REGULAR POSITIVE TERNARY QUADRATIC FORMS

G. L. WATSON

1. *Introduction*

Let f be a positive-definite ternary quadratic form with integer coefficients. We shall, *cf.* [1], say that f is *regular* if it represents all integers not excluded by congruence conditions. More precisely, we consider the equation and congruence

$$f(x_1, x_2, x_3) = a, \tag{1.1}$$

$$f(x_1, x_2, x_3) \equiv a \pmod{m}, \tag{1.2}$$

where a, m are positive integers and x_1, x_2, x_3 are integer-valued variables. Trivially, if (1.1) is soluble then (1.2) is soluble for every m; and f is regular if the converse holds. The regularity of some forms, e.g. $x_1^2+x_2^2+x_3^2$, has been long known and has many applications. For one such application, and references to others, see [2].

It is trivial that f cannot represent the positive integer a properly, that is, (1.1) cannot have a solution with g.c.d. $(x_1, x_2, x_3) = 1$, unless (1.2) has such a solution, for every m. Let us say that f is *strictly regular* if this condition for proper representation is sufficient. Strict regularity implies regularity. To see this, suppose that f is strictly regular and (1.2) is soluble for every m. Then there exists q, with $q^2 \mid a$, such that (1.2) is always soluble with g.c.d. $(x_1, x_2, x_3) = q$. So f represents aq^{-2} properly; and then trivially f represents a.

Now consider the genus of f, and denote by $c(f)$, the class-number of f, the number of classes in it. As shown, e.g., in [3; p. 101, Lemma 6] $c(f) = 1$ implies that f is strictly regular.

Let A be the 3×3 matrix with (i,j) element $\partial^2 f/\partial x_i\, \partial x_j$; so det A is an even positive integer. As in [3], and elsewhere, I define the discriminant $d(f)$ as $-\frac{1}{2}\det A$, a negative integer. We shall assume till the end of §8 that $d(f)$ is square-free; this assumption makes the problem easier because it makes (1.2) soluble (for all m) for a dense set of integers a, see [3; p. 99, Lemma 4].

I am indebted to Professor Kneser for reading my first draft of this paper; he led me to write it by his enquiries about some questions arising from my earlier paper [4].

2. *Statement of results*

With the definitions of §1, we shall prove two theorems. The first was in my Ph.D. thesis (London, 1953) but was never published till now.

THEOREM 1. *Let f be a positive-definite ternary quadratic form with integer coefficients and square-free discriminant. Suppose further that the class-number of f is at least* 2. *Then f is regular if and only if it is equivalent to one of*:

$$x_1^2+x_2^2+x_2x_3+3x_3^2, \tag{2.1}$$

$$x_1^2+2x_2^2+x_2x_3+2x_3^2, \tag{2.2}$$

$$x_1^2+x_1x_2+2x_2^2+2x_2x_3+3x_3^2, \tag{2.3}$$

$$x_1^2+x_1x_2+2x_2^2+3x_3^2. \tag{2.4}$$

Received 31 August, 1974.

[J. LONDON MATH. SOC. (2), 13 (1976), 97–102]

If we omit the restriction $c(f) > 1$ then there are just 20 other possibilities, all strictly regular as noted above, see [**3**; pp. 96–7, Theorem 1].

THEOREM 2. *The three forms* (2.2)–(2.4) *are all strictly regular, but* (2.1) *is not so.*

3. *The genera of the forms* (2.1)–(2.4)

Let f be one of these four forms, with $d = d(f) = -11, -15, -17, -21$ respectively, and write $P = P(f) = 11, 5, 17, 3$. For prime p, we find easily that f is a p-adic zero form for every $p \neq P$. Taking m in (1.2) to be a prime power p^t, and referring again to [3; Lemma 4], we find that (1.2) is soluble for every a unless $p = P$. If so, (1.2) is soluble for every $a \not\equiv 0 \pmod{P}$; and it implies $x_1, x_2, x_3 \equiv 0, 0, 0 \pmod{P}$ if $P^2 \mid a$ and $t \geqslant 2$. Finally, if $a = bP, P \nmid b$, then (1.2) is soluble for all t if and only if the Legendre symbol $(b \mid P)$ has the value $-(P^{-1}d \mid P), = 1, 1, -1, 1$ in the four cases.

Using the theory of reduction, see [**3**; p. 97, Lemma 1], and excluding forms not having the generic properties noted above, we search for reduced forms f' with $f' \simeq f$ but $f' \nsim f$. We find no possibilities except:

$$x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + 4x_3^2, \tag{3.1}$$

$$x_1^2 + x_1x_2 + x_2^2 + 5x_3^2, \tag{3.2}$$

$$x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + 6x_3^2, \tag{3.3}$$

$$x_1^2 + x_1x_2 + x_2^2 + 7x_3^2, \tag{3.4}$$

for $f = $ (2.1), ..., (2.4) respectively. In each of these four cases $f' \simeq f$ is easily verified, see [**3**; p. 100, Lemma 5], but $f' \sim f$ is false because f represents 2 but f' does not. So we have $c(f) = 2$.

4. *Regularity of* (2.1)–(2.4)

Let f be any one of the forms (2.1)–(2.4), and f' the corresponding one of (3.1)–(3.4), and consider the equation

$$f'(y_1, y_2, y_3) = a, \tag{4.1}$$

with integer-valued variables y_i. Suppose $a > 0$ such that (1.2) is soluble for every m; then, as is well known, some f'' in the genus of f must represent a. As we have seen in §3, $f'' \simeq f$ implies that either $f'' \sim f$ or $f'' \sim f'$; so either f or f' represents a. So either we have the desired result at once, or we may suppose (4.1) soluble.

We notice that $f'(x_1, x_2, x_3)$ has two integral automorphs which may be expressed briefly as

$$x_1 \to -x_1 - x_2 \quad \text{and} \quad x_2 \to -x_2 - x_1 - kx_3, \tag{4.2}$$

with $k = 1, 0, 1, 0$ in the four cases. Using the first of these we see that (4.1) has a solution with either $2 \mid y_2$ or $2 \nmid y_1 + ky_3$. Then, by using the second of (4.2), (4.1) has a solution with $2 \mid y_2$.

Now we have the desired result, that (1.1) is soluble, if we can construct an identity of the shape

$$f'(y_1, y_2, y_3) = f(z_1, z_2, z_3), \tag{4.3}$$

where the z_i are linear forms, with integer coefficients, in y_1, $\frac{1}{2}y_2$, and y_3. It may be verified that (4.3) holds if we take

$$z_1, z_2, z_3 = \begin{cases} y_1+\frac{1}{2}y_2,\ 2y_3,\ \frac{1}{2}y_2; \\ y_1+\frac{1}{2}y_2,\ y_3-\frac{1}{2}y_2,\ y_3+\frac{1}{2}y_2; \\ y_1+\frac{1}{2}y_2-y_3,\ 2y_3,\ -\frac{1}{2}y_2-y_3; \quad \text{or} \\ y_1+\frac{1}{2}y_2-y_3,\ 2y_3,\ \frac{1}{2}y_2. \end{cases} \tag{4.4}$$

5. *Proof of Theorem* 2, *cases* (2.1), (2.2), (2.4)

Arguing as at the beginning of §4 we see that f is strictly regular if and only if (1.1) has a solution with g.c.d. $(x_1, x_2, x_3) = 1$ for every a for which (4.1) has one with g.c.d. $(y_1, y_2, y_3) = 1$. In the case (2.1), (3.1) we see by taking $a = 8 = f'(1, 1, 1)$ that this is not so. For (1.1) is easily seen to imply $x_1 = \pm 2$ and $x_2, x_3 \equiv 0, 0 \pmod 2$. So (2.1) is not strictly regular.

In the other three cases we note that by using the integral automorphs (4.2) we do not alter the g.c.d. of the variables; so we may suppose (4.1) soluble with $2 \mid y_2$ and g.c.d. $(y_1, y_2, y_3) = 1$. Then obviously the g.c.d. of the numbers on the right of (4.4) is either 1 or 2. We have nothing to prove unless it is 2 (implying $4 \mid a$). So, changing the notation slightly, we assume the solubility of

$$f(x_1, x_2, x_3) = 4a, \quad \text{g.c.d.}\ (x_1, x_2, x_3) = 2, \tag{5.1}$$

and it suffices to prove the solubility of

$$f(y_1, y_2, y_3) = 4a, \quad \text{g.c.d.}\ (y_1, y_2, y_3) = 1. \tag{5.2}$$

We take the three cases separately.

In case (2.2), note first that if $x_2 = x_3 = 0$ then (5.1) gives $x_1 = \pm 2$ and so $4a = 4 = f(1, 1, -1)$. So we suppose $x_2, x_3 \neq 0, 0$, and we put $y_1 = x_1$. We weaken (5.2) to

$$2y_2^2+y_2y_3+2y_3^2 = 2x_2^2+x_2x_3+2x_3^2, \quad \text{g.c.d.}\ (y_2, y_3) = \tfrac{1}{2}\ \text{g.c.d.}\ (x_2, x_3). \tag{5.3}$$

(If this does not give (5.2) at once, we repeat the process.) Now we can satisfy the first of (5.3) by taking $y_2 = -x_2-\frac{1}{2}x_3$, $y_3 = x_3$, or $y_2 = x_2$ and $y_3 = -x_3-\frac{1}{2}x_2$. One at least of these choices gives us the second part of (5.3) too. So (2.2) is strictly regular.

In case (2.4), we note that $x_1, x_2 = 0, 0$ gives $x_3 = \pm 2$, $4a = 12 = f(3, 0, 1)$, so we suppose $x_1, x_2 \neq 0, 0$, and put $y_3 = x_3$. Then we seek a solution of

$$y_1^2+y_1y_2+2y_2^2 = x_1^2+x_1x_2+2x_2^2, \quad \text{g.c.d.}\ (y_1, y_2) = \tfrac{1}{2}\ \text{g.c.d.}\ (x_1, x_2). \tag{5.4}$$

One solution of the first of these is $y_1 = x_1$, $y_2 = -x_2-\frac{1}{2}x_1$. If that does not satisfy the second condition then we take $y_1 = -x_1-x_2$, $y_2 = \frac{1}{2}x_1-\frac{1}{2}x_2$. So we find that (2.4) is strictly regular.

6. *Proof of Theorem* 2, *case* (2.3)

In this remaining case, which is more complicated since f is not disjoint, we begin by using (5.1) to construct a solution of

$$z_1^2+z_1z_2+2z_2^2+17z_3^2 = 28a, \tag{6.1}$$

in integers z_i with

$$\text{g.c.d.}\,(z_1, z_2, z_3) = 2 \text{ or } 14, \tag{6.2}$$

and

$$z_3, a \not\equiv 0, 0 \pmod{49}. \tag{6.3}$$

We do this by putting $z_1 = -x_1-4x_2-2x_3$, $z_2 = 2x_1+x_2$, $z_3 = x_3$. Then (6.1) and (6.2) are easily verified. If (6.3) fails then reducing (6.1) modulo 7^3 we find that $7 \mid z_2$ and $49 \mid 2z_1+z_2$, whence the contradiction $7 \mid x_1, x_2, x_3$.

The next step is to choose integers w_i to satisfy

$$w_1^2+w_1w_2+2w_2^2+17w_3^2 = 28a, \tag{6.4}$$

$$\text{g.c.d.}\,(w_1, w_2, w_3) = 1 \text{ or } 7, \tag{6.5}$$

and

$$w_3, a \not\equiv 0, 0 \pmod{49}. \tag{6.6}$$

If $z_1 = z_2 = 0$ then $z_3 = 14$, $a = 119$, and we take $w_1 = 17$, $w_2 = 34$, $w_3 = 3$. If $z_1, z_2 \neq 0, 0$ then we take $w_3 = z_3$ and choose w_1, w_2 as we chose y_1, y_2 in (5.4).

We notice that (6.4) implies $(2w_1+w_2)^2 \equiv 9w_3^2 \pmod 7$; so by putting $-w_3$ for w_3 if necessary, and using (6.6), we may suppose that

$$2w_1+w_2+4w_3 \equiv 0 \pmod 7$$

and if $7 \mid w_3$ then also

$$2w_1+w_2+4w_3,\ a \not\equiv 0, 0 \pmod{49}. \tag{6.7}$$

We now choose y_1, y_2, y_3 to satisfy

$$w_1 = -y_1-4y_2-2y_3, \quad w_2 = 2y_1+y_2, \quad w_3 = y_3. \tag{6.8}$$

Substituting from (6.8) in (6.4) we find that the y_i satisfy the first of the conditions (5.2). By (6.7) and (6.8) the y_i are integers; by (6.5), their g.c.d. is 1 or 7. If it is 7, then $49 \mid a$ and $7 \mid w_3$, so (6.7) gives $49 \nmid 2w_1+w_2+4w_3 = -7y_2$, $7 \nmid y_2$. This contradiction completes the proof that (2.3) is strictly regular.

7. *The "only if" of Theorem* 1

We now suppose that f is regular; and we may also suppose f reduced, see e.g. [**3**; p. 97, Lemma 1]. For brevity write F for $f(x_1, x_2, 0)$ and D for the discriminant of F. Now in [**3**; p. 101, §5] I have shown (for f with square-free d) that $c(f) = 1 \Rightarrow f$ regular $\Rightarrow$ that F is one of

$$x_1^2+x_1x_2+x_2^2,\ x_1^2+x_2^2,\ x_1^2+x_1x_2+2x_2^2,\ x_1^2+2x_2^2,$$
$$x_1^2+x_1x_2+3x_2^2,\ x_1^2+x_1x_2+5x_2^2, \tag{7.1}$$

with $D = -3, -4, -7, -8, -11, -19$. Here we need only the second of these two implications; and we note, see [**3**; p. 98, Lemma 2], that D and d determine f uniquely up to equivalence. The lemma just quoted also gives some restrictions on d when D is given, e.g. $d \not\equiv -1 \pmod 3$ when $D = -3$.

We now examine the arguments in [**3**; pp. 101–103, §6] for the six cases (7.1). For $D = -3$ these arguments, like those quoted above, give $d = -2, -3, -5, -6, -14$ or -30 without any hypothesis except f regular and d square-free. So we have six possibilities for the class of f, all proved in [**3**; p. 100, §4] to have class-number 1, and so excluded since we assume $c(f) > 1$. For $D = -19$ the argument is similar; there is just one possibility $d = -78$, which makes $c(f) = 1$.

If $D = -4$ then $d \not\equiv -1 \pmod 4$, $|d| \leqslant 60$, and $d \equiv 3 \pmod 9$ if $|d| > 12$; also $7 \mid d$ if $|d| > 28$. This gives eight possible d; five of these, namely $-6, -7, -10, -15$, and -42, give $c(f) = 1$, and one is -11, giving $f \sim (2.1)$. The other two, -2 and -3, can each be excluded by constructing f and noticing that it represents the first of the forms (7.1).

We next take $D = -11$. In this case $d \equiv 2 \pmod{16}$, $|d| \leqslant 66$, and $(d \mid 11) \neq -1$. So $d = -30, -46$, or -62, with $c(f) = 1$ in the first two cases. $c(f) > 1$ is proved for $d = -62$, in [3], by constructing f' with $f' \nsim f \simeq f'$. Here we must instead prove f irregular by finding an integer a which is not represented by f, though (1.2) is soluble for every m. We take $a = 26$; then for (1.2) see [3; p. 99, Lemma 4]. The equation (1.1) is

$$x_1^2+x_1x_2+3x_2^2+2x_2x_3+6x_3^2 = 26. \tag{7.2}$$

To prove (7.2) insoluble, express it, with $y_1 = 11x_2+4x_3$, $y_2 = 2x_1+x_2$, as

$$y_1^2+11y_2^2 = 1144-248x_3^2 = 1144,\ 896 \text{ or } 152. \tag{7.3}$$

Each of these three is easily seen to be impossible, so the case $D = -11$ is disposed of.

We now take $D = -7$. From [3] we see that $|d| < 42$, and either $|d| \leqslant 21$ or $d \equiv 3 \pmod 9$. Further, $(d \mid 7) \neq -1$; and we have $|d| \geqslant 10$ since otherwise, constructing f, we find $|D| < 7$. We have $c(f) = 1$ if $d = -10, -13$, or -33, $f \sim (2.3)$ if $d = -17$, $f \sim (2.4)$ if $d = -21$. The only other possibilities, each with $c(f) > 1$, are $d = -14, -19$. In these two cases we take $a = 5, 10$ and prove as above that (1.2) is always soluble but (1.1) is insoluble.

There remains only the case $D = -8$, which is more difficult.

8. *Theorem* 1, *completion of proof*

It remains only to prove that if f is regular and reduced, with d square-free, and $f(x_1, x_2, 0) = x_1^2+2x_2^2$, then $d = -15, -21, -22$, or -70. For the first of these cases gives $f \sim (2.2)$ and the others, as shown in [3], give $c(f) = 1$. We have $d \not\equiv -1, 3 \pmod 8$ and $|d| \geqslant 15$, since otherwise, constructing f, we find that it represents a binary form with discriminant $-3, -4$, or -7.

In the discussion of this case in [3], not only were some possible d excluded by proving $c(f) > 1$ directly, but others were excluded by using $c(f) = 1 \Rightarrow f$ strictly regular to show that f must represent 4 properly in certain cases. Avoiding these arguments, as we here must, [3] crudely gives $|d| \leqslant 120$ and either $|d| \leqslant 40$ or $d \equiv \pm 5 \pmod{25}$. Using also $d \not\equiv -1, -3 \pmod 8$, the cases in which we must prove f irregular are:

$$-d = 23, 26, 29, 30, 31, 34, 37, 38, 39, 55, 95. \tag{8.1}$$

We appeal to [3; p. 99, Lemma 4] to verify that (1.2) is soluble for every m if we take

$$a = 23, 5, 87, 7, 31, 10, 185, 14, 91, 15, 7 \tag{8.2}$$

in the 11 cases (8.1) respectively.

Now the proof is complete if we show that (1.1) is insoluble in each of these 11 cases. Observing that f is of the shape

$$x_1^2+2x_2^2+a_{13}x_1x_3+a_{23}x_2x_3+a_{33}x_3^2,$$

with $d = a_{23}^2 + 2a_{13}^2 - 8a_{33}$, we multiply by 8, complete the square, and express (1.1) as

$$y_1^2 + 2y_2^2 = 8a - |d|\, x_3^2. \tag{8.3}$$

We verify that the right member of (8.3), when $\geqslant 0$, always has a prime factor $\equiv 5$ or 7 (mod 8), in odd multiplicity. So (8.3) and (1.1) are impossible, and the proof of Theorem 1 is complete.

9. *Strongly primitive forms*

The ternary form f may (as in [5], with $n = 3$) be called *strongly primitive* if, for every prime p, it has a binary section with discriminant not divisible by p. Clearly $d(f)$ square-free implies f strongly primitive, for brevity SP; but not conversely. The following result is somewhat inelegant, but easy to prove:

COROLLARY TO THEOREM 1. *Weaken the hypothesis $d(f)$ square-free to $p^2 \nmid d(f)$ for $p = 2, 3, 5$ and f SP (see definition above). Then the conclusion still holds.*

Proof (outline). Assuming further that f is regular, we shall show that the present hypotheses imply

$$|d(f)| \leqslant 120, \text{ always, } \leqslant 40 \text{ if } 3 \nmid d(f) \quad \text{and} \quad 5 \nmid d(f). \tag{9.1}$$

It then follows at once that $p^2 \mid d(f)$ is impossible for $p \geqslant 7$, so $d(f)$ is square-free and the hypotheses and conclusion of the theorem hold.

We proved (9.1) in §§7, 8 by quoting some results from [3]. The proofs of these results do not make full use of all that would follow about the congruence $f \equiv a \pmod{p^t}$ from $d(f)$ square-free. More precisely, this congruence is soluble for all t if $p \nmid a$, which follows easily from the hypothesis that f is SP. It is soluble for all a, t if $(D \mid p) = 1$, D as in §7. These two remarks and $p^2 \nmid d$ for $p \leqslant 5$ suffice for the proof of (9.1) contained in [3].

This completes the proof; and the result could be a useful first step towards finding all regular ternary f. If any one of the conditions $4 \nmid d$, $9 \nmid d$, $25 \nmid d$ is omitted the arguments get more difficult and the list of regular forms has to be lengthened.

In conclusion, let $E(f)$ be the number of $a > 0$ such that (1.1) is insoluble although (1.2) is soluble for every m. Then in [4] I showed that $E(f)$ is large with $|d(f)|$ (for primitive f). I conjectured, but have not yet proved, that $E(f)$ is usually infinite.

References

1. Gordon Pall and Burton W. Jones, " Regular and semi-regular positive ternary quadratic forms ", *Acta Mathematica*, 70 (1939), 165–191.
2. G. L. Watson, " On sums of a square and five cubes ", *J. London Math. Soc.*, 5 (1972), 215–218.
3. ———, " One-class genera of positive ternary quadratic forms ", *Mathematika*, 19 (1972), 96–104.
4. ———, " The representation of integers by positive ternary quadratic forms ", *Mathematika*, 1 (1954), 104–110.
5. ———, "Transformations of a quadratic form which do not increase the class-number ", *Proc. London Math. Soc.*, 12 (1962), 577–587.

University College,
London.