence of a genus of binary quadratic forms:

THEOREM 6.1. *If d, D, ι, and the characters of* §2 (1) *are assigned, subject to the necessary conditions* $(-1)^\iota D<0$, $D\equiv 0$ *or* 1 mod 4, $0\leqq\iota\leqq 2$, *and* §2 (2), *then there exists an integral binary quadratic form f with the assigned values for its invariants.*

Now if a is any number represented by f_1, it will be found by use of (7)–(9) of §3 that

$$(a, D)_\infty = (-1)^{[\iota/2]}, \qquad (a, D)_2 = (2\,|\,f_1)^\omega(-1\,|\,f_1)^{(e+1)/2}, \tag{1}$$
$$(a, D)_p = (f_1\,|\,p) \text{ if } p > 2 \text{ and } p \text{ divides } D \text{ to an odd power.}$$

The existence condition §2 (2) therefore takes the simpler form (cf. §5 (7))

$$\prod_p (a, D)_p = 1. \tag{2}$$

An analysis of Gauss's existence theorem will be found to yield the following theorem.

THEOREM 6.2. *Let d be a nonzero rational number, and let j_p be assigned equal to* $+1$ *or* -1 *for every prime p, including the prime* ∞. *However, let j_p be* -1 *for only a finite even number of primes p, and let j_p be* $+1$ *whenever d is in the p-adic class of* 1. *Then there exists a nonzero rational number h such that*

$$(h, d)_p = j_p \text{ for every } p. \tag{3}$$

In many problems, it will be found that either the construction of a binary quadratic form of a suitably determined genus, or the choice of a number represented by such a form, or a direct use of Theorem 6.2, will serve the same end as the choice of a prime by means of Dirichlet's theorem.

We shall illustrate this by giving a proof, noteworthy for its simplicity, of Legendre's theorem that every positive integer not of the form $4^h(8n+7)$ is a sum of three squares.

Let a denote a positive squarefree integer not of the form $8n+7$. It will suffice to prove that a is represented by a positive, properly primitive form of determinant 1, since every such form is equivalent to $x_1^2+x_2^2+x_3^2$ (cf. [5, p. 121]).

I. *Case* $a\equiv 3$ mod 8. We obtain by Gauss's theorem a positive, primitive form $\psi=C_1x^2+Rxy+B_1y^2$ of discriminant $R^2-4B_1C_1=-a$, with characters such that

$$(\psi\,|\,p) = (-2\,|\,p) \quad \text{if} \quad p\,|\,a. \tag{4}$$

This is consistent with the condition of possibility §2 (2), since

$$\prod_{p|a}(\psi\,|\,p) = \prod_{p|a}(-2\,|\,p) = 1,$$

the number of prime factors in a of the form $8k+5$ or 7 being even. We can take C_1 prime to $2a$, and then by a translation $x\rightarrow x+hy$ secure $R\equiv a$ mod $2a$, and hence (comparing discriminants) $B_1\equiv 0$ mod a. Set $C=2C_1$, $B=2B_1$. In view of (4) we can solve

$$-C \equiv t^2 \pmod{a} \tag{5}$$

for an integer t. We set $s=0$, and write $b=(C+t^2)/a$, $c=(B+s^2)/a$, $r=(st-R)/a$. Then $ax^2+by^2+cz^2+2ryz+2szx+2txy$ has determinant 1 and solves our problem.

II. *Case* $a\equiv 1$ or 2 mod 4. We can choose a positive primitive form $\psi=Cx^2+2Rxy+By^2$ of discriminant $-4a=4R^2-4BC$, with characters such that

$$\begin{aligned}(\psi\,|\,p) &= (-1\,|\,p) \text{ if } p\,|\,a,\ p>2; &\quad (-1\,|\,\psi) &= 1 \text{ if } a\equiv 1 \bmod 4,\\ (2\,|\,\psi) &= 1 \text{ if } a\equiv 2 \bmod 8, &\quad (-2\,|\,\psi) &= -1 \text{ if } a\equiv 6 \bmod 8.\end{aligned} \tag{6}$$

This is consistent with §2 (2), since the number of prime factors $4k+3$ in a is correctly adjusted. As before, we can secure $R\equiv 0$, $B\equiv 0$ mod a, C being prime to $2a$. We have (5), and so on, exactly as in case I.

References

1. H. Braun, Journal für Mathematik vol. 182 (1940) pp. 32–49.
2. G. Eisenstein, Journal für Mathematik vol. 35 (1847) pp. 117–136.
3. H. Hasse, Journal für Mathematik vol. 152 (1923) pp. 129–148 and 205–224.

4. K. Hensel, *Zahlentheorie*, 1913.

5. E. Landau, *Vorlesungen über Zahlentheorie*, I.

6. H. Minkowski, *Gesammelte Abhandlungen*, I.

7. G. Pall, Quart. J. Math. vol. 6 (1935) pp. 30–51.

8. C. L. Siegel, Amer. J. Math. vol. 63 (1941) pp. 658–680.

9. H. J. S. Smith, *Collected mathematical papers*, I, pp. 510 et seq.; II, pp. 623 et seq.

McGill University