THE MODULARITY CONJECTURE

Contents

1. Introduction

This is a blueprint for the full proof of the modularity conjecture:

We begin by recalling the definition of an elliptic curve, which is a pair $(E, \mathcal{O})$ consisting of a smooth projective curve E of genus one and $\mathcal{O}$ a point on E. Now, every elliptic curve can be embedded as a smooth cubic curve in $\mathbb{P}^2$ given by an equation of the form $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ and this is the basis for the current definition of an elliptic curve in mathlib, where roughly it is described by the above equation, with the extra condition that the discriminant of this cubic is invertible over the base ring.

Definition 1.1. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be the Weierstrass equation of an elliptic curve and for p a prime number, let $n_p(E)$ denote the number of solutions to $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in $\mathbb{F}_p$. Then we define $a_p(E) := p - n_p(E)$.

Theorem 1.2. *Let E be an elliptic curve over $\mathbb{Q}$. Then there exists $N \in \mathbb{N}$ and a normalised cuspidal eigenform $f \in S_2(\Gamma_0(N))$ such that for all primes p with $p \nmid N$, we have $a_p(E) = a_p(f)$ where $f = \sum_n a_n(f)q^n$ is the q-expansion of f.*