Wake Forest University WADE Into Research REU

Intersecting Finite Sets of Positive Definite Integral Binary Quadratic Forms

Havi Ellers

Introduction and Definitions

It is well know what integers can be written in the form $x^2 + y^2$ for $x, y \in \mathbb{Z}$, but what if we add x^2 and y^2 coefficients? What if we add a cross term? Our research this summer explored these possibilities.

The Forms

Definition 1. *An **integral binary quadratic form** is a homogeneous polynomial*

$$Q : \mathbb{Z}^2 \to \mathbb{Z}$$
$$(x, y) \mapsto ax^2 + bxy + cy^2$$

*where $a, b, c \in \mathbb{Z}$. Q is **positive-definite** if $Q(x, y) > 0$ for all $(x, y) \neq (0, 0)$, **primitive** if $\gcd(a, b, c) = 1$, and **reduced** if*

$$(R1)\ |b| \leq a \leq c,$$
$$(R2)\ b \geq 0 \text{ if } |b| = a \text{ or if } a = c.$$

Definition 2. *An integer m is **represented** by Q if there exist $x, y \in \mathbb{Z}$ such that $Q(x, y) = m$.*

Definition 3. *The **discriminant** of Q is $\Delta = b^2 - 4ac$, and is **fundamental** if*

$$(i)\ \Delta \equiv 1 \ (\text{mod } 4) \text{ is square free, or}$$
$$(ii)\ \Delta = 4n, \text{ with } n \equiv 2, 3 \ (\text{mod } 4) \text{ square free.}$$

Henceforth, by "form" we mean primitive positive-definite integral binary quadratic form.
Note: there are finitely many reduced forms of a fixed discriminant, and the discriminant of a positive-definite form is negative.

Definition 4. *The **class number**, $h(\Delta)$, is the number of reduced forms of discriminant Δ.*

The Equivalence Relation

There is an equivalence relation between forms of the same discriminant, which is defined using a $\mathbb{Z}$-linear matrix transformation.

Definition 5. *Equivalence is **proper** if the determinant of this matrix is 1, and **improper** if the determinant is -1. Two forms are in the same **proper equivalence class** if they are properly equivalent.*

Fact: Properly or improperly equivalent forms represent exactly the same integers (see [1] for details).

The Group

Proper equivalence classes partition the set of forms of a fixed discriminant and create a group:

Definition 6. *The **form class group**, $C(\Delta)$, is the set of these proper equivalence classes, and has order $h(\Delta)$.*

Each proper equivalence class has a unique reduced form, so we define the group operation of the form class group to be the **composition** of reduced forms (see [1] for a definition of composition). The composition of forms Q_1 and Q_2 is denoted as $Q_1 \circ Q_2$.
Fact: If n_1 and n_2 are represented by Q_1 and Q_2, respectively, then $n_1 n_2$ is represented by $Q_1 \circ Q_2$.
The inverse of a reduced form $Q(x, y) = ax^2 + bxy + cy^2$ is $Q^{-1}(x, y) = ax^2 - bxy + cy^2$, and the identity element of the class group, the **principal form**, is the unique reduced form that represents 1.
Note: A nice formula can be found for the principle form (see [1]).

Definition 7. *Let $a, b \in \mathbb{Z}$ and $a \not\equiv 0 \pmod{b}$. Then a is a **quadratic residue** modulo b if there is a solution to the equation $a \equiv x^2 \pmod{b}$ for $x \in \mathbb{Z}$, and a is a **quadratic non-residue** modulo b if there is no solution.*

Results

Theorem (DEOTW) 1. *Let $\Delta < 0$ and let S_Δ be the collection of all forms of discriminant Δ. If $h(\Delta)$ is odd then there are infinitely-many positive integers represented by all forms in S_Δ.*
Theorem (DEOTW) 2. *Let $\Delta < 0$ be a fundamental discriminant, and let S_Δ be the set of all forms of discriminant Δ. If $h(\Delta)$ is even, then $m = 0$ is the only integer represented by all forms in S_Δ.*

Ask me about the Hilbert class field!!

Proofs

Proof. (of Theorem 1)
Since $h(\Delta)$ is odd, $C(\Delta)$ has the following structure:

$$Q_1(x, y) = x^2 + b_0xy + c_0y^2$$
$$Q_2(x, y) = a_1x^2 + b_1xy + c_1y^2$$
$$Q_3(x, y) = a_1x^2 - b_1xy + c_1y^2$$
$$\vdots$$
$$Q_{2n}(x, y) = a_nx^2 + b_nxy + c_ny^2$$
$$Q_{2n+1}(x, y) = a_nx^2 - b_nxy + c_ny^2.$$

Using this structure we can create compositions to show that each form represents $\prod_{i=1}^{2n+1} a_i c_i$. Also, if a form represents an integer m then it represents $k^2 m$ for all $k \in \mathbb{Z}$. Thus all integers in the infinite set $\left\{ k^2 \left(\prod_{i=1}^{2n+1} a_i c_i \right) \right\}$ are represented by all forms of discriminant Δ. □

Proof. (of Theorem 2)
We are guaranteed a reduced form, Q_1, that represents only quadratic residues and integers that are zero modulo Δ, and a reduced form, Q_2, that represents only quadratic non-residues and integers that are zero modulo Δ. Any integer $m \equiv 0 \pmod{\Delta}$ can be written in the form $m = \Delta^k \ell$ for some $k, \ell \in \mathbb{Z}$ such that $\ell \not\equiv 0 \pmod{\Delta}$ or $\ell = 0$. We can show that if m is represented by Q_1 and Q_2 then so is ℓ. This forces ℓ to be zero, since the only integers represented by both Q_1 and Q_2 are zero modulo Δ. □

For Further Information

1. My email address: hellers@g.hmc.edu
2. Link to our paper on arXiv: https://arxiv.org/pdf/1708.04877.pdf
3. Reference [1]: D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Vol. 34, John Wiley & Sons, 2011.

Acknowledgements

I would like to thank the National Science Foundation for funding the WADE Into Research REU (DMS-1461189), Professor Katherine Thompson and Jeremy Rouse for mentoring me over the summer, and my fellow research team members: Chris Donnay, Kate O'Connor, and Erin Wood. Thank you also to Claire Connelly for providing this poster format.

Advisor: Katherine Thompson