MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 341–345

THE FIRST NONTRIVIAL GENUS OF POSITIVE DEFINITE TERNARY FORMS

IRVING KAPLANSKY

ABSTRACT. The first nontrivial genus of positive ternary forms has discriminant 7. The paper presents all known results concerning this genus, including some computations.

1. INTRODUCTION

The subject of ternary forms is venerable. In Dickson's History the account begins with Diophantus for the basic case of sums of three squares; for the general ternary form the story begins with Gauss.

There is much to study concerning ternary forms, but in this paper I am concerned only with finding the integers they represent. This topic took a big jump when Jones [1] proved that, taken together, the forms of a genus represent all numbers not ruled out by congruences (I will call these the *eligible* numbers). Thus, attention is confined to genera containing two or more forms.

Despite a history approaching two hundred years, the very first nontrivial case is still not completely understood. In this first case (meaning that the discriminant is smallest) the genus consists of $f = x^2 + y^2 + 7z^2$ and $g = x^2+2y^2+2yz+4z^2$. The eligible numbers are those not of the following form: the product of an odd power of 7 by a number congruent to 3, 5, or 6 mod 7. The problem is to disentangle which eligible numbers are represented by f, which by g, and which by both.

In this paper I collect everything that is known about this problem, including some computations. If the conjectures spawned by the computations are confirmed by theorems some day, our knowledge will be complete.

In remark (a) at the end of the paper I report the result of a computation concerning a question raised by Jones and Pall in [2].

2. THREE THEOREMS

The theorems assert that eligible numbers which satisfy certain congruences are represented, subject to a supplementary condition in the case of Theorem 2. Proofs are presented in §5 below.

Theorem 1. *The form g represents all eligible numbers congruent to* 0 *or* 2 mod 3.

Received by the editor October 12, 1993.
1991 *Mathematics Subject Classification.* Primary 11E20.
Key words and phrases. Ternary form, genus, representations of integers.

©1995 American Mathematical Society
0025-5718/95 $1.00 + $.25 per page

Theorem 2. *The form f represents all eligible multiples of 9; it also represents all numbers congruent to 2 mod 3 which are not of the form $14t^2$.*

Theorem 3. *The forms f and g represent all eligible numbers that are congruent to 0 or 1 mod 4.*

3. A connection with two other forms

The forms $h = x^2 + y^2 + 14z^2$ and $k = x^2 + 2y^2 + 7y^2$ constitute a genus. They have discriminant 14, twice the discriminant of f and g. The two genera have the same eligible numbers.

The forms h and k are so closely connected to f and g that studying them is equivalent to studying f and g. The advantage of making a change is that we avoid the bothersome cross product in g.

Lemma 1. *The form f represents an integer A if and only if h represents $2A$.*

Proof. From $f = A$ we get

$$2A = 2f = 2x^2 + 2y^2 + 14z^2 = (x+y)^2 + (x-y)^2 + 14z^2.$$

Conversely, assume $x^2 + y^2 + 14z^2 = 2A$. Necessarily x and y have the same parity. Write $u = (x+y)/2$, $v = (x-y)/2$. Then $2u^2 + 2v^2 = x^2 + y^2$ and $u^2 + v^2 + 7z^2 = A$. □

Lemma 2. *The form g represents an integer A if and only if k represents $2A$.*

Proof. We have

$$2g = 2x^2 + (2y+z)^2 + 7z^2 = 2A.$$

Conversely, assume $2x^2 + u^2 + 7z^2 = 2A$. Necessarily u and z have the same parity. Write $u = 2y + z$. Then $x^2 + 2y^2 + 2yz + 4z^2 = A$. □

These two lemmas are all we need in this paper. The connection is completed by the following easily proved statement: an odd number A is represented by h (resp. k) if and only if $2A$ is represented by f (resp. g).

4. Computations

In studying the numbers represented by f it is advantageous to introduce the companion form $f^* = x^2 + 7y^2 + 7z^2$. That gives us two forms to study, but we gain a significant simplification: we can ignore multiples of 7, which merely bounce us back and forth between f and f^*. As for the form g, we shall take advantage of Lemma 2 and study k instead, pairing it similarly with $k^* = x^2 + 7y^2 + 14z^2$.

I am greatly indebted to Michael Reid who programmed and ran the following four computations, as well as the one reported in remark (a) at the end of the paper.

List I. Up to 100,000 there are 27 numbers prime to 7 not represented by f: 3, 6, 19, 22, 31, 51, 55, 66, 94, 139, 142, 159, 166, 214, 235, 283, 439, 534, 559, 670, 874, 946, 1726, 2131, 2419, 3559, 4759.

List II. Up to 100,000 there are 26 numbers congruent to 1, 2, or 4 mod 7 which are not represented by f^*: 2, 22, 46, 58, 85, 93, 102, 205, 298, 310, 330, 358, 466, 478, 697, 862, 949, 1222, 1402, 1513, 1957, 1978, 2962, 3502, 7165, 10558.

Nontrivial Definite

The complete list of eligible numbers not represented by f is obtained as follows: multiply List I by any even powers of 7 and List II by any odd powers of 7. A similar remark applies to k.

List III. Up to 100,000 there are 3 numbers prime to 7 not represented by k: 5, 20, 158.

List IV. Up to 100,000 there are 3 numbers congruent to 1, 2, or 4 mod 7 which are not represented by k^*: 2, 74, 506.

If it is proved some day that these four lists are complete, our knowledge of the integers represented by f and g will be complete.

5. Proofs of the theorems

Proof of Theorem 1. In [3] Pall proved that k represents all eligible numbers congruent to 0 or 1 mod 3. By using Lemma 2 we deduce Theorem 1. □

Lemma 1 enables us to replace Theorem 2 by Theorem 2′.

Theorem 2′. *The form h represents all eligible numbers which are multiples of* 9; *it also represents all eligible numbers which are congruent to* 1 mod 3 *but not of the form* $7t^2$.

Proof. The basic idea is Pall's, but I run it backwards, and some additional arguments are needed.

Let A be an eligible number for which we plan to prove representability by h. If k does not represent A, then h does (because h and k together represent all eligible integers). So we may assume that k represents A. We have the following identity:

$$k = x^2 + 2y^2 + 7z^2 = x^2 + (2y + 7z)^2/9 + 14(y - z)^2/9. \tag{1}$$

The left side of (1) represents A and therefore so does the right side. Our goal will be achieved if we can arrange $y \equiv z \pmod 3$, for then $2y + 7z$ and $y - z$ will be divisible by 3 and we will deduce that h represents A. Since we can change the sign of y and/or z, we can alternatively say that the goal is to arrange $y^2 \equiv z^2 \pmod 3$. Since all squares are congruent to 0 or 1 mod 3, failure means that we have either $y^2 \equiv 0$, $z^2 \equiv 1 \pmod 3$ or $y^2 \equiv 1$, $z^2 \equiv 0 \pmod 3$. We now distinguish the two cases of Theorem 2.

Assume that A is divisible by 9. In particular, $x^2 + 2y^2 + 7z^2$ is divisible by 3. We see that $y^2 \equiv 0$, $z^2 \equiv 1$ is ruled out, and we must have $y^2 \equiv 1$, $z^2 \equiv 0$, from which $x^2 \equiv 1$ follows. Then $x^2 + 2y^2$ is divisible by 9. It is known that $u = (x^2 + 2y^2)/9$ is again expressible as $v^2 + 2w^2$. Then $x^2 + 2y^2 + 7z^2$ becomes $(3v)^2 + 2(3w)^2 + 7z^2$. In this expression for A, $3w$ and z are both divisible by 3, and so we have achieved our goal.

Assume $A \equiv 1 \pmod 3$. This time it is $y^2 \equiv 1$, $z^2 \equiv 0 \pmod 3$ that is ruled out. So $y^2 \equiv 0$, $z^2 \equiv 1$ must hold, and $x^2 \equiv 0$ follows. We interrupt the main proof at this point for a lemma. It is probably known, but I could not find a reference.

Lemma 3. *Suppose that r is a nonzero integer divisible by* 3 *and expressible as $s^2 + 2t^2$. Then r can be so written with s and t both prime to* 3.

Proof. The proof is by induction on r and starts with $r = 3$, where it is evident by inspection. It is known that $r/3$ can be written $a^2 + 2b^2$. If $r/3$ is prime

KAPLANSKY, Math. Comp. (1995)

to 3, then it is not possible for a and b both to be divisible by 3. If $r/3$ is divisible by 3, by induction we can even arrange that both a and b are prime to 3. In any event, we can suppose that at least one of a, b is prime to 3. We now write

$$r = 3(a^2 + 2b^2) = (a \pm 2b)^2 + 2(a \mp b)^2. \tag{2}$$

By appropriate choice of sign we can make the two summands on the far right of (2) both prime to 3, as required. □

We return to the proof of Theorem 2. Recall that we had $A = x^2 + 2y^2 + 7z^2$ with x and y both divisible by 3 and z prime to 3. Write $r = x^2 + 2y^2$ and note that r is divisible by 3 (in fact by 9). If $r = 0$ then $A = 7z^2$, which is ruled out by the hypothesis of Theorem 2. So we assume $r \neq 0$. Lemma 3 is applicable, enabling us to write A as $u^2 + 2v^2 + 7z^2$ with u and v prime to 3. Now v and z are both prime to 3, and our goal is achieved. □

Remark. The exceptional case in Theorem 2′ really occurs at least twice: $x^2 + y^2 + 14z^2$ does not represent 7 or 28. But it may be that there are no further exceptions. To scan this numerically, let us switch to Theorem 2. We have that $f = x^2 + y^2 + 7z^2$ does not represent 14. List II shows that up to 700,000 there are no further eligible numbers of the form $14t^2$ that are missed by f (this comes down to the fact that 2 is the only entry in List II which is twice a square).

Proof of Theorem 3. Pall [4, p. 344] stated this theorem without proof. Dennis Estes showed me the following proof, which he kindly allowed me to incorporate in this paper.

Remark. For Theorem 3 it seems to be counterproductive to switch from f, g to h, k, even though we get rid of the cross product term in g.

Let B be an eligible number with $B \equiv 0$ or $1 \pmod 4$. The plan is the usual one. For instance, in proving that f represents B we are entitled to assume that g represents B. The basic identity to be used is

$$f(x, w - 2z, w) = g(x, 2w - z, z), \tag{3}$$

together with the automorphism of g given by

$$g(x, -y - z, z) = g(x, y, z). \tag{4}$$

Now suppose that $g(u, v, w) = B$. If v and w have the same parity, we see from (3) that f represents B. If v is even, use (4) to rewrite $g(u, v, w)$ as $g(u, -v-w, w)$; now the second and third arguments have the same parity, so again all is well. The only remaining case is that where v is odd and w is even. Then in

$$B = u^2 + 2v^2 + 2vw + 4w^2$$

the terms $2vw$ and $4w^2$ are divisible by 4, $2v^2 \equiv 2 \pmod 4$, and $u^2 \equiv 0$ or $1 \pmod 4$. This is incompatible with $B \equiv 0$ or $1 \pmod 4$.

The argument is similar the other way around. We assume that $B = f(u, v, w)$ and seek to prove that g represents B. If v and w have the same parity, (3) does the job. Since f is symmetric in its first two arguments, it is just as good to have u and w with the same parity. Surviving are two

cases: (a) u, v odd and w even, (b) u, v even and w odd. In case (a), $u^2+v^2+7w^2 \equiv 2 \pmod 4$, and in case (b), $u^2+v^2+7w^2 \equiv 3 \pmod 4$. This concludes the proof of Theorem 3. □

Remarks. (a) In [2, p. 181] Jones and Pall discussed the numbers of the form $8n+3$ not represented by $2x^2+4y^2+4yz+9z^2$. They noted 3, 43, and 163 and asked if these were all. Up to 100,000 there is just one more: 907.

(b) John Hsia called my attention to the fact that there are several different conventions for the discriminant of a ternary form. For some of these the nontrivial genus with smallest discriminant consists of $x^2+y^2+3z^2+xz$ and $x^2+y^2+4z^2+xy+xz+yz$. The first of these forms is regular (i.e., it represents all eligible integers); the second is not regular and, as far as I know, there has been no computational exploration of the integers it represents.

Added in proof (June 22, 1994). Recently two anticipations came to my attention. (1) Theorem 3 for the form f appears in Jones's unpublished 1928 University of Chicago Ph.D. thesis. The proof is different. (2) Lemma 3 can be found on page 173 of [2]. It is not stated explicitly but arises in the middle of a proof. The proof is the same.

BIBLIOGRAPHY

1. Burton Jones, *The regularity of a genus of positive ternary quadratic forms*, Trans. Amer. Math. Soc. **33** (1931), 111–124.
2. Burton Jones and Gordon Pall, *Regular and semi-regular positive ternary quadratic forms*, Acta Math. **70** (1939), 165–191.
3. Gordon Pall, *An almost universal form*, Bull. Amer. Math. Soc. **46** (1940), 291.
4. ———, *Representations by quadratic forms*, Canad. J. Math. **1** (1949), 344–364.

MATHEMATICAL SCIENCES RESEARCH INSTITUTE, BERKELEY, CALIFORNIA 94720