Five regular or nearly-regular ternary quadratic forms

by

William C. Jagy (Berkeley, Calif.)

1. Introduction. In a recent article [6], the positive definite ternary quadratic forms that can possibly represent all odd positive integers were found. There are only twenty-three such forms (up to equivalence). Of these, the first nineteen were proven to represent all odd numbers. The next four are listed as "candidates". The aim of the present paper is to show that one of the candidate forms $h = x^2 + 3y^2 + 11z^2 + xy + 7yz$ does represent all odd (positive) integers, and that it is regular in the sense of Dickson. We will consider a few other forms, including one in the same genus as h that is a "near miss", i.e. it fails to represent only a single number which it is eligible to represent. Our methods are similar to those in [4]. A more recent article with a short history and bibliography of work on regular ternary forms is [3].

2. Techniques. Our main tool is the relation of a form with diagonal forms of known behavior. For instance, with the form h above, we represent a number $4n$ as $r^2 + s^2 + 2t^2$, and arrange for certain congruence conditions to hold among $\{r, s, t\}$. Then we are able to represent the original n by the form h. In this framework, a particular representation of some number may not be suitable, requiring a different expression using the diagonal form. There are two major types of revision.

Given a square m^2, we may need an alternative way to write m^2 as $r^2 + as^2 + bt^2$. All cases we consider are covered among four alternatives, separated by ways of expressing m itself:

(1) $$(r^2 + as^2)^2 = (r^2 - as^2)^2 + a(2rs)^2,$$
(2) $$(r^2 + bt^2)^2 = (r^2 - bt^2)^2 + b(2rt)^2,$$
(3) $$(r^2 + as^2 + bt^2)^2 = (r^2 - as^2 - bt^2)^2 + a(2rs)^2 + b(2rt)^2.$$

Finally, if m is not itself represented by $r^2 + as^2 + bt^2$, we might still get a nontrivial expression for m^2 from

$$(4) \quad \left\{ \begin{array}{c} r^2 + as^2 \\ + bt^2 + abu^2 \end{array} \right\}^2 = \left\{ \begin{array}{c} (r^2 - as^2 - bt^2 + abu^2)^2 \\ + a(2rs - 2btu)^2 + b(2rt + 2asu)^2 \end{array} \right\}.$$

The formula (4) was found using the quaternions underlying the quaternary form $r^2 + as^2 + bt^2 + abu^2$, searching for a way to make the ab term vanish upon squaring.

The second type of revision is present in a variety of articles, including [5] and [6]. It deals with a binary diagonal form $r^2 + ks^2$, $k \geq 1$. We give the formulation (Theorem 9, p. 51) in the unpublished Ph.D. dissertation of Burton Jones, Univ. of Chicago, 1928.

LEMMA (Jones). *If $f = r^2 + ks^2$ represents an odd prime p, where k is a positive integer prime to p, then every mp represented by f (m a positive integer) is represented by f with r and s prime to p.*

Some of the amusing behavior of ternary forms arises precisely because the lemma fails when $m = 0$.

It is worthwhile to make a digression on an interesting process, used in the present work, for finding diagonal ternary forms that are related to a given nondiagonal form. We begin by expressing an integer multiple of the form as the sum of three squares (when possible). The original form f (or twice the form) can be represented by an integer 3×3 matrix B that is symmetric and positive definite. We use a test based on the local-global principle in number theory, due to Minkowski, Hasse, and Witt. Among other applications, the test decides whether or not such a matrix B is congruent to the identity over the rationals, i.e. $B = QQ'$, with Q a matrix of rationals and Q' its transpose. The determinant of B is not necessarily a square, so we apply the test to mB, where the determinant of mB is a square.

Once mB is congruent to the identity over the rationals, it is congruent to the identity matrix over the integers, by a theorem of Hsia [2]. That theorem applies to matrices of size 7×7 or smaller, as well as to 8×8 matrices that have at least one odd entry on the diagonal. Simple examples that exhibit a distinction (between rational and integer congruence to the identity) are the $k \times k$ matrices with every diagonal element 2 and every nondiagonal element 1, where $k = 8, 15, 24, 35, \ldots$ is a square minus 1, and $k \geq 8$.

When the numbers in this mB are small, it is generally quite easy to guess an integer matrix H such that $mB = HH'$. The result is an expression for mf or $2mf$ as the sum of squares of three linear polynomials with integer coefficients, the coefficients found as the columns of H. Further manipulation sometimes gives useful expressions for f. Two common steps are

$$2(r^2 + s^2) = (r - s)^2 + (r + s)^2$$

and

(5) $\qquad 4(r^2 + s^2 + 2t^2) = (r + s - 2t)^2 + (r + s + 2t)^2 + 2(r - s)^2.$

3. The form h. The twenty-second form in [5] can be written as

$$h = x^2 + 3y^2 + 11z^2 + xy + 7yz,$$

or

(6) $\qquad 4h = (2x + y)^2 + (3y + 6z)^2 + 2(-y + 2z)^2.$

A different representative for the equivalence class of this form is given in [1]. Equation (6) shows that h cannot represent any numbers of the form $4^k(16m + 14)$. Furthermore, h does not represent any numbers congruent to 2 (mod 4): note that $h \equiv (x + z)^2 + (x + z)y + y^2$ (mod 2), and $h \equiv (y + x + z)(x - z) - y^2$ (mod 4). If h is even, then $y, x + z$, and $x - z$ are even. The mod 4 equivalence then shows that h is 0 (mod 4).

We will show that h represents all odd positive integers. It follows that h represents every number of the form $4^k o$, where o denotes an odd positive integer. We also show that h represents all numbers $n \geq 0$ with $n \equiv 8$ (mod 16) but $n \not\equiv 56$ (mod 64). Together, these will show that h represents all eligible numbers.

We proceed by showing how to represent numbers $4n$ as $r^2 + s^2 + 2t^2$, with

$$r \equiv s \pmod 2, \quad s \equiv 0 \pmod 3, \quad s \equiv t \pmod 4.$$

Once that is achieved, equation (6) shows that n itself is represented by h with

$$x = \frac{6r - s + 3t}{12}, \quad y = \frac{s - 3t}{6}, \quad z = \frac{s + 3t}{12}.$$

The first case to consider is $n \geq 0$, n even, where it suffices to restrict to

$$n \equiv 8 \pmod{16}, \quad \text{but} \quad n \not\equiv 56 \pmod{64}.$$

It follows that $n/8$ is odd, and $n/8 \not\equiv 7$ (mod 8). We may therefore write

$$n/8 = a^2 + b^2 + c^2.$$

There must be a match of values mod 3, since we have three squares and there are only two values $\{0, 1\}$ for squares mod 3. We re-label and choose $\pm$ signs so that $a \equiv b$ (mod 3). We arrive at

$$4n = (4a + 4b)^2 + (4a - 4b)^2 + 2(4c)^2,$$

with all terms congruent (mod 4), the middle term $4a - 4b$ congruent to 0 (mod 3). It follows that n is represented by h.

Next we consider n odd. To begin, we may write

$$n = o^2 + e^2 + 2w^2,$$

with o odd and e even, but w undecided. We separate into subcases.

A. If $o \equiv e \equiv 0 \pmod{3}$, then

$$4n = (2o)^2 + (2e)^2 + 2(2w)^2$$

works, because $2w$ is congruent $\pmod 4$ to either $2o$ or $2e$, depending on whether w is odd or even.

B. If at most one of the numbers $\{o, e, w\}$ is divisible by 3, we choose $\pm$ signs for each so that

$$o + e + 2w \equiv 0 \pmod{3}.$$

Define $s = o + e + 2w$ and $r = o + e - 2w$. Then choose $t = \pm(o - e)$ such that $s \equiv t \pmod 4$. From formula (5) we know that

$$4n = r^2 + s^2 + 2t^2,$$

with r, s, t all odd, s divisible by 3, and $s \equiv t \pmod 4$. Once again, n is represented by h.

C. Conditions $\bmod 3$ are:

$$o \not\equiv 0, \quad e \equiv w \equiv 0 \pmod{3}.$$

If w is even, including $w = 0$, then $2w \equiv 2e \pmod 4$, which suffices. If w is odd, we need to revise the expression for n. With w odd, we have $e^2 + 2w^2 \neq 0$, and $e^2 + 2w^2 \equiv 0 \pmod 3$. The lemma of Jones says that there are integers e_1 and w_1 such that $e_1 \not\equiv 0 \pmod 3$, and $w_1 \not\equiv 0 \pmod 3$, but $o^2 + e_1^2 + 2w_1^2 = n$. The new expression for n has all three numbers prime to 3, and we complete the argument by repeating case B.

D. Conditions $\bmod 3$ are:

$$o \equiv w \equiv 0, \quad e \not\equiv 0 \pmod{3}.$$

This time, if w is odd we are finished. If w is even, we still have $o \neq 0$, and we are able to adapt the argument in case C, finding a revised expression $n = o_1^2 + e^2 + 2w_1^2$ and repeating case B. This completes the proof of regularity for h.

4. The genus mate of h. A form closely linked with h is

$$f = 3x^2 + 9y^2 + 9xy + 3z^2 + xz,$$

or

(7) $$4f = (3x + 6y)^2 + (x - 2z)^2 + 2(x + 2z)^2.$$

Notice the similar appearance of (7) to (6). We will show that f is quite mildly irregular: it does not represent 1, yet represents all other numbers that are represented by h. Together, h and f give an example of a rare phenomenon, a genus composed of two forms, one regular and the second missing exactly one eligible number. For another example, see [4] (Theorem 7, p. 182).

There is a small change from the treatment of h. For the form f, r (instead of s) is divisible by 3. That is, we represent numbers $4n$ as $r^2 + s^2 + 2t^2$, with

$$r \equiv s \pmod 2, \quad r \equiv 0 \pmod 3, \quad s \equiv t \pmod 4.$$

Then n itself is represented by f with

$$x = \frac{s+t}{2}, \quad y = \frac{2r - 3s - 3t}{12}, \quad z = \frac{-s+t}{4}.$$

The proof for

$$n \equiv 8 \pmod{16}, \quad \text{but} \quad n \not\equiv 56 \pmod{64}$$

is nearly identical to that for h. For odd numbers, in cases A and B, the proof also differs trivially from that for h. We discuss case D, then case C. We have written

$$n = o^2 + e^2 + 2w^2.$$

D. Conditions $\bmod\, 3$ are:

$$o \equiv w \equiv 0, \quad e \not\equiv 0 \pmod 3.$$

If w is even we are finished, using $4n = (2o)^2 + (2e)^2 + 2(2w)^2$. If w is odd, we have $w \neq 0$, and we are able to find a revised expression $n = o_1^2 + e^2 + 2w_1^2$ with all three variables prime to 3, then repeat case B.

C. Conditions $\bmod\, 3$ are:

$$o \not\equiv 0, \quad e \equiv w \equiv 0 \pmod 3.$$

If w is odd we are done. If w is even and $e \neq 0$ or $w \neq 0$, then $e^2 + 2w^2 > 0$ and we may revise the expression for n appropriately.

If, however, e and w are actually 0, we have $n = o^2$.

Note f does not represent 1. We proceed with $n \geq 9$. The result will follow if we can demonstrate it for $n = p^2$, with p a (positive) odd prime. First, write

$$p = r^2 + s^2 + 2t^2.$$

If p is congruent to 1 mod 4, we may take $t = 0$ and use

(8) $$p^2 = (r^2 + s^2)^2 = (r^2 - s^2)^2 + (2rs)^2.$$

Since p is a prime, r and s are nonzero in the above. Since p is odd, one of r and s is even and the other odd, so $r^2 - s^2 \neq 0$.

If p is congruent to 3 $\pmod 8$, take $s = 0$, with

(9) $$p^2 = (r^2 + 2t^2)^2 = (r^2 - 2t^2)^2 + 2(2rt)^2.$$

If p is congruent to 7 $\pmod 8$, we have $r, s, t \neq 0$, and

(10) $$p^2 = (r^2 + s^2 + 2t^2)^2 = (r^2 - s^2 - 2t^2)^2 + (2rs)^2 + 2(2rt)^2.$$

This concludes the proof.

5. A few other forms. We begin by showing that a form we shall call g_{25} is regular, with

$$g_{25} = x^2 + 2y^2 + 2yz + 13z^2,$$

or

(11) $$g_{25} = x^2 + (y + 3z)^2 + (y - 2z)^2.$$

The genus of g_{25} misses $\{(25m \pm 5, 10); 4^k(8m+7)\}$ but represents all other nonnegative integers. According to (11), we need only express an eligible number n as the sum of three squares,

$$n = r^2 + s^2 + t^2,$$

with $s \equiv t \pmod 5$. Renaming the variables and choosing $\pm$ signs, this is immediately possible unless the values $(\bmod\, 5)$ are 0, ± 1, ± 2, which can occur if n is divisible by 5. If n is actually divisible by 25, we can simply express $n/25$ as the sum of three squares, then multiply through by 5, getting a new expression for n as the sum of three squares. Finally, the form g_{25} does not represent any positive integers that are divisible by 5 but not by 25; this statement follows quickly from the expression

$$2g_{25} = (2y + z)^2 + 2x^2 + 25z^2.$$

This shows regularity for g_{25}.

Two other forms show behavior similar to that of f, which missed 1 but represented all other numbers allowed to its genus. The first,

$$f_{25} = 2x^2 + 3y^2 + 5z^2 + 2yz + 2xz,$$

or

(12) $$f_{25} = (x + y)^2 + (-x + y - z)^2 + (y + 2z)^2,$$

misses 1, and, indeed, all 4^k. The genus of f_{25} represents all nonnegative integers other than $\{4^k(8m + 7)\}$. The proof involves writing

$$n = a^2 + b^2 + c^2$$

with $2a + 2b + c \equiv 0 \pmod 5$. The 4^k failure appears when we look for alternative expressions for squares as the sum of three squares, and there is no improvement on $4 = 2^2 + 0^2 + 0^2$.

Finally, we have

$$g_{18} = 2x^2 + 2y^2 + 2yz + 5z^2,$$

or

(13) $$g_{18} = (y + 2z)^2 + (y - z)^2 + 2x^2.$$

This form misses only the number 1 among those integers represented by its genus, those being the nonnegative integers other than $\{9m \pm 3, 4^k(16m +$

14)}. To contrast with the proof for f_{25}, we note that an alternative expression for 4 is $2^2 = 1^2 + 1^2 + 2 \cdot 1^2$. The proof involves writing

$$n = a^2 + b^2 + 2c^2$$

with $a \equiv b \pmod 3$, and proceeding as with the other forms.

References

[1]   H. B r a n d t und O. I n t r a u, *Tabelle reduzierten positiver ternärer quadratischer Formen*, Abh. Sächs. Akad. Wiss. Math.-Natur. Kl. 45 (1958).
[2]   J. S. H s i a, *Two theorems on integral matrices*, Linear and Multilinear Algebra 5 (1978), 257–264.
[3]   —, *Regular positive ternary quadratic forms*, Mathematika 28 (1981), 231–238.
[4]   B. W. J o n e s and G. P a l l, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. 70 (1939), 165–191.
[5]   I. K a p l a n s k y, *The first nontrivial genus of positive definite ternary forms*, Math. Comp. 64 (1995), 341–345.
[6]   —, *Ternary positive quadratic forms that represent all odd positive integers*, Acta Arith. 70 (1995), 209–214.

Mathematical Sciences Research Institute
1000 Centennial Drive
Berkeley, California 94720-5070
U.S.A.
E-mail: jagy@msri.org