Binary Quadratic Forms and Hecke Operators for $\mathrm{SL}_2(\mathbb{Z})$

Mark McConnell

Princeton University

October 13, 2021

Joint with Erik Bahnson and Kyrie McIntosh.

Background

Let $\mathbf{G}$ be the algebraic group SL_n of a finite-dimensional division algebra D over $\mathbb{Q}$, possibly commutative. Let $G = \mathbf{G}(\mathbb{R})$.

In most of this talk, D will be $\mathbb{Q}$, so $G = \mathrm{SL}_n(\mathbb{R})$ as usual.

$X = G/(\mathrm{maxl\ cpct}) =$ Riemannian symmetric space.
$\Gamma \subset G$ arithmetic subgroup.
$\Gamma \backslash X$ locally symmetric space.

A rational finite-dimensional representation of G gives a representation of Γ, hence a local system $\mathcal{M}$ on $\Gamma \backslash X$. Will suppose $\mathcal{M}$ satisfies integrality conditions so that Hecke operators are defined.

Goal

Compute the Hecke operators on $H^*(\Gamma \backslash X; \mathcal{M})$.

Computations using the Well-Rounded Retract

Avner Ash and his collaborators have done such computations
for $G = \mathrm{SL}_3(\mathbb{R})$ and $\mathrm{SL}_4(\mathbb{R})$
for a range of subgroups Γ and coefficient systems $\mathcal{M}$.

Compute a range of Hecke operators on the cohomology,
identify Hecke eigenclasses,
and identify Galois representations which match the Hecke data
and therefore are (conjecturally) attached to the eigenclasses.

Ash–Gunnells–M. have a series of papers for SL_4.

Based on the *well-rounded retract*, which we now recall.

Consider $\mathbb{R}^n$ with a positive-definite quadratic form.
Lattice $L \subset \mathbb{R}^n$ of rank n.
Arithmetic minimum $m(L) = \min\{\|x\| : x \in L,\, x \neq 0\}$.
The *minimal vectors* of L are $\{x \in L : \|x\| = m(L)\}$.
L is *well rounded* if its minimal vectors span $\mathbb{R}^n$.
Let $W \subset X$ be the space of bases of well-rounded lattices.

Theorem (Ash, late 1970s)

- *There is an* $\mathrm{SL}_n(\mathbb{Z})$*-equivariant deformation retraction* $X \to W$. *Call* W *the* well-rounded retract.
- $\dim W = \dim X - (n-1) = \binom{n}{2}$, *the virtual coh'l dim (vcd).*
- W *is a locally finite regular cell complex. Cells characterized by coords in* $\mathbb{Z}^n$ *of their minimal vectors w.r.t. the basis.*
- $\Gamma\backslash W$ *is a finite cell complex.*

W is dual to Voronoi's decomposition of X into polyhedral cones via *perfect forms*.
The vertices of the retract W are the perfect forms.
Ash [1984] generalizes this to $\mathbf{G} = \mathrm{SL}_n$ over any D.

The Ash–Rudolph algorithm computes the Hecke operators on H^i when $i = \mathrm{vcd}$.

An algorithm of Gunnells computes the Hecke operators on H^i for $i = \mathrm{vcd} - 1$.

The Well-Tempered Retract

Robert MacPherson and I introduced an algorithm
for Hecke operators on $H^i(\Gamma\backslash X; \mathcal{M})$
for $\mathbf{G} = \mathrm{SL}_n$ for any n
over any finite-dimensional division algebra D over $\mathbb{Q}$
and for all i.

This talk will take $G = \mathrm{SL}_n(\mathbb{R})$ and $\Gamma \subseteq \mathrm{SL}_n(\mathbb{Z})$, for simplicity.

I have working code for $\Gamma \subseteq \mathrm{SL}_n(\mathbb{Z})$ for $n = 2, 3, 4$.

ArXiv paper, 2020, for general D.
Case of $G = \mathrm{SL}_n(\mathbb{R})$ in Galt–M., *Tbilisi Math. Journal*.

Our algorithm uses the *well-tempered retract*,
an extension of the well-rounded retract from [Ash 1984],
which will be described on the next few slides.

Let ℓ be a prime. Let $k \in \{1, \ldots, n\}$ $\rightsquigarrow$ Hecke operator $T(\ell, k)$.
Consider $X \times [1, \ell]$. Second coordinate called τ, the *temperament*.
In each slice of $X \times [1, \ell]$ for a given τ,
we will perform a variant of the well-rounded retraction.

Let $L \subset \mathbb{R}^n$ be any lattice of rank n.
Take $M \subset L$, a sublattice with $L/M \cong (\mathbb{Z}/\ell\mathbb{Z})^k$.

Definition

$y \in L$ has *tempered length* $\begin{cases} \tau \cdot \|y\| & \text{if } y \notin M \\ \|y\| & \text{if } y \in M. \end{cases}$

Do well-rounded retraction with this notion, in each τ-slice separately. Get $\tilde{W} \subset X \times [1, \ell]$, the *well-tempered retract*.

Let $\tilde{W}_\tau$ be the slice of $\tilde{W}$ at τ.

$\tilde{W}_1$ is the well-rounded retract.
$\tilde{W}_\ell$ is the well-rounded retract twisted by $\mathrm{diag}(1, \ldots, 1, \underbrace{\ell, \ldots, \ell}_{k})$.

$\tilde{W}$ interpolates between $\tilde{W}_1$, which makes L well rounded, and $\tilde{W}_\ell$, which makes M well rounded.

The Γ-action preserves the slices.

As τ goes from 1 to ℓ, there is a finite number of *critical temperaments* where the cell structure abruptly changes.

Movie of $T(5, 1)$ for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Theorem

$\tilde{W}$ is a locally finite regular cell complex of dim $\mathrm{vcd}+1$. Cells characterized by coords in $\mathbb{Z}^n$ of their minimal vectors in both L and M together with intervals in τ. $\Gamma\backslash\tilde{W}$ is a finite cell complex.

Let $\Gamma_0(\ell, k) \subset \mathrm{SL}_n(\mathbb{Z})$ be $\equiv \left[\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right]$ mod ℓ, lower-right block $k \times k$.

Definition

The *Hecke operator* $T(\ell, k)$ is $p_* q^*$ on the cohomology of

$$\begin{array}{c} (\Gamma \cap \Gamma_0(\ell, k))\backslash\tilde{W} \\ p\downarrow \quad \downarrow q \\ \Gamma\backslash W \end{array}$$

p is the projection onto $\tilde{W}_1$.
q is the twisted projection onto $\tilde{W}_\ell$.
$T(\ell, k)$ is computed by p_* on $\Gamma\backslash\tilde{W}_1$ on left, q^* on $\Gamma\backslash\tilde{W}_\ell$ on right.
Computation interpolates between these by the cells in the middle.

One approach to computing $\tilde{W}$ is to compute a bounded subset of a polytope $\tilde{\Pi}$ dual to $\tilde{W}$, the *Hecketope*.
This is the Voronoi polyhedron (Ryskov polyhedron),
adapted with one extra dimension for the temperament.

I used Sage's class `Polyhedron` over $\mathbb{Q}$.
But $\dim \tilde{\Pi} = n(n+1)/2 + 1$ is big.
Must choose the bounds large enough to get all cells mod Γ.
Computation is delicate as ℓ grows, even for $n = 3$.
Slow for $n = 4$.

Goal for this project

Understand the cells of $\tilde{W}$ intrinsically,
without computing with $\tilde{\Pi}$.

Tempered Perfect Forms

It suffices to understand the *vertices* of $\tilde{W}$,
because we can compute all other cells from them.

Given a set of vertices, take the intersection of their minimal vectors and check by linear algebra what kind of cell they determine (edge, 2-cell, ...).

Vertices occur only at critical temperaments.

Just as the vertices of the well-rounded retract are perfect forms,

Definition

Vertices of the well-tempered retract are *tempered perfect forms*.

Proposition

A tempered perfect form has rational Gram matrix and rational τ^2.

Case of SL_2

For the rest of the talk, specialize to the classical case of
$G = \mathrm{SL}_2(\mathbb{R})$.
$\Gamma = \mathrm{SL}_2(\mathbb{Z})$ for simplicity.

$k = 1$, so $M \subset L$ with index ℓ.
Hecke operators denoted $T_\ell = T(\ell, 1)$.

Result

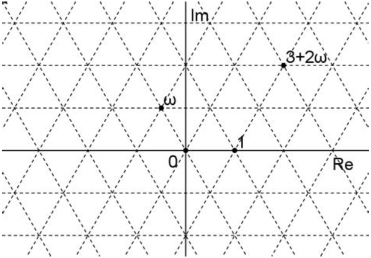
We have a description of tempered perfect forms
in terms of binary quadratic forms
and their class field theory.

3-and-1 Forms, 3-and-3 Forms

Sometimes three vectors in L are minimal vectors.
Then we have a perfect form on L already.
The only perfect form for $n = 2$ is for the hexagonal lattice,
Change coordinates so $L = \mathbb{Z}[\omega]$ with $\omega^2 + \omega + 1 = 0$.

At least one vector in M must also be tempered-minimal.
$\Rightarrow \tau^2$ must be the *norm* of some $\alpha \in \mathbb{Z}[\omega]$.

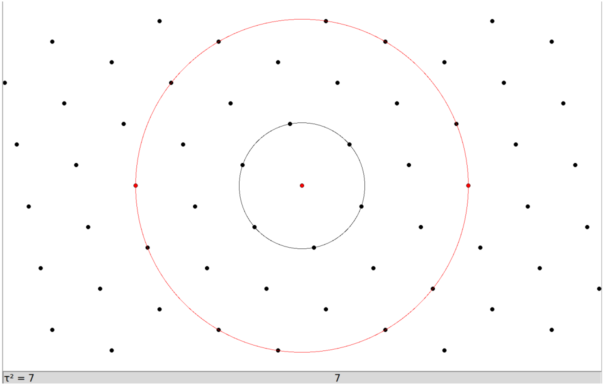
The norm $|a + b\omega|^2 = a^2 - ab + b^2$.
In the picture, $|3 + 2\omega|^2 = 7$.



$\alpha = 3 + 2\omega$ of norm 7 gives rise to tempered perfect forms for T_ℓ for all $\ell \geqslant 7$.

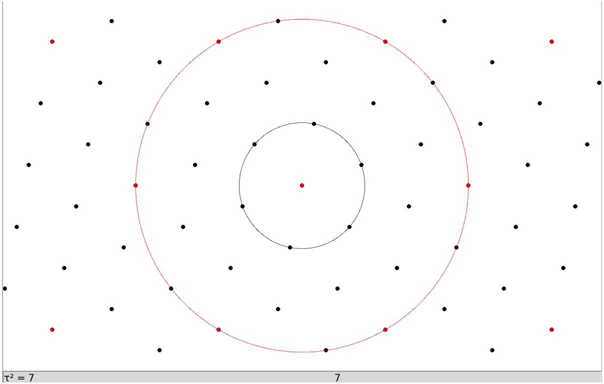
Here is a vertex in the well-tempered retract for T_{11}.
$L \cong \mathbb{Z}[\omega]$ is the lattice. M is a sublattice of index 11.
It is a *3-and-1 form*: 3 pairs of minimal vectors in L, 1 pair in M.

τ is always the ratio of the radii of the circles. Here $\tau = \sqrt{7}$.



When $|\alpha|^2$ happens to $= \ell$, we get a *3-and-3 form*:
3 pairs of minimal vectors in L, 3 pairs in M,
at the *middle* critical temperament $\tau = \sqrt{\ell}$,
the geometric mean $\sqrt{\ell} \in [1, \ell]$.

Example for $\alpha = 3 + 2\omega$ and T_7:



A prime ℓ is the norm of an element of $\mathbb{Z}[\omega]$ iff $\ell = 3$ or $\ell \equiv 1 \pmod 6$.

Corollary

When $\ell = 3$ or $\ell \equiv 1 \pmod 6$, the well-tempered retract for T_p has, at $\tau^2 = \ell$,

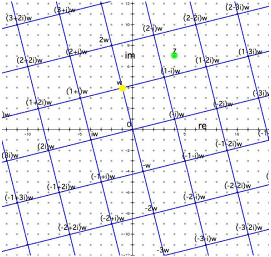
- vertices that are 3-and-1 forms, for every prime $p > \ell$,
- vertices that are 3-and-3 forms, when $p = \ell$.

The Gaussian Integers

Other vertices of $\tilde{W}$ have two pairs of minimal vectors in L
and two pairs in M.
These are *2-and-2 forms*, or *doubly well-rounded* lattices.

For example, the Gaussian integers give 2-and-2 forms
with 90° between the two minimal vectors in L
and 90° between the two in M.

Here the fine grid is $L = \mathbb{Z}[i]$.
The large grid is $M = (-1 + 4i)L$, where $-1 + 4i$ has norm 17.



Fermat: a prime ℓ is the sum of two squares
iff $\ell = 2$ or $\ell \equiv 1 \pmod 4$.

Since M as well as L has a *basis* of minimal vectors,
$|\alpha|^2$ must equal $[L : M]$. Hence

Corollary

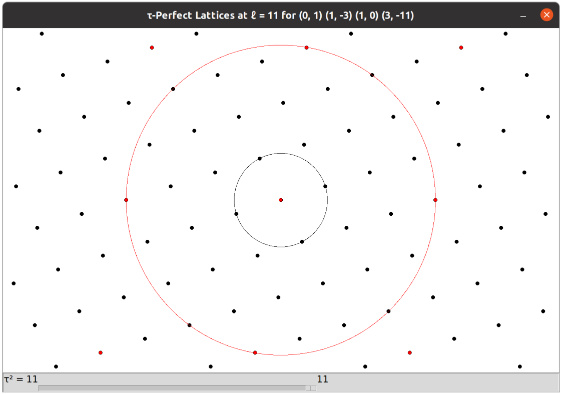
When $\ell = 2$ or $\ell \equiv 1 \pmod 4$, the well-tempered retract for T_ℓ
has vertices that are 2-and-2 forms coming from $\mathbb{Z}[i]$
at the middle temperament $\tau = \sqrt{\ell}$.

Other 2-and-2 Forms

Even for small ℓ we see 2-and-2 forms not based on equilateral triangles or squares.

Example

T_{11} at the middle temperament $\tau = \sqrt{11}$.
The lattice vectors have coordinates in $\mathbb{Q}(\sqrt{-35})$, with $35 = 5 \cdot 7$.

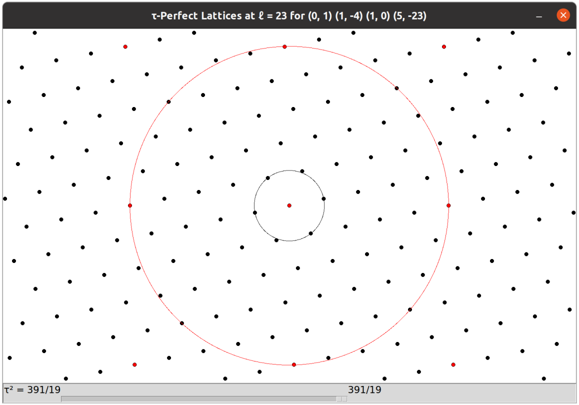


We knew something cool was going on when we found a 2-and-2 form with *non-integer* τ^2 and *different* angles on the two circles.

Example

$\ell = 23$. $\tau^2 = \frac{391}{19} = \frac{17 \cdot 23}{19}$.

Vectors have coordinates in $\mathbb{Q}(\sqrt{-1155})$, where $1155 = 3 \cdot 5 \cdot 7 \cdot 11$.



Review of Binary Quadratic Forms

Consider positive-definite quadratic forms for $x, y \in \mathbb{Z}$,
$ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$ primitive (gcd 1).
Discriminant $D = b^2 - 4ac$.
$D < 0$ throughout this talk.

Correspondence between forms and certain rank-2 lattices in $\mathbb{C}$,

$$ax^2 + bxy + cy^2 \quad \leftrightarrow \quad \mathbb{Z}\left\langle 1, \frac{-b + \sqrt{D}}{2a} \right\rangle .$$

The lattice is a *fractional ideal* contained in $K = \mathbb{Q}(\sqrt{D})$.

Let $\mathcal{O}_K$ be the ring of integers of K, of discriminant $d_K < 0$.
$\mathcal{O}_K = \mathbb{Z}[r]$.[1]

An *order* $\mathcal{O} \subseteq \mathcal{O}_K$ is a subring which contains 1 and has rank 2.

$\mathcal{O}_K$ is the maximal order.
Every order is $\mathcal{O} = \mathbb{Z}[fr]$ for an integer $f \geqslant 1$.
This $\mathcal{O}$ has discriminant $D = f^2 d_K$. Conversely, D determines $\mathcal{O}$.

For a rank-2 lattice L in K, the *order for L* is
the ring of all $\alpha \in K$ satisfying $\alpha L \subseteq L$.
This ring *is* an order.
We say L has *complex multiplication*.

[1] $r = \frac{1+\sqrt{d_K}}{2}$ when $d_K \equiv 1 \pmod 4$. $r = \frac{\sqrt{d_K}}{2}$ when $d_K \equiv 0 \pmod 4$.

The product of two lattices (fractional ideals) of K having order $\mathcal{O}$ has the same order $\mathcal{O}$.
(False in general for cubic and higher fields.)

If a lattice $\subseteq$ its order $\mathcal{O}$, define its *norm* to be its index in $\mathcal{O}$. These norms are multiplicative.

Say lattices L_1, L_2 are *similar* if $L_2 = \alpha L_1$ for $\alpha \in K$, $\alpha \neq 0$.

Theorem (Lagrange, Legendre, Gauss): The similarity classes of lattices in K having a given order $\mathcal{O}$ form a finite abelian group under multiplication, the *class group of $\mathcal{O}$*.

Our proofs sometimes use lattices, sometimes $ax^2 + bxy + cy^2$.
The form $ax^2 + bxy + cy^2$ for L has the same D as the order for L.
Quadratic forms are *equivalent* if they differ by an $\mathrm{SL}_2(\mathbb{Z})$ change of coords.
Equivalent forms $\leftrightarrow$ similar lattices. Class groups are $\cong$.
See Appendix for more of the $ax^2 + bxy + cy^2$ perspective.

Well-Rounded Classes

Proposition

A lattice in K is well rounded iff every similar lattice is well rounded.

In $\mathbb{C}$, multiplication by α is a rotation times a homothety.

We change our thinking from well-rounded lattices
to *well-rounded classes* in the class group of an order $\mathcal{O}$.

This and the next theorem are the heart of our classification of 2-and-2 forms.

As before, $M \subset L$ with prime index ℓ.

Proposition

If $M \subset L$ is a tempered 2-and-2 perfect form, then L and M have the same order $\mathcal{O}$.

Theorem

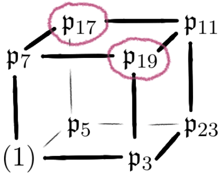
Fix a discriminant $D < 0$. Let $\mathcal{O}$ be the order of discriminant D. Let $\mathcal{C}_1$, $\mathcal{C}_2$ be well-rounded classes in the class group of $\mathcal{O}$. Suppose there is a class $\mathcal{L}$ in which some lattice has norm ℓ in $\mathcal{O}$. Then there is a 2-and-2 form $M \subset L$ in the well-tempered retract for T_ℓ where the minimal vectors in L are a basis of a well-rounded lattice of class $\mathcal{C}_1$, and the minimal vectors in M are a basis of a well-rounded lattice of class $\mathcal{C}_2$.

$$\tau^2 = \ell \cdot \frac{\mathrm{norm}(L)}{\mathrm{norm}(M)}.$$

Conversely, every 2-and-2 form arises in this way for some D.

Example of $D = -1155$

D belongs to the maximal order $\mathcal{O}_K = \mathbb{Z}[r]$ with $r = \frac{1+\sqrt{-1155}}{2}$.
$K = \mathbb{Q}(\sqrt{-1155})$. Recall $1155 = 3 \cdot 5 \cdot 7 \cdot 11$.
The class group of $\mathcal{O}_K$ is $(\mathbb{Z}/2\mathbb{Z})^3$. Draw it as a cube.



$\mathfrak{p}_p$ is a prime ideal of $\mathcal{O}_K$ of prime norm p.
The ramified $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$ generate the group (x, y, z axes).
In each of the eight classes, the $\mathfrak{p}_p$ with smallest p is shown.
Exactly two of the eight classes are well rounded, $\mathfrak{p}_{17}$ and $\mathfrak{p}_{19}$.
$\mathfrak{p}_{17} \cdot \mathfrak{p}_{23} \sim \mathfrak{p}_{19}$. This explains page 22.

Idea

Each discriminant D defines a finite number (zero or more) of "patterns" that a 2-and-2 vertex in $\tilde{W}$ can have.

For a given class $\mathcal{C}$ in the class group of $\mathcal{O}$, there are infinitely many primes ℓ such that $\mathcal{C}$ has an ideal of norm ℓ.

Therefore each "pattern" will occur for infinitely many ℓ.

Example of $D = -1155$

This D gives a 2-and-2 form iff $\mathfrak{p}_\ell$ is split and $\sim (1)$ or $\sim \mathfrak{p}_{23}$.
$\mathbb{Z}/1155\mathbb{Z}$ has $\varphi(1155) = 480$ units. 240 give $\mathfrak{p}_\ell$ that split.
8 classes $\Rightarrow$ 30 elements per class.
$\mathfrak{p}_\ell \sim (1)$ (resp., $\mathfrak{p}_\ell \sim \mathfrak{p}_{23}$) iff $\ell \equiv$ the following mod 1155:

$$1, 4, 16, 64, 169, 214, 256, 289, 331, 361, 379, 394, 421, 466, 499,$$
$$526, 529, 631, 676, 694, 709, 751, 841, 856, 949, 961, 991, 1024, 1054, 1114;$$
$$23, 53, 92, 113, 137, 158, 212, 218, 302, 317, 323, 368, 422, 443, 452,$$
$$533, 548, 617, 632, 653, 683, 848, 863, 872, 947, 977, 1037, 1082, 1103, 1142.$$

To compute T_ℓ for a given ℓ, we need a finiteness theorem in the converse direction.
We need to know that, for a given ℓ, only finitely many patterns can arise, and which ones.

This converse is another part of our main result.

Theorem

Given ℓ, 2-and-2 vertices will appear in the well-tempered retract for T_ℓ only for discriminants D with

$$|D| < 4\ell^2.$$

In the cases we have seen so far, the ℓ have been determined by congruences modulo D.

Genus theory (Lagrange) tells us there is a subgroup $\mathcal{H}$, the *principal genus*, of the class group $\mathcal{G}$.

A prime $\ell \nmid D$ is the norm of an element of a coset of $\mathcal{G}/\mathcal{H}$ iff ℓ satisfies a $\equiv$ condition mod D.

When the principal genus is the union of two or more classes, congruences mod D are not enough to determine which class contains elements of norm ℓ.
Instead, ℓ must satisfy higher-degree polynomial conditions mod D derived from the Hilbert class field.

We see examples at $D = -55$, etc., where class group $\cong \mathbb{Z}/4\mathbb{Z}$.

The Rule of Three

Proposition

The order $\mathcal{O}$ of discriminant $D \equiv 1 \pmod 4$ has a well-rounded class iff we can factor $|D| = FG$ with $F \leqslant G$ relatively prime and

$$\frac{G}{F} \leqslant 3.$$

(There is a similar statement for $D \equiv 0 \pmod 4$.)

This is why we encounter many $|D| = pq$ with p, q primes near each other: $35 = 5 \cdot 7$, $55 = 5 \cdot 11$, 15, 91, 143, 731, ...

To get two well-rounded classes, factor $|D|$ in two different ways:

$$1155 = 3 \cdot 5 \cdot 7 \cdot 11 = \underbrace{33 \cdot 35}_{\text{ratio } 1.06} = \underbrace{21 \cdot 55}_{\text{ratio } 2.62}.$$

Appendix on Binary Quadratic Forms

$ax^2 + bxy + cy^2$ is *reduced* if

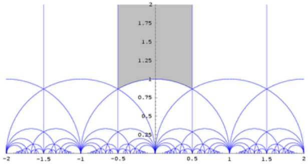
$$-a \leqslant b < a, \quad c \geqslant a \text{ when } b \leqslant 0, \quad c > a \text{ when } b > 0.$$

Reduced forms satisfy $|b| \leqslant a \leqslant \sqrt{-D/3}$,
so it is easy to enumerate them for small $|D|$.

Theorem (Lagrange, Gauss): every equivalence class of quadratic forms contains a unique reduced form.

Lemma

A reduced form $ax^2 + bxy + cy^2$ is well rounded iff $a = c$.



$a = c$ is the arc at the bottom of the fundamental domain.

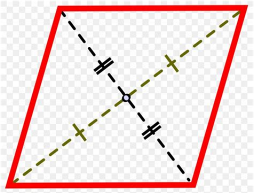
$b = 0$ is the vertical line up the middle of the fundamental domain.

$b = \frac{1}{2}$ is the vertical line up the right-hand boundary.

Proposition

A well-rounded class has order 1 or 2 in the class group.

Proof. A well-rounded lattice L has a $\mathbb{Z}$-basis $\{v_1, v_2\}$ of vectors of equal length.
Let $\alpha = v_1 + v_2$, the diagonal of the rhombus spanned by v_1, v_2.



Then $\alpha^{-1}L = \diamond$ is symmetric under complex conjugation.
But complex conjugation is the inverse on the class group.