Formalization of codes

NRR

July 16, 2024

Chapter 1

Introduction

Fermat's Last Theorem is the statement that if a, b, c, n are positive whole numbers with $n \geq 3$, then $a^n + b^n \neq c^n$. It is thus a statement about a family of *Diophantine equations* ($a^3 + b^3 = c^3, a^4 + b^4 = c^4, ...$). Diophantus was a Greek mathematician who lived around 1800 years ago, and he would have been able to understand the statement of the theorem (he knew about positive integers, addition and multiplication).

Chapter 2

First reductions of the problem

2.1 Overview

The proof of Fermat's Last Theorem is by contradiction. We assume that we have a counterexample $a^n + b^n = c^n$, and manipulate it until it satisfies the axioms of a "Frey package". From the Frey package we build a Frey curve – an elliptic curve defined over the rationals. We then look at a certain representation of a Galois group coming from this elliptic curve, and finally using two very deep and independent theorems (one due to Mazur, the other due to Wiles) we show that this representation is neither reducible or irreducible, a contradiction.