One-class genera of positive quaternary quadratic forms

by

G. L. Watson (London)

Dedicated to O. L. Siegel on his 70th birthday

1. Introduction. We shall use the letters \( f, F, g, h, p, \psi \) 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 \( n \geq 11 \). This suggests the problem of finding all the (genera of primitive) positive \( n \)-ary forms \( f \) with \( c(f) = 1 \) and given \( n \leq 10 \). 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 \( 5 \leq n \leq 10 \), 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 \( f(x_1, \ldots, x_n) \) are defined by

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

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

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 \( d = 0 \) or \( 1 \) (mod 4). There may or may not be primes \( p \) such that \( p^2 \mid d \) is also a binary discriminant, that is,

\[
p^2 \mid d(f) \quad \text{and} \quad p^{-2} d(f) = 0 \text{ or } 1 \text{ (mod 4)};
\]

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

In the special case \( n = 4 \), consider the possibility

\[
f \sim \varphi_0(x_1, x_2) + p \varphi_1(x_0, x_3), \quad p^4 d(\varphi_0) d(\varphi_1),
\]

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

\[(1.5) \quad (1.4) \text{ holds for each } p \text{ satisfying (1.3)}\]

for forms \(v_0, v_1\) 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 classnumber 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 \(f_1\); 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 quaternary quadratic form, with integer coefficients, and let (1.5) above hold. Then either \(c(f) > 1\) or \(d(f) < 11329\).

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 hypothesis of Theorem 1, \(c(f) = 1\) if and only if \(f\) is equivalent to one of the 21 forms listed in Table 1 below; these forms are pairwise inequivalent.

(Incidentally, \(a_p\) is the coefficient of \(x_0x_3\), \(d\) is the discriminant of the quaternary form and \(d_1, d_2\) 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 \(\sim_p\) for \(p\)-adic equivalence, as above. Temporarily, let \(\sim\) denote equivalence over the real field; then \(f \sim f'\) means \(f \sim_f f'\) and \(f \sim f\) for every \(p\). The genus of \(f\) is the set \(\{f' : f \sim f'\}\), the class is \(\{f' : f \sim f'\}\). Trivially \(f \sim f\) implies \(f \sim f\); and, for fixed \(f\), \(c(f) = 1\) if and only if the converse holds. If \(k\) is an integer, \(k \equiv k\) means that \(f\) represents \(k\) properly over the rational integers; that is, \(f(x_0, \ldots, x_3) = k\) is soluble in integers \(x_i\) with g.c.d. 1. \(f \equiv k\) (\(f\) represents \(k\) properly over the \(p\)-adic integers) may be taken to mean that for every \(i\) the congruence \(f = k \pmod{p^i}\) is soluble in integers not all congruent to 0 modulo \(p\).

<table>
<thead>
<tr>
<th>Serial no.</th>
<th>(a_{11}, a_{12}, a_{23})</th>
<th>(d_2)</th>
<th>(a_{12}, a_{23}, a_{32})</th>
<th>(d_3)</th>
<th>(a_{14}, a_{24}, a_{32}, a_{43})</th>
<th>(d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (-7)</td>
<td>1, 1, 1</td>
<td>-3</td>
<td>1, 1, 1</td>
<td>-2</td>
<td>0, 1, 1, 1</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 1</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 1, 2</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 2</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 1, 3</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 3</td>
<td>21</td>
</tr>
<tr>
<td>8 (-12)</td>
<td>1, 1, 1</td>
<td>-3</td>
<td>0, 0, 1</td>
<td>-3</td>
<td>0, 0, 1, 1</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 2</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1, 2</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1, 4</td>
<td>45</td>
</tr>
<tr>
<td>13 (14)</td>
<td>1, 1, 1</td>
<td>-3</td>
<td>1, 1, 2</td>
<td>-5</td>
<td>1, 1, 1, 2</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 2</td>
<td>28</td>
</tr>
<tr>
<td>15 (16)</td>
<td>1, 1, 1</td>
<td>-3</td>
<td>0, 0, 2</td>
<td>-6</td>
<td>0, 0, 2, 2</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1, 2</td>
<td>45</td>
</tr>
<tr>
<td>17 (18)</td>
<td>1, 0, 1</td>
<td>-4</td>
<td>0, 0, 1</td>
<td>-4</td>
<td>1, 1, 1, 2</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 0, 1, 2</td>
<td>24</td>
</tr>
<tr>
<td>19 (20)</td>
<td>1, 0, 1</td>
<td>-4</td>
<td>0, 1, 2</td>
<td>-7</td>
<td>1, 0, 0, 2</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1, 1, 1, 3</td>
<td>69</td>
</tr>
<tr>
<td>21 (22)</td>
<td>1, 0, 1</td>
<td>-4</td>
<td>1, 1, 1</td>
<td>-10</td>
<td>1, 1, 1, 3</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 2, 2</td>
<td>60</td>
</tr>
<tr>
<td>23 (24)</td>
<td>1, 0, 1</td>
<td>-4</td>
<td>0, 1, 2</td>
<td>-10</td>
<td>0, 1, 1, 2</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 2, 2</td>
<td>60</td>
</tr>
<tr>
<td>25 (26)</td>
<td>1, 1, 2</td>
<td>-7</td>
<td>0, 1, 2</td>
<td>-13</td>
<td>1, 1, 2, 4</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 2, 2</td>
<td>60</td>
</tr>
</tbody>
</table>

For each \(p > 2\) let \(N_p\) be a fixed quadratic non-residue modulo \(p\); to be precise we may define \(N_p = \inf\{a : a \geq -1, (a|p) = -1\}\) (Legendre symbol). Then for \(p > 2\) let \(v_p\) be the binary form \(x_0^2 + x_1^2 + x_2^2 + x_3^2\), and let \(v_p\) be \(x_0^2 + x_1^2 + x_2^2 + x_3^2\). Then it is well known that for binary \(\varphi\) with \(p^3|\text{disc}(\varphi)\) either \(\varphi \equiv x_0^2 + x_1^2 + x_2^2 + x_3^2\) or \(\varphi \equiv v_p\). The two cases are distinguished by the value of \(|\text{disc}(\varphi)|\) (which we may take to be 1, -1 for \(d(\varphi) = 1, -3 \pmod{8}\) in case \(p = 2\)). It is also elementary that \(x_0^2 + x_1^2 \equiv k\) for every integer \(k\),
Supposing therefore $p=1$ and $(3.3)_4$, we note that if $x_p + y_p = 0 \pmod p^2$, then $x_1 + y_1 = 0 \pmod p$, which gives $y_p(x_1, x_2) = 0$, and $x_p = y_p = 0 \pmod p$.

This gives $f \equiv k \pmod p$ 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 $f \equiv k \pmod p$ for every $p$. Then $f \equiv k$.

**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 $f' \sim f$ and $f' \equiv k$. Then $c(f) = 1$ gives $f' \sim f$, and so $f \equiv k$. 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, 191, Lemma 6]. Using Lemma 2, we have immediately:

**Corollary to Lemma 3.** If the positive-definite quadratic form $f$ satisfies (1.5) and $c(f) = 1$ then $f \equiv k$ for every positive square-free integer $k$, and $f \equiv k$ implies $d(f) = 4 \pmod {32}$.

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 $f \equiv 1$ and $f \equiv 2$ whence trivially, by an integral unimodular transformation, we may suppose $a_{11} = 1$ and $a_{22} = 2$.

We write

\[(4.1) \quad f = f_1(x_1, x_2) = f(x_1, x_2, 0, 0), \quad d_1 = d_1(f) = d(f_1).\]

We notice that by what we have done we may trivially suppose $f_1$ to be one of the four forms

\[(4.2) \quad w_1^2 + x_1^2 + x_1^2, \quad w_2^2 + x_2^2, \quad w_1^2 + x_1^2 + 2x_2^2, \quad w_1^2 + 2x_2^2.\]

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

\[(4.3) \quad |d_1(f)| = \inf \{|d_1(f')| : f' \sim f, f_1 = \text{one of (4.2)}.\}\]

We next define

\[(4.4) \quad f_2 = f_2(x_1, x_2, x_3) = f(x_1, x_2, x_3, 0), \quad d_2 = d_2(f) = d(f_2).\]

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

\[(4.5) \quad |d_2(f)| = \inf \{|d_2(f')| : f' \sim f, f_2 = \text{one of (4.4)}.\}\]

In the four cases $d = -3, -4, -7, -8$, see (4.2), (4.3), write temporarily $k = 2, 3, 3, 5$, and verify that $f \equiv k$ 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 $g \equiv k$, from which we deduce $|d(g)| \leq |d_2|$, see (3, 98, (2.7)), or cf. (4.7) below. From this inequality and (4.5),

\[(4.6) \quad d_2 = -3, -4, -7, -8 \leq |d_2| \leq 6, 12, 21, 40 \quad \text{respectively}.\]
Without upsetting (4.3) or (4.5), indeed without altering \( f_2 \) or the class of \( f_1 \), we can normalize \( a_{12}, a_{13} \), and consequently \( a_{15} \) and \( f_1 \), by proceeding as in [3, 99, Lemma 2]. It is best to take the four cases separately.

(i) If \( d_1 = -3 \) we may restrict \( a_{12}, a_{13} \) to be \( 0, 0, 1, 1 \), if \( d_1 \equiv 1 \pmod{3} \), and we cannot have \( d_1 \equiv -1 \pmod{3} \). Then \( d_2 = f_2(a_{22}, -a_{13} + a_{12}a_{21}, +a_{21}a_{32}) \) reduces to \( d_2 = -3a_{13} \) or \( -3a_{12} + 1 \).

(ii) If \( d_1 = -4 \) then we may suppose \( 0 \leq a_{12} \leq a_{13} \leq 1 \), \( d_2 = -4a_{13} + a_{12}a_{21} + a_{21}a_{32} \). So \( d_2 \equiv -1 \pmod{4} \) is impossible, and \( d_2 \) determines \( a_{12}, a_{13} \) and \( a_{32} \).

(iii) If \( d_1 = -7 \), we take \( a_{12}, a_{13} \) to be \( 0, 0, 1, 1, 1, 0, \) or \( 2, 0, 0, 1, 1, 0, 0, 1, 1, 2, 0, \). \( d_2 \equiv -7a_{13} + a_{12} - 2 \pmod{2} \) are all impossible.

(iv) If \( d_1 = -8 \), suppose \( 0 \leq a_{12} \leq a_{13} \leq 1, \) \( 0 \leq a_{21} \leq 2 \). Then the residue of \( d_1 \) modulo 8 clearly distinguishes the six cases, and we cannot have \( d_1 \equiv 0 \pmod{2} \), \( -3 \pmod{8} \). Further, we have \( 8(a_{12} + 1) < |d_2| \leq 8a_{12} \).

We now have a finite set of possibilities for \( f_2 \), for each of which we may write (with rational \( r_1 \))

\[
f = f_2(x_1 + r_1x_2, x_2 + r_2a_2x_3, x_3 + r_3a_3x_3) + r_4a_4\phi.
\]

We obtain a bound for \( d(f) \), for each \( f_2 \), by choosing a positive integer \( k \) such that \( f \geq k \) but \( f_2 \neq k \). Clearly this is possible only if \( r_1 \leq k \); but then since (4.7) gives \( d(f) = -4r_1d(f_2) = 4r_1d_2 \) we have \( d(f) \leq 4kd_2 \).

We shall choose \( k \) with the desired properties by first choosing a prime \( p \) such that \( f_2 \) is not a \( p \)-adic zero form; then any positive square-free \( k \) with \( f_2 \neq k \) will do. We take the cases \( d_2 = -3, -4, -7, -8 \) separately, and in each of these cases we note that \( d_2 \) determines \( f_2 \), as shown above.

(i) For \( d_2 = -3 \) and \( d_2 = -2, -3, -5, -6, -7, -8, -9, -10, \) \( d_2 \equiv -1 \pmod{3} \), choose \( p = 2, 3, 5, 8, 14, 6, 5, 18 \). Here, and in many of the cases below, [3, 99, Lemma 4] would help to prove \( f_2 \neq k \). Now we have \( d(f) \leq 112, 72, 100, 240 \). All these bounds are amply good enough for Theorem 1, but we note that the first and last could be improved to 32, 66 if we could use \( k = 4 \). If we cannot do so, then by the corollary to Lemma 3 we have \( d(f) = 4 \pmod{32} \). In the first case this gives \( d(f) \leq 32 \) or \( 68 \), since \( d(f) = 32 \) would contradict (4.5).

(ii) For \( d_2 = -4 \), we see that if \( d_2 = -2, -3 \) then \( f(0, a_2, a_3, 0) \) has discriminant \( -3, -4 \), contradicting (4.3). So by (4.6) and \( d_2 \neq -1 \pmod{4} \) we have \( d_2 = -4, -6, -7, -8, -10, -11, -12 \). We shall later see that \( d_2 = -8, -11 \) or \( -12 \); but here we consider all seven cases, taking \( p = 2, 3, 5, 7, 11, 13, 17, 19, 5, 3, 21, 14, 6, 23, 22, 6 \). The resulting bounds are small enough.

### Table 2

| \( d_2 \) | 12 15 16 18 20 21 22 23 24 25 26 29 30 31 32 34 36 37 38 39 40 |
| \( p \) | 2 5 2 2 5 7 2 2 2 2 3 17 2 3 2 2 3 17 3 2 5 3 2 2 3 17 3 2 5 |
| \( k \) | 5 10 7 14 5 7 10 11 14 14 10 10 26 21 29 5 33 14 14 7 37 10 10 10 |

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

5. Preliminaries for Theorem 2. In (3.2), for odd \( p \), we may take \( a = 1 \) or \( \eta_{a_2} b = 1 \) or \( \eta_{a_2} \), \( (\eta_{a_2} | p) = -1 \) as in §3. Then \( (p^{-1}d(p)) = (ab | p) \) determines \( b \) in terms of \( a, d_1 \) and \( a, (ab) | p \), or a \( p \)-adic invariant of \( f_2 \).

To see this, note that the congruence \( f(x_1, \ldots, x_k) = a \pmod{p} \) has more solutions than \( f = a_2 \pmod{p} \) (4, 31, Theorem 29). In the case \( p = 2, \) \( d_2 = 8 \pmod{16} \), we may take \( a = 1 \) or \( -3, b = \pm 1 \) or \( \pm 3 \), and we have \( \text{Sub} = d \pmod{64} \). If \( p = 2 \) and \( d = 12 \pmod{16} \), we may in (3.2), take \( a = \pm 1 \) or \( b = -a \) or \( a = \pm 3, b = -a, a = \pm 3 \). In either case this makes \( a \) a 2-adic invariant. For with \( b = 0 \) in the two cases the congruence \( f = a \pmod{2^{24}} \) has more solutions than \( f = a + 2^{24} \pmod{2^{32}} \).

In case (3.3) we notice that the congruence \( f = 0 \pmod{p} \) has more than \( p^2 \) solutions in the first two sub-cases, fewer in the third and fourth.

From these remarks it is easy to determine whether or not \( f \sim f' \), for given \( f, f' \), \( p \). To determine whether or not \( f \sim f' \) (obviously not unless \( d(f) = d(f') \)), we need only consider \( p | d(f) \). We prove:\n
**Lemma 4.** Theorem 2 is true for forms \( f \) with \( d(f) \leq 64 \); and the forms \( P_1, \ldots, P_27 \) 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 \( d \leq 64 \) in [5, 7, 76].

Repeating these that do not satisfy (1.5), and arranging the others in genera as above, we obtain a complete list of one-class genera with \( d \leq 64 \), which we compare with Table 1. The calculations are quite simple.

We now introduce some further notation. If \( \varphi \) is a form in fewer variables than \( F, F \equiv \varphi, \varphi \equiv F \) mean that \( F \) represents \( \varphi \) properly over the rational, \( p \)-adic integers respectively. For unary \( \varphi = x_1^2 \), we write as before \( \equiv \pmod{p} \). This notation will be used with \( F = f \), \( g \), \( h \), and
\( \varphi = \varphi, \) \( h, f \) 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 \( \varphi = \varphi(f) \) as the product of the distinct primes \( p \) for which (1.4), or (3.3), holds. Then by (1.3) we have

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

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

\[ A(\operatorname{adj}f) = A(f), \]

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

\[ \operatorname{adj}f \geq k \implies \varphi = g \quad \text{for some } g \text{ with } d(g) = -h. \]

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

**Lemma 5.** For given \( f \) satisfying (1.5), and given \( p \), suppose first that \( p \mid h \), then \( \operatorname{adj}f \equiv k \) is false if and only if (3.3) holds with \( k = k \).

Next suppose \( p \mid h \). Then \( \operatorname{adj}f \equiv k \) 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 \( \operatorname{adj}f \equiv k \) is

\[ -(a+b)p = 1, \quad -ab = 1 \text{ or } 1 - 4d(\text{mod } 8), \quad h = -a(\text{mod } 4). \]

**Proof.** First suppose \( p \mid d(f), \) that is, assume (3.1). Then \( \operatorname{adj}f = d^3 \), by (5.3), so \( \operatorname{adj}f \equiv k \) for all \( h \), by Lemma 2. In case \( p \mid d(f), \) (1.4) gives \( \operatorname{adj}f \equiv p^4f_p + p^2q \), so \( p \mid \operatorname{adj}f \) and \( p \nmid \operatorname{adj}f \) is of the same shape (3.3) as \( f \), except that sub-cases (3.3) \( 1 \) and (3.3) \( 2 \) are interchanged. Now we use Lemma 2 with \( p \nmid \operatorname{adj}f \) for \( f \). In the remaining case (3.2) we have

\[ \operatorname{adj}f \equiv ma_2 + b^2 - ac_2, \]

with \( m = 4abp, 8ab, 4ab \), and \( b = bp, 2b, b \) in the three sub-cases. It follows easily, using \( a_2 \leq x_1 \) for \( k \), that \( \operatorname{adj}f \equiv k \) if and only if \( \operatorname{adj}f \equiv k (\text{mod } m') \) is solvable, where \( m' = p, 8, 4 \). Modulo \( m' \), we may replace \( b \) by \( 0, 1 - 2d, -a \). The first and third cases are now easy, and for the second we lose nothing by first taking \( x_1 = 1 \), then \( x_1 = 0 \) or \( 1 \), giving the result.

We now consider sufficient conditions for \( f \equiv h, \) \( h \) 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 \( x_1^2 + px_2^2 \) (\( p \geq 2 \)) or \( x_1^2 + x_2^2 \) (\( p = 2 \)). Then in case (i) we have \( f \equiv h \) unless (1.4) holds with \( d(h) \equiv d(q_a) \) not a p-adic square. In case (ii), \( f \equiv h \) unless (3.2) holds with \( d(h) \equiv f \) a p-adic square and \( a(p) = -1 \) if \( p > 2, a = -b = -1 \) if \( p = 2 \).

**Proof.** Writing any of (1.4) and (3.1)-(3.3) as \( f = p^2h_1 + h_2 \), we transform \( h_1 = h_1(a_1, x_1) \) into \( F_1(y_1, y_2), \) \( y_1, y_2, 1 \). If we can do this with \( F_1, F_2 \) such that \( F_1(y_1, y_2) + F_2(y_1, y_2) \equiv h \), 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 \( x_1^2 + ax_2 - x_1x_2, x_1^2 - x_1x_2 - x_2^2 - Np = y_1^2 + p^2y_2^2 \). Writing \( w \) for the coefficient of \( x_2 \), we have \( f \equiv h \) if we can choose \( F_1 = y_1^2 \) and \( F_2 = w_2y_2^2 \) or vice versa. For \( p \mid w \) 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 \( w = 0 \); the construction goes through except in case (3.2), and then fails only if \( h = wx_1^2 + p^2x_2^2 \) \( \equiv 1 \), \( p \) are both false. If \( a(p) = -1 \) and \( -b(p) = -1 \), and \( p^{-2}d(h)(\operatorname{adj}f)(p) = 1 \) follows.

If \( p = 2^d(h), (1.4) \) is easy, as above. In the other two cases (3.2) and (3.3), \( h_1 = x_1x_2 \) and we may take \( F_1 = y_1^2 + y_2, F_2 = w_2y_2^2 \).

So suppose \( p = 2^d(h), \) and if \( h = x_1x_2 \) take \( F_1 = y_1^2 + w_2^2 \). If \( h = x_1x_2 \) take \( F_1 = y_1^2 + 3w_2^2 \). In either case we can be any integer. Choosing \( F_2 = w_2y_2^2, h \equiv 2 \), we have \( f \equiv h \) if we can choose \( w \) so that \( w \equiv u \) or \( c \equiv 2w \) 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 \( f \equiv h \) if the congruence

\[ u^2 + ax_1^2 - 2bx_2^2 = 2 \text{ (mod 16)} \]

or \( u^2 + ax_1^2 - bx_2^2 = 1 \text{ (mod 8)} \) is solvable in integers \( x_1, x_2, x_3 \). 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 \( d = d(F_i) > 1 \). It is easy to dispose of the case \( d = 69 \), proving \( a(F_2) = 1 \), by the method of [5]. Suppose \( d > 72 \), and note that this implies \( d = q_1^2, q_1 = 10, 13, 22, \) see entries nos. 23, 25, 26, 27 in Table 1. In each case, denote \( F_i(x_1, x_2, x_3) \) by \( g_i \), and note that

\[ d(g_i) = -g, \quad e(g_i) = 1; \]

for \( e(g_1) = 1 \) see [3, Theorem 1].

Now suppose we are given a form \( f \) with \( f = F_i \); we have to prove \( f \sim E_i \). We first note that

\[ f_i = g_i \quad \text{and} \quad df = q^a \sim f \sim E_i; \]
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 $a_{23}, a_3, a_2$; we normalize $a_3, a_2, a_1$ in the same way. Using (6.1) and (6.2) and taking $d(f) = g^2 = d(f')$ for granted, since it is implied by $f = f'$, we see that

$$f_3 \simeq g_1 \Rightarrow f \sim F_4,$$

We notice, see [3, 100, Lemma 5] that if $d(f_3) = d(g_1) (\equiv -q)$ is square-free, then $f_3 \simeq g_1$ can be false only if $p \mid d(g_1)$ and one of $d_3, g$ is a $p$-adic zero form, the other not. If so it easily follows, for some $p \mid q$, that one of $f, F_4$ is of the shape (3.3)$_3$, the other (3.3)$_4$, which contradicts $f \sim F_4$. So $d(f_3) = -q$ implies $f_3 \simeq g_1$, which with (6.3) gives

$$d(f_3) = -q \Rightarrow f \sim F_4.$$  

Since one of (3.3)$_3$, (3.3)$_4$ holds for each $p \mid d(f) = g^2$, we see that $d_3 = qf', f \simeq f$. 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 $f \simeq F_4$ implies $\min f = 1$, we must have $\min f' = 1$, and we can make use of (6.4). So

$$f \sim F_4 \Rightarrow \min f = 1, \text{ then } o(F_4) = 1.$$  

We assume for the moment that

$$f \simeq F_4 \text{ and } d(f_3) = -2g = \min f_3 = 1 \Rightarrow \min f = 1,$$

and note that this is true with $-g$ in place of $-2g$. (Note that $g_3 > 1$ and $d(f_3) = -q \Rightarrow f_3 \sim g_1$, proved above.) Then we can use $d_3 = qf'$ again to see that we may suppose $d(f_3) = -q$ or $-2g$: and this gives $\min f = 1$, so we can use (5.3). This gives us that

$$f \sim F_4 \Rightarrow \min f = 2, \text{ then } o(F_4) = 1.$$  

We now use the well known inequality $4(\min f)^2 \leq d(f)$ to give, for $f \simeq F_4$, $2(\min f) \leq q$, whence $\min f = 2, 3$ 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 $q = 23$ it will suffice to prove that

$$f \simeq F_3 \text{ and } d(f_3) = -66 \Rightarrow \min f_3 \leq 2.$$  

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 $a_{21}, a_{22}, a_2$ to be the successive minima of $f_3$, whose product is $1/\sqrt{d(f_3)}$. So if (6.8) is false we may suppose $d(f_3) = -66$ and $a_{21} = a_{22} = a_2 = 3, 0 \leq a_{ij} \leq 3$ for $1 \leq i < j \leq 3$. If each of the $a_{ij}$ is $\pm 1$ we may trivally take the signs to be all the same, and then in either case we have the contradiction $11 | d(f_3) = 66$. If each $a_{ij}$ is 0 or 3, we have the contradiction $27 | 66$. So we may suppose $a_{21} = 2$; but then $f_3(3, -1, 0) = 4, f = 4$, and this contradicts $f \sim F_7 \sim g_1 + 2g_2$. 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 $o(f) = 1$, 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 $f \sim g$. One of these possibilities is $g = f_3 = f(x_1, x_2, x_3, 0)$. We note that $d(f)$ determines $g(f)$ by (5.1) and so by the definition of $g(f)$ we have

$$f \simeq g \Rightarrow g = qd(g), \text{ whence } qd(g).$$  

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

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

For the hypotheses of (7.2) give $f \sim h(x_1, x_2) + \varphi_2(x_1, x_2)$ with $p \mid d(f)$ but $p \varphi_1(1, 0)$, whence $d(\varphi_2) = 1$ (or $d(\varphi) = 1 (\text{mod } 8)$ if $p = 2$), whence the result.

We shall show next that

$$f \simeq g \Rightarrow g \simeq g' \text{ and } o(f) = 1 \Rightarrow f \sim g'.$$

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

$$f(x_1, \ldots, x_4) = g(y_1 + r_1 y_2, \ldots, y_1 + r_3 y_4) + r_4 y_5^2,$$

Here the $r_i$ are rational, $d(f) = -4r_4d(g)$, and the new variables $y_1$ 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 $f' = f'' (\text{mod } m)$ (identically) imply $f' \simeq f''$ (whence $f \sim f'$ and $o(f) = 1$, gives $f' \sim f$). So (7.3) is proved if we can find $g$ so that $d(f') = d(f), f' \sim f'' (\text{mod } m), \text{ and } f''(y_1, y_2, y_3, 0) \sim g'$. Now if we choose $g'$, for a suitable $m > 0$, to satisfy $g' = g (\text{mod } m)$ and $g' \sim g$, then $f'' = g'(y_1 + r_1 y_2, \ldots, y_1 + r_3 y_4)$ 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

$$f_3 \simeq g \Rightarrow h \text{ and } o(f) = 1 \Rightarrow f \sim h,
We next notice that if \( 8 < d_0 \) then all the conditions of Lemma 5 hold with \( k = \frac{1}{8} d_0 \) instead of \( d_0 \). Now with \( f \equiv g \) and \( d(g) = \frac{1}{8} d_0 \), so \( |d(g)| \leq 20 \), we find by a simple calculation see [3, 97, Lemma 1] that \( g \equiv h \) with \( |d(h)| \leq 7 \). The calculations in \( \S \) 4 now show that \( d_0 \) can only be \(-8\); but now \( d(g) = -2 \) gives \( g \equiv h \) with \( |d(h)| = 3 \), so \( d_0 = -3 \) and this, as in \( \S \) 4, gives \( |d_0| \leq 8 \). So

\[
(7.7)
\]

\[ e(f) = 1 \Rightarrow 8^3 d_0. \]

It is useful in some cases to notice that the construction of \( \S \) 4 gives

\[
(7.8)
\]

\[
|d_0| \leq \left| d_0 \right| \frac{d(f)_{125}}{3d_0} = \frac{1}{8} d_0 |d(f)|_{125}
\]

by a fairly obvious argument like that of [3, 97, Lemma 1]. This enables us to dispose of the troublesome case \( d_0 = -8 \), \( d_0 = -30 \). In this case \( e(f) \neq 1 \), by [3, Theorem 1] and so we can use (7.6) to give \( |d(f)| \leq 240 \), and then (7.8) gives the contradiction \( |d_0| < 30 \).

We shall find it useful later to note that the theorem just quoted gives \( e(f) > 1 \) if \( d(g) = -42 \) and \( g \equiv x_1^5 + 2x_2^2 \). So if we have \( f \equiv g \) with \( e(f) > 1 \) we find \( d(f) \leq 336 \). In the case \( d_0, d_0, d(f) = -8, -18, 224 = 4 \cdot 3 \cdot 7 \cdot 11 \) we can use such a \( g \) in (7.6), because \( (18, 42, 11) = 1 \), and so we have a contradiction.

8. Representation of binary forms. Using the methods of \( \S \) 7 and the inequalities of \( \S \) 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 \( f \equiv h \) for every \( p \). Then \( f \equiv f' \) for some \( f' \).

**Proof.** See [6, 106, Theorem 40]; take \( m = 4, w = 2 \).

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

\[
(9.1)
\]

\[ f \equiv h \quad \forall \ p \equiv f \equiv h. \]

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

\[
(9.2)
\]

\[ f \equiv h \equiv f_0 \equiv |d_0| \equiv |d_0| \equiv \max\{h(1,0), h(0,1)\}. \]

\[
(9.3)
\]

\[ f \equiv h \equiv f_0 \equiv d(f) \equiv |d_0| \equiv \max\{h(1,0), h(0,1)\}. \]

As an example of the use of these formulae, consider the case \( d_0 = -3 \), \( d_0 = -5 \), in which (7.1) gives \( g = 3 \) or \( 5 \), and we saw in \( \S \) 4 that \( d(f) \leq 100 \), with strict inequality since \( g 
eq 10 \). We seek to prove \( d(f) \leq 64 \), see Lemma
4, and so may suppose $q = 1$, since $d = 25$ if $q = 5$. We now notice that (9.2) gives the contradiction $d \leq 3$ if $f = a_2^2 + a_2^2$; so we suppose not, and then (9.1) shows that $f \geq a_2^2 + a_2^2$ is false for some $p$. By Lemma 6 and $q = 1$, this $p$ can only be 2, and we must have $-4d\equiv 2\pmod{32}$, giving $d = 10\pmod{32}$. This with $64 < d < 100$, $d = 92$. Now we use (7.5) with $d \equiv g = -10$, and so with $a_{32} = 2$ we have the contradiction $d \leq 80$. The possibility of taking $d(g) = -10$ follows easily from Lemma 5 and (5.10) [23] = 1.

Now consider the case $d_2 = -3, d_2 = -6, d(f) \leq 240, \ d(f) \leq 96$ unless $d = 4\pmod{32}$. Again using $f \geq a_2^2 + a_2^2$ and (7.6) we easily find $d < 64$. 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 $f = (2, -3), \ where (2, d)$ denotes a 2-ary form with discriminant $d$.

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

Now suppose $d_2 = -4, f \equiv (2, -4)$ in the notation just explained. Of the possibilities for $d_3$, given in § 4, we excluded $11$ and $-10$ in § 7; the others are $-4, -6, -7, -10, -12$. In the first and second of these two cases we find $d \leq 64$ just as for $d_3 = -3, d_3 = -2, -3$. In the next case $d_3 = -7$ we have $d \leq 588, q = 1$ or $7$. The case $q = 7$ is easily excluded (except for $d = 49 < 64$) by using (7.6). So take $q = 1, \ and \ d \equiv 6 \pmod{9}$, because $f \equiv (2, -3)$, 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 $f_2$ cannot be bordered to give an $f$ with $d = 69$ but not equivalent to $F_{21}$; we also note that $q = 1$ makes $d$ a fundamental binary discriminant. (7.6) gives $d \leq 8d(g)$ if $f \equiv g$ and $d(g) \neq -7$, so we can exclude any $d$ for which some $k < d/g$ satisfies the hypothesis of Lemma 5, and $k \neq 7$. Such a $k$ is easily found except for $d = 105$; note for example that one of $k = 6, 12, 18, 20$ 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 $g \equiv 1$ to get a contradiction from (7.6). The form $f$ to be proved to have $d(f) > 1$ is $(2, -7)(a_1, a_2) + (2, -15)(a_3, a_4)$, with an obvious temporary notation; the coefficient of $a_3^2$ is 1. We verify that $f \equiv f'$ but $f \neq f'$ for $f'$ with coefficients (arranged as in Table 1) $2, -1, 2, 1, 2, 1, -2, 0, 2$.

In the cases $d_4 = -4, d_4 = -10, -12$, we notice that (9.2) gives a contradiction if $f \equiv (2, -8)$. So $f \equiv (2, -8)$, and $f \equiv (2, -8)$ is false for some odd $p \nmid q$ or $f \equiv (2, -8)$, giving $d = -8$ (mod 64); and we cannot have $q = 2$. Further, in case $d_4 = -12, f_3 = a_1^2 + a_2^2 + 3a_3^2$.

whence clearly $f \equiv (2, -3)$ is true for every $p > 2$, so false for $p = 2$. This gives $2 | d, d \equiv 4 \pmod{16}$. With these remarks it is easy to complete the proof for $d_4 = -4$. So we suppose $f \equiv (2, -4)$. This gives $q \equiv 2$ and either $f \equiv (2, -4)$ false for some odd $p \nmid q$ or $d \equiv 4 \pmod{32}$.

The outstanding cases with $d_4 = -24$ are easily disposed of as above. For example, when $d_4 = -20 = 4 \pmod{32}$, $f \equiv (2, -3)$ is true for any $d$ if $p = 3$, so must be false for some $p \nmid q$, clearly not for $p = 3$, and so, since $q \neq 2$, we must have $q \equiv 10, q = 100, f \equiv q$ with $d(g) = -10$.

Suppose therefore $f \equiv (2, -3), d_4 = -38$. 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 $f \equiv (2, -3), (2, -4), (2, -7)$ we have $d \equiv 6 \pmod{9}, \ d \equiv 4 \pmod{32}, 0 \pmod{7}, 924 \pmod{2016}$, and $(7 \cdot d / 7) = -1$. So either $d \equiv 924$ or $d \equiv 9898$. It is easy to see that $d \leq 9898$, so $d = 924$. We find $d < 924$ except for $d_4 = -18$; then the remark at the end of § 7 completes the proof.

References


UNITED KINGDOM

Received on 28. 12. 1972