# MATHEMATIKA

A JOURNAL OF PURE AND APPLIED MATHEMATICS

*Founded by*

H. DAVENPORT

*Edited by*

C. A. ROGERS, J. G. SEMPLE, K. STEWARTSON

MATHEMATIKA is published by the Department of Mathematics, University College, London. It contains original notes and memoirs on mathematics and its applications. Any diagrams submitted with manuscripts should be of a size not exceeding 1·5 times the final size for printing.

Two parts of MATHEMATIKA are published each year. The parts normally appear in June and December but are at the moment subject to delay. The part for December 1974 was issued in March 1975. Each part normally consists of about 150 pages, but to avoid delays the parts for 1975 will be rather smaller.

The subscription price for the volume of two parts for 1976 is £6·50. Subscriptions should be sent to

MATHEMATIKA,
UNIVERSITY COLLEGE,
GOWER STREET,
LONDON, WC1E 6BT,
ENGLAND.

Cheques and Postal Orders should be made payable to University College, London.

A special subscription rate of £4·25 applies to members of some national Mathematical Societies requiring MATHEMATIKA for their personal use.

Back numbers are available. The price is £6·00 per volume on orders received by the 31st of December, 1975, but will be £6·50 on orders received on or after the 1st of January 1976.





1975

# MATHEMATIKA

A JOURNAL OF PURE AND APPLIED MATHEMATICS

VOL. 22. PART 1. June, 1975. No. 43.


## ONE-CLASS GENERA OF POSITIVE TERNARY QUADRATIC FORMS—II

G. L. WATSON

1. *Introduction.* Let $f$ be a positive–definite ternary quadratic form with integer coefficients; by $c(f)$, the class-number of $f$, is meant the number of classes in the genus of $f$. The object of this paper is to find all the $f$ with $c(f) = 1$; these $f$ are the ones for which $f \simeq f' \Rightarrow f \sim f'$, where $f'$ is an arbitrary ternary form and $\sim$, $\simeq$ denote equivalence and semi-equivalence respectively. Trivially, it suffices to find the primitive $f$ with $c(f) = 1$.

In matrix notation, with $\mathbf{x} = \operatorname{col}\{x_1, x_2, x_3\}$, and using an accent to denote transposition, we have

$$f = f(\mathbf{x}) = \tfrac{1}{2}\mathbf{x}'A\mathbf{x}, \text{ where } A = A(f) = (\partial^2 f/\partial x_i \partial x_j). \tag{1.1}$$

The $3 \times 3$ matrix $A$ satisfies $A' = A \equiv -A \pmod 2$ and has even diagonal elements, whence $2 \mid \det A$, and $\det A > 0$, so

$$d = d(f) = -\tfrac{1}{2}\det A(f) \tag{1.2}$$

is a negative integer. In [1: 97, Table 1] I gave a list of 20 forms $f_1, \ldots, f_{20}$, in 20 different genera, and proved that

$$c(f) = 1 \text{ and } d(f) \text{ square-free} \Leftrightarrow f \sim \text{one of } f_1, \ldots, f_{20}. \tag{1.3}$$

With the same $f_1, \ldots, f_{20}$ (all primitive) as in (1.3), and suitably chosen $f_{21}, \ldots$, the result to be here proved could be stated as

$$c(f) = 1 \text{ and } f \text{ primitive} \Leftrightarrow f \sim \text{one of } f_1, \ldots, f_{790}. \tag{1.4}$$

(In [1; 104, Theorem 2] I stated without proof that (1.4) held with suitable $f_{21}, \ldots$ and with 787 in place of 790; but I found three omissions on checking the calculations.)

Some results proved in [2] and improved in [3] will here be used to formulate, and deduce from (1.3), a result equivalent to (1.4), but more concise.

I have proved analogues of (1.3) for positive $n$-ary forms $f(x_1, \ldots, x_n)$ with $n \geqslant 4$; see [4] for $n = 4$, [5] for $n \geqslant 5$. From these, analogues of (1.4) for $n \geqslant 4$ could be deduced; but it seems best to do the case $n = 3$ separately, since it presents special features.

I am obliged to the referee for checking the paper very thoroughly and detecting numerous minor errors and some obscurities.

2. *Transformations which do not increase the class-number.* For $f$, $\mathbf{x}$, as above, $m$ a positive integer, and $\varepsilon = 0$ or 1, we consider the two congruences

$$A(f)\mathbf{x} \equiv \mathbf{0} \pmod{m}, \quad 2^r f(\mathbf{x}) \equiv 0 \pmod{m}, \tag{2.1}$$

in which $\mathbf{0} = \text{col}\{0, 0, 0\}$. Denote by $\Lambda(m, \varepsilon, f)$ the set of all $\mathbf{x}$ with integer elements that satisfy (2.1). As shown in [3; 172, §2], $\Lambda(m, \varepsilon, f)$ is a lattice, obviously a sub-lattice of $\Lambda_3$, the set of all $\mathbf{x}$ with integer elements. So there exists a matrix $M$, $3 \times 3$ and with integer elements, such that

$$M\Lambda_3 = \Lambda(m, \varepsilon, f); \tag{2.2}$$

and for any such $M$ the form $g$ defined by the identity

$$g(\mathbf{y}) = 2^{\varepsilon} m^{-1} f(M\mathbf{y}), \text{ whence } A(g) = 2^{\varepsilon} m^{-1} M' A(f) M, \tag{2.3}$$

has integer elements.

Define $f \to (m, \varepsilon)g$ to mean that there exists $M$ such that (2.2), (2.3) hold; then, see [3; Theorem 1],

$$f \to (m, \varepsilon)g \Rightarrow c(g) \leqslant c(f). \tag{2.4}$$

We shall apply (2.4) repeatedly, with $m$, $\varepsilon$ not necessarily the same at each step. So we define $f \to g$ to mean that forms $F_i$, positive integers $m_i$, and integers $\varepsilon_i$ each 0 or 1, may be chosen so that (for some $k$)

$$F_0 \sim f, \; F_{i-1} \to (m_i, \varepsilon_i)F_i (i = 1, \ldots, k), \text{ and } F_k \sim g. \tag{2.5}$$

From this definition and (2.4) we see that

$$f \to g \Rightarrow c(g) \leqslant c(f). \tag{2.6}$$

3. *Statement of result.* We shall prove the following

THEOREM. *Let $f$ be a positive-definite ternary quadratic form with integer coefficients. Then $f$ has class-number* 1, *if, and only if, the relation $\phi_i \to f$, defined above, and in* [3], *holds for at least one of the* 68 *forms $\phi_1, \ldots, \phi_{68}$ listed in Table* 1.

The second column of the table gives the coefficients of $x_1^2, x_1x_2, x_2^2$, in that order. The third column gives, also in natural order, the other three coefficients of $\phi_i$.

We shall see that for each $\phi_i$ there is at least one $f_j$, with $1 \leqslant j \leqslant 20$, see (1.3), such that

$$\phi_i \to f_j. \tag{3.1}$$

The pairs $(i, j)$ for which (3.1) holds are shown in Table 2. For convenience, Table 2 also gives the values of $d(f_j)$ and of $P(f_j)$, $= P(\phi_i)$ when (3.1) holds, where $P$ is defined by

$$P(f) = \Pi\{p : f \text{ is not a } p\text{-adic zero form}\}. \tag{3.2}$$

($p$ always denotes a prime.)

4. *Table* 2. The invariants $d$, $P$ determine a ternary genus uniquely when $d$ is square-free; see if necessary [1; 100, Lemma 5]. We therefore have $g \sim f_j$, if $d(g) = d(f_j)$ and $P(g) = P(f_j)$, for any of the $f_j$ of (1.3). (3.1) therefore follows, if we can construct a chain of the shape (2.5) with $F_0 \sim \phi_i$, $d(F_k) = d(f_j)$, and $P(F_k) = P(f_j)$.



TABLE 1

| $i$ | Coefficients of $\phi_i$ | | $d(\phi_i)$ | $i$ | Coefficients of $\phi_i$ | | $d(\phi_i)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1, 0, 2 | 1, 2, 3 | −18 | 35 | 5, 2, 7 | 2, −6, 13 | −1536 |
| 2 | 1, 0, 4 | 1, 2, 5 | −72 | 36 | 5, 2, 13 | 0, 0, 24 | −6144 |
| 3 | 1, 0, 1 | 0, 0, 8 | −32 | 37 | 5, 2, 13 | 4, −12, 28 | −6144 |
| 4 | 2, 2, 3 | 2, 2, 7 | −128 | 38 | 7, 4, 20 | 2, −4, 23 | −12288 |
| 5 | 1, 0, 2 | 0, 0, 16 | −128 | 39 | 1, 0, 9 | 0, 0, 24 | −864 |
| 6 | 2, 0, 3 | 0, 2, 11 | −256 | 40 | 2, 2, 5 | 0, 0, 24 | −864 |
| 7 | 3, 2, 5 | 0, 4, 10 | −512 | 41 | 7, 2, 10 | 6, −6, 15 | −3456 |
| 8 | 3, 0, 4 | 2, 0, 11 | −512 | 42 | 6, 0, 9 | 0, 6, 17 | −3456 |
| 9 | 3, 2, 7 | 2, −2, 7 | −512 | 43 | 5, 0, 6 | 2, 0, 29 | −3456 |
| 10 | 3, 2, 11 | 2, −10, 19 | −2048 | 44 | 7, 2, 13 | 6, 6, 21 | −6912 |
| 11 | 5, 4, 12 | 4, −8, 12 | −2048 | 45 | 7, 4, 10 | 4, 8, 28 | −6912 |
| 12 | 5, 0, 8 | 2, 0, 13 | −2048 | 46 | 11, 6, 15 | 2, −6, 23 | −13824 |
| 13 | 5, 4, 12 | 4, 8, 20 | −4096 | 47 | 8, 4, 11 | 8, 8, 44 | −13824 |
| 14 | 2, 1, 2 | 2, 2, 8 | −108 | 48 | 11, 10, 35 | 4, 28, 44 | −55296 |
| 15 | 1, 1, 7 | 1, 5, 13 | −324 | 49 | 15, 12, 20 | 0, 16, 56 | −55296 |
| 16 | 3, 0, 5 | 0, 4, 8 | −432 | 50 | 1, 1, 3 | 1, −1, 3 | −28 |
| 17 | 1, 1, 2 | 0, 1, 3 | −20 | 51 | 1, 1, 9 | 1, −7, 9 | −250 |
| 18 | 1, 0, 3 | 0, 2, 7 | −80 | 52 | 3, 2, 7 | 1, −3, 13 | −1000 |
| 19 | 1, 1, 7 | 0, 3, 7 | −180 | 53 | 5, 5, 5 | 2, −2, 8 | −540 |
| 20 | 1, 1, 9 | 0, 5, 15 | −500 | 54 | 7, 1, 7 | 2, −2, 8 | −1500 |
| 21 | 1, 0, 6 | 1, 0, 7 | −162 | 55 | 1, 0, 4 | 1, 2, 11 | −168 |
| 22 | 2, 2, 11 | 2, 10, 23 | −1728 | 56 | 1, 0, 9 | 1, 9, 13 | −378 |
| 23 | 6, 6, 7 | 6, 6, 15 | −1728 | 57 | 2, 2, 5 | 2, 1, 11 | −378 |
| 24 | 7, 6, 15 | 2, −6, 19 | −6912 | 58 | 5, 2, 10 | 1, 10, 13 | −2058 |
| 25 | 1, 1, 5 | 1, −1, 7 | −126 | 59 | 1, 0, 5 | 0, 0, 8 | −160 |
| 26 | 1, 1, 9 | 0, 7, 21 | −686 | 60 | 3, 2, 6 | 0, 6, 11 | −640 |
| 27 | 1, 0, 5 | 0, 4, 12 | −224 | 61 | 1, 1, 3 | 1, 0, 5 | −52 |
| 28 | 3, 2, 6 | 2, 2, 7 | −448 | 62 | 5, 2, 8 | 3, 6, 9 | −1188 |
| 29 | 6, 6, 7 | 0, 4, 8 | −960 | 63 | 1, 1, 13 | 0, 3, 15 | −756 |
| 30 | 7, 4, 8 | 2, 4, 19 | −3840 | 64 | 1, 0, 2 | 1, 0, 3 | −22 |
| 31 | 3, 0, 11 | 0, 10, 35 | −4320 | 65 | 1, 0, 2 | 1, 0, 9 | −70 |
| 32 | 7, 6, 18 | 2, 6, 19 | −8640 | 66 | 5, 5, 17 | 5, −2, 23 | −6750 |
| 33 | 3, 3, 17 | 6, 8, 38 | −6750 | 67 | 1, 1, 3 | 0, 3, 5 | −46 |
| 34 | 1, 1, 7 | 1, 5, 31 | −810 | 68 | 5, 4, 5 | 3, 3, 9 | −702 |

TABLE 2

| $i$ | $j$ | $d(f_j)$ | $P(f_j)$ | $i$ | $j$ | $d(f_j)$ | $P(f_j)$ |
|---|---|---|---|---|---|---|---|
| 1–13 | 1 | − 2 | 2 | 55–58 | 11 | −42 | 42 |
| 14–16 | 2 | − 3 | 3 | 18, 59, 60 | 12 | −10 | 5 |
| 17–20 | 3 | − 5 | 5 | 61 | 13 | −13 | 13 |
| 21–24 | 4 | − 6 | 2 | 62 | 14 | −33 | 3 |
| 25–28 | 5 | −14 | 2 | 63 | 15 | −21 | 7 |
| 29–34 | 6 | −30 | 30 | 64 | 16 | −22 | 2 |
| 16, 35–49 | 7 | − 6 | 3 | 65 | 17 | −70 | 70 |
| 50 | 8 | − 7 | 7 | 66 | 18 | −30 | 2 |
| 51, 52 | 9 | −10 | 2 | 67 | 19 | −46 | 2 |
| 53, 54 | 10 | −15 | 3 | 68 | 20 | −78 | 78 |

One way to construct such a chain is to take each $\varepsilon_i = 0$ and each $m_i$ prime, with $m_i^2 \mid d(F_{i-1})$; and $i - 1 = k$ (that is, the chain breaks off) if no such $m_i$ exists. By so doing it will be found that (3.1) follows for all the pairs $(i, j)$ of Table 2, except 16, 7 and 18, 12. For these two cases we may begin the chain with $\to$ (4, 1) and then proceed as above with $\to (p, 0)$.

As shown in [3; §2], $f' \sim f \to (m, \varepsilon)g \sim g'$ implies $f' \to (m, \varepsilon)g'$, so the $\to (m, \varepsilon)$ and $\to$ are essentially relations between classes. So regarded, the $\to (m, \varepsilon)$ are mappings since $f \to (m, \varepsilon)g$ and $f \to (m, \varepsilon)g'$ together imply $g \sim g'$. Obviously therefore it is convenient to choose $f$, from its class, supposed given, so that a diagonal $M$ will satisfy (2.2).

If we put $m = p$ and $\varepsilon = 0$, and suppose $p \mid d$, then $M = [1, 1, 1]$ will do if $f \equiv 0 \pmod p$, identically; and $M = [p, 1, 1]$ if $f \equiv ax_1^2 \pmod p$, $p \nmid a$. If $f$ is not equivalent to a form of either of these shapes, then, see if necessary [1; §7], it is equivalent to one $\equiv \psi(x_1, x_2) \pmod p$, $p \nmid d(\psi)$, and for such a form $M = [p, p, 1]$ will do.

With these remarks the calculations needed to complete the verification of Table 2 are quite simple and they are left to the reader.

5. *Determination of* $\min\{c(f), 2\}$ *for given* $f$. We prove:

LEMMA 1. *Suppose that* $f, g, h, p$ *satisfy* $c(h) = 1$ *and*

$$f \to (p, 0)g \to (p, 0)h; \tag{5.1}$$

*and let* $P, Q, R, S, I, U$ *denote* $3 \times 3$ *matrices with integer elements, such that* $PQ = RS = pI$, $I$ *being the identity, and* $U$ *is an automorph of* $h$. *Then:*

(i) $f(\mathbf{x}) = h(Q\mathbf{x})$ (identically), *for some pair* $P, Q$;

(ii) *every* $f' \simeq f$ *is expressible as* $h(S\mathbf{x})$, *for some pair* $R, S$;

(iii) $h(Q\mathbf{x}) \sim h(S\mathbf{x})$, *if, and only if, there exists* $U$ *such that*

$$PU\mathbf{y} \equiv \mathbf{0} \pmod p \Leftrightarrow R\mathbf{y} \equiv \mathbf{0} \pmod p \ (\textit{for } \mathbf{y} \in \Lambda_3); \tag{5.2}$$

(iv) $c(f) = 1$, *if, and only if, for every pair* $R, S$ *such that* $h(S\mathbf{x}) \sim_p h(Q\mathbf{x})(= f)$, *there exists* $U$ *satisfying* (5.2).

*Proof.* For (i), take $m = p$, $\varepsilon = 0$, in [3; 174, (3.7)]. For (ii), choose $g', h'$ so that $f' \to (p, 0)g' \to (p, 0)h'$. By [3; 173, (2.11)] we have $g' \simeq g$, $h' \simeq h$; so by the hypothesis $c(h) = 1$ we have $h' \sim h$, and we appeal to (i).

In [3; 176, Theorem 3] $f \to (m, \varepsilon)\, g \to (m, \varepsilon)h$ and $f' \to (m, \varepsilon)g \to (m, \varepsilon)h$ are assumed, and two necessary and sufficient conditions, (i) and (ii), for $f \sim f'$ are given. The argument shows that, if the second condition (on $f'$) is weakened by putting $g'$ $(\simeq g)$ for $g$, we still have (ii) $\Leftrightarrow f \sim f'$. So from (ii) (of the theorem quoted) we have (iii) of the present lemma, after specialization and a little change of notation.

Clearly $\det Q$ and $\det S$ are non-zero integers, each dividing $p^3$. It follows that $h(Q\mathbf{x})$ and $h(S\mathbf{x})$ are always equivalent over the real field, and also, for every prime $q \neq p$, over the $q$-adic integers. So $h(S\mathbf{x}) \sim_p f \Leftrightarrow h(S\mathbf{x}) \simeq f$. With this remark, (iv) follows immediately from (i)–(iii), and the lemma is proved.

It will be useful to notice that, for vectors $\mathbf{x}, \mathbf{y}$ with integer elements, $\mathbf{y}$ is expressible as $Q\mathbf{x}$, if, and only if, $P\mathbf{y} \equiv \mathbf{0} \pmod p$: and similarly for $R, S$. We may therefore regard $f, f'$ as $h(\mathbf{y})$ with $\mathbf{y}$ restricted to satisfy $P\mathbf{y}, R\mathbf{y} \equiv \mathbf{0} \pmod p$.



To determine whether or not $c(f) = 1$, for given $f$, we use (1.3) if $d(f)$ is square-free, and if not choose $p, g\ h$, to satisfy (5.1) and $p^2 \mid d(f)$. We then determine whether or not the condition of part (iv) of the lemma holds; if not, $c(f) > 1$, by the lemma or (2.6). So suppose the condition satisfied, and then we know that $c(f) = 1 \Leftrightarrow c(h) = 1$. If $|d(h)| < |d(f)|$, we repeat the process, with $h$ in place of $f$; so suppose $|d(h)| \geqslant |d(f)|$, whence, by (i) of the lemma, $\det Q = \pm 1$ and $f \sim h$. Now (5.1) and (2.6) give $c(f) = 1 \Leftrightarrow c(g) = 1$, and if $|d(g)| < |d(f)|$ we repeat the process, with $g$ for $f$ (and a different choice of $p$). It suffices now to note that, if $f \to (p, 0)g \to (p, 0)f$, then $d(f)d(g)$ is exactly divisible by $p^3$, so

$$p^2 \mid d(f) \Rightarrow p^2 \nmid d(g),$$

and $d(f)/d(g)$ is a power of $p$. The latter assertion is clear from (2.3). For the former see [2; 580, Theorem 4]; it will also be clear from §§7, 8 below.

It is possible to prove $c(\phi_1) = 1$ for $i = 1, \ldots, 68$ by the foregoing method. Then we have the "if" of the theorem, since $\phi_i \to f$ implies $c(f) = c(\phi_i) = 1$, by (2.6).

We shall have to apply Lemma 1 in a large number of cases, in some of which the condition of part (iv) holds, in others not. Obviously it is not practicable to give all the details, but a number of examples will be given later.

6. *The "only if" of the theorem; a special case.* If $a$ is a positive integer then $f \supset a$ means that $f(\mathbf{x}) = a$ is soluble (in integers $x_i$); and $f \supset_p a$ means that $f(\mathbf{x}) \equiv a \pmod{p^t}$ is soluble for every $t$. As in [6], $f$ is *regular*, if $f \supset_p a$ for every $p \Rightarrow f \supset a$. As in [2], $f$ *is strongly* primitive (SP), if for every prime $p$ it has a binary section with discriminant not divisible by $p$; and trivially, if $f$ is SP then $p \nmid a$ implies $f \supset_p a$. It is well known that $c(f) = 1$ implies that $f$ is regular. (In [1], $f \supset a$ meant that $f$ represents $a$ properly, but here it is convenient not to distinguish between proper and improper representation.)

As shown in [6], the argument used in [1; 101–3, §§5, 6] to prove the $\Rightarrow$ of (1.3) does not make full use of the hypotheses. Nearly all of it remains valid with $f$ regular in place of $c(f) = 1$. $p^2 \nmid d(f)$ gives an improvement on $p \nmid a \Rightarrow f \supset_p a$ which is used only for small $p$. And finally, if we were satisfied with a weaker conclusion, say $|d|$ small enough not to be divisible by the square of any large prime, then the argument could be shortened.

The argument quoted above makes use of two fairly obvious remarks. First, if $f \supset a_1$, $f \supset a_2$, and $a_1 a_2$ is not a square, then $f$ must represent some binary $F$ with $|d(F)| \leqslant 4a_1 a_2$. (Taking $f$ to be reduced, put $F = f(x_1, x_2, 0)$ and note that the diagonal coefficients of $f$ are its successive minima. So we must have $F(1, 0) \leqslant \min(a_1, a_2)$ and $F(0, 1) \leqslant \max(a_1, a_2)$; and we note that

$$|d(F)| = -d(F) \leqslant 4F(1, 0)F(0, 1)).$$

Secondly,

$$f \supset a \text{ and } F = f(x_1, x_2, 0) \not\supset a \Rightarrow |d((f)| \leqslant a\,|d(F)|, \tag{6.1}$$

for which see [1; 98, (2.7)]. These remarks are useful, if $f$ regular, or $c(f) = 1$, is assumed and $f \supset_p a$ for all $p$ is true for a number of small values of $a$. In particular, we have:

LEMMA 2. *Suppose that* $c(f) = 1$, $f$ *is SP, and* $p^2 \mid d = d(f)$ *is false for* $p = 2, 3, 5$. *Then* $d$ *is square-free.*

*Proof.* Since $c(f) = 1$ implies that $f$ is regular, the hypotheses of the lemma imply those of [6; Corollary to Theorem 1], the conclusion of which gives a finite set of possibilities for $|d|$, all square-free (crudely, $|d| < 80$, $\neq 49$). $p^2 | d$ is therefore false also for $p \geqslant 7$, as was to be proved; and of course we have $f \sim$ some $f_j$ by (1.3).

The condition $25 \nmid d$ could be omitted in this lemma, though not in the result quoted from [6].

Lemma 2 will be used to show (in Lemma 4) that we need only use Lemma 1 with either $p \leqslant 13$ or $p = 23$; but we have yet to show that we need only use it finitely many times.

7. *Odd primes.* We note that $f \leftrightarrow g$, meaning $f \to g \to f$, implies $c(f) = c(g)$, by (2.6); so it suffices to prove the "only if" of the theorem with the further hypothesis that $f$ is *normalized under* $\to$. That means, as in [3], that

$$f \leftrightarrow g \Rightarrow |d(g)| \geqslant |d(f)|. \tag{7.1}$$

We note also that, for any $f$, there is a form $g$ with $f \to g$ and $d(g)$ square-free; see §4. Assuming $c(f) = 1$, and using (2.6), we may suppose henceforth that

$$f \to f_j \text{ for some } j,\ 1 \leqslant j \leqslant 20, \text{ see (1.3)}. \tag{7.2}$$

For odd $p$ it is well known that

$$\left.\begin{aligned} f \sim_p a_1 p^{e_1} x_1^2 + a_2 p^{e_2} x_2^2 + a_3 p^{e_3} x_3^2, \\ p \nmid 2a_1 a_2 a_3,\ 0 \leqslant e_1 \leqslant e_2 \leqslant e_3. \end{aligned}\right\} \tag{7.3}$$

If we write briefly $(e_1, e_2, e_3)$ for $f$ satisfying (7.3) then, see [3; 179, (7.4)–(7.9)], we have for $w \geqslant 0$

$$(e_1, e_2, e_3) \to (p^w, 0)\,(|w-e_1|, |w-e_2|, |w-e_3|) \tag{7.4}$$

and

$$f \leftrightarrow pf, f \leftrightarrow F_p, \text{ where } F_p = (0, e_3-e_2, e_3-e_1). \tag{7.5}$$

($F_p$ is the right member of (7.4) with $w = e_3$.) The first part of (7.5) gives $f \leftrightarrow p^{-1}f$, if $e_1 > 0$; so by taking $g = p^{-1}f$ or $F_p$ we see that

$$(7.1) \Rightarrow e_1 = 0 \quad \text{and} \quad e_2 \leqslant \tfrac{1}{2}e_3. \tag{7.6}$$

We now prove:

LEMMA 3. *If there exists an odd prime such that* (7.3) *holds with one of the following sets of exponents* $(e_1, e_2, e_3)$:

$$\begin{gathered} (0,0,2)(p \geqslant 5),\ (0,0,3)(p \geqslant 3),\ (0,0,4,)(p = 3), \\ (0,1,2)(p = 11, 13, \text{or } 23),\ (0,1,3)(p = 5, 7), \\ (0,1,4)(p = 3),\ (0,2,4)(p = 3), \end{gathered} \tag{7.7}$$

*then* $c(f) > 1$.

*Proof.* We first notice that if $p \nmid m$ and $f \to (m, \varepsilon)g$ then, see (2.3), $g \sim_p 2^{\varepsilon} mf$, whence the exponents $e_i$ are the same for $g$ as for $f$; and if we prove $c(g) > 1$, $c(f) > 1$ follows from (2.6). Repeating this argument sufficiently often, with suitable $m$ at each stage, we see that it suffices to prove the lemma with the additional hypothesis that $q^2 \nmid d(f)$ for every prime $q$ except the prime $p$ for which the $e_i$ have one of the sets of values (7.7). Next, repeated application of $\to(p, 0)$ will give (7.2) for some $j$; and Lemma 2 disposes of $e_2 = 0$ for $p \geqslant 7$.

Now we have finitely many genera to consider, and the lemma can be proved by showing in finitely many cases that condition (iv) of Lemma 1 does not hold. Some examples will be given later to show how this is done; there are also ways of cutting down the number of cases to be considered. Subject to these remarks we consider the lemma as proved.

It will be convenient to define $\alpha_p(f)$, for odd $p$ only, to be 0, if (7.3) holds with $e_1 \equiv e_2 \equiv e_3 \pmod 2$, 1 if not; and to prove that $\alpha_p$ is invariant under $\to (m, \varepsilon)$ and so under $\to$. Factorizing $\to (m, \varepsilon)$ as in [3; 174, (3.10)], we see that it suffices to prove this assertion in the two cases $m = p^w$, $p \nmid m$, with $\varepsilon = 0$ for $m = p^w$. Now see (7.4) and the beginning of the foregoing proof. The invariance is thus proved, and so in (7.2) we necessarily have $d(f_j) = -d'$ or $-2d'$, $d'$ being the product of the odd $p$ with $\alpha_p(f) = 1$.

The canonical expression (7.3) is classical, as are (8.1) and (8.2) below; but the reader may refer if necessary to [7; ch. 4]. In particular, Theorem 34 on p. 58 of [7] shows how (8.2) can be transformed into (8.1) when the $e_i$ are all equal.

LEMMA 4. (7.1) *and* $c(f) = 1$ *imply, for odd* $p$, *that the* $e_i$ *in* (7.3) *have one of the following sets of values:*

$$\left.\begin{gathered} (0,0,0)\ (\textit{for any } p),\ (0,0,1)\ (\textit{for } p \leqslant 13 \textit{ or } p = 23), \\ (0,0,2)\ (p = 3),\ (0,1,2)\ (p = 3, 5 \textit{ or } 7),\ (0,1,3)\ (p = 3). \end{gathered}\right\} \tag{7.8}$$

*Proof.* Assuming the lemma false we choose a $p$ for which the $e_i$ are not as in (7.8). We may also assume, by Lemma 3, that they are not as in (7.7); and this gives $e_3 \geqslant 3$. Now we apply $\to (p, 0)$ once if $e_2 = 1$, twice otherwise. Using (7.4) with $w = 1$, we find that thereby $(e_1, e_2, e_3)$ goes into $(e_1', e_2', e_3')$, where $e_1' = 0$ always, $e_2' = e_2$ if $e_2 \leqslant 1$, $e_2 - 2$ otherwise, and $e_3' = e_3 - 1$ if $e_2 = 1$, $e_3 - 2$ if not. It follows that $e_2' \leqslant \frac{1}{2}e_3'$.

Now, from (2.6), we may assume, using induction on $e_3$, that the $e_i'$ are as in (7.8). It follows easily that the $e_i$ are as in (7.7) or (7.8), giving a contradiction which completes the proof.

8. *The prime* 2. We consider first the case

$$f \sim_2 2^r \theta(x_1, x_2) + 2^e a x_3^2, \quad 2 \nmid ad(\theta). \tag{8.1}$$

$f \leftrightarrow pf$ is true for $p = 2$, so, assuming (7.1), we have $re = 0$. We may suppose without loss of generality that the two sides of (8.1) are identically congruent modulo $2^t$, for a suitably large $t$. Now if $r \geqslant 2$ and $e = 0$ we find (with an obvious diagonal $M$ in (2.3) at each step) that $f \to (2^r, 0)F_2 \to (2^{r-1}, 1)f$, whence $f \leftrightarrow F_2$, $F_2$ being of the shape (8.1) with exponents 0, $r-2$ for $r$, 0, and $d(F_2) = 2^{-r-2}d(f)$. So, by (7.1), $r \leqslant 1$. For $r = 1$, $e = 0$, we have $f \to (2, 0)F_2 \to (2, 0)f$, whence again $f \leftrightarrow F_2$, and $F_2$ has exponents 0, 1. In this case $d(F_2) = \frac{1}{2}d(f)$; so by (7.1) we may suppose $r \neq 1$; and now $r = 0$, $e \geqslant 0$.

We see that we shall have to prove that, with $c(f) = 1$ and $r = 0$ in (8.1), we cannot have $e \geqslant 4$. Since two applications of $\to (2, 0)$ replace $e$ by $e-2$ if $e \geqslant 2$, $e \leqslant 3$ follows if we prove $e \neq 4, 5$; and this in turn need only be proved in the case

$p^2 \nmid d$ for all $p \geqslant 3$, by an argument used in Lemma 3. Some applications of Lemma 1 are required, details of which are again postponed.

When $f$ is not of the shape (8.1), we have instead

$$f \sim_2 2^{e_1} a_1 x_1^2 + 2^{e_2} a_2 x_2^2 + 2^{e_3} a_3 x_3^2, \quad 2 \nmid a_1 a_2 a_3, \tag{8.2}$$

where, using $f \leftrightarrow 2f$, we may suppose $0 = e_1 \leqslant e_2 \leqslant e_3$. If the $e_i$ are all equal (8.2) can be put into the shape (8.1), with $e = e_1$, $r = e + 1$. (7.4) holds with $(2^{w+1}, 1)$ for $(p^w, 0)$, and we have (7.5), so (7.1) gives us (7.6), and (8.1) impossible for $r = e + 1$ gives also $e_3 > e_1$.

To see the possibilities for the $e_i$ in (8.2) when $c(f) = 1$, we consider several cases; in each $g$, $h$, satisfy $f \to (2, 0)\ g \to (2, 0)\ h$.

(i) $e_2 = 0$, $a_1 a_2 \equiv -1 \pmod 4$, $e_3 \geqslant 2$. Here $h$ is of the shape (8.1) with $r = 0$, $e = e_3 - 2$; so $e_3 \leqslant 5$, which is best possible, will follow, if (see above) we prove $e \leqslant 3$.

(ii) $e_2 = 0$, $a_1 a_2 \equiv 1 \pmod 4$, $e_3 \geqslant 2$. Define $\varepsilon = 1$, if $a_1 \equiv a_2 \pmod 8$, $-1$ if not. Then $g$ is of the shape (8.2) with exponents $0, 0, e_3 - 1$ and coefficients $\varepsilon a_1, \varepsilon a_2, a_3$. So, if we prove that $e_3 = 6$ is impossible, it will follow that $e_3 \leqslant 5$.

(iii) $e_1, e_2 = 0, 1$, $e_3 \geqslant 3$. $g$ has exponents $0, 1, e_3 - 1$. $e_3 \leqslant 6$ is needed, and will follow, if we prove $e_3 \neq 7$.

(iv) $e_1, e_2 = 0, 2$, $e_3 \geqslant 4$. $h$ has exponents $0, 0, e_3 - 2$ so, if we prove $e_3 \leqslant 5$ in cases (i), (ii) we shall here have $e_3 \leqslant 7$; we need $e_3 \leqslant 5$, so must exclude $e_3 = 6, 7$.

(v) $e_1, e_2 = 0, 3$, $e_3 \geqslant 6$. $h$ has exponents $0, 1, e_2 - 2$ and if we prove $e_3 \leqslant 6$ in case (iii) then here we have $e_3 \leqslant 8$, which we need to improve, by excluding $e_3 = 8$, to $e_3 \leqslant 7$.

(vi) $e_1 = 0$, $e_2 \geqslant 4$. $h$ has exponents $0, e_2 - 2, e_3 - 2$. So by induction from $e_2 - 2$ to $e_2$ we have $e_3 - e_2 \leqslant 3, 4$ for even, odd $e_2$, if we prove the inequalities for $e_2 = 2, 3$, see (iv), (v). Then we have a contradiction with (7.6); so $e_2 \leqslant 3$.

Two cases of (8.2) are of special interest:

$$f \sim_2 a_1 x_1^2 + a_2 x_2^2 + 2a_3 x_3^2, \quad 2 \nmid a_1 a_2 a_3; \tag{8.3}$$

and

$$f \sim_2 a_1 x_1^2 + a_2 x_2^2 + 4a_3 x_3^2, \ a_1 a_2 = -1 \pmod 4, \ 2 \nmid a_3. \tag{8.4}$$

Using $\to (2, 0)$ as in (i)–(vi) above, also $\to (2^{e_3+1}, 1)$, it can easily be shown that every $f$ of the shape (8.2) with $e_3 > e_1$ satisfies $f \to g$ for some $g$ of one of the shapes (8.3), (8.4).

With $f \to (2, 0)\ g \to (2, 0)\ h$ as above, (8.4) gives $2 \nmid d(h)$; but with $f \to (4, 1)\ g' \to (2, 0)\ g'' \to (2, 0)\ h'$, $d(h') \equiv 2 \pmod 4$. So, with the notation of the remark at the end of §7, we have in case (8.4) both of $f \to G$, $f \to G'$, $d(G) = -d'$, $d(G') = -2d'$, $c(f) = 1$ only if $c(G) = c(G') = 1$; and if so (7.2) holds for two different $j$.

9. *Further deductions from* $c(f) = 1$. If we assume $c(f) = 1$ and (7.1), and use Lemma 4 and the analogous results for $p = 2$ given in §8, the number of possibilities for the genus of $f$ is clearly finite, but inconveniently large. An obvious way to cut the number down is to improve on Lemma 4 by considering separately the cases $j = 1, \ldots, 20$ in (7.2).



For example, suppose $7^2 \mid d$; then by Lemma 4, we can only have $e_1, e_2, e_3 = 0, 1, 2$ in (7.3) (with $p = 7$). In (7.2) we must have $7 \parallel d(f_j)$, giving $j = 5, 8, 11, 15$, or 17 (see Table 2). We can however exclude three of these cases by using Lemma 1, assuming as in Lemma 3 that $p^2 \nmid d$ for $p \neq 7$. Then $j = 5$ or 11, $d(f_j) = -14$ or $-42$; and we notice that $5 \nmid d(f_j)$. So, by the beginning of this argument with 5 for 7, $5^2 \nmid d$. Using Lemma 1 to exclude a finite number of possibilities with $7^2 \mid d$, $j = 5$ or 11, and $9 \mid d$ (we may suppose $p^2 \nmid d$ for $p \neq 3, 7$), we find that $9 \nmid d$; and similarly $4 \nmid d$. Now however $d(f) = 49 d(f_j) = -686$ or $-2058$; and using Lemma 1 again we find three possibilities for the class of $f$. One of these is $f \sim \phi_{58}$, one is $f \sim \phi_{26}$, and the other satisfies $f \to (49, 0)\phi_{26} \to (49, 0) f$.

The foregoing argument finishes the proof of the theorem for the case $49 \mid d$; so we assume $49 \nmid d$ and prove in the same sort of way that the theorem is true for $25 \mid d$. Assuming $p^2 \nmid d$ for $p \geqslant 5$, we consider separately the three cases $d \equiv \pm 9 \pmod{27}$, $d \equiv \pm 27 \pmod{81}$, $d \equiv 0 \pmod{81}$, in which, in (7.3) with $p = 3$, the exponents $e_i$ are $(0, 0, 2)$, $(0, 1, 2)$, $(0, 1, 3)$. The number of cases of the third type to be tested may be cut down by using (2.6) and $(0, 1, 3) \to (3, 0)\ (0, 1, 2)$.

Now it suffices to deal with the prime 2 with the simplifying assumption $p^2 \nmid d$ for $p \geqslant 3$. With this, suppose first that (8.1) holds with $r = 0$ and $e = 0, 1, 2$, or 3; for $e = 0, 1$ we use (1.3) and Table 2. For $e = 2$ or 3, we use Lemma 1 to see whether or not $c(f) = 1$; and if so, a $\phi_i$ with $\phi_i \to f$ is easily found. The case (8.2) may be conveniently broken up into $f \to$ (8.3) and $f \to$ (8.4), each rather more complicated.

10. *Amplification of* §5. We now consider more fully how Lemma 1 can be used, or sometimes avoided. Assuming (5.1) and using part (i) of the lemma we see that, because of the restrictions on $P$, $Q$, we have $f \sim h$ or $p^2 h$, both trivial, unless one of $\det Q$ is $\pm p$ and the other $\pm p^2$. Then we restrict $R$, $S$ to satisfy $\det R = \pm \det P$, $\det S = \pm \det Q$, since otherwise $h(S\mathbf{x}) \sim_p h(Q\mathbf{x})$ is obviously impossible.

In the non-trivial case $\det Q = \pm p$, $\det S = \pm p$, it is clear that each of $h(Q\mathbf{x})$, $h(S\mathbf{x})$ is equivalent to one of the $p^2 + p + 1$ forms

$$h(x_1, x_2, tx_1 + ux_2 + px_3),\ h(x_1, vx_1 + px_2, x_3),\ h(px_1, x_2, x_3), \tag{10.1}$$

where each of $t, u, v$ is an integer between 0 and $p - 1$. Then $P\mathbf{y}$, or $R\mathbf{y}$, $\equiv 0 \pmod p$ can be written as a single scalar congruence, which must be the corresponding one of

$$y_3 \equiv ty_1 + uy_2,\ y_2 \equiv vy_1, \text{ or } y_1 \equiv 0 \pmod p. \tag{10.2}$$

In the other non-trivial case $h(Q\mathbf{x})$, or $h(S\mathbf{x})$, could not be of the shape (10.1), with $p^2 = |\det Q| = |\det S|$ for $p$; for then $pQ^{-1}$ and $pS^{-1}$ would not have integer elements. Instead, we may replace (10.1), (10.2) by

$$h(x_1, tx_1 + px_2, ux_1 + px_3),\ h(px_1, x_2, vx_2 + px_3),\ h(px_1, px_2, x_3), \tag{10.3}$$

$$y_2, y_3 \equiv ty_1, uy_1;\ y_1, y_3 \equiv 0, vx_2;\ y_1, y_2 \equiv 0, 0 \pmod p. \tag{10.4}$$

It will be convenient to denote by $F$, $G$, $H$ the leading binary sections of $f$, $g$, $h$ respectively; that is, to put

$$F = F(x_1, x_2) = f(x_1, x_2, 0),\ G = g(x_1, x_2, 0),\ H = h(x_1, x_2, 0). \tag{10.5}$$

One problem is to pick out, from the $p^2 + p + 1$ cases (10.2) or (10.4), those that correspond to a form $f' = h(S\mathbf{x}) \sim_p f = h(Q\mathbf{x})$. The examples to be given below

will show how this is done; but we note that failure of the condition in part (iv) of the lemma can be proved by considering two congruences only; also that sometimes $h(S\mathbf{x}) \sim_p h(Q\mathbf{x})$ implies that (5.2) holds with $U = \mathrm{I}$.

We have also to consider the possibilities for $U$. If the condition in part (iv) of the lemma is to be proved satisfied, it suffices to find one $U$ for each $R$. In the other case, we may be able to prove indirectly, for some $R$, that a suitable $U$ cannot exist. Now we discuss some examples.

(i) $p \nmid d(h)$, $p > 2$, $f$ of the shape (0, 0, 2), see (7.3). We have (10.1), (10.2), and we cannot exclude more than about half of the $p^2 + p + 1$ cases. $c(f) = 1$, when true, can be proved without much difficulty by using the theory of reduction. $c(h) = 1 \not\Rightarrow c(f) = 1$ can generally be proved by using (6.1).

(ii) $p = 2 \nmid d(h)$. We consider case (10.1), and we may suppose $h \equiv x_1 x_2 \pm x_3^2 \pmod 4$. We shall be interested only in the case $2 \nmid A(f)$. So, to get $f' = h(S\mathbf{x}) \sim_2 f$, the congruence $R\mathbf{y} \equiv 0 \pmod 2$ cannot be any of $(10.1)_2$, $(10.1)_3$. Distinguishing the cases $d(\theta) \equiv 1, -3 \pmod 8$ in (8.1) (with $r = 0$, $e = 2$) and noting that in the second $f$ is never $\equiv 2 \pmod 4$, we have two genera to consider. In one of them $f$ may be supposed to correspond to $t, u = 0, 0$ in (10.1), $f'$ to $t, u = 1, 0$ or $0, 1$, and we seek two $U$'s. In the other, $t = u = 1$ corresponds to $f$ and there is no other possibility for $f'$; no $U$ is needed and we have $c(h) = c(f)$. See, *e.g.*, $\phi_{17}, \phi_{28}, \phi_{61}$.

(iii) $f$ of shape (8.4), $p = 2$. We have $h$ as in (ii) and have to consider three cases of (10.4), namely $x_1 \equiv 0$ and $x_2 \equiv x_3$, $x_1 \equiv x_3$ and $x_2 \equiv 0$, $x_1 \equiv x_2$ and $x_3 \equiv 0 \pmod 4$.

(iv) $p = 3$, $f$ of shape (7.3) with exponents 0, 1, 2. If $a_1 a_3 \equiv -1 \pmod 3$ no non-trivial $U$ is needed; otherwise just one; see [3; 176–77].

(v) $p = 7$ and $h = \phi_{65} = f_{17}$. We may suppose $H = x_1^2 + 2x_2^2$ and $h \equiv H \pmod 7$. $c(f) = 1$ is possible only if $f$ is of the shape (0, 1, 2), see (7.3). Then, with $\varepsilon = \pm 1 = (a_1 \mid 7)$ (Legendre symbol), $f' \sim_7 f$ corresponds to a congruence (10.1) which is consistent with $(h(\mathbf{y}) \mid 7) = \varepsilon$ but not with $(h(\mathbf{y}) \mid 7) = -\varepsilon$. So $(10.1)_1$ must be excluded. For $\varepsilon = 1$ we may take $P\mathbf{y}, R\mathbf{y} \equiv \mathbf{0}$ to be $x_2, x_1 \equiv 0$ respectively; and for $\varepsilon = -1$, $x_1 \equiv x_2$, $x_1 \equiv 2x_2$. Then in each we notice that $P\mathbf{y} \equiv \mathbf{0}$ is consistent with $h(\mathbf{y}) = 2 - \varepsilon$, but $R\mathbf{y} \equiv \mathbf{0}$ is not. Clearly no $U$ can satisfy (5.2), and so $c(f) > 1$.

(vi) Finally suppose $p = 2$, and $f$ of the shape (8.2) with exponents 0, 3, $e$, $e \geqslant 6$; then $h$ is of the same shape with exponents 0, 1, $e - 2$. We are concerned with (10.4), but all the cases $(10.4)_2$, $(10.4)_3$ correspond to imprimitive $f'$. Without loss of generality, let $P\mathbf{y} \equiv \mathbf{0}$ be $x_2, x_3 \equiv 0, 0 \pmod 2$. $f'$ is of the shape (8.2) with $a_1 \pm 2$ for $a_1$ if it corresponds to $x_2 \equiv x_1$, $x_3 \equiv x_1$ or 0. So take $R\mathbf{y} \equiv 0$ to be $x_2, x_3 \equiv 0, x_1 \pmod 2$; this does give $h(S\mathbf{x}) \sim_2 f$.

We notice that there are just two possibilities modulo 2 for $\mathbf{y}$ satisfying $h(\mathbf{y}) \equiv a_1 \pmod 8$; they are $\{1, 0, 0\}$ and $\{1, 0, 1\}$; and $U$ satisfies (5.2), if, and only if, it alters one of them, and so necessarily takes it into the other. For an example, taking $f = \phi_{13}$, $a_1 = 5$, $h = \frac{1}{4}f(4x_1, x_2, x_3)$ is unaltered by interchange of $x_1, x_3$, giving the desired $U$ since $h(1, 0, 0) = h(0, 0, 1) = 5$.



## References


1. G. L. Watson. "One-class genera of positive ternary quadratic forms", *Mathematika*, 19 (1972), 96–104.
2. ———. "Transformations of a quadratic form which do not increase the class-number", *Proc. London Math. Soc.*, (3), 12 (1962), 577–587.
3. ———. "Transformations of a quadratic form which do not increase the class-number (II), *Acta Arithmetica*, 27 (1974), 171–189.
4. ———. "One-class genera of positive quaternary quadratic forms", *Acta Arithmetica*, 24 (1974), 461–475.
5. ———. "One-class genera of positive quadratic forms in $n \geqslant 5$ variables", *Acta Arithmetica*, 26 (1974), 309–327.
6. ———. "Regular, positive, ternary quadratic forms", *J. London Math. Soc.* (2) [to appear].
7. ———. *Integral quadratic forms*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 51 (Cambridge, 1960).


University College,
London.

10C05: *NUMBER THEORY; Forms, Quadratic forms.*

*Received on the 2nd of December*, 1974.