July 1996

13 pages

Notes on the classification of regular ternary forms

Irving Kaplansky

Not intended for publication

1. Introduction. In [2] there is the following promise:

"A followup paper is planned; it will present detailed proofs and descriptions of the computations."

This note is not the promised paper. It will take a while till that is ready. In the meantime I decided to do a rush job on a preliminary note. It is crude but I hope that it will give interested people an adequate idea of how the classification was done.

A serious reader should have at hand part 7 of Watson's thesis [4] (31 typed pages). A postcard request to me or to WCJ (will Jagy) will be promptly honored.

For convenience I repeat from [2] some matters of notation and terminology. A form g = ax^2 + by^2 + cz^2 + dyz + exz + fxy is briefly denoted by a b c d e f; g is called even if d, e, and f are all even and odd otherwise. Attached is the matrix

$$A = \begin{pmatrix} a & f/2 & e/2 \\ f/2 & b & d/2 \\ e/2 & d/2 & c \end{pmatrix},$$

PAGE 7 : speculation for odd forms failed at discriminants 2592.

The discriminant of g is det(A) if g is even and det(2A)/2 if g is odd.

2. Schiemann's tables. The tables [1] give all odd forms up to discriminant 1000 and all even forms up to discriminant 250, divided into genera. Thanks to the courtesy of John Hsia I have a portion of these tables. In December, 1995 I received from AS (Alexander Schiemann) an online version of these tables. I have done a spotcheck comparison and they agree, modulo occasional different choices of a canonical form.

I promptly did a complete search of these tables for regular forms. Here's how that was done, genus by genus. let a form g in a genus G be given. First remark: to be regular, g must have as its initial coefficient the smallest that occurs in G (because in the tables the initial coefficient of a form is the smallest number represented by that form). Suppose that this is so. Now the task is to check whether g represents every number that is represented by h, where h ranges over the other forms in G. WCJ devised an effective program, written within Mathematica. In many cases I was able to dismiss th genus at a glance. Failing that, I used the program. The input is a set of 12 numbers: the coefficients of g and h. A bound B is set in advance. The output lists all numbers up to B represented by g (resp. h) that are not represented by h (resp. g) Note that if neither dominates the other we have killed both g and h; this is what happens most of the time. In practice B was usually set somewhere between 50 and 100, but for small discriminants B = 15 was usually good enough. If g passed the test the bound was raised. If g survived B = 200 it was declared a provisional candidate. For these runs a few secons sufficed, but on a few occasions B was taken as large as 2000 and then the program ran for about an hour. A stab was next made at proving regularity; there were a fair number of successes (mostly due to WCJ) but 34 forms were stubborn. These 34 were then checked for regularity up to a million. This was done by a different program, written in C. The numbers forbidden to all of G were determined (an easy task) and the program checked whther g represented the complement, up to a million. This also required about an hour per form.

Later in the procedure it was necessary to check discriminants above 1000 in the odd case and 250 in the even case. For these selected discriminants (about 200 in all) AS furnished electronically tables of forms and genera. The largest discriminants treated in this fashion were 24334 for odd and 8000 for even.

In addition, AS devised a program that identified (up to a preset limit) all forms that are alone in their genera. WCJ and I nicknamed these "loners". For odd loners AS's search went to 30,000 and the largest discriminant that appeared was 13068. Eventually it was proved that there are no larger odd loners. For even loners the search went to 62600 and there was no end in sight; the largest discriminant obtained was 57600 (two forms). By another method (see item 10 below) the 12 remaining even loners were identified, ending with discriminant 338688.

WCJ and I are extremely grateful to AS for his expert, cheerful, and prompt responses to our requests. The project would have been impossible without his contribution.

3. Odd square-free. The method calls for first classifying the odd forms and then proceeding to the even ones. So: until item 10 all forms are odd.

There are 24 regular odd forms with square-free discriminants. This is Theorem 2 in [4] and the list itself appears as Table I. (In all, there are 6 theorems and 3 tables.) This much of part 7 of his thesis was published in [5].

I will candidly confess that I still find parts of Watson's work hard to follow; furthermore, at times he is admittedly sketchy. So, when I first read [5] I redid it a little differently. His argument achieves a priori bounds for the discriminants in question, and this is interlaced with further arguments that identify the forms themselves. I chose to concentrate on the bounds, relying on the tables to complete the job.

Getting such bounds is a standard kind of thing. Let me give three examples.

i) A form that represents 1,2,3 and 5 has discriminant $\leq$ 40. Here is a sketch but I remark that additional details are needed Take vector that represent 1 and 2. We get an upper left corner

$$\begin{pmatrix} 1 & ? \\ ? & 2 \end{pmatrix}$$

and the ? must be 0, 1, or 2 (positive definiteness). The worst case is ? = 0 where we cannot use 3 for the lower right corner (since x^2 + 2y^2 represents 3) and must use 5. So we have the estimate

$$\frac{1}{2}\begin{vmatrix} 2 & 0 & ? \\ 0 & 4 & ? \\ ? & ? & 10 \end{vmatrix}$$

The determinant is bounded by the product 80 of its diagonal elements, and so we get 40.

(ii) A form that represents 1, 3, 5 and 7 has discriminant ≤ 77. The argument is similar. This is what I really did in getting a bound in [3], although I did not put it that way.

(iii) Three numbers may be enough. For instance, a form that represents 1, 2 and 15 has discriminant ≤ 120..

I have accumulated a library of such bounds. As I write this I am engaged in the project of finding the forms that are regular with exactly one exception. For this I need to enlarge the library.

4. The admissible primes. The only primes that can divide the discriminant of a regular form are those ≤ 17, together with 23. This covered by Theorems 3, 4, and 5 of [4].

Part 7 of Watson's thesis became available to me about two months before the completion of the project. By then I had my own proof of this statement; it is similar but differs in numerous details.

5. The invariant (a, b). I treat the prime 2 in a special way (see below) and p will always denote an odd prime. One knows that over the p-adic numbers a primitive form can be written

$$rx^2 + sp^ay^2 + tp^bz^2 \quad = r x^2 + s p^a y^2 + t p^b z^2$$

with r, s, and t prime to p and $a \leqq b$. The numbers a and b are unique, and thus the pair (a, b) is an invariant. Watson instead used the greatest common divisor of the 2 by 2 minors of the form. I find it a little clearer to use (a, b). Note that (a, b) depends on p, but there should be no confusion.

6. The case $a \geqq 2$. In his Theorem 5 Watson proved that p must be 3. Once again: my proof is similar but differs in details.

Now one has to figure out what happens for $a \geqq 2$, p = 3. I handled this by a program for "going up by 81". I shall say something about this below.

From now on, until item 9, assume that the discriminant is not divisible by 4.

7. The case a = 0, $b \geqq 2$. In Theorem 3 of [4] Watson proved that p must be 3 or 5. But much more is true: there are just 11 such forms. For p = 5 there is the one example 50: 1 2 7 2 1 0; it leads off Table 2. For p = 3 there are 10 examples: the first 10 forms in Table 3.

Watson's proofs become really sketchy at this point. My proof uses additional a priori bounds for the discriminant plus brutal examination of tables supplied by AS for selected discriminants above 1000.

8. The case a = 1. This is the only possibility left. It is handled by a simple, well known procedure for dropping from a regular form with discriminant D and invariant (1, b) to a regular form with discriminant D/p and invariant (1, b - 1)

(At this point I shall mention a certain "speculation" that occurred in an early manuscript. For those who never saw it or don't remember, it doesn't matter. Suffice it to say that in the end the speculation turned out to be false, failing for exactly two forms: 2592: 5 9 17 6 5 3 and 8232: 5 13 40 20 4 1.)

The problem is to reverse the procedure, so as to go up by p. How did Watson do this? I'm stumped. The ideas in [6] and the papers on which it builds may provide a clue, but I haven't pursued this. I shall tell you how I did it. Let there be given a regular form D with discriminant divisible by p. I asked AS for the table for pD (actually some such pD's were not needed because of the behavior at other primes) and kept doing this until regularity expired.

9. Discriminant divisible by 4. Did Watson try this? Did he try and give up? Quote from page 72: "A complete enumeration would be very laborious..."

I have a theorem about going down by 4 on odd forms that Watson may have missed. It is quite a simple matter and I shall give a little detail.

An easy argument shows that any odd form can be normalized so that two of the off-diagonal entries are even (the remaining one is of course odd). Let us write g = a b c 2d 2e f, f odd. The discriminant D of g is given by

D = 4abc - 4ad^2 - 4be^2 - cf^2 + 4def.

We see that D is divisible by 4 if and only if c is divisible by 4. We are assuming that this is the case. Let us abuse notation by changing c to $4c$. Then g is $a\ b\ 4c\ 2d\ 2e\ f$. We are ready to name the target of the descent: it is $h = a\ b\ c\ d\ e\ f$.

(The following is a fact which is not needed: quite aside from regularity, $g \to h$ is a well defined mapping, i. e., independent of the choice of basis. That is, there is a canonical map from odd forms of discriminant $4E$ to odd forms of discriminant E. The mapping is onto but usually not one-to-one.)

Our business is with the statement that g regular implies h regular. There are two cases.

(i) a and b odd. Suppose g represents an even number L. Then $ax^2 + fxy + by^2$ is even. Since a, b, and f are all odd, this implies that x and y are even. It follows that L is a multiple of 4. Divide by 4 and we get that h represents $L/4$. This is reversible: if h represents $L/4$ then g represents L. We have identified the numbers represented by h with the multiples of 4 represented by g, and this suffices to prove that h is regular.

(ii) a or b (or both) even. Here the argument is quite different: one shows that g and h represent exactly the same numbers, whence h is regular. It is obvious that if g represents L then h does, for

$$(*) \qquad h(x, y, 2z) = g(x, y, z).$$

In the other direction we assume that h represents L and have to prove that g represents L. We take advantage of the regularity of g: it suffices to prove that g represents L q-adically for every prime q. For q odd this is clear from (*). For $q = 2$ we get the needed information simply because it is standard that the binary section $ax^2 + fxy + by^2$ represents everything q-adically.

With this result in hand we can proceed as above: knowing that there is a regular form of discriminant D we examine all forms of discriminant 4D for regularity and iterate till regularity expires. But there is also a program for "going up by 4" which will be mentioned below. In fact, a combination of the two methods was used. Then, after the list of regular odd forms was tentatively in final form, going up by 4 was applied to the entire list as an additional check.

10. The reduction procedure for even forms. The discussion starts with a normalization analogous to the one that was just used: one can arrange that the diagonal entries of an even form are odd, even, even. Thus we take g = a 2b 2c 2d 2e 2f of discriminant D with a odd. Suppose that g represents an even number ~~2M~~. Then x has to be even. Replace x by 2x and divide by 2. We get the form h = 2a b c d 2e 2f and we know that h is regular. However, h may not be primitive and we distinguish cases.

(i) d odd (which is true if and only if D is odd). Then h is a primitive odd form of discriminant 2D. We have a "descent" from regular even forms of odd discriminant D to regular even forms of discriminant 2D.

Remark. More is true. Put aside regularity. Then we actually get a one-to one correspondence between the forms in question. This result is not needed so I skip the easy proof. (Query: has any student of ternary forms noticed this ?) The correspondence preserves genera and so a loner goes to a loner both ways. We already know that regularity of the even form implies regularity of the odd form. The reverse is also true but I have no a priori proof; it simply turned out to be true when all the facts were in. This provided a welcome additional check.

(ii) d even. Now h is an even form of discriminant D/2. If h is primitive we have a reduction from D to D/2. If h is not primitive we move further down to h/2 which is primitive (since a is odd). If h is even it has discriminant D/16 and if it is odd it has discriminant D/4.

Remark. We are paying a price here for not treating odd and even forms uniformly. If we did (i. e., if we multiplied discriminants of even forms by 4) we could say that all descents are divisions by 2 or 16. However, I feel that the price is well worth paying.

By iterating it is clear that any target form will eventually descend to a regular odd form.. But we know all regular odd forms.

Remark. Just this much gives some quick information. For instance, we deduce that the admissible primes for regular even forms must be a subset of those for regular odd forms (see item 4 above); ≤ 17 or 23. In fact 17 does not appear in the even case and the rest do.)

We are ready to proceed: climb up the eligible discriminants till regularity expires. We began doing just that. But after a while it became apparent that it wasn't going to work -- the discriminants would get too large. Now that the facts are in we can see in retrospect how vexing the problem was going to be: the largest even loner has discriminant 338688. And that's not the worst of it. This still has to be raised by 16 to the monstrous 5419008. Impossible.

So an alternate method was sought. Let us review in matrix style what was done above in a descent by 16 from even to even. Write A and C for the matrices upstairs and downstairs. We find

$$4C = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and deduce A = ECE where E is the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

So the ascent back up from C to A is very simple. But wait: we could replace C by an equivalent matrix C* = PCP' and EC*E is an equally acceptable lift. Trouble: there are an infinite number of changes of basis. Is there a way out?

Yes, there is. Set $Q = EPE^{-1}$ so that EP = QE, P'E = EQ'. Then EC*E = EPCP'E = QECEQ'. If Q is an integral matrix, we are getting an equivalent matrix upstairs and all is well. It turns out that the condition for this is that the 12 and 13 entries of P are even.

Let's look at the situation mod 2. The group of 3 by 3 invertible matrices has order 168 and the subgroup with 0 entries in the 12 and 13 positions has order 21 and index 7. Take coset representatives. Then we can restrict our choices of P to integral matrices with determinant ± 1 that map to these 7. Somewhat arbitrarily, the following 7 were picked: the identity matrix and

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

It would have been feasible but very tedious to treat by hand the output, form by form. Fortunately a way was found to virtually automate it. The following is easily seen to be a necessary (but by no means sufficient) condition for an upstairs form g to be regular. Suppose both g and the downstairs form h represent an odd number L and that h represents M with $M \equiv L \pmod 8$; then g has to represent M. This requirement was enforced and skilfully programmed by WCJ. Moreover it was feasible to feed a whole file of forms to the program and go away for a few hours to take a swim. It worked out as follows: most of the output turned out to consist of forms already known. The handful of new ones were treated individually; each was put under a microscope to answer the following questions: What are the other forms in the genus (if any)? Is the form a viable candidate? Can we even prove regularity?

Slight changes produced a program for going up by 2. These successes suggested returning to odd forms to exploit the same ideas. The result: programs for going up by 4, 81, and 3 on odd forms. For 81 and 3, 13 matrices were needed (13 = (3^3 - 1)/2). And then we returned to even forms and ran going up by 81 and 3 on what we regarded as the final list. It was pleasant that no new forms arose. The project closed.

Final remark. In doing the work there was a constant needed for checking whether two forms that look different are actually equivalent. Doubtless there are lots of suitable programs out there somewhere. Not having one available, WCJ wrote one that worked brilliantly. Even with the large discriminants needed here it gave an instant answer, and as a bonus in the case of equivalence it furnished a suitable change of basis. The command word is "siam" (for Siamese twins).

References

1. BI tables.

2. J, K, and S, There are 913 regular ternary forms.

3. IK, Ternary positive quadratic forms that represent all odd positive integers, Acta Arithmetica 70(1995), 209-214.

4. Watson. References 4, 5, and 6 are [8], [10], and [9] in [2].