Quadratic and Modular Forms

Trajan Hammonds

Fall 2017

1 Introduction

The goal of this paper, is to talk a bit about quadratic and modular forms.
We will talk about the 290 theorem, a famous result of Manjul Bhargava and
Jonathan Hanke, and really understand what’s it about. Then, maybe we’ll do
some stuff with modular forms.

1.1 Quadratic Forms

Definition 1.1. Quadratic Form
An \(n\)-ary quadratic form is a polynomial

\[ Q(x) = Q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_i x_j. \]

Definition 1.2. Positive Definite
A positive definite quadratic form is one where \(Q(x) > 0 \forall x \neq 0\).

Remark. Recall from Linear Algebra, a \(n \times n\) Hermitian matrix \(M\) is positive
definite if \(z^* M z > 0\) and real for all non-zero vectors \(z\). Perhaps we will end
up representing quadratic forms with matrices...?

Next, suppose we have a quadratic form

\[ Q : \mathbb{Z}^n \to \mathbb{N} \cup \{0\}. \]

Let \(m \in \mathbb{N}\). We say \(m\) is represented by \(Q\) if there exists \(x \in \mathbb{Z}^n\) such that
\(Q(x) = m\). There are a few natural questions we can ask about representations
of quadratic forms.

Question 1.1. What \(m\)’s are represented by a given quadratic form?

Question 1.2. Fix some infinite subset \(S \subseteq \mathbb{N}\). Which positive definite quadratic
forms represent every \(x \in S\)?
Question 1.3. Which sets can we avoid? For example, can we come up with a quadratic form that represents only prime numbers? Only composite numbers?

There are many properties of quadratic forms, but so far we have only defined the idea of positive-definite-ness. Why? Something something level sets are compact. (Note to self: Figure this out later). Consider the quadratic form $Q(x, y) = x^2 + y^2$. If we want to represent a number $m$, we can write $x^2 + y^2 = m$. Recall a level set of $f$ is

$$L_f = \{(x_1, \ldots, x_n) | f(x_1, \ldots, x_n) = c\}.$$ 

Indeed the set of points that satisfy our equation is a level set known as a circle, with radius $\sqrt{m}$. Note that if we make the usual restriction that $x, y \in \mathbb{Z}$, then there are clearly only finitely many points. So we can just count them!

1.2 A Bit of History

Theorem 1.1 (1640, Fermat). A prime $p$ can be written as a sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

The first proof was presented by Euler using the method of infinite descent in 1750. In 1775, Lagrange gave a proof using the theory of integral quadratic forms. Then in 1877, Dedekind provided a proof using the properties of addition under the Gaussian integers $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. In particular, Dedekind’s idea was to write

$$x^2 + y^2 = (x + iy)(x - iy) = p,$$

and factor accordingly in the ring $\mathbb{Z}[i]$. Then in 1990, Don Zagier, who will be coming up a lot later, provided a beautiful one line proof of Fermat’s sum of squares theorem. However, for our purposes we will mainly be focusing on the proof due to Minkowski. But first, we must know Minkowski’s Theorem.

Theorem 1.2 (Minkowski’s Theorem). Let $L$ be a lattice in $\mathbb{R}^n$ with fundamental domain $D$. Let $B$ be a convex, centrally symmetric body. Then if

$$\text{vol}(B) > 2^n \text{vol}(D),$$

$B$ contains a non-zero lattice point.