ACTA ARITHMETICA
XXIV (1974)

One-class genera of positive quaternary quadratic forms

by

G. L. WATSON (London)

Dedicated to C. L. Siegel on his 75th birthday

1. Introduction. We shall use the letters $f, F, g, h, \varphi, \psi$ to denote quadratic forms, always with integer coefficients. (Other small letters denote integers, p being prime, unless otherwise stated.) Such forms can be arranged in classes and genera, each genus a union of classes; $c(f)$, the class-number of f, denotes the number of classes in the genus of f. I have been interested for some years in positive-definite f with $c(f) = 1$, which I have investigated by a method based on the results of [1]. Thereby I proved in [2] that $c(f) > 1$ for all positive-definite n-ary f with $n \geqslant 11$. This suggests the problem of finding all the (genera of primitive) positive n-ary forms f with $c(f) = 1$ and given $n \leqslant 10$. I shall here give a partial solution of this problem for $n = 4$; the case $n = 1$ is trivial, $n = 2$ seems hopeless, for $n = 3$ see [3], and $5 \leqslant n \leqslant 10$, which I hope to do later, is in some ways easier than $n = 4$.

The matrix $A(f)$ and discriminant $d(f)$ of a form $f = f(x_1, \ldots, x_n)$ are defined by

$$A(f) = (\partial^2 f/\partial x_i \partial x_j)_{i,j=1,\ldots,n}, \tag{1.1}$$

$$d = d(f) = \begin{cases} (-1)^{\frac{1}{2}n} \det A(f) & \text{if} \quad 2 \mid n, \\ \frac{1}{2}(-1)^{\frac{1}{2}n-\frac{1}{2}} \det A(f) & \text{if} \quad 2 \nmid n. \end{cases} \tag{1.2}$$

It is well known, see, e. g., [4, 3, and 21, (52)] that this makes d an integer always. Further, if $2 \mid n$, d is a binary discriminant, that is $d \equiv 0$ or $1 \pmod 4$. There may or may not be primes p such that $p^{-2}d$ is also a binary discriminant, that is,

$$p^2 \mid d(f) \quad \text{and} \quad p^{-2}d(f) \equiv 0 \text{ or } 1 \pmod 4; \tag{1.3}$$

$d(f)$ is a fundamental binary discriminant if and only if $d(f) \equiv 0$ or $1 \pmod 4$ and (1.3) is false for every p.

In the special case $n = 4$, consider the possibility

$$f \underset{p}{\sim} \varphi_0(x_1, x_2) + p\varphi_1(x_3, x_4), \quad p \nmid d(\varphi_0)d(\varphi_1), \tag{1.4}$$

where $\underset{p}{\sim}$ denotes equivalence over the ring of p-adic integers. Trivially, (1.4) implies (1.3), for each p; we shall consider forms for which

(1.5) (1.4) holds for each p satisfying (1.3)

(for forms φ_0, φ_1 which may depend on f and on p).

This restriction makes the problem manageable because as we shall see a positive-definite f with $n = 4$ and $c(f) = 1$, satisfying (1.5), represents every positive integer. It may however seem that the restriction (1.5) is artificial and so that the result based on it is of little interest. To explain briefly why this is not so, let F denote a 4-ary positive form with class-number 1, and f an F with the property (1.5). Then [1] shows that every F is equivalent over the rational field to a multiple of some f; also that all the F so corresponding to a given f can be found by calculation. The calculation is unfortunately long, inevitably so since the number of possibilities for F is large for some f. I have found some improvements on the results of [1], which I am thinking of publishing and which would shorten the calculations.

We shall see that (1.5) holds (for $n = 4$) if and only if f is strongly primitive (SP) and square-free (SF), these terms defined as in [1].

2. Statement of results. We shall first prove, without much calculation, a somewhat imperfect result:

THEOREM 1. *Let f be a positive-definite quarternary quadratic form, with integer coefficients, and let* (1.5) *above hold. Then either $c(f) > 1$ or $d(f) \leqslant 11532$.*

Then we shall continue the argument, with more powerful methods and more calculation (some of which will be left to the reader), and prove:

THEOREM 2. *With the hypotheses of Theorem* 1, *$c(f) = 1$ if and only if f is equivalent to one of the* 27 *forms listed in Table* 1 *below; these forms are pairwise inequivalent.*

(In the table, a_{rs} is the coefficient of $x_r x_s$, d is the discriminant of the quarternary form and d_2, d_3 those of its leading 2-ary, 3-ary sections.

3. Notation and preliminaries for Theorem 1. We shall use the symbol $\sim$ to denote equivalence over the rational integers, and $\underset{p}{\sim}$ for p-adic equivalence, as above. Temporarily, let $\underset{\infty}{\sim}$ denote equivalence over the real field; then $f \simeq f'$ means $f \underset{\infty}{\sim} f'$ and $f \underset{p}{\sim} f'$ for every p. The genus of f is the set $\{f' : f \simeq f'\}$, the class is $\{f' : f \sim f'\}$. Trivially $f \sim f'$ implies $f \simeq f'$; and, for fixed f, $c(f) = 1$ if and only if the converse holds. If k is an integer, $f \supset k$ means that f represents k properly over the rational integers; that is, $f(x_1, \ldots, x_n) = k$ is soluble in integers x_i with g. c. d. 1. $f \underset{p}{\supset} k$ (f represents k properly over the p-adic integers) may be taken to mean that for every t the congruence $f \equiv k \pmod{p^t}$ is soluble in integers not all congruent to 0 modulo p.

Table 1

Serial no.	a_{11}, a_{12}, a_{22}	d_2	a_{13}, a_{23}, a_{33}	d_3	$a_{14}, a_{24}, a_{23}, a_{44}$	d
1–7	1, 1, 1	−3	1, 1, 1	−2	0, 1, 1, 1 1, 1, 1, 1 0, 0, 0, 1 0, 1, 1, 2 1, 1, 1, 2 0, 1, 1, 3 1, 1, 1, 3	4 5 8 12 13 20 21
8–12	1, 1, 1	−3	0, 0, 1	−3	0, 0, 1, 1 0, 0, 0, 1 1, 1, 1, 2 0, 0, 1, 2 0, 0, 1, 4	9 12 17 21 45
13, 14	1, 1, 1	−3	1, 1, 2	−5	1, 1, −1, 2 1, 1, 2, 1	25 28
15, 16	1, 1, 1	−3	0, 0, 2	−6	0, 0, 2, 2 0, 0, 1, 2	36 45
17, 18	1, 0, 1	−4	0, 0, 1	−4	1, 1, 1, 2 0, 1, 1, 2	20 24
19, 20	1, 0, 1	−4	1, 1, 2	−6	0, 1, −1, 2 1, 1, 1, 2	33 36
21, 22	1, 0, 1	−4	0, 1, 2	−7	1, 0, 0, 2 1, 1, 1, 3	49 69
23	1, 0, 1	−4	1, 1, 1	−10	1, 1, 1, 3	100
24, 25	1, 1, 2	−7	0, 2, 2	−10	0, 1, 2, 2 0, 1, 2, 3	60 100
26	1, 1, 2	−7	0, 1, 2	−13	1, 1, 2, 4	169
27	1, 0, 2	−8	1, 0, 3	−22	0, 2, 0, 6	484

For each $p > 2$ let N_p be a fixed quadratic non-residue modulo p; to be precise we may define $N_p = \inf\{a : a \geqslant -1, (a|p) = -1\}$ (Legendre symbol). Then for $p > 2$ let ψ_p be the binary form $x_1^2 - N_p x_2^2$; and let ψ_2 be $x_1^2 + x_1x_2 + x_2^2$. Then it is well known that for binary φ with $p \nmid d(\varphi)$ either $\varphi \underset{p}{\sim} x_1x_2$ or $\varphi \underset{p}{\sim} \psi_p$. The two cases are distinguished by the value of $(d(\varphi)|p)$ (which we may take to be 1, -1 for $d(\varphi) \equiv 1, -3 \pmod 8$ in case $p = 2$). It is also elementary that $x_1x_2 \underset{p}{\supset} k$ for every integer k,

$\psi_p \underset{p}{\supset} k$ for every $k \not\equiv 0 \pmod{p}$, and $\psi_p(x_1, x_2) \equiv 0 \pmod{p}$ only if $x_1 \equiv x_2 \equiv 0 \pmod{p}$.

We now consider the following possibilities for a quarternary f:

$$f \underset{p}{\sim} x_1x_2 + x_3x_4 \quad \text{or} \quad x_1x_2 + \psi_p(x_3, x_4), \tag{3.1}$$

$$f \underset{p}{\sim} x_1x_2 + ax_3^2 - \begin{cases} pbx_4^2 & (2 \leqslant p \nmid ab) \\ \text{or} & \\ bx_4^2 & (p = 2 \nmid a,\ 4 \mid a+b), \end{cases} \tag{3.2}$$

$$\begin{aligned} f \underset{p}{\sim} x_1x_2 + px_3x_4, &\quad x_1x_2 + p\psi_p(x_3, x_4), \\ \psi_p(x_1, x_2) + px_3x_4, &\quad \text{or} \quad \psi_p(x_1, x_2) + p\psi_p(x_3, x_4). \end{aligned} \tag{3.3}$$

LEMMA 1. (1.5) *holds if and only if for each prime p one of* (3.1)–(3.3) *holds.*

Proof. We shall consider also, and exclude, the three possibilities:

(i) $f \underset{p}{\sim} x_1x_2 + ax_3^2 + pbx_3x_4 + p^2kx_4^2$,

(ii) $f \underset{p}{\sim} \varphi(x_1, x_2) + ph(x_3, x_4)$, $p \nmid d(\varphi)$, $p \mid d(h)$,

(iii) every binary section of f has discriminant $\equiv 0 \pmod{p}$.

It is easy, see [4, 54, Theorem 32, and 59, Theorem 35] to see that one of (3.1)–(iii) must hold.

It is immediate from the case $n = 4$ of the definitions in [1] that f is SP if and only if (iii) is false for every p; also that if this is so then f is SF if and only if neither of (i), (ii) holds for any p. The statement at the end of § 1 will therefore be a corollary of the lemma. (The example $x_3^2 - x_4^2 \sim x_3^2 + 2x_3x_4$, by $x_3 \to x_3 + x_4$, will show why we cannot have $b \equiv a \pmod 4$ in case $(3.2)_2$.)

It is clear that (i) implies (1.3) but contradicts (1.4), and so also (1.5). (ii) also implies (1.3), since $d(\varphi)d(h) \equiv 0$ or $1 \pmod 4$; but it implies $p^3 \mid d(f)$ and so contradicts (1.4). Assuming (iii), we have clearly $p^3 \mid d(f)$; but if $p = 2$, we have $2 \mid a_{ij}$ for $i \neq j$, so $2 \mid A(f)$, $16 \mid d(f)$. So we have (1.3), and (1.5) gives (1.4), implying $p^3 \nmid d(f)$. So (1.5) fails if any of (i)–(iii) holds for any p. The converse is easy and so the lemma is proved. We deduce:

LEMMA 2. *If f satisfies* (1.5) *and k is an integer, then $f \underset{p}{\supset} k$ is false if and only if $p^2 \mid k$ and the fourth case of* (3.3) *holds (implying $(p^{-2}d(f) \mid p) = 1$, or $d(f) \equiv 4 \pmod{32}$ if $p = 2$).*

Proof. Using Lemma 1 and the preceding remarks about binary forms we see at once (putting $x_3 = x_4 = 0$) that $f \underset{p}{\supset} k$ is true in cases (3.1), (3.2), and the first two sub-cases of (3.3) (for all k), and in the other two sub-cases it is true for $k \not\equiv 0 \pmod{p}$. Now putting $x_1 = x_2 = 0$, $f \underset{p}{\supset} k$ is true for all $k \equiv 0 \pmod{p}$ if $(3.3)_3$ holds, and for $p \| k$ in case $(3.3)_4$.

Supposing therefore $p^2 \mid k$ and $(3.3)_4$, we note that if $\psi_p + p\psi_p \equiv 0 \pmod{p^2}$ then $x_1, x_2 \equiv 0, 0 \pmod{p}$, which gives $\psi_p(x_3, x_4) \equiv 0$, $x_3 \equiv x_4 \equiv 0 \pmod{p}$. This gives $f \underset{p}{\not\supset} k$ and completes the proof. Next, we need:

LEMMA 3. *Let f be a positive-definite quadratic form, with $c(f) = 1$, and k a positive integer such that $f \underset{p}{\supset} k$ for every p. Then $f \supset k$.*

Proof. By hypothesis we have, crudely, that f represents k over the real field. From this and the p-adic hypothesis, there exists f' with $f' \simeq f$ and $f' \supset k$. Then $c(f) = 1$ gives $f' \sim f$, and so $f \supset k$. For the existence of f' with the required properties see e.g. [4, 80, Theorem 51]. The argument does not depend on (1.5), nor on $n = 4$, and it is essentially that of [3, 101, Lemma 6]. Using Lemma 2, we have immediately:

COROLLARY TO LEMMA 3. *If the positive-definite quarternary form f satisfies* (1.5) *and $c(f) = 1$ then $f \supset k$ for every positive square-free integer k, and $f \not\supset 4$ implies $d(f) \equiv 4 \pmod{32}$.*

4. Proof of Theorem 1. We shall assume $c(f) = 1$ and deduce the bound for $d(f)$ without using anything else except the Corollary to Lemma 3. We begin by noticing that $f \supset 1$ and $f \supset 2$, whence trivially, by an integral unimodular transformation, we may suppose $a_{11} = 1$ and $a_{22} \leqslant 2$. We write

$$f_2 = f_2(x_1, x_2) = f(x_1, x_2, 0, 0), \qquad d_2 = d_2(f) = d(f_2). \tag{4.1}$$

We notice that by what we have done we may trivially suppose f_2 to be one of the four forms

$$x_1^2 + x_1x_2 + x_2^2, \qquad x_1^2 + x_2^2, \qquad x_1^2 + x_1x_2 + 2x_2^2, \qquad x_1^2 + 2x_2^2. \tag{4.2}$$

We have this and a little more if we further suppose, as we clearly may, that

$$|d_2(f)| = \inf\{|d_2(f')| : f' \sim f, f_2 = \text{one of } (4.2)\}. \tag{4.3}$$

We next define

$$f_3 = f_3(x_1, x_2, x_3) = f(x_1, x_2, x_3, 0), \qquad d_3 = d_3(f) = d(f_3). \tag{4.4}$$

By a transformation which does not affect what we have done, we may suppose that

$$|d_3(f)| = \inf\{|d_3(f')| : f' \sim f, f'(x_1, x_2, 0, 0) = f_2\}. \tag{4.5}$$

In the four cases $d_2 = -3, -4, -7, -8$, see (4.2), (4.3), write temporarily $k = 2, 3, 3, 5$, and verify that $f_2 \not\supset k$; but $f \supset k$ by the Corollary to Lemma 3. It follows that f must have a ternary section g with $g(x_1, x_2, 0) = f_2$ and $g \supset k$, from which we deduce $|d(g)| \leqslant k|d_2|$, see [3, 98, (2.7)], or cf. (4.7) below. From this inequality and (4.5),

$$d_2 = -3, -4, -7, -8 \Rightarrow |d_3| \leqslant 6, 12, 21, 40 \tag{4.6}$$

respectively.

Without upsetting (4.3) or (4.5), indeed without altering f_2 or the class of f_3, we can normalize a_{13}, a_{23}, and consequently a_{33} and f_3, by proceeding as in [3, 98, Lemma 2]. It is best to take the four cases separately.

(i) If $d_2 = -3$ we may restrict a_{12}, a_{13} to be $0, 0$, if $3 | d_3$, $1, 1$ if $d_3 \equiv 1 \pmod 3$, and we cannot have $d_3 \equiv -1 \pmod 3$. Then $d_3 = f_2(a_{13}, -a_{23}) + a_{33} d_2$ reduces to $d_3 = -3a_{33}$ or $-3a_{33}+1$.

(ii) If $d_2 = -4$ then we may suppose $0 \leqslant a_{13} \leqslant a_{23} \leqslant 1$, $d_3 = -4a_{33} + a_{13} + a_{23}$. So $d_3 \equiv -1 \pmod 4$ is impossible, and d_3 determines a_{13}, a_{23} and a_{33}.

(iii) If $d_2 = -7$, we take a_{12}, a_{13} to be $0, 0$; $1, 0$; $0, 1$; or $2, 0$, giving $d_3 = -7a_{33} + 0, 1, 2$, or 4. $d_3 \equiv -1, -2, -4 \pmod 7$ are all impossible.

(iv) If $d_2 = -8$, suppose $0 \leqslant a_{13} \leqslant 1$, $0 \leqslant a_{23} \leqslant 2$. Then the residue of d_3 modulo 8 clearly distinguishes the six cases, and we cannot have $d_3 \equiv -1$ or $-3 \pmod 8$. Further, we have $8(a_{33}-1) < |d_3| \leqslant 8a_{33}$.

We now have a finite set of possibilities for f_3, for each of which we may write (with rational r_i)

$$f = f_3(x_1 + r_1 x_4, x_2 + r_2 x_4, x_3 + r_3 x_4) + r_4 x_4^2. \tag{4.7}$$

We obtain a bound for $d(f)$, for each f_3, by choosing a positive integer k such that $f \supset k$ but $f_3 \not\supset k$. Clearly this is possible only if $r_4 \leqslant k$; but then since (4.7) gives $d(f) = -4r_4 d(f_3) = 4r_4 |d_3|$ we have $d(f) \leqslant 4k|d_3|$. We shall choose k with the desired properties by first choosing a prime p such that f_3 is not a p-adic zero form; then any positive square-free k with $f_3 \not\supset_p k$ will do. We take the cases $d_2 = -3, -4, -7, -8$ separately, and in each of these cases we note that d_3 determines f_3, as shown above.

(i) For $d_2 = -3$ and $d_3 = -2, -3, -5, -6$, (by 4.6) and $d_3 \not\equiv -1 \pmod 3$, choose $p = 2, 3, 5, 3$, $k = 14, 6, 5, 10$. Here, and in many of the cases below, [3, 99, Lemma 4] would help to prove $f_3 \not\supset_p k$. Now we have $d(f) \leqslant 112, 72, 100, 240$. All these bounds are amply good enough for Theorem 1, but we note that the first and last could be improved to $32, 96$ if we could take $k = 4$. If we cannot do so, then by the corollary to Lemma 3 we have $d(f) \equiv 4 \pmod{32}$. In the first case this gives $d(f) \leqslant 32$ or $= 68$, since $d(f) = 36$ or 100 would contradict (1.5).

(ii) For $d_2 = -4$, we see that if $d_3 = -2$ or -3 then $f(0, x_2, x_3, 0)$ has discriminant -3, contradicting (4.3). So by (4.6) and $d_3 \not\equiv -1 \pmod 4$ we have $d_3 = -4, -6, -7, -8, -10, -11$, or -12. We shall later see that $d_3 \neq -8, -11$ or -12; but here we consider all seven cases, taking $p = 2, 3, 7, 2, 2, 11, 3$, and $k = 7, 3, 21, 14, 6, 22, 6$. The resulting bounds are small enough.

(iii) For $d_2 = -7$, $|d_3| < 10$ contradicts (4.3), as in (ii), we have seen that $(d_3|7) \neq -1$, and so with (4.6) we have $d_3 = -10, -12, -13, -14, -17, -19, -20$, or -21. We take $p = 5, 3, 13, 7, 17, 19, 5, 3$, and $k = 10, 6, 13, 21, 17, 38, 5, 6$. Then crudely $d(f) \leqslant 4 \cdot 38 \cdot 21 < 3000$.

(iv) With $d_2 = -8$ we have $|d_3| \leqslant 40$, $\not\equiv 1, 3 \pmod 8$, and we find on looking at obvious sections of f_3 that $|d_3| < 12$ or $= 13$ or 14 contradicts (4.3). The calculations may conveniently be set out in tabular form.

Table 2

d_3	12	15	16	18	20	21	22	23	24	26	28	29	30	31	32	34	36	37	38	39	40
p	2	5	2	2	5	7	2	23	2	13	7	29	5	31	2	2	2	37	2	13	5
k	5	10	7	14	5	7	10	115	10	26	21	29	5	93	14	14	7	37	10	13	10

Clearly $d(f) \leqslant 4 \cdot 93 \cdot 31 = 11532$, so Theorem 1 is proved.

5. Preliminaries for Theorem 2. In (3.2), for odd p, we may take $a = 1$ or N_p, $b = 1$ or N_p, $(N_p|p) = -1$ as in § 3. Then $(p^{-1}d|p) = (ab|p)$ determines b in terms of a, d; and a, or $(a|p)$, is a p-adic invariant of f. To see this, note that the congruence $f(x_1, \ldots, x_4) \equiv a \pmod p$ has more solutions than $f \equiv aN_p \pmod p$ [4, 51, Theorem 29]. In the case $p = 2$, $d \equiv 8 \pmod{16}$, we may take $a = 1$ or -3, $b = \pm 1$ or ± 3, and we have $8ab \equiv d \pmod{64}$. If $p = 2$ and $d \equiv 12 \pmod{16}$, we may in $(3.2)_2$ take $a = \pm 1$ and $b = -a$ or $4-a$. In either case this makes a a 2-adic invariant. For with $\varepsilon = 1, 0$ in the two cases the congruence $f \equiv a \pmod{2^{2+\varepsilon}}$ has more solutions than $f \equiv a + 2^{1+\varepsilon} \pmod{2^{2+\varepsilon}}$.

In case (3.3) we notice that the congruence $f \equiv 0 \pmod p$ has more than p^3 solutions in the first two sub-cases, fewer in the third and fourth.

From these remarks it is easy to determine whether or not $f \underset{p}{\sim} f'$, for given, f, f', p. To determine whether or not $f \simeq f'$ (obviously not unless $d(f') = d(f)$), we need only consider $p | d(f)$. We prove:

Lemma 4. *Theorem 2 is true for forms f with $d(f) \leqslant 64$; and the forms $F_1, \ldots, F_{27}$ represent 27 different genera each having the property* (1.5).

Proof. The second assertion is easily verified, as explained above. For the first, we refer to the list of reduced forms with $d \leqslant 64$ in [5, 74–76]. Rejecting those that do not satisfy (1.5), and arranging the others in genera as above, we obtain a complete list of one-class genera with $d \leqslant 64$, which we compare with Table 1. The calculations are quite simple.

We now introduce some further notation. If φ is a form in fewer variables than F, $F \supset \varphi$, $F \underset{p}{\supset} \varphi$ mean that F represents φ properly over the rational, p-adic integers respectively. For unary $\varphi = kx_1^2$, we write as before $\supset k$, $\underset{p}{\supset} k$. This notation will be needed with $F = f, g, h$, and

$\varphi = g, h, k, f$ as in Theorems 1, 2, and g, h 3-ary and 2-ary respectively and k a positive integer.

For f satisfying (1.5), and positive-definite, we define $q = q(f)$ as the product of the distinct primes p for which (1.4), or (3.3), holds. Then by (1.5) we have

(5.1) $$d(f) = q^3 D,\ q \text{ square-free, } D \text{ prime to } q,\ D \text{ a fundamental binary discriminant.}$$

We also define the adjoint form $\operatorname{adj} f$ by (1.1) and

(5.2) $$A(\operatorname{adj} f) = \operatorname{adj} A(f),$$

the right member being the adjoint matrix of $A(f)$. It is well known (see e. g., [4, 25]) that

(5.3) $$\operatorname{adj} f \supset k \Leftrightarrow f \supset g \quad \text{for some } g \text{ with } d(g) = -k.$$

It is also known that $c(\operatorname{adj} f) = c(f)$. This can be got from [1, Theorem 1] by taking $m = d = d(f)$, whence $c(\operatorname{adj} f) \leqslant c(f)$, with equality because of the obvious $\operatorname{adj}(\operatorname{adj} f) = d^2 f$. We therefore need:

LEMMA 5. *For given f satisfying* (1.5), *and given p, suppose first that $p \mid k$; then $\operatorname{adj} f \underset{p}{\supset} k$ is false if and only if $(3.3)_4$ holds and $p^3 \mid k$.*

Next suppose $p \nmid k$. Then $\operatorname{adj} f \underset{p}{\supset} k$ is true in case (3.1), *false in case* (3.3). *And in the three cases $p > 2$, $p = 2$ and $8 \mid d(f)$, $p = 2$ and $8 \nmid d(f)$ of* (3.2) *the necessary and sufficient condition for $\operatorname{adj} f \underset{p}{\supset} k$ is*

(5.4) $$(-ak \mid p) = 1, \qquad -ak \equiv 1 \text{ or } 1 - \tfrac{1}{4} d \pmod 8, \qquad k \equiv -a \pmod 4).$$

Proof. First suppose $p \nmid d = d(f)$, that is, assume (3.1). Then $d(\operatorname{adj} f) = d^3$, by (5.3), so $\operatorname{adj} f \underset{p}{\supset} k$ for all k, by Lemma 2. In case $p \mid q$, (1.4) gives $\operatorname{adj} f \underset{p}{\sim} p^2 \varphi_0 + p\varphi_1$, so $p \mid \operatorname{adj} f$ and $p^{-1} \operatorname{adj} f$ is of the same shape (3.3) as f, except that sub-cases $(3.3)_2$, $(3.3)_3$ are interchanged. Now we use Lemma 2 with $p^{-1} \operatorname{adj} f$ for f. In the remaining case (3.2) we have

$$\operatorname{adj} f \underset{p}{\sim} m x_1 x_2 + b' x_3^2 - a x_4^2,$$

with $m = 4abp$, $8ab$, $4ab$ and $b' = bp$, $2b$, b in the three sub-cases. It follows easily, using $x_1 x_2 \underset{p}{\supset} k$ for every k, that $\operatorname{adj} f \underset{p}{\supset} k$ if and only if $\operatorname{adj} f \equiv k \pmod{m'}$ is soluble, where $m' = p$, 8, or 4. Modulo m', we may replace b' by 0, $-\frac{1}{4} ad$, $-a$. The first and third cases are now easy, and for the second we lose nothing by first taking $x_4 = 1$, then $x_3 = 0$ or 1, giving the result.

We now consider sufficient conditions for $f \underset{p}{\supset} h$, h binary. The following is needed only when h is one of the forms (4.2).

LEMMA 6. *For f satisfying* (1.5) *and prime p, let h be a binary form such that either* (i) *$p \nmid d(h)$ or* (ii) *$p \mid d(h)$ and h is either $x_1^2 + p x_2^2$ $(p \geqslant 2)$ or $x_1^2 + x_2^2$ $(p = 2)$. Then in case* (i) *we have $f \underset{p}{\supset} h$ unless* (1.4) *holds with $d(h) d(\varphi_0)$ not a p-adic square. In case* (ii), *$f \underset{p}{\supset} h$ unless* (3.2) *holds with $d(h) d(f)$ a p-adic square and $(a \mid p) = -1$ if $p > 2$, $a = -b = -1$ if $p = 2$.*

Proof. Writing any of (1.4) and (3.1)–(3.3) as $f \underset{p}{\sim} h_1 + h_2$, we transform $h_i = h_i(x_1, x_2)$ into $F_i(y_1, y_2)$, $i = 1, 2$. If we can do this with F_1, F_2 such that $F_1(y_1, y_2) + F_2(y_1, y_2) \underset{p}{\sim} h$, then we have a p-adic representation of h by f, which cannot be improper since $p^{-2} d(h)$ is not a binary discriminant.

First suppose $p > 2$, and without loss of generality take h to be one of $x_1^2 - x_2^2 \underset{p}{\sim} x_1 x_2$, $x_1^2 - N_p x_2^2 = \psi_p$, $x_1^2 + p x_2^2$. Writing u for the coefficient of x_2^2, we have $f \underset{p}{\supset} h$ if we can choose $F_1 = y_1^2$ and $F_2 = u y_2^2$, or *vice versa*. For $p \nmid u$ this is easily seen to be possible unless (1.4) holds, in which case we either have nothing to prove or may take $F_2 = 0$. So take $u = p$; the construction goes through except in case (3.2), and then fails only if $h_2 = a x_3^2 - p b x_4^2 \underset{p}{\supset} 1$, p are both false. If so, $(a \mid p) = -1$ and $(-b \mid p) = -1$, whence $\left(p^{-2} d(h) d(f) \mid p\right) = 1$ follows.

If $p = 2 \nmid d(h)$, (1.4) is easy, as above. In the other two cases, (3.1) and (3.2), $h_1 = x_1 x_2$ and we may take $F_1 = y_1^2 + y_1 y_2$, $F_2 = v y_2$, $2 \nmid v$.

So suppose $p = 2 \mid d(h)$, and if $h_1 = x_1 x_2$ take $F_1 = y_1^2 - u^2 y_2^2$. If $h_1 = \psi_2 = x_1^2 + x_1 x_2 + x_2^2$, take $F_1 = y_1^2 + 3u^2 y_2^2$. In either case u can be any integer. Choosing F_2 to be $c y_2^2$, with $h_2 \underset{2}{\supset} c$, we have $f \underset{2}{\supset} h$ if we can choose c so that $c - u^2$ or $c + 3u^2$ is congruent to 2 (mod 16), or to 1 (mod 8), for $d(h) = -8, -4$. This is quite easy in cases (3.1), (3.3). In case (3.2) we have $f \underset{2}{\supset} h$ if the congruence

(5.5) $$-u^2 + a x_3^2 - 2b x_4^2 \equiv 2 \pmod{16} \quad \text{or} \quad -u^2 + a x_3^2 - b x_4^2 \equiv 1 \pmod 8$$

is soluble in integers u, x_3, x_4. A simple calculation now completes the proof.

6. The 'if' of Theorem 2.

By Lemma 4, the assertion of Theorem 2 that each of the F_i has class-number 1 need only be proved for the F_i with $d = d(F_i) > 64$. It is easy to dispose of the case $d = 69$, proving $c(F_{22}) = 1$, by the method of [5]. So suppose $d \geqslant 72$, and note that this implies $d = q^2$, $q = 10, 10, 13, 22$, see entries nos. 23, 25, 26, 27 in Table 1. In each case, denote $F_i(x_1, x_2, x_3, 0)$ by g_i, and note that

(6.1) $$d(g_i) = -q, \qquad c(g_i) = 1;$$

for $c(g_i) = 1$ see [3, Theorem 1].

Now suppose we are given a form f with $f \simeq F_i$; we have to prove $f \sim F_i$. We first note that

(6.2) $$f_3 = g_i \quad \text{and} \quad d(f) = q^2 \Rightarrow f \sim F_i;$$

here f_3 is $f(x_1, x_2, x_3, 0)$, as before. This is quite easily proved by arguments like those used in § 4 to normalize a_{13}, a_{23}; we normalize a_{i4}, $i = 1, 2, 3$, in the same way. Using (6.1) and (6.2) and taking $d(f) = q^2 = d(F_i)$ for granted, since it is implied by $f \simeq f_i$, we see that

(6.3) $$f_3 \simeq g_i \Rightarrow f \sim F_i.$$

We notice, see [3, 100, Lemma 5] that if $d(f_3) = d(g_i)$ $(= -q)$ is square-free, then $f_3 \underset{p}{\simeq} g_i$ can be false only if $p \mid d(g_i)$ and one of f_3, g is a p-adic zero form, the other not. If so it easily follows, for some $p \mid q$, that one of f, F_i is of the shape $(3.3)_1$, the other $(3.3)_4$, which contradicts $f \simeq F_i$. So $d(f_3) = -q$ implies $f_3 \simeq g_i$, which with (6.3) gives

(6.4) $$d(f_3) = -q \Rightarrow f \sim F_i.$$

Since one of $(3.3)_1$, $(3.3)_4$ holds for each $p \mid d(f) = q^2$, we see that $\operatorname{adj} f = qf'$, $f' \simeq f$. So, using (5.3), we can transform f into an equivalent form so as to have $d(f_3) = -q \min f'$, $\min f'$ being the minimum of f'. Now if we know that $f \simeq F_i$ implies $\min f = 1$, we must have $\min f' = 1$ and we can make use of (6.4). So

(6.5) $$\text{if } f \simeq F_i \Rightarrow \min f = 1, \text{ then } c(F_i) = 1.$$

We assume for the moment that

(6.6) $$f \simeq F_i \quad \text{and} \quad d(f_3) = -2q \Rightarrow \min f_3 = 1 \Rightarrow \min f = 1,$$

and note that this is true with $-q$ in place of $-2q$. (Note that $g_i \supset 1$ and use $d(f_3) = -q \Rightarrow f_3 \sim g_i$, proved above.) Then we can use $\operatorname{adj} f \simeq qf$ again to see that we may suppose $d(f_3) = -q$ or $-2q$: and this gives $\min f = 1$, so we can use (6.5). This gives us that

(6.7) $$\text{if } f \simeq F_i \Rightarrow \min f \leqslant 2, \text{ then } c(F_i) = 1.$$

We now use the well known inequality $4(\min f)^4 \leqslant d(f)$ to give, for $f \simeq F_i$, $2(\min f)^2 \leqslant q$, whence $\min f = 2, 2, 2, 3$ in the four cases $q = 10, 10, 13, 22$. Clearly this completes the proof for the first three cases; and the argument leading to (6.7) shows that for $q = 22$ it will suffice to prove that

(6.8) $$f \simeq F_{27} \quad \text{and} \quad d(f_3) = -66 \Rightarrow \min f_3 \leqslant 2.$$

The proof of (6.6) will now be omitted, since it is like that of (6.8), and not too difficult. Now we need only prove (6.8).

We know that by an integral unimodular transformation we may take a_{11}, a_{22}, a_{33} to be the successive minima of f_3, whose product is $\leqslant \frac{1}{2}|d(f_3)|$. So if (6.8) is false we may suppose $d(f_3) = -66$ and $a_{11} = a_{22} = a_{33} = 3$, $0 \leqslant |a_{ij}| \leqslant 3$ for $1 \leqslant i \leqslant j \leqslant 3$. If each of the a_{ij} is ± 1 we may

trivially take the signs to be all the same, and then in either case we have the contradiction $11 \nmid d(f_3) = 66$. If each $|a_{ij}|$ is 0 or 3, we have the contradiction $27 \mid 66$. So we may suppose $a_{12} = 2$; but then $f_3(1, -1, 0) = 4$, $f \supset 4$, and this contradicts $f \underset{2}{\sim} F_{27} \underset{2}{\sim} \psi_2 + 2\psi_2$. The 'if' of the theorem is now proved.

By Lemma 4, it remains only to prove the 'only if' for f with $d(f) > 64$.

7. Use of ternary sections. In this section we assume (1.6) and $c(f) = 1$, normalize as in § 4, and seek to improve the bound for $d(f)$ found in that section, by considering the possibilities for a ternary g with $f \supset g$. One of these possibilities is $g = f_3 = f(x_1, x_2, x_3, 0)$. We note that $d(f)$ determines $q(f)$ by (5.1) and so by the definition of $q(f)$ we have

(7.1) $$f \supset g \Rightarrow q \mid d(g), \quad \text{whence} \quad q \mid d(f_3).$$

We notice also that (with g ternary and h binary)

(7.2) $$f \supset g \supset h,\ p \nmid d(f)d(h), \text{ and } p \mid d(g) \Rightarrow d(f)d(h) \text{ is a } p\text{-adic square.}$$

For the hypotheses of (7.2) give $f \underset{p}{\sim} h(x_1, x_2) + \varphi(x_3, x_4)$ with $p \nmid d(\varphi)$ but $p \mid \varphi(1, 0)$, whence $\big(d(\varphi) \mid p\big) = 1$ (or $d(\varphi) \equiv 1 \pmod 8$ if $p = 2$), whence the result.

We shall show next that

(7.3) $$f \supset g \simeq g' \quad \text{and} \quad c(f) = 1 \Rightarrow f \supset g'.$$

To prove this, write $f \supset g$ more explicitly as

(7.4) $$f(x_1, \ldots, x_4) \sim f'(y_1, \ldots, y_4) = g(y_1 + r_1 y_4, \ldots, y_3 + r_3 y_4) + r_4 y_4^2.$$

Here the r_i are rational, $d(f) = -4r_4 d(g)$, and the new variables y_i, related to the x_i by an integral unimodular transformation, are introduced for convenience later. We choose a positive integer m such that (for positive f', f'') $d(f') = d(f'')$ and $f' \equiv f'' \pmod m$ (identically) imply $f' \simeq f''$ (whence $f \sim f'$ and $c(f) = 1$ give $f'' \sim f$). So (7.3) is proved if we can find f'' so that $d(f'') = d(f)$, $f'' \equiv f' \pmod m$, and $f''(y_1, y_2, y_3, 0) \sim g'$. Now if we choose g'', for a suitable $m_1 > 0$, to satisfy $g'' \equiv g \pmod{m_1}$ and $g'' \sim g'$, then $f'' = g''(y_1 + r_1 y_4, \ldots) + r_4 y_4^2$ gives what is wanted. For the choices of m, g'' see [4, 69, Corollary, and 80, Theorem 51].

Putting f_3, g for g, g' in (7.3), we have

(7.5) $$f_3 \simeq g \supset h \quad \text{and} \quad c(f) = 1 \Rightarrow f \supset h,$$

which is a contradiction if $|d(h)| < |d_2|$. We can obtain this contradiction in many of the cases of § 4 by constructing g with $g \supset h$ and $d(g) = d_3$, and verifying, see [3, 100, Lemma 5] that $g \simeq f_3$. Taking $h = x_1^2 + x_1 x_2 +$

$+x_2^2, f \supset h$ is possible only when $d_2 = -3$, and so we find that with $c(f) = 1$

$$d_2 = -4, -7, -8 \Rightarrow d_3 \neq -11; -17, -21; -15, -23, -29, -38.$$

Similarly, with $h = x_1^2+x_2^2, x_1^2+x_1x_2+2x_2^2$,

$$d_2 = -7, -8, \Rightarrow d_3 \neq -14, -19; -31, -34,$$

$$d_2 = -8 \Rightarrow d_3 \neq -26.$$

We note that $2\nmid d_3 \Rightarrow 2\nmid q \Rightarrow f \underset{2}{\supset} 4$. So, in the case $d_2 = -8$, we can improve the inequality $|d_3| \leqslant 5\cdot 8$ to $|d_3| \leqslant 4\cdot 8$ for odd d_3, giving $d_3 \neq -37$, -39, by using $f_2 \supset 4$.

We next show that (for $c(f) = 1$)

$$(7.6) \qquad f \supset g \text{ and } \begin{Bmatrix} g \not\supset 1 \\ g \not\supset f_2 \\ g \nsim f_3 \end{Bmatrix} \Rightarrow \text{resp. } d(f) \leqslant \begin{cases} 4\,|d(g)| \\ 4a_{22}\,|d(g)|. \\ 4a_{33}\,|d(g)| \end{cases}$$

To prove this, note that in (7.4) we have obviously $f(x_1, \ldots, x_4) \geqslant r_4$ unless the point $(x_1, \ldots, x_4)$ corresponds to a point $(y_1, \ldots, y_4)$ with $y_4 = 0$. Taking $x_4 = 0$ and x_1, x_2, x_3 a permutation of 1, 0, 0, if $y_4 = 0$ in every case we have clearly $g \sim f_3$, and if not we have $r_4 \leqslant \max(a_{11}, a_{22}, a_{33})$. The third case of (7.6) follows from this (and the first two are similar but simpler) on noting that $a_{11} = 1$, $a_{22} = 1$ or 2, and $a_{33} = 1$ implies that f represents one of the first two of (4.2), giving $a_{22} = 1$.

By using (7.3) we see that in the second part of the hypothesis of (7.6) we could replace g by any $g' \simeq g$. So in (7.6) we could replace $g \sim f_3$ by $c(g) > 1$; we could also replace $g \not\supset f_2$ by $c(g) > 1$. For in normalizing a_{13}, a_{23} in § 4, we saw in effect that $d(g) = d(f_3)$ and $g(x_1, x_2, 0) = f_2$ imply $g \sim f_3$.

Crudely, (7.6) gives us that $d(f) \leqslant 4a_{33}k$ if $k \neq |d_3|$ and there exists g with $f \supset g$ and $d(g) = -k$; assuming $c(f) = 1$ and using (5.3) and $c(\operatorname{adj} f) = c(f)$, we can eliminate g and seek a k, $\neq |d_3|$, satisfying the conditions of Lemma 5, implying $\operatorname{adj} f \underset{p}{\supset} k$, for every p. If we know the value of $d(f)$ and use the obvious fact that $k = |d(f_3)|$ satisfies the conditions of Lemma 5, it is usually possible to find a small $k \neq |d_3|$ that also satisfies these conditions. For example, if $d_2, d_3, d(f) = -3, -2, 68$ we may take $k = 4$ since $(2\,|17) = 1$; then with $a_{33} = 1$ (7.6) gives the contradiction $68 \leqslant 4\cdot 4$. Referring back to § 4 and recalling that $d \leqslant 64$ has been dealt with, this gives us that Theorem 2 is true in the case $d_2, d_3 = -3, -2$. The case $d_2, d_3 = -3, -3$ can be dealt with in the same way by taking $k = 10, 6, 6$ for $d(f) = 65, 69, 72$ and noting that (7.1) gives $d(f) \neq 68$ $\equiv 4 \pmod{16}$.

We next notice that if $8\,|\,d_3$ then all the conditions of Lemma 5 hold with $k = \frac{1}{4}|d_3|$ instead of $|d_3|$. Now with $f \supset g$ and $d(g) = \frac{1}{4}d_3$, so $|d(g)| \leqslant 10$, we find by a simple calculation see [3, 97, Lemma 1] that $g \supset h$ with $|d(h)| \leqslant 7$. The calculations in § 4 now show that d_3 can only be -8; but now $d(g) = -2$ gives $g \supset h$ with $|d(h)| = 3$, so $d_2 = -3$ and this, as in § 4, gives $|d_3| < 8$. So

$$(7.7) \qquad c(f) = 1 \Rightarrow 8\nmid d_3.$$

It is useful in some cases to notice that the construction of § 4 gives

$$(7.8) \qquad |d_3| \leqslant |d_2| \left|\frac{d(f)}{3d_2}\right|^{1/2} = |\tfrac{1}{3}d_2 d(f)|^{1/2}$$

by a fairly obvious argument like that of [3, 97, Lemma 1]. This enables us to dispose of the troublesome case $d_2 = -8$, $d_3 = -30$. In this case $c(f_3) \neq 1$, by [3, Theorem 1] and so we can use (7.6) to give $|d(f)| \leqslant 240$, and then (7.8) gives the contradiction $|d_3| < 30$.

We shall find it useful later to note that the theorem just quoted gives $c(g) > 1$ if $d(g) = -42$ and $g \supset x_1^2+2x_2^2$. So if we have $f \supset g$ with such a g (7.6) gives $d(f) \leqslant 336$. In the case $d_2, d_3, d(f) = -8, -18$, $924 = 4\cdot 3\cdot 7\cdot 11$ we can use such a g in (7.6), because $(18\cdot 42\,|\,11) = 1$, and so we have a contradiction.

8. Representation of binary forms. Using the methods of § 7 and the inequalities of § 4 it would be possible to finish the proof of Theorem 2 by a finite calculation. To make the calculation manageable it is very desirable to use:

LEMMA 7. *Let f be a positive 4-ary and h a positive 2-ary quadratic form, such that $f \underset{p}{\supset} h$ for every p. Then $f \simeq f' \supset h$ for some f'.*

Proof. See [6, 106, Theorem 40]; take $n = 4$, $m = 2$.

9. Use of binary sections. We assume all the hypotheses of Theorem 2, and $c(f) = 1$ and $d(f) > 64$, see Lemma 4. Then Lemma 7 gives, for positive binary h,

$$(9.1) \qquad f \underset{p}{\supset} h \quad \text{for all } p \Rightarrow f \supset h.$$

By the argument used for (7.6) we see, using (4.5), that

$$(9.2) \qquad f \supset h \sim f_2 \Rightarrow |d_3| \leqslant |d_2| \max\{h(1, 0), h(0, 1)\},$$

$$(9.3) \qquad f \supset h \text{ and } f_3 \not\supset h \Rightarrow d(f) \leqslant 4\,|d_3| \max\{h(1, 0), h(0, 1)\}.$$

As an example of the use of these formulae, consider the case $d_2 = -3$, $d_3 = -5$, in which (7.1) gives $q = 1$ or 5, and we saw in § 4 that $d(f) \leqslant 100$, with strict inequality since $q \neq 10$. We seek to prove $d(f) \leqslant 64$, see Lemma

4, and so may suppose $q = 1$, since $d = 25$ if $q = 5$. We now notice that (9.2) gives the contradiction $|d_3| \leqslant 3$ if $f \supset x_1^2 + x_2^2$; so we suppose not, and then (9.1) shows that $f \underset{p}{\supset} x_1^2 + x_2^2$ is false for some p. By Lemma 6 and $q = 1$, this p can only be 2, and we must have $-4d$ a 2-adic square, giving $d \equiv -4 \pmod{32}$. With this and $64 < d < 100$, $d = 92$. Now we use (7.6) with $d(g) = -10$, and so with $a_{33} = 2$ have the contradiction $d \leqslant 80$. The possibility of taking $d(g) = -10$ follows easily from Lemma 5 and $(5 \cdot 10 | 23) = 1$.

Now consider the case $d_2 = -3$, $d_3 = -6$, $d(f) \leqslant 240$, $d(f) \leqslant 96$ unless $d \equiv 4 \pmod{32}$. Again using $f \not\supset x_1^2 + x_2^2$ and (7.6) we easily find $d \leqslant 64$. We have now disposed of all sub-cases of the case $d_2 = -3$. We may therefore suppose, for the rest of the paper, by (4.3), that $f \not\supset (2, -3)$, where $(2, d)$ denotes a 2-ary form with discriminant d.

It follows that there must be a p with $f \underset{p}{\not\supset} (2, -3)$. Supposing first that this is true for $p = 3$, we must by Lemma 6 have $d_3 \not\equiv 1 \pmod 3$ and $d(f) \equiv 6 \pmod 9$. Next supposing $f \underset{p}{\supset} (2, -3)$ false for $p \neq 3$, Lemma 6 gives $p | q$ and, if $p \nmid d_2$, $-3d$ the square of a p-adic unit. This implies e.g. that p cannot be 5 if $d_2 = -7$ or -8. From these remarks it is clear that $q \neq 3$.

Now suppose $d_2 = -4$, or $f \supset (2, -4)$ in the notation just explained. Of the possibilities for d_3 given in § 4, we excluded -11 and -8 in § 7; the others are -4, -6, -7, -10, -12. In the first and second of these two cases we find $d \leqslant 64$ just as for $d_2 = -3$, $d_3 = -2, -3$. In the next case $d_3 = -7$ we have $d \leqslant 588$, $q = 1$ or 7. The case $q = 7$ is easily excluded (except for $d = 49 < 64$) by using (7.6). So take $q = 1$, and use $d \equiv 6 \pmod 9$, because $f \not\supset (2, -3)$, and $(d | 7) = 0$ or -1, by (7.2) with $h = f_2 = (2, -4)$. We cut down further the number of d to be excluded by noticing that f_3 cannot be bordered to give an f with $d = 69$ but not equivalent to F_{22}; we also note that $q = 1$ makes d a fundamental binary discriminant. (7.6) gives $d \leqslant 8|d(g)|$ if $f \supset g$ and $d(g) \neq -7$, so we can exclude any d for which some $k < d/8$ satisfies the hypotheses of Lemma 5, and $k \neq 7$. Such a k is easily found except for $d = 105$; note for example that one of $k = 6, 12, 18$ will do unless some $p > 3$ divides d and satisfies $(2|p) = (3|p) = 1$. For $d = 105$ we choose $d(g) = -18$ and we need $g \not\supset 1$ to get a contradiction from (7.6). The form f to be proved to have $c(f) > 1$ is $(2, -7)(x_1, x_2) + (2, -15)(x_3, x_4)$, with an obvious temporary notation; the coefficient of x_3^2 is 1. We verify that $f \simeq f'$ but $f \nsim f'$ for f' with coefficients (arranged as in Table 1) 2, -1, 2; 1, 1, 2; 1, -2, 0, 2.

In the cases $d_2 = -4$, $d_3 = -10, -12$, we notice that (9.2) gives a contradiction if $f \supset (2, -8)$. So $f \not\supset (2, -8)$, and either $f \underset{p}{\supset} (2, -8)$ is false for some odd $p \nmid q$ or $f \not\supset (2, -8)$, giving $d \equiv -8 \pmod{64}$; and we cannot have $q = 2$. Further, in case $d_3 = -12$, $f_3 = x_1^2 + x_2^2 + 3x_3^2$,

whence clearly $f \underset{p}{\supset} (2, -3)$ is true for every $p > 2$, so false for $p = 2$. This gives $2 | q$, $d \equiv 4 \pmod{16}$. With these remarks it is easy to complete the proof for $d_2 = -4$. So we suppose $f \not\supset (2, -4)$. This gives $q \neq 2$ and either $f \underset{p}{\supset} (2, -4)$ false for some odd $p | q$ or $d \equiv 4 \pmod{32}$.

The outstanding cases with $d_2 = -7$ are easily disposed of as above. For example, when $d_2 = -20 \equiv 1 \pmod 3$, $f \underset{p}{\supset} (2, -3)$ is true for any d if $p = 3$, so must be false for some $p | q$, clearly not for $p = 5$, and so, since $q \neq 2$, we must have $q = 10$, $d = 100$, $f \supset g$ with $d(g) = -10$.

Suppose therefore $f \not\supset (2, -7)$, $d_2 = -8$. We have $q \neq 2, 3, 7$. Other q except 1 are not too difficult to deal with, since $D = q^{-2} d$ is not too large. So suppose $q = 1$. With this and $f \not\supset (2, -3)$, $(2, -4)$, $(2, -7)$ we have $q \equiv 6 \pmod 9$, $-4 \pmod{32}$, $0 \pmod 7$, $924 \pmod{2016}$, and $(7^{-1} d | 7) = -1$. So either $d = 924$ or $d \geqslant 8988$. It is easy to see that $d < 8988$, so $d = 924$. We find $d < 924$ except for $d_3 = -18$; then the remark at the end of § 7 completes the proof.

References

[1] G. L. Watson, *Transformations of a quadratic form which do not increase the class-number*, Proc. London Math. Soc. (3) 12 (1962), pp. 577–587.

[2] — *The class-number of a positive quadratic form*, Proc. London Math. Soc. (3) 13 (1962), pp. 549–576.

[3] — *One-class genera of positive ternary quadratic forms*, Mathematika 19 (1972), pp. 96–104.

[4] — *Integral Quadratic Forms*, Cambridge 1960

[5] Kurt Germann, *Tabellen reduzierter, positiver quaternärer quadratisher Formen*, Commentarii Mathematici Helvetici 38 (1963–4), pp. 56–83.

[6] Burton W. Jones, *The Arithmetic Theory of Quadratic Forms*, New York 1950.

UNIVERSITY COLLEGE
London, England

Received on 28. 12. 1972 (262)