Algebraic Number Theory and Algebraic Curves

Prerequisites: MATH342

Advisor: Alex Barrios

Terms: Fall/Winter

Historical Motivation: In 1637, Pierre de Fermat famously wrote his marginal note claiming to have proven that the only integer solutions x, y, z to the equation

$$x^n + y^n = z^n \tag{1}$$

satisfy $xyz = 0$ for $n \geq 3$. While Fermat did provide a proof for $n = 4$, it would take an additional hundred years until the $n = 3$ case was proven by Leonhard Euler in 1753. These proofs attacked Fermat's Last Theorem one exponent at a time. Then, in 1821, Sophie Germain revolutionized number theory by attempting to prove Fermat's Last Theorem for infinitely many exponents n. This dream was realized twenty years later by Gabriel Lamé and Ernst Kummer who laid the foundations of what is today known as Algebraic Number Theory.

In 1847, Lamé presented a "false proof" of Fermat's Last Theorem to the Académie des Sciences in Paris. His proof assumed that the Fundamental Theorem of Arithmetic held in what are known as rings of integers (the Gaussian integers is one example of these rings). Namely, Lamé assumed that if there exists a solution to (1) with $xyz \neq 0$ for some prime exponent $p \geq 3$, then the factorization

$$x^p + y^p = \prod_{j=0}^{p-1} \left(x + \zeta^j y\right) = z^p \tag{2}$$

holds over the "ring of integers"

$$\mathbb{Z}[\zeta] = \left\{a_1 + a_2\zeta + a_3\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \mid a_j \in \mathbb{Z}\right\} \qquad \text{where } \zeta = e^{2\pi i/p}.$$

By incorrectly assuming that unique factorization held in $\mathbb{Z}[\zeta]$ (it does for $p \leq 19$), Lamé arrived at a contradiction which led him to claim that he had proven Fermat's Last Theorem. Unbeknownst to Lamé, Kummer had already shown that the ring $\mathbb{Z}[\zeta]$ was not a Unique Factorization Domain in general and the two arguments led to the first proof that Fermat's Last Theorem is true for infinitely many prime exponents.

In 1871, Richard Dedekind introduced the modern language of rings and began studying what we call today *Dedekind Domains*, which are rings that share many of the nice properties that the integers satisfy. In this comps project, we will focus on two types of Dedekind Domains: (1) Rings of integers which are subrings of fields that are finite extensions of $\mathbb{Q}$ and (2) the coordinate rings of nonsingular algebraic curves. For the latter, we will trace works of David Hilbert and Emmy Noether in the early 1900's to realize smooth curves algebraically. For instance, a curve $y = f(x)$ where $f(x)$ is a polynomial can be viewed algebraically via the coordinate ring $\mathbb{C}[x,y]/(y - f(x))$ where $(y - f(x))$ is viewed as a principal ideal of $\mathbb{C}[x,y]$.

The Class Group. Consider the Dedekind domain $\mathbb{Z}\left[\sqrt{-5}\right]$. In this ring, we have that 6 has two different factorizations into irreducibles

$$\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 6 = 2 \cdot 3.$$

This illustrates the major flaw that Lamé had in assuming that the factorization in (2) was unique. This raises the question: Given a Dedekind domain D, how can we know if it is a unique factorization domain? This was answered in the late 1800's as mathematicians began to home in on what we call today the class group of a Dedekind domain. Our project will focus on understanding the construction of the class group as well as its number-theoretic properties. As part of this project we will study and learn the proofs of the following results:

- **Finiteness of the Class Group of Rings of Integers**. The order of the class group of a Dedekind domain which is a subring of a field which is a finite extension of $\mathbb{Q}$ is finite. In fact, we will see that if the order of the class group is 2 for a Dedekind domain D, then there at most two different factorizations into irreducibles in D. The ring $\mathbb{Z}\left[\sqrt{-5}\right]$ is an example of a Dedekind domain whose class group is of order 2.

- **Every Abelian Group is a Class Group of some Dedekind Domain**. By studying those Dedekind domains that arise as coordinate rings of algebraic curves, we will learn and understand Luther Claborn's 1966 proof that every abelian group is a class group of some Dedekind domain.

Sources: The main sources that will be used in this comps project are the following two books:

1. An Invitation to Arithmetic Geometry by Dino Lorenzini
2. Algebraic Number Theory and Fermat's Last Theorem by Ian Stewart and David Tall