AN EXTENSION OF MEYER'S THEOREM ON INDEFINITE TERNARY QUADRATIC FORMS

BURTON W. JONES

1. Introduction. Let f be a ternary quadratic form whose matrix F has integral elements with g.c.d. 1, that is, an improperly or properly primitive form according as all diagonal elements are even or not. Let d be the determinant of f (denoted by $|f|$), Ω the g.c.d. of the 2-rowed minors of F. Then $d = \Omega^2\Delta$ determines an integer Δ. Two forms f in the same genus have the same invariants Ω, Δ, d. The form whose matrix is adj F/Ω is called the *reciprocal form* of f. A theorem of Meyer, as extended by Dickson [**1**], who completely reworked Meyer's inadequate proof, is the following:

THEOREM 1. *If f_1 and f_2 are two properly or improperly primitive indefinite ternary quadratic forms in the same genus, they are equivalent if*

(1) $$(\Omega, \Delta) \leqslant 2, \Omega \not\equiv 0 \pmod 4, \Delta \not\equiv 0 \pmod 4.$$

Meyer [**3**] also gave the number of classes in a genus of ternary indefinite forms in terms of sets of quadratic characters with respect to the primes common to Ω and Δ, but his proofs are obscure. Siegel recently showed the author that the forms

$$f = x_1^2 - 2x_2^2 + 64x_3^2, \quad g = (2x_1 + x_3)^2 - 2x_2^2 + 16x_3^2$$

are in the same genus but are not equivalent since the latter represents no perfect square whose factors are all congruent to 1 (mod 8). It is the purpose of this article to give a large set of genera of one class whose invariants are not relatively prime.

Let p be an odd prime factor common to Ω and Δ. It is well known [**2**, Theorem 25] that for k arbitrary, f is equivalent to a form

(2) $$f_0 \equiv a_1x_1^2 + p^2a_2x_2^2 + pa_3x_3^2 \pmod{p^k}, \qquad (a_1, p) = 1.$$

Then the transformation K: $x_1 = py_1$, $x_2 = y_2$, $x_3 = y_3$, takes f_0 into pg where g is a form whose matrix has integral elements and

$$g \equiv pa_1y_1^2 + pa_2y_2^2 + a_3y_3^2 \pmod{p^{k-1}}.$$

We call g the *related* or *p-related* form of f and shall prove

THEOREM 2. *If a form g above is in a genus of one class, if p^3 does not divide $|g|$, and if there is an integer q, prime to p and satisfying the following conditions:*

(i) *$|q|$ is an odd prime or double an odd prime;*

(ii) *$-q$ is represented by the reciprocal form of g;*

(iii) *every solution of the congruence*

$$x^2 - qy^2 \equiv 1 \pmod p \tag{3}$$

is congruent (mod p) *to a solution of the Pell equation*

$$x^2 - qy^2 = 1; \tag{4}$$

then the form f is in a genus of one class.

Notice that (ii) imposes only congruence conditions on q and that q must be double a prime if the reciprocal of g is improperly primitive.

Theorems 1 and 2 then imply

COROLLARY 1. *There is only one class in the genus of a (properly or improperly) primitive form f if*

(i) $\Omega \not\equiv 0 \pmod 4$, $\Delta \not\equiv 0 \pmod 4$;

(ii) *for any odd prime factor p dividing both Ω and Δ, it is true that p^3 does not divide $|g|$ and there exists a q satisfying the conditions of Theorem 2.*

The conditions of Theorem 2 will be further considered in §4.

2. Equivalence of f_1 and f_2 implies that of g_1 and g_2. We consider f_1 and f_2 two primitive forms of the same genus. Then [**2**, Theorem 40] we may assume f_1 and f_2 congruent modulo an arbitrary power of p. Suppose $U = (u_{ij})$ is a unimodular transformation (determinant ± 1, integral elements) taking f_1 into f_2, then

$$K^{-1}UK = \begin{bmatrix} u_{11} & u_{12}p^{-1} & u_{13}p^{-1} \\ pu_{21} & u_{22} & u_{23} \\ pu_{31} & u_{32} & u_{33} \end{bmatrix},$$

which is unimodular if $u_{12} \equiv u_{13} \equiv 0 \pmod p$ and takes g_1 into g_2. Now U takes f_1 into f_2, both of the form (2), which implies:

$$a_1(u_{11}x_1 + u_{12}x_2 + u_{13}x_3)^2 + pa_3(u_{31}x_1 + u_{32}x_2 + u_{33}x_3)^2$$
$$\equiv a_1x_1^2 + pa_3x_3^2 \pmod{p^2}.$$

This implies

$$a_1u_{12}^2 \equiv a_1u_{13}^2 \equiv 0 \pmod p$$

which, since $(a_1,p) = 1$, implies $u_{12} \equiv u_{13} \equiv 0 \pmod p$ which completes our proof that $f_1 \cong f_2$ implies $g_1 \cong g_2$ where $\cong$ is the sign for equivalence. Hence the number of classes in the genus of f is not less than the number of classes in the genus of g.

3. Conditions under which $g_1 \cong g_2$ implies $f_1 \cong f_2$. As above, we may assume g_1 and g_2 congruent modulo p^k. Now let the unimodular transformation $U = (u_{ij})$ take g_1 into g_2. Then KUK^{-1} takes f_1 into f_2,

$$KUK^{-1} = \begin{bmatrix} u_{11} & pu_{12} & pu_{13} \\ u_{21}p^{-1} & u_{22} & u_{23} \\ u_{31}p^{-1} & u_{32} & u_{33} \end{bmatrix},$$

and we need $u_{21} \equiv u_{31} \equiv 0 \pmod{p}$. But

$$a_3(u_{31}x_1 + u_{32}x_2 + u_{33}x_3)^2 \equiv a_3x_3^2 \pmod{p}$$

follows from that fact that U takes g_1 into g_2 and g_1 and g_2 are both in form mod p^{k-1} given above. This implies $u_{31} \equiv u_{32} \equiv 0 \pmod{p}$ since $a_3 \equiv 0 \pmod{p}$ would imply p^3 a divisor of $|g|$ contrary to hypothesis. It remains to make $u_{21} \equiv 0 \pmod{p}$. This we do by showing that under certain circumstances we can find an automorph P of g such that the last two elements of the first column of PU are divisible by p.

Write G, the matrix of g, in the form

$$\begin{bmatrix} pB & pb_1 \\ pb_1^T & b \end{bmatrix} \equiv \begin{bmatrix} pB & 0 \\ 0 & b \end{bmatrix} \pmod{p^{k-1}}.$$

Since, under the conditions of Theorem 2, the reciprocal form of g represents $-q \pmod{p^{k-1}}$ we may take $|B| = -q$. Let the unimodular transformation U taking g_1 into g_2 be written

$$U = \begin{bmatrix} U_0 & u_1 \\ u_2 & u_{33} \end{bmatrix}$$

where $u_2 = (u_{31}, u_{32}) \equiv (0,0) \pmod{p}$. We shall first prove

LEMMA 1. *If B has an automorph A such that*

(i) $(A \mp I)B^{-1}$ *is integral for proper choice of* $\pm$,

(ii) $A \equiv U_0 \pmod{p}$,

then an integral 1×2 *matrix w may be determined so that*

$$P = \begin{bmatrix} A & w \\ 0 & \pm 1 \end{bmatrix},$$

and hence P^{-1} are integral automorphs of G and

$$P^{-1}U \equiv \begin{bmatrix} 1 & 0 & u_{13} \\ 0 & 1 & u_{23} \\ 0 & 0 & \pm u_{33} \end{bmatrix} \pmod{p}.$$

In order to prove this, we need to make $P^TGP = G$, that is

$$\begin{bmatrix} A^T pBA & pA^TBw \pm pA^Tb_1 \\ pw^TBA \pm pb_1^TA & pw^TBw \pm pb_1^Tw \pm pw^Tb_1 + b \end{bmatrix} = \begin{bmatrix} pB & pb_1 \\ pb_1^T & b \end{bmatrix}. \tag{5}$$

But $A^TBA = B$ and, if we can determine an integral w so that

$$A^TBw \pm A^Tb_1 = b_1, \tag{6}$$

$|P| = \pm 1$ with $|B| \neq 0$ implies that b is equal to the corresponding member in the left-hand matrix of (5). However (6) is equivalent to

$$BA^{-1}w = \mp (A^T \mp I)b_1,$$

or

$$w = \mp AB^{-1}(A^T \mp I)b_1 = \mp (I \mp A)B^{-1}b_1 = (A \mp I)B^{-1}b_1.$$

Hence w is integral if condition (i) of the Lemma holds. Furthermore, $b_1 \equiv 0 \pmod{p}$ implies $w \equiv 0 \pmod{p}$.

If, in addition, condition (ii) holds, we have

$$P^{-1} = \begin{bmatrix} A^{-1} & \mp A^{-1}w \\ 0 & \pm 1 \end{bmatrix} \equiv \begin{bmatrix} A^{-1} & 0 \\ 0 & \pm 1 \end{bmatrix} \pmod{p},$$

$$P^{-1}U \equiv \begin{bmatrix} A^{-1} & 0 \\ 0 & \pm 1 \end{bmatrix} \begin{bmatrix} U_0 & u_1 \\ 0 & u_{33} \end{bmatrix} \equiv \begin{bmatrix} I & A^{-1}u_1 \\ 0 & \pm u_{33} \end{bmatrix} \pmod{p},$$

and our proof is complete. That is, we can, under the conditions of Lemma 1, find a transformation U taking g_1 into g_2 for which $u_{21} \equiv u_{31} \equiv 0 \pmod{p}$. In other words, $g_1 \cong g_2$ implies $f_1 \cong f_2$.

It may easily be verified that

$$A = \begin{bmatrix} t - bu & -cu \\ au & t + bu \end{bmatrix} \tag{7}$$

is an automorph of $ax^2 + 2bxy + cy^2$, the form whose matrix is B, if t,u is a solution of $x^2 - qy^2 = 1$, where $-q = ac - b^2$. We prove

LEMMA 2. *Condition* (i) *of Lemma* 1 *holds if A is expressed in form* (7) *with* $t \equiv \pm 1 \pmod{q}$.

To prove this, note that

$$(A \mp I)B^{-1} = -q^{-1}\begin{bmatrix} c(t \mp 1) & qu - b(t \mp 1) \\ -qu - b(t \mp 1) & a(t \mp 1) \end{bmatrix},$$

which is integral if $t \equiv \pm 1 \pmod{q}$. Notice that any solution of $x^2 - qy^2 = 1$ satisfies the condition if q is an odd prime or double an odd prime.

Now, as may be shown in the same way as one establishes the automorphs of a binary form,

$$U_0^T B U_0 \equiv B \pmod{p}$$

implies, for p an odd prime,

$$U_0 \equiv \begin{bmatrix} t' - bu' & -cu' \\ au' & t' + bu' \end{bmatrix} \pmod{p},$$

where $t'^2 - qu'^2 \equiv 1 \pmod{p}$. Hence if there is a solution t, u of the Pell equation $x^2 - qy^2 = 1$ such that $t \equiv t' \pmod{p}$ we have $qu^2 \equiv qu'^2 \pmod{p}$ and thus by proper choice of sign of u' we have $A \equiv U_0 \pmod{p}$. We have proved

LEMMA 3. *If for every solution t',u' of the congruence $x^2 - qy^2 \equiv 1 \pmod{p}$ there is a solution t,u of the Pell equation $x^2 - qy^2 = 1$ such that $t \equiv t' \pmod{p}$, condition* (ii) *of Lemma* 1 *holds.*

These three lemmas establish Theorem 2. We now consider in more detail the conditions (ii) and (iii) of Theorem 2 and investigate the permissible values of p and q.

4. Modifications of the conditions of Theorem 2. Consider first the condition that $-q$ be represented by a ternary quadratic form h whose determinant is prime to q. We shall prove

THEOREM 3. *If h is an indefinite ternary form satisfying the conditions of Theorem* 1, *it represents $-q$ with $(q, |h|) \leqslant 2$ if and only if it represents $-q$ in $R(2)$, the ring of 2-adic integers, and in $R(r)$ for every odd prime factor of Ω, that is, if $h \equiv -q \pmod r$ is solvable for every such r.*

We know from Corollary 44b of [**2**] that if h represents $-q$ in $R(r)$ for $r = \infty$ and every prime factor, r, of $2|h|q$, there is a form h' in the genus of h which represents $-q$. But our Theorem 1 implies that h' is equivalent to h which therefore represents $-q$ if h' does. Since h is indefinite it represents $-q$ in the field of reals. It remains to show that h represents $-q$ in $R(r)$ for r an odd prime factor of $q|h|$. If $r = q$ or $\frac{1}{2}q$, Corollary 34b of [**2**] gives the desired result. Now for any odd prime r we may consider

$$h \equiv a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \pmod{r^2}.$$

First, if $a_1a_2 \not\equiv 0 \pmod r$, then

$$a_1x_1^2 + a_2x_2^2 \equiv -q \pmod{r^2}$$

solvable shows that h represents $-q$ in $R(r)$. Second, two of a_1,a_2,a_3 are divisible by r if and only if r divides Ω. Suppose $a_1 \equiv a_2 \equiv 0 \pmod r$. Then $h = -q$ is solvable in $R(r)$ if and only if $h \equiv -q \pmod r$ is solvable [**2**, Theorem 9a]. This completes the proof.

Since g is a ternary form $\operatorname{adj}(\operatorname{adj} G) = dG$ where $d = |G|$. If Ω is the g.c.d. of the 2×2 minors of G it divides all elements of dG, and g primitive implies $d = \Omega^2\Delta$, where Δ is an integer. Furthermore, d is the g.c.d. of all elements of $\operatorname{adj}(\operatorname{adj} G)$ and hence of all 2-rowed minors of $\operatorname{adj} G$. This implies that Δ is the g.c.d. of the 2-rowed minors of the matrix of the reciprocal form of g. Hence we have

THEOREM 4. *Let p be a fixed odd prime and f a primitive form for which $\Omega \equiv \Delta \equiv 0 \pmod p$, neither Ω nor Δ being divisible by* 4 *or p^2, and g its p-related form. Then the reciprocal form of g represents $-q$ if and only if it represents it in $R(r)$ for all prime divisors r of $2\Delta/p$.*

This has the effect of imposing on $-q$ certain conditions modulo powers of 2 and mod r for odd prime factors of Δ/p.

COROLLARY. *Condition* (ii) *of Theorem* 2 *may be replaced by the conditions of Theorem* 4.

Now let us consider further the condition (iii) of Theorem 2. It may be shown that the number of solutions of the congruence (3) is

$$p - (q|p).$$

https://doi.org/10.4153/CJM-1952-012-2 Published online by Cambridge University Press

The number of solutions with $y = 0$ is 2, with $x = 0$ is $1 + (-q|p)$. Hence the number of solutions with neither x nor y zero is

$$p - (q|p) - (-q|p) - 3$$

and the number of distinct pairs of solutions x^2, y^2 with neither zero is one fourth of this number. Hence the number of distinct (mod p) pairs x^2, y^2 of solutions is

$$M = \tfrac{1}{4}\{p - (q|p) + (-q|p) + 3\}.$$

That is

$$M = \tfrac{1}{4}(p + 3) \text{ if } p \equiv 1 \pmod 4,$$

$$M = \tfrac{1}{4}(p + 1) \text{ if } p \equiv -1 \pmod 4 \text{ and } (q|p) = 1,$$

$$M = \tfrac{1}{4}(p + 5) \text{ if } p \equiv -1 \pmod 4 \text{ and } (q|p) = -1.$$

First we consider two special cases. Suppose $p = 3$ and $q \equiv 1 \pmod 3$. Then there is only one pair of solutions of the congruence, namely, $x^2 \equiv 1$, $y^2 \equiv 0 \pmod 3$, and hence condition (iii) of Theorem 2 holds. Then from Theorem 4 and Corollary 1 we prove

THEOREM 5. *An indefinite primitive ternary quadratic form f is in a genus of one class provided*

(i) (Ω,Δ) *divides* 6,

(ii) $\Omega \not\equiv 0 \not\equiv \Delta \pmod 4$,

(iii) $|f| \not\equiv 0 \pmod{81}$.

To prove this we need merely show the existence of a prime or double a prime q with $(q|3) = 1$ and satisfying the conditions of Theorem 4. This means that $q \equiv 1 \pmod 3$ and satisfies certain congruence conditions modulo powers of r where r is a prime factor of $2\Delta/3$. Dirichlet's theorem shows that such a q exists provided that these conditions are consistent and the conditions of the theorem imply that $\Delta/3$ is not divisible by 3. This completes the proof.

Furthermore, for $p = 3$, $(q|3) = 1$, condition (iii) of Theorem 2 holds even if q is negative and g a positive form. Thus we have

THEOREM 6. *For $p = 3$, a positive ternary quadratic form f is in a genus of only one class if its 3-related form g is, and if $|f| \not\equiv 0 \pmod{81}$.*

Two examples are

$$f = x^2 + 18y^2 + 3z^2, \quad g = 3x^2 + 6y^2 + z^2,$$
$$f = x^2 + 18y^2 + 6z^2, \quad g = 3x^2 + 6y^2 + 2z^2.$$

Group theoretic considerations lead to another special case of interest. Let T, U be the fundamental solution of $x^2 - qy^2 = 1$. It is well known that all solutions are given by

$$t_n + u_n\sqrt{q} = \pm (T + U\sqrt{q})^n$$

for integral powers of n. Hence under this law of combination, the solutions

https://doi.org/10.4153/CJM-1952-012-2 Published online by Cambridge University Press

(mod p) of the Pell equation form a multiplicative group H_p which must be a subgroup of the multiplicative group of solutions of the congruence (mod p). Hence s, the order of H_p, is a divisor of $2u = p - (q|p)$. Condition (iii) of Theorem 2 will be met if and only if $s = 2u$. Now s must be even since (t,u), a solution of the Pell equation, implies that $(-t,u)$ is a solution and $(0,u)$, a solution, implies that $(0,-u)$ is. Hence $s = 2s'$. But $s > 2$ unless, for the fundamental solution, $U \equiv 0$ (mod p) and, with this exception, u a prime would imply $s' = u$ and $s = 2u$. Hence, *if for proper choice of sign* $\frac{1}{2}(p \pm 1)$ *is a prime, condition* (iii) of Theorem 2 holds and q *may be chosen to satisfy conditions* (i) *and* (ii) *unless* $U \equiv 0$ (mod p) for the fundamental solution of the Pell equation.

To consider the general case we notice again that any solution t,u of $x^2 - qy^2 = 1$ is expressible in the form

$$t_r + u_r\sqrt{q} = \pm\ (T + U\sqrt{q})^r$$

where T,U is the fundamental solution. Now

$$t_r + u_r\sqrt{q} \equiv t_s + u_s\sqrt{q} \pmod{p}$$

implies

$$t_r - u_r\sqrt{q} \equiv t_s - u_s\sqrt{q} \pmod{p}$$

where if $(q|p) = -1$ by such a congruence we mean that corresponding parts are congruent and if $(q|p) = 1$ we replace $\sqrt{q}$ by a solution of $q \equiv r^2$ (mod p). Hence $t_r \equiv t_s$, since p is odd and thus $u_r \equiv u_s$.

First, if $(q|p) = 1$, there are $p - 1$ solutions of the congruence and $\pm\ (T + U\sqrt{q}\ )^k$ yields all solutions if and only if one of the following holds:

(a) $\omega = T + U\sqrt{q}$ is a primitive root (mod p).

(b) ω belongs to $\frac{1}{2}(p - 1)$ (mod p) and no power of ω is congruent to -1 (mod p).

We can show that condition (b) may be replaced by

(b′) ω belongs to $\frac{1}{2}(p - 1)$ (mod p) and $p \equiv 3$ (mod 4).

Suppose $p \equiv 1$ (mod 4). Then ω belonging to $\frac{1}{2}(p - 1)$ would imply $\omega^t \equiv -1$ (mod p) for $t = \frac{1}{4}(p - 1)$. On the other hand, if $p \equiv 3$ (mod 4), $\omega^t \equiv -1$ (mod p) would imply $\frac{1}{2}(p - 1)$ divides $2t$ and since the former is odd it must divide t. This would make it impossible for ω to belong to $\frac{1}{2}(p - 1)$.

Second, if $(q|p) = -1$ there are $p + 1$ solutions of the congruence and $\pm\ (T + U\sqrt{q})^k$ yields all solutions if and only if one of the following holds:

(a) ω belongs to $p + 1$ (mod p).

(b) ω belongs to $\frac{1}{2}(p + 1)$ (mod p) and no power of ω is congruent to -1 (mod p).

As above, we may replace condition (b) by

(b′) ω belongs to $\frac{1}{2}(p + 1)$ (mod p) and $p \equiv 1$ (mod 4).

5. Examples. We consider $p = 5$ and $p = 7$, giving explicit conditions for primes q or doubles of primes q satisfying condition (iii) of Theorem 2 and append a short table of values.

$$p = 5$$

Case 1. Suppose $(q|p) = 1$. The primitive roots (mod 5) are 2 and 3. Let $a^2 \equiv q \pmod 5$ and have

$$T^2 - a^2U^2 \equiv 1 \pmod 5,\ T - aU \equiv \pm 2 \pmod 5$$

imply

$$T + aU \equiv \pm 3 \pmod 5$$

and hence

$$T \equiv 0 \pmod 5$$

is the necessary and sufficient condition for (iii) of Theorem 2, since $T^2 \equiv -1 \pmod 5$ would imply $a^2U^2 \equiv -2 \pmod 5$ which is impossible.

Case 2. Suppose $(q|p) = -1$. Since $p + 1 \equiv 2 \pmod 4$ we want $\omega \not\equiv \pm 1 \pmod 5$ and $\omega^3 \equiv \pm 1 \pmod 5$. Now

$$\omega^2 = T^2 + qU^2 + 2UT\sqrt{q} \equiv 1 \pmod 5$$

only if $UT \equiv 0 \pmod 5$. But $T \equiv 0 \pmod 5$ would imply $-qU^2 \equiv 1 \pmod 5$ which would deny $(q|p) = -1$. Hence $U \equiv 0 \pmod 5$, $T \equiv \pm 1 \pmod 5$ which must be excluded. Thus the necessary and sufficient condition for (iii) is

$$T \equiv \pm 2 \pmod 5.$$

We can include both case 1 and 2 by writing

$$T \equiv 0, \pm 2 \pmod 5. \tag{8}$$

The prime and double prime values of q less than 50 for which (8) holds are:

3, 6, 7, 11, 14, 17, 19, 22, 31, 34, 37, 38, 43, 46, 47.

In terms of our general results this means that Ω and Δ may have a common factor 5 if the negative of one of the numbers in the table is represented by the reciprocal form of g.

$$p = 7$$

Case 1. Suppose $(q|p) = 1$. The primitive roots (mod 7) are 3 and 5. Here we want $\omega^3 \equiv \pm 1$ and $\omega \not\equiv \pm 1$, all congruences being (mod 7). Suppose $T + aU \equiv \pm 1$; then $T \equiv \pm 1$ which is excluded. Similarly it is easily shown that $T \equiv 0$ and $T \equiv \pm 2$ are impossible. Hence a necessary and sufficient condition for (iii) is

$$T \equiv \pm 3 \pmod 7.$$

Case 2. Suppose $(q|p) = -1$. Then ω must belong to 8 (mod 7), that is, $\omega^2 \not\equiv \pm 1$. But

https://doi.org/10.4153/CJM-1952-012-2 Published online by Cambridge University Press

$$(T + U\sqrt{q})^2 = T^2 + U^2q + 2TU\sqrt{q} \equiv \pm 1$$

imply $TU \equiv 0$. Thus $U \equiv 0$ and $T^2 \equiv 1$ or $T \equiv 0$ and $qU^2 \equiv \pm 1$ both of which are excluded. But $T^2 \equiv 9$ is impossible. We include both cases in

$$T \equiv \pm 2, \pm 3 \pmod 7. \tag{9}$$

The prime and double prime values of q less than 50 for which (9) holds are:

3, 5, 6, 10, 11, 13, 17, 19, 23, 26, 37, 38, 41, 43, 46.

Extensions of the results of this paper are being considered by the author and his students.

References

1. L. E. Dickson, *Studies in the theory of numbers* (Chicago, 1930).
2. B. W. Jones, *The arithmetic theory of quadratic forms* (Tenth Carus Monograph, Math. Assoc. Amer., 1950).
3. A. Meyer, *Über indefinite ternare quadratische Formen*, J. Reine Angew. Math., vol. 116 (1896), 317-325.