Lecture 24: Quadratic Forms IV
The Class Group

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

1 Can You Hear the Shape of a Lattice?

After Lecture 23, Emanuele Viola asked me whether or not the following is true: *"If f_1 and f_2 are binary quadratic forms that represent exactly the same integers, is $f_1 \sim f_2$?"* The answer is no. For example, $f_1 = (2,1,3) = 2x^2 + xy + 3y^2$ and $f_2 = (2,-1,3) = 2x^2 - xy + 3y^2$ are inequivalent reduced positive definite binary quadratic forms that represent exactly the same integers. Note that $\mathrm{disc}(f_1) = \mathrm{disc}(f_2) = -23$. There appears to be a sense in which all counterexamples resemble the one just given.

Questions like these are central to John H. Conway's book *The sensual (quadratic) form*, which I've never seen because the Cabot library copy is checked out and the Birkhoff copy has gone missing. The following is taken from the MATHSCINET review (I changed the text slightly so that it makes sense):

> Chapter 2 begins by posing Mark Kac's question of "hearing the shape of a drum", and the author relates the higher-dimensional analogue of this idea on tori—quotients of $\mathbf{R}^n$ by a lattice—to the question of what properties of a positive definite integral quadratic form are determined by the numbers the form represents. A property of such a form is called "audible" if the property is determined by these numbers, or equivalently, by the theta function of the quadratic form. As examples, he shows that the determinant of the form and the theta function of the dual form are audible. He also provides counterexamples to the higher-dimensional Kac question, the first of which were found by J. Milnor...

2 Class Numbers

Proposition 2.1. *Let $D < 0$ be a discriminant. There are only finitely many equivalence classes of positive definite binary quadratic forms of discriminant D.*

Proof. Since there is exactly one reduced binary quadratic form in each equivalence class, it suffices to show that there are only finitely many reduced forms of discriminant D. Recall that if a form (a,b,c) is reduced, then $|b| \le a \le c$. If (a,b,c) has discriminant D then $b^2-4ac = D$. Since $b^2 \le a^2 \le ac$, we have $D = b^2-4ac \le -3ac$, so

$$3ac \le -D.$$

There are only finitely many positive integers a, c that satisfy this inequality. □

Definition 2.2. A binary quadratic form (a, b, c) is *primitive* if $\gcd(a, b, c) = 1$.

Definition 2.3. The *class number* h_D of discriminant $D < 0$ is the number of equivalence classes of primitive positive definite binary quadratic forms of discriminant D.

I computed the following table of class number h_D for $-D \le 839$ using the built-in PARI function `qfbclassno(D,1)`. Notice that there are just a few 1s at the beginning and then no more.

$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D	$-D$	h_D
3	**1**	123	2	243	3	363	4	483	4	603	4	723	4
7	**1**	127	5	247	6	367	9	487	7	607	13	727	13
11	**1**	131	5	251	7	371	8	491	9	611	10	731	12
15	2	135	6	255	12	375	10	495	16	615	20	735	16
19	**1**	139	3	259	4	379	3	499	3	619	5	739	5
23	3	143	10	263	13	383	17	503	21	623	22	743	21
27	**1**	147	2	267	2	387	4	507	4	627	4	747	6
31	3	151	7	271	11	391	14	511	14	631	13	751	15
35	2	155	4	275	4	395	8	515	6	635	10	755	12
39	4	159	10	279	12	399	16	519	18	639	14	759	24
43	**1**	163	**1**	283	3	403	2	523	5	643	3	763	4
47	5	167	11	287	14	407	16	527	18	647	23	767	22
51	2	171	4	291	4	411	6	531	6	651	8	771	6
55	4	175	6	295	8	415	10	535	14	655	12	775	12
59	3	179	5	299	8	419	9	539	8	659	11	779	10
63	4	183	8	303	10	423	10	543	12	663	16	783	18
67	**1**	187	2	307	3	427	2	547	3	667	4	787	5
71	7	191	13	311	19	431	21	551	26	671	30	791	32
75	2	195	4	315	4	435	4	555	4	675	6	795	4
79	5	199	9	319	10	439	15	559	16	679	18	799	16
83	3	203	4	323	4	443	5	563	9	683	5	803	10
87	6	207	6	327	12	447	14	567	12	687	12	807	14
91	2	211	3	331	3	451	6	571	5	691	5	811	7
95	8	215	14	335	18	455	20	575	18	695	24	815	30
99	2	219	4	339	6	459	6	579	8	699	10	819	8
103	5	223	7	343	7	463	7	583	8	703	14	823	9
107	3	227	5	347	5	467	7	587	7	707	6	827	7
111	8	231	12	351	12	471	16	591	22	711	20	831	28
115	2	235	2	355	4	475	4	595	4	715	4	835	6
119	10	239	15	359	19	479	25	599	25	719	31	839	33

We can compute these numbers using Proposition 2.1. The following PARI program enumerates the primitive reduced forms of discriminant D.

```
{isreduced(a,b,c) =
   if(b^2-4*a*c>=0 || a<0,
      error("reduce: (a,b,c) must be positive definite."));
   if(!(abs(b)<=a && a<=c), return(0));
   if(abs(b)==a || a==c, return(b>=0));
   return(1);
}
{reduce(f) =
   local(D, k, t, a,b,c);
   a=f[1]; b=f[2]; c=f[3]; D=b^2-4*a*c;
   if(D>=0 || a<0, error("reduce: (a,b,c) must be positive definite."));
   while(!isreduced(a,b,c),       \\ ! means ‘‘not’’
      if(c<a,
         b = -b; t = a; a = c; c = t,
      \\ else
         if (abs(b)>a || -b==a,
            k = floor((a-b)/(2*a));
            b = b+2*k*a;
            c = (b^2-D)/(4*a);
         )
      )
   );
   return([a,b,c])
}
{reducedforms(D)=
   local(bound, forms, b, r);
   if (D > 0 || D%4 == 2 || D%4==3, error("Invalid discriminant"));
   bound = floor(-D/3);
   forms = [];
   for(a = 1, bound,
      for(c = 1, bound,
         if(3*a*c<=-D && issquare(4*a*c+D),
            b = floor(sqrt(4*a*c+D));
            r = reduce([a,b,c]);
            print1([a,b,c], " ----> ", r);
            if (gcd(r[1],gcd(r[2],r[3])) == 1,
               forms = setunion(forms,[r]); print(""),
               \\ else
               print ("  \t(not primitive)")
            )
         )
      )
   );
   return(eval(forms));    \\ eval gets rid of the annoying quotes.
}
```

For example, when $D = -419$ the program finds exactly 9 reduced forms:

```
? D = -419
%21 = -419
? qfbclassno(D,1)
%22 = 9
? reducedforms(D)
[1, 1, 105] ----> [1, 1, 105]
[1, 3, 107] ----> [1, 1, 105]
[1, 5, 111] ----> [1, 1, 105]
[1, 7, 117] ----> [1, 1, 105]
[1, 9, 125] ----> [1, 1, 105]
[1, 11, 135] ----> [1, 1, 105]
[3, 1, 35] ----> [3, 1, 35]
[3, 5, 37] ----> [3, -1, 35]
[3, 7, 39] ----> [3, 1, 35]
[3, 11, 45] ----> [3, -1, 35]
[5, 1, 21] ----> [5, 1, 21]
[5, 9, 25] ----> [5, -1, 21]
[5, 11, 27] ----> [5, 1, 21]
[7, 1, 15] ----> [7, 1, 15]
[9, 7, 13] ----> [9, 7, 13]
[9, 11, 15] ----> [9, -7, 13]
[13, 7, 9] ----> [9, -7, 13]
[15, 1, 7] ----> [7, -1, 15]
[15, 11, 9] ----> [9, 7, 13]
[21, 1, 5] ----> [5, -1, 21]
[25, 9, 5] ----> [5, 1, 21]
[27, 11, 5] ----> [5, -1, 21]
[35, 1, 3] ----> [3, -1, 35]
[37, 5, 3] ----> [3, 1, 35]
[39, 7, 3] ----> [3, -1, 35]
[45, 11, 3] ----> [3, 1, 35]
[105, 1, 1] ----> [1, 1, 105]
[107, 3, 1] ----> [1, 1, 105]
[111, 5, 1] ----> [1, 1, 105]
[117, 7, 1] ----> [1, 1, 105]
[125, 9, 1] ----> [1, 1, 105]
[135, 11, 1] ----> [1, 1, 105]
%23 = [[1, 1, 105], [3, -1, 35], [3, 1, 35], [5, -1, 21], [5, 1, 21],
       [7, -1, 15], [7, 1, 15], [9, -7, 13], [9, 7, 13]]
? length(%23)
%24 = 9
```

Theorem 2.4 (Heegner, Stark-Baker, Goldfeld-Gross-Zagier). *Suppose D is a negative discriminant that is either square free or 4 times a square-free number. Then*

- $h_D = 1$ *only for* $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$.
- $h_D = 2$ *only for* $D = -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427$.
- $h_D = 3$ *only for* $D = -23, -31, -59, -83, -107, -139, -211, -283, -307, -331, -379, -499, -547, -643, -883, -907$.
- $h_D = 4$ *only for* $D = -39, -55, -56, -68, \ldots, -1555$.

To quote Henri Cohen: "The first two statements concerning class numbers 1 and 2 are very difficult theorems proved in 1952 by Heegner and in 1968–1970 by Stark and Baker. The general problem of determing all imaginary quadratic fields with a given class number has been solved in principle by Goldfeld-Gross-Zagier, but to my knowledge the explicit computations have been carried to the end only for class numbers 3 and 4 (in addition to the already known class numbers 1 and 2).

3 The Class Group

There are *much* more sophisticated ways to compute h_D than simply listing the reduced binary quadratic forms of discriminant D, which is an $O(|D|)$ algorithm. For example, there is an algorithm that can compute h_D for D having 50 digits in a reasonable amount of time. These more sophisticated algorithms use the fact that the set of primitive positive definite binary quadratic forms of given discriminant is a finite abelian group.

Definition 3.1. Let $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ be two quadratic forms of the same discriminant D. Set $s = (b_1 + b_2)/2$, $n = (b_1 - b_2)/2$ and let u, v, w and d be such that

$$ua_1 + va_2 + ws = d = \gcd(a_1, a_2, s)$$

(obtained by two applications of Euclid's algorithm), and let $d_0 = \gcd(d, c_1, c_2, n)$. Define the composite of the equivalence classes of the two forms f_1 and f_2 to be the equivalence class of the form

$$(a_3, b_3, c_3) = \left(d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(v(s - b_2) - wc_2), \frac{b_3^2 - D}{4a_3}\right).$$

This mysterious-looking group law is induced by "multiplication of ideals" in the "ring of integers" of the quadratic imaginary number field $\mathbb{Q}(\sqrt{D})$. The following PARI program computes this group operation:

```
{composition(f1, f2)=
   local(a1,b1,c1,a2,b2,c2,D,s,n,bz0,bz1,u,v,w);
   a1=f1[1]; b1=f1[2]; c1=f1[3];
   a2=f2[1]; b2=f2[2]; c2=f2[3];
   D = b1^2 - 4*a1*c1;
   if(b2^2 - 4*a2*c2 != D, error("Forms must have the same discriminant."));
```

```
    s = (b1+b2)/2;
    n = (b1-b2)/2;
    bz0 = bezout(a1,a2);
    bz1 = bezout(bz0[3],s);
    u = bz1[1]*bz0[1];
    v = bz1[1]*bz0[2];
    w = bz1[2];
    d = bz1[3];
    d0 = gcd(gcd(gcd(d,c1),c2),n);
    a3 = d0*a1*a2/d^2;
    b3 = b2+2*a2*(v*(s-b2)-w*c2)/d;
    c3 = (b3^2-D)/(4*a3);
    f3 = reduce([a3,b3,c3]);
    return(f3);
}
```

Let's try the group out in the case when $D = -23$.

```
? reducedforms(-23)
[1, 1, 6] ----> [1, 1, 6]
[2, 1, 3] ----> [2, 1, 3]
[3, 1, 2] ----> [2, -1, 3]
[6, 1, 1] ----> [1, 1, 6]
%56 = [[1, 1, 6], [2, -1, 3], [2, 1, 3]]
```

Thus the group has elements $(1, 1, 6)$, $(2, -1, 3)$, and $(2, 1, 3)$. Since $h_{-23} = 3$, the group must be cyclic of order 3. Let's find the identity element.

```
? composition([1,1,6],[2,-1,3])
%58 = [2, -1, 3]
```

Thus the identity element must be $(1, 1, 6)$. The element $(2, -1, 3)$ is a generator for the group:

```
? composition([2,-1,3],[2,-1,3])
%59 = [2, 1, 3]
? composition([2,-1,3],[2,1,3])
%60 = [1, 1, 6]
```