BLOG

William C. Jagy

July 16, 2014

I wrote an article with Irving Kaplansky on indefinite binary quadratic forms, integral coefficients. At the time, I believe I used high-precision continued fractions or similar. It took me years to realize that the right way to solve Pell's equation, or find out the "minimum" of an indefinite form (and other small primitively represented values), or the period of its continued fraction, was the method of "reduced" forms in cycles/chains, due to Lagrange, Legendre, Gauss. It is also the cheapest way to find the class number and group multiplication for ideals in real quadratic fields, this probably due to Dirichlet. For imaginary quadratic fields, we have easier "reduced" positive forms.

A binary quadratic form, with integer coefficients, is some

$$f(x,y) = Ax^2 + Bxy + Cy^2.$$

The discriminant is

$$\Delta = B^2 - 4AC.$$

We will abbreviate this by

$$\langle A, B, C \rangle.$$

It is primitive if $\gcd(A,B,C) = 1$. Standard fact, hard to discover but easy to check:

$$(Ax^2 + Bxy + CDy^2)(Cz^2 + Bzw + ADw^2) = ACX^2 + BXY + DY^2,$$

where $X = xz - Dyw$, $Y = Axw + Cyz + Byw$. This gives us Dirichlet's definition of "composition" of quadratic forms of the same discriminant,

$$\langle A, B, CD \rangle \circ \langle C, B, AD \rangle = \langle AC, B, D \rangle.$$

In particular, if this $D = 1$, the result represents 1 and is ($SL_2\mathbf{Z}$) equivalent to the "principal" form for this discriminant. Oh, duplication or squaring in the group; if $\gcd(A, B) = 1$,

$$\langle A, B, AD\rangle^2 = \langle A^2, B, D\rangle.$$

This comes up with positive forms: $\langle A, B, C\rangle \circ \langle A, -B, C\rangle = \langle 1, B, AC\rangle$ is principal, the group identity. Probably should display some $SL_2\mathbf{Z}$ equivalence rules, these are how we calculate when things are not quite right for Dirichlet's rule:

$$\langle A, B, C\rangle \cong \langle C, -B, A\rangle,$$

$$\langle A, B, C\rangle \cong \langle A, B + 2A, A + B + C\rangle,$$

$$\langle A, B, C\rangle \cong \langle A, B - 2A, A - B + C\rangle.$$

Imaginary first. Suppose we want to know about $\mathbf{Q}(\sqrt{-47})$. Reduced positive forms $\langle A, B, C\rangle$ obey $|B| \leq A \leq C$ and $B \neq -A$, also whenever $A = C$ we have $B \geq 0$. Our group of binary forms is

```
-47
  class  number  5

 all
( 1, 1, 12)
( 2, -1, 6)
( 2, 1, 6)
( 3, -1, 4)
( 3, 1, 4)
```

This is an abelian group in any case, so it is cyclic of order 5. These are also the five elements in the ring of integers of $\mathbf{Q}(\sqrt{-47})$. Here is the mapping from forms to ideals: given $\langle A, B, C\rangle$, drop the letter C. That's it.

$$\langle A, B, C\rangle \mapsto \left[A, \frac{B + \sqrt{\Delta}}{2}\right].$$

Oh, why is this an ideal, rather than just some $\mathbf{Z}$-lattice? Because, given α, β rational integers,

$$\left[\alpha, \frac{\beta + \sqrt{\Delta}}{2}\right]$$

is an ideal if and only if

$$4\alpha|(\Delta - \beta^2).$$

Group: we already see how to do

$$\langle 2,1,6\rangle^2 \cong \langle 4,1,3\rangle \cong \langle 3,-1,4\rangle;$$

$$\langle 2,1,6\rangle \circ \langle 3,-1,4\rangle \cong \langle 2,5,9\rangle \circ \langle 3,5,6\rangle \cong \langle 6,5,3\rangle \cong \langle 3,-5,6\rangle \cong \langle 3,1,4\rangle;$$

$$\langle 2,1,6\rangle \circ \langle 3,1,4\rangle \cong \langle 6,1,2\rangle \cong \langle 2,-1,6\rangle.$$

$$\langle 2,1,6\rangle \circ \langle 2,-1,6\rangle \cong \langle 1,1,12\rangle$$

in any case.

There are a few extra tricks for indefinite forms. The right way to calculate things is to use "reduced" forms. The definition of $\langle A,B,C\rangle$ being reduced is

$$0 < B < \sqrt{\Delta}, \text{ and } \sqrt{\Delta} - B < 2|A| < \sqrt{\Delta} + B,$$

this being equivalent to

$$0 < B < \sqrt{\Delta}, \text{ and } \sqrt{\Delta} - B < 2|C| < \sqrt{\Delta} + B.$$

If you actually calculate enough Conway topographs, you realize eventually that

THEOREM $\langle A,B,C\rangle$ is reduced if and only if

$$AC < 0 \text{ and } B > |A + C|$$

I have never seen this in print, it should be attributed to Conway or to Jagy or to Marty Weissman of UC Santa Cruz and Singapore; Conway knows much more than he writes down. With the required relation

$$B^2 - 4AC = \Delta$$

and evident inequalities, this gives a quick way to find all reduced forms.

Now, different reduced forms may be equivalent, which sounds bad, but the cycle method quickly decides these relationships. No decimal accuracy or "cycle detection" is ever required. A single calculation is done, $\left\lfloor \sqrt{\Delta} \right\rfloor$ and remembered forever. I actually wrote Newton's square root method with integer arithmetic. Everything else, forever, is integer arithmetic. Given a

form $\langle A, B, C\rangle$ we want to find its "right neighbor." First, we find a nonzero integer I like to call δ, with

$$\delta C > 0 \text{ and } |\delta| = \left\lfloor \frac{B + \left\lfloor \sqrt{\Delta} \right\rfloor}{2|C|} \right\rfloor .$$

The absolute values of the δ's are the partial quotients in the continued fraction of, well, something. Note that B and $\left\lfloor \sqrt{\Delta} \right\rfloor$ are positive.

Alright, given a δ, the form and its right neighbor are

$$\langle A, B, C\rangle \to \langle C, -B + 2C\delta, A - B\delta + C\delta^2\rangle.$$

For those who know what a Gram matrix is, call it G, the Gram matrix of the right neighbor is $P^T G P$, where

$$P = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}.$$

Keeping a cumulative product of these P matrices is how we solve Pell, quickly and without tears. Note that the first computer they gave me was called phoebus after Phoebus Apollo, this was intended to be phoebusjunior but the spelling went sideways.

```
jagy@phobeusjunior:~/old drive/home/jagy/Cplusplus$ ./Pell 61


0  form   1 14 -12   delta  -1
1  form   -12 10 3   delta  4
2  form   3 14 -4   delta  -3
3  form   -4 10 9   delta  1
4  form   9 8 -5   delta  -2
5  form   -5 12 5   delta  2
6  form   5 8 -9   delta  -1
7  form   -9 10 4   delta  3
8  form   4 14 -3   delta  -4
9  form   -3 10 12   delta  1
10  form   12 14 -1   delta  -14
11  form   -1 14 12   delta  1
12  form   12 10 -3   delta  -4
```

```
13  form   -3 14 4   delta  3
14  form   4 10 -9   delta  -1
15  form   -9 8 5   delta  2
16  form   5 12 -5   delta  -2
17  form   -5 8 9   delta  1
18  form   9 10 -4   delta  -3
19  form   -4 14 3   delta  4
20  form   3 10 -12   delta  -1
21  form   -12 14 1   delta  14
22  form   1 14 -12

 disc   244
Automorph, written on right of Gram matrix:
183241189  2713847760
226153980  3349396909


 Pell automorph
1766319049  13795392780
226153980    1766319049

Pell unit
1766319049^2 - 61 * 226153980^2 = 1

========================================

Pell NEGATIVE
29718^2 - 61 * 3805^2 = -1

========================================

  4 PRIMITIVE
1523^2 - 61 * 195^2 = 4

========================================

  -4 PRIMITIVE
39^2 - 61 * 5^2 = -4
```

==========

Here we are using

$$\langle 1, 0, -61 \rangle \cong \langle 1, 14, -12 \rangle.$$

It begins with $\langle 1, 14, -12 \rangle$ and does not end until it gets $\langle 1, 14, -12 \rangle$ again, this being guaranteed. No floating point reals anywhere, no decimal accuracy, no doubts. Think Gwen Stefani. Note that "Automorph" is a traditional word for the matrix P when $P^T G P = G$.

Ideals; with positive prime discriminant $p \equiv 1 \pmod 4$, the principal form always represents both 1 and -1, and, just as with positive forms, the mapping to ideals is a bijection a group isomorphism. I did some example with class number above one:

```
jagy@phobeusjunior: ./indefCycle_All_Reduced 229

   1.             1          15          -1   cycle length  2
   2.             3          13          -5   cycle length  6
   3.             5          13          -3   cycle length  6

  form class number is   3


jagy@phobeusjunior: ./indefCycle_All_Reduced 257

   1.             1          15          -8   cycle length  6
   2.             2          15          -4   cycle length  6
   3.             4          15          -2   cycle length  6

  form class number is   3

jagy@phobeusjunior: ./indefCycle_All_Reduced 401

   1.             1          19         -10   cycle length  6
   2.             2          19          -5   cycle length  6
   3.             5          19          -2   cycle length  6
   4.             4          17          -7   cycle length 10
```

```
    5.             7          17          -4   cycle length 10

  form class number is   5

jagy@phobeusjunior:
```

Now, if the discriminant is divisible by any prime $q \equiv 3 \pmod 4$, or we just have bad luck with the prime factors $p \equiv 1 \pmod 4$, then the principal form does not represent -1 and the mapping from forms to ideals becomes two to one. I really thought there was a big mystery, but no. Here is an example $\Delta = 5 \cdot 13 \cdot 17 \cdot 41 = 45305$. There are 316 reduced forms collected into 16 cycles:

```
jagy@phobeusjunior: ./indefCycle_All_Reduced 45305
45305    factored   5 * 13 * 17 *  41

    1.             1         211        -196   cycle length 12
    2.            -1         211         196   cycle length 12
    3.             2         211         -98   cycle length 16
    4.            -2         211          98   cycle length 16
    5.             7         211         -28   cycle length 18
    6.            -7         211          28   cycle length 18
    7.            14         211         -14   cycle length 20
    8.           -14         211          14   cycle length 20
    9.             5         205        -164   cycle length 20
   10.            -5         205         164   cycle length 20
   11.            10         205         -82   cycle length 24
   12.           -10         205          82   cycle length 24
   13.            13         195        -140   cycle length 22
   14.           -13         195         140   cycle length 22
   15.            26         195         -70   cycle length 26
   16.           -26         195          70   cycle length 26

  form class number is   16

jagy@phobeusjunior:
```

My software tends to report, for each cycle, a form with particularly large B. Now, as you can see, $\langle 1, 211, -196\rangle$ and $\langle -1, 211, 196\rangle$ are distinct $SL_2\mathbf{Z}$ classes, distinct cycles.

When this happens, in slang I like $1 \neq -1$, we can prove that

$$\langle A, B, -C\rangle$$

and

$$\langle -A, B, C\rangle$$

are ALWAYS DISTINCT $SL_2\mathbf{Z}$ classes. Because, you see,

$$\langle -1, B, AC\rangle \circ \langle A, B, -C\rangle = \langle -A, B, C\rangle.$$

So, the mapping to ideals says IDENTIFY $\langle A, B, -C\rangle$ and $\langle -A, B, C\rangle$, send them to the same ideal. Why not? We already have an equality of ideals in

$$\left[A, \frac{B+\sqrt{\Delta}}{2}\right] = \left[-A, \frac{B+\sqrt{\Delta}}{2}\right].$$

So, we just take the form from each pair with positive A, which cuts the form class number by half, down from 16 to 8, and the ideals are

$$\left[1, \frac{211+\sqrt{45305}}{2}\right],$$

$$\left[2, \frac{211+\sqrt{45305}}{2}\right],$$

$$\left[7, \frac{211+\sqrt{45305}}{2}\right],$$

$$\left[14, \frac{211+\sqrt{45305}}{2}\right],$$

$$\left[5, \frac{205+\sqrt{45305}}{2}\right],$$

$$\left[10, \frac{205+\sqrt{45305}}{2}\right],$$

$$\left[13, \frac{195+\sqrt{45305}}{2}\right],$$
$$\left[26, \frac{195+\sqrt{45305}}{2}\right].$$

One other valuable idea that I can impart here is that of genus. If you check, with either the forms or the ideals, you will find that each one squares to the identity. We say that each genus has only one class. It follows automatically the=at the ideal class group is not cyclic, it is $(\mathbf{Z}/2\mathbf{Z})^3$. I worked a fair amount to get the group table, then I thought, why not just use the Legendre symbols? And that works perfectly.

	5	13	17	41
1	+	+	+	+
2	−	−	+	+
7	−	−	−	−
14	+	+	−	−
$5 \to 46$	+	−	−	+
$10 \to 23$	−	+	−	+
$13 \to 38$	−	+	+	−
$26 \to 19$	+	−	+	−

As you can see, if the first coefficient has a common divisor with the discriminant, we switch to some other number represented by the quadratic form. This table, because there is just one class per genus, immediately tells the multiplication. Just multiply the Legendre symbols for each factor $5, 13, 17, 41$.

The Cohen-Lenstra heuristics say that the vast majority of class groups are cyclic. I did an example where that works, despite having more than one genus. Here, most forms do not square to the identity.

```
jagy@phobeusjunior: ./indefCycle_All_Reduced 1345
1345    factored   5 *  269

    1.             1          35         -30   cycle length  6
    2.            -1          35          30   cycle length  6
    3.             2          35         -15   cycle length  8
    4.            -2          35          15   cycle length  8
    5.             3          35         -10   cycle length  8
```

```
 6.          -3          35          10   cycle length  8
 7.           4          33         -16   cycle length 10
 8.          -4          33          16   cycle length 10
 9.           8          33          -8   cycle length 10
10.          -8          33           8   cycle length 10
11.          16          33          -4   cycle length 10
12.         -16          33           4   cycle length 10

 form class number is   12

jagy@phobeusjunior:~/old drive/home/jagy/Cplusplus$
```

Now, as forms,

$$\langle 8, 33, -8 \rangle^2 = \langle 64, 33, -1 \rangle$$

is minus the identity. However, as ideals this is identified with the principal class. I worked it all out, the multiplication table is

	1	4	16	8	2	3
1	1	4	16	8	2	3
4	4	16	1	2	3	8
16	16	1	4	3	8	2
8	8	2	3	1	4	16
2	2	3	8	4	16	1
3	3	8	2	16	1	4

I placed outlines around the two genera; $1, 4, 16$ are quadratic residues (mod 5) and (mod 269). Then $8, 2, 3$ are nonresidues. The group is cyclic, either 2 or 3 is a generator.

Finally, something quite tricky. The ideal viewpoint identifies the quadratic forms $\langle 1, 13, -13 \rangle$ and $\langle -1, 13, 13 \rangle$ of discriminant $221 = 13 \cdot 17$. However, the traditional concern is to find out the (positive) primes integrally represented by a form. This then moves to what is called class field theory; the primes represented by $\langle 1, 13, -13 \rangle$ are those (answer by Noam Elkies) for which

$$x^8 + 34x^6 + 83x^4 + 34x^2 + 1 \pmod{p}$$

factors into all linear factors. Put another way, $\langle 1, 13, -13 \rangle$ represents 17 and all primes $(p|13) = (p|17) = 1$ such that

$$x^4 + x^3 + x^2 + 2x + 4 \pmod{p}$$

factors into all linear factors. Go Figure. In comparison, the primes represented by $\langle 5, 11, -5\rangle$ are simply all those that are quadratic nonresidues (mod 13) and (mod 17), becuase the other class in its (form) genus is $\langle -5, 11, 5\rangle$ which represents exactly the same numbers. Oh, and this is a Markov form: the nonzero number represented of smallest absolute value is 5, which is called the "minimum" and might be written m. Then, $\Delta/m^2 = 221/25 = 8.84 < 9$, which means this must be a Markov form, parametrised by the Markov Numbers, which include 5. There is considerable rigidity when $9m^2 > \Delta$, i.e. extremely large minimum.