Positive definite binary quadratic forms that represent the same primes

William C. Jagy and Irving Kaplansky

Abstract

We exhibit a table of 118 positive definite quadratic forms which, arranged in pairs and triples, represent the same odd primes. Evidence is presented that, after discarding certain trivial pairs, this list may be complete.

1 Introduction

This investigation began with the observation that $x^2 + 9y^2$ and $x^2 + 12y^2$ represent the same primes: those of the form $12n + 1$. This led us to wonder what other such pairs of forms exist.

We have made a partial search and the result appears in Table II at the end of this note. This was achieved by dismissing certain trivial examples and making certain assumptions, as described below.

It is convenient to change our problem slightly by studying forms that represent the same odd primes.

As background we mention a repeatedly rediscovered theorem of Schering: the only forms representing the same numbers are $x^2 + xy + y^2$ and $x^2 + 3y^2$ (up to scaling).

We shorten $ax^2 + bxy + cy^2$ to a, b, c. We call the form odd (even) if b is odd (even). The discriminant is $b^2 - 4ac$.

2 Trivial pairs

Let f be odd with discriminant congruent to 1 $\pmod 8$. It is known that there is a certain even g, with discriminant 4 times that of f, that "sits above" f, and that f and g represent the same odd numbers (a fortiori, the same odd primes). Let us throw in Schering's pair in addition. Next take a even and b odd, with $a < b$. Then a, a, b and $4a, 2a, b$ represent the same odd numbers and the same is true for b, a, b and $b, 2a, 4b$. It would be redundant in our deliberations to include both versions of any of these pairs. We shall discard the top version and keep the lower one.

3 Isoprime forms

It will be convenient to have a name for the crucial property we are studying.

Definition. The forms f and g will be called isoprime if they satisfy the following conditions:

(a) $f \neq g$,

(b) Each is Gauss-reduced with middle coefficient ≥ 0,

(c) Neither is the top version of a trivial pair,

(d) They represent exactly the same odd primes.

We call f isoprime if it is a member of an isoprime pair. "Isoprime triple" is self-explanatory. So far, no isoprime quadruple has surfaced.

4 Bi-idoneal forms

Borrowing Euler's term we call a form idoneal if it is alone in its genus. We call f bi-idoneal if it is either idoneal or its genus consists of f and its opposite. There exists a list of bi-idoneal forms which seems to be complete, but there is as yet no proof of completeness.

The thinking that underlies the restriction to bi-idoneal forms is as follows. In all other cases the forms in a genus split up the relevant primes in a way that is subtle. This (perhaps) makes it unlikely that the primes represented could exactly match the primes represented by some other form.

Here is a fact that simplifies the search (the proof is easy): if two bi-idoneal forms are to represent the same odd primes then the odd primes dividing their discriminants must be the same, ignoring multiplicities.

The search examined all known bi-idoneal forms and identified the isoprime ones. This was done partly by hand, a notorious source of error. To diminish the chance of error the search was done twice, using different methods.

The outcome appears in Table II. There are 56 entries of which 6 (marked by asterisks) are triples. The total number of forms is thus 118.

Table II is sorted out according to the primes dividing the discriminant. Thus in items 2-6 the only odd prime dividing the discriminant is 3. This continues, winding up with 3,5,7 and 13 for the final four items.

5 A general search

To get additional evidence for the completeness of the list in Table II, a search was made that was not restricted to bi-idoneal forms. The method selected was as follows. Fix two odd primes p, q with $p < q$. We collect the forms for which p and q are the first two odd primes represented. There are only a finite number: an upper bound is $(p+1)q$. These were examined and all isoprime pairs were extracted. A program was written to do all of this mechanically and was executed for $q \leq 2237$. The list in Table II reappeared and there were no others.

It turns out that, with one exception, the second odd prime for all the known bi-idoneal forms is less than 1500. The exception is $1, 0, 1848$ (1848 is the largest known idoneal number). This was treated individually. The conclusion: if a known bi-idoneal form is isoprime, it appears in Table II.

The investigation of $1, 0, 1848$ turned up something worth mentioning: it and the form $9, 6, 1849$ represent the same first 43 odd primes before disagreeing on the 44^{th}.

6 Near misses

In the bi-idoneal search 10 "near misses" were observed and collected. They are displayed in Table I. We shall explain what a near miss is by citing the second item on the list: 3,0,8 and 8,8,11. The first form of course represents 3. Delete this. Then the remaining primes represented by 3,0,8 coincide exactly with the primes represented by 8,8,11.

We have nothing to say about the possible completeness of Table I.

	Table I.	10 near misses
1.	1,1,1	1,1,7
2.	3,0,8	8,8,11
3.	3,0,16	~~4,4,9~~ 4,4,19
4.	1,0,5	1,0,25
5.	5,0,8	13,8,32
6.	2,2,23	3,0,20
7.	5,0,9	9,6,26
8.	5,0,24	21,6,29
9.	3,0,80	27,24,32
10.	3,0,56	20,12,27

7 A salute to Bertrand

Here is a narrowly circumscribed problem. Let t be a positive integer. For what values of t is it the case that $1, 0, t$ and $1, 0, 2t$ represent the same primes? This is true for $t = 8$, 24, and 120. Are there any others?

One way of attacking this is a variation on Bertrand's theme. Bertrand "postulated" that (for $t > 1$) there is always a prime between t and $2t$, and this soon became a theorem. Let us demand more: that $1, 0, t$ represents a prime between t and $2t$. Now there are exceptions. A program was written to check this out. Up to 156,123,456 there are 104 exceptions, the last being 41,383. The 37 prime exceptions: 3, 5, 11, 17, 23, 29, 41, 59, 83, 89, 107, 179, 251, 263, 269, 293, 389, 401, 461, 479, 491, 569, 593, 881, 929, 1319, 1619, 1931, 2531, 2789, 3461, 3701, 4919, 5309, 7589, 9749, 26171, are irrelevant for the application. There remain the 67 composite exceptions: 8, 24, 26, 35, 56, 68, 119, 120, 125, 134, 185, 194, 206, 290, 314, 326, 341, 356, 371, 404, 464, 489, 524, 545, 626, 635, 671, 698, 699, 749, 755, 815, 914, 978, 1011, 1141, 1161, 1190, 1205, 1232, 1316, 1529, 1595, 1634, 1760, 1784, 2021, 2546, 3419, 3464, 3485, 3561, 3674, 3746, 3806, 4094, 4616, 4904, 6041, 7061, 7556, 8876, 9974, 12326, 17531, 17786, 43181. After a little attention to these we conclude that up to $t = 156, 123, 456$ the only cases where $1, 0, t$ and $1, 0, 2t$ represent the same primes are $t = 8$, 24, and 120.

A related computation was carried out. Suppose given $1, 0, t$ and $1, 0, u$, with $t < u \leq 100000$. When do they represent the same odd primes? They do for the pairs that appear in Table II and also for $t = 1$, $u = 4$, but not otherwise. Furthermore the first four primes suffice to do the job except for

$t = 86970$, $u = 87810$, for which the fifth prime represented is needed.

Table II. 118 isoprime forms
Triples are marked by an asterisk

1.	1,0,8	1,0,16		
2.*	1,0,24	1,0,48	1,0,72	6A, 7A
3.	1,0,9	1,0,12		
4.	4,4,7	7,2,7		
5.	5,2,5	5,2,29		
6.	8,0,9	9,6,17		
7.	7,6,7	7,4,12		
8.*	7,4,52	7,6,87	7,2,103	30A 31
9.*	11,2,11	11,8,56	11,10,35	18B, 19B
10.*	8,0,15	12,12,23	23,8,32	17D, 21B
11.	1,1,4	1,1,19		
12.	1,0,45	1,0,60		
13.	1,0,120	1,0,240		
14.	4,4,31	15,0,16		
15.	8,8,17	17,14,17		
16.	12,12,13	13,4,28		
17.*	8,8,23	15,6,23	23,4,44	21A, 23A
18.	2,2,11	11,2,23		
19.	11,8,32	11,4,92		
20.	12,12,17	17,4,20		
21.	13,2,13	13,8,40		
22.	5,4,68	5,2,101		
23.	8,0,21	29,12,36		
24.	7,4,76	7,6,39		
25.	13,2,61	13,6,21		
26.	15,12,20	23,12,36		
27.	19,4,28	19,10,43		
28.	8,0,39	15,12,44		
29.	8,8,41	20,12,33		
30.	20,4,23	23,20,44		

Table II is continued on next page

Table II continued

31.*	15,0,56	36,12,71	39,12,44	35C, 36A
32.	11,8,11	11,10,50		
33.	6,6,19	19,16,31		
34.	31,10,55	31,22,31		
35.	8,0,105	32,24,57		
36.	12,12,73	33,12,52		
37.	19,14,91	19,16,136		
38.	28,28,37	37,24,72		
39.	21,0,40	45,30,61		
40.	20,20,47	47,42,63		
41.	8,8,167	32,24,87		
42.	24,0,55	39,36,76		
43.	41,38,41	41,10,65		
44.	33,0,40	52,36,57		
45.	21,12,76	45,30,109		
46.	23,4,68	23,18,207		
47.	28,12,57	72,48,73		
48.	35,30,51	36,12,131		
49.	28,20,85	45,30,157		
50.	51,48,56	59,4,116		
51.	57,6,97	33,24,88		
52.	71,70,95	39,6,71		
53.	55,10,199	159,120,160		
54.	57,18,193	148,132,177		
55.	76,20,145	96,72,241		
56.	88,32,127	127,4,172		

Mathematical Sciences Research Institute
1000 Centennial Drive
Berkeley, CA 94720-5070

jagy@msri.org
kap@msri.org