Today we begin studying quadratic forms, which is a vast and interesting subject of its own, but we will only get a brief glimpse of it over the next week or so.

1. Quadratic Forms

- motivation - we figured out weeks ago which integers can be written as sums of squares
- think of that problem this way: let $f(x, y) = x^2 + y^2$. What are the outputs (range) of this function, as $x$ and $y$ range over all integers?
- question: if we replace $f$ above by some other quadratic function of two variables, how does the answer change?
- for example, if $f(x, y) = 2x^2 - y^2$, what are the outputs of $f$?

**Definition 1.** A form (also called a homogeneous polynomial) in $n$ variables is a polynomial $f(x_1, \ldots, x_n)$ in which every term has the same degree. In general, the coefficients may be integers, rational numbers, real numbers, etc., but for us, they will usually be integers unless stated otherwise.

A quadratic form is a form of degree two. Binary means the form has two variables, ternary means it has three, etc.

**Examples 1.1.**
- $f(x, y) = x^2 + y^2$ is a binary quadratic form, but $f(x, y) = x^2 + y^2 - 1$ is not.
- $f(x, y, z) = x^2 - y^2 - z^2$ is a ternary quadratic form, whereas $f(x, y, z) = x^3 + xyz + xyz^2$ is not a form at all.

To relate this notion to the “sums of squares” problem:

**Definition 2.** If $n$ is any integer, and $f(x_1, \ldots, x_n)$ is a quadratic form, we say $f$ represents $n$ if there are integers $a_1, \ldots, a_n$ such that $f(a_1, \ldots, a_n) = n$. We say $f$ properly represents $n$ if the gcd of the $a_i$ is 1.

Note - If $f$ represents $n$, but not properly, then gcd of the $a_i$ is some $g > 1$, and dividing through by $g$ gives: $f$ represents $n/g^2$ properly. So it’s enough to consider proper representations.

- **main question:** given a form $f$, which integers does it represent?
- for now focus on binary quadratic forms:
- much of this can be found by looking at the discriminant:

2. Discriminants

**Definition 3.** Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form. The discriminant of $f$ is $d = b^2 - 4ac$.

- the discriminant can tell us when $f$ has nontrivial zeroes:
Theorem 1. Let \( f, d \) be as in above definition. If \( d \) is nonzero and not a perfect square, then the only solution of \( f(x, y) = 0 \) is \( x = y = 0 \).

Proof. - note that if \( a \) or \( c \) is zero, then \( d = b^2 \), contradicting our assumption that \( d \) is not a square. So they’re both nonzero.
- If either of \( x \) or \( y \) is zero, then so is the other.
- assume there is a point \( (x, y) \neq (0, 0) \) with \( f(x, y) = (0, 0) \). We look for a contradiction.
- key formula:

\[
4af(x, y) = (2ax + by)^2 - dy^2
\]
- set equal to zero, and get \( d \) is a perfect square. Contradiction.

\( \square \)

3. Definiteness

The first thing we can ask about a form is whether its outputs are always positive, always negative, or both.

Definition 4. The form \( f(x, y) \) is indefinite if it has both positive and negative outputs. It’s positive semidefinite if all its outputs are \( \geq 0 \). It’s positive definite if all its outputs are strictly greater than 0. Define negative (semi-)definite similarly.

Good news: the discriminant can tell us whether a form is definite or not.

Theorem 2. Let \( f \) be a binary quadratic form with discriminant \( d \).

1. If \( d > 0 \) the \( f \) is indefinite.
2. If \( d = 0 \) then \( f \) is semidefinite, but not definite.
3. If \( d < 0 \), then the coefficients \( a \) and \( c \) have the same sign, and \( f \) is positive definite if they’re both positive and negative definite if they’re both negative.

Proof. Boring - see book. Deal with three cases separately and be clever with the “key formula” from the last proof.

\( \square \)

Which integers \( d \) can be discriminants of some form? The answer is actually easy:

Proposition 1. There is a form having discriminant \( d \) if and only if \( d \) is congruent to 0 or 1 mod 4.

Proof. - assume there is a form with discriminant \( d \). Then the integer \( d \) can be written as \( b^2 - 4ac \equiv b^2 \) mod 4. But squares mod 4 are always 0 or 1.
- other way: suppose \( d \) is congruent to 0, say \( d = 4k \). Set \( f = x^2 - ky^2 \). it has discriminant \( 4k \)
- now suppose \( d \equiv 1 \) mod 4, say \( d = 4k + 1 \). Set \( f = x^2 + xy - ky^2 \) it has disc \( d \).

\( \square \)
4. Lattices

To introduce some of the ideas of linear algebra, think of forms in the following way:

Let \( \mathbb{Z}^2 = \{(a, b) \mid a, b \in \mathbb{Z}\} \)
- It’s a subset of \( \mathbb{R}^2 \) (draw picture)
- We think of a binary form as a function from \( \mathbb{Z}^2 \to \mathbb{Z} \)
- Can regard two integers \( x, y \) as a vector \( \mathbf{x} = (x, y) \). Draw it.
- Consider the expression:
  \[
  \mathbf{x}^T A \mathbf{x} = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}
  \]
- expand it: get \( ax^2 + bxy + cxy + dy^2 \). This is a quadratic form.
- other way, given \( ax^2 + bxy + cy^2 \), can write it using a matrix
  \[
  A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}
  \]
Notice it’s symmetric (\( A = A^T \))
- so can interchange the two:
  binary quadratic forms \( \leftrightarrow \) symmetric \( 2 \times 2 \) integer matrices
- now check that if \( d \) is defined as above, then \( d = -4 \det A \).
- use this to prove part (2) of previous theorem on discriminants and definiteness.

---

Problem Session

- For each form, find the discriminant and say whether it’s indefinite/pos/neg semidefinite, or pos/neg definite:
  (1) \( f(x, y) = 2x^2 - xy \)
  (2) \( f(x, y) = x^2 + 3xy + y^2 \).
  (3) \( f(x, y) = x^2 - 2xy + y^2 \)
- For which of the values \( d = -1, 0, 1 \) is there a quadratic form having that discriminant? Write down an explicit form in each case.
- If a form factors as \( f(x, y) = (\alpha x + \beta y)(\gamma x + \delta y) \), show that it must be semidefinite. Show further that the discriminant of such a form must be a perfect square (maybe 0).
- Prove that a polynomial \( f(x, y) \) is homogeneous (of degree \( d \)) if and only if \( f(\lambda x, \lambda y) = \lambda^d f(x, y) \).