Math 356: Number Theory (Rutgers)

David Yang

Winter Break, 2023

Abstract

These notes arise from lecture videos of Math 356: Number Theory (Quadratic Forms), originally taught by Professor Alex Kontorovich, at Rutgers University. I am grateful to Professor Kontorovich for releasing the lecture videos online. I am responsible for all faults in this document, mathematical or otherwise; any merits of the material here should be credited to Professor Kontorovich and not to me. Feel free to message me with any suggestions or corrections at dyang5@swarthmore.edu.

Contents

1 Introduction to Fermat's Last Theorem

Theorem 1 (Fermat's Last Theorem, 1637)

There are no positive integers x, y, z that satisfy

$$x^n + y^n = z^n$$

for integer $n > 2$.

An equivalent formulation is the one discussed in lecture:

$$x^n + y^n = z^n$$

where $n > 2$ is an integer, has no non-trivial solutions x, y, and z in $\mathbb{Q}, \mathbb{Z}$.

Definition 2 (Diophantine Problem)

A **Diophantine problem** is a polynomial equation solved in $\mathbb{Z}$ and $\mathbb{Q}$.

Fermat's Last Theorem is an example of a Diophantine problem.

Historically, in 1993, Andrew Wiles published a proof of Fermat's Last Theorem. Later, Wiles and his student Richard Taylor rectified the 1993 proof and published the first successful proof. For these efforts, Wiles won the 2016 Abel Prize and the 2017 Copley Medal.

With some extra background, we can prove Fermat's Last Theorem for $n = 4$.

1.1 Parameterization of Pythagorean Triples

Theorem 3 (Primitive Pythagorean Triple Generation)

If (x, y, z) is a **primitive** pythagorean triple[a] ($\nexists\, d$ such that $d \mid x$, $d \mid y$ and $d \mid z$), then z is odd. Furthermore, assuming that x is odd and y is even, then there exists coprime $r, s \in \mathbb{Z}$ with such that

$$x = r^2 - s^2,\ y = 2rs,\ z = r^2 + s^2.$$

[a] if (x, y, z) is a primitive Pythagorean triple, then it follows that x, y, and z are pairwise primtiive.

Proof Sketch (Theorem 3). Since y is even, we can rewrite $y = 2y_1$ for some integer y_1. Since (x, y, z) are a Pythagorean triple, it follows that $y^2 = z^2 - x^2 = (z - x)(z + x)$. Substituting and expanding, we get that

$$4y_1^2 = (z - x)(z + x).$$

Since x, z are both odd, we can rewrite $z - x = 2a$ and $z + x = 2b$, so

$$y_1^2 = ab$$

where $(a, b) = 1$. Consequently, a, b must themselves be perfect squares. We conclude that $y_1 = rs$, where $r^2 = a$, $s^2 = b$, and so it follows that $y = 2rs$ for coprime r, s. □

1.2 Pythagorean Varieties

Definition 4 (Variety)

A **variety** is a set of solutions to a system of polynomial equations.

Consider the variety $\mathcal{V} : x^2 + y^2 - z^2$, which is a Pythagorean variety. Note that $\mathcal{V}(\mathbb{R})$ is a structure consisting of two cones which are reflections about the z-axis, and $\mathcal{V}(\mathbb{Z})$, $\mathcal{V}(\mathbb{Q})$ are subsets of $\mathcal{V}(\mathbb{R})$.

Lemma

For every $\vec{v} \in \mathcal{V}(\mathbb{Q})$, there exists a unique primitive $\vec{w} \in \mathcal{V}(\mathbb{Z})^0_+$ with $\vec{w} \sim \vec{v}$, where $\vec{u} \sim \vec{v} \iff \vec{u} = \lambda\vec{v}$, $\lambda \in \mathbb{R} \setminus \{0\}$.

Note that $\mathcal{V}(\mathbb{R})_+/\sim$ can be thought of as S^1; for a point $(x, y, z) \in \mathcal{V}(\mathbb{R})_+ \mapsto \left(\frac{x}{z}, \frac{y}{z}, 1\right)$. Furthermore, $\mathcal{V}(\mathbb{R})/\sim = S^1 \cup \{0\}$.

Furthermore, note that another set of representatives of $\mathcal{V}(\mathbb{Q})_+/\sim$ is $S^1(\mathbb{Q})$. This gives a notion for why Pythagorean triples are fundamental: they parameterize rational points on the unit circle. Formally,

$$\left(\frac{r}{u}, \frac{t}{u}\right) \in S^1(\mathbb{Q}) \iff (r, t, u) \in \mathcal{V}(\mathbb{Z})^0_+$$

1.3 Proof of Fermat's Last Theorem for $n = 4$

Statement. $x^4 + y^4 = z^4$ in $\mathbb{Z}$ implies $xyz = 0$.
Stronger Statement. $x^4 + y^4 = z^2$ in $\mathbb{Z}$ implies $xyz = 0$.

Proof. Note that if $x^4 + y^4 - z^2 = 0$, then $(x^2, y^2, z^2) \in \mathcal{V}(\mathbb{Z})^0_+$, a primitive Pythagorean triple. By the Parameterization of primitive Pythagorean triples, there exists $r, s \in \mathbb{Z}$ such that

$$x^2 = r^2 - s^2,\ y^2 = 2rs,\ z = r^2 + s^2.$$

□