THE MODULARITY CONJECTURE

Contents

1. Introduction

This is a blueprint for the full proof of the modularity conjecture. We are following [CSS13].

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.*

Definition 1.3. Let K be a number field. An elliptic curve E/K has good, multiplicative or additive reductions depending on...

Definition 1.4. Let K be a number field and E/K an elliptic curve. Then the conductor of E/K is

$$N_{E/K} \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E/K)}$$

where $f_{\mathfrak{p}}(E/K)$ is $0, 1, 2$ depending on if E has good, multiplicative or additive reduction at $\mathfrak{p}$ (and in the last case $\mathfrak{p} \nmid 6$).

Definition 1.5. The L-function of an elliptic curve is defined as..

Definition 1.6. The L-function of a modular form is...

Definition 1.7. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N_E is *modular* is there is a weight 2 newform of level $\Gamma_0(N_E)$ and trivial character for which

$$L(E, s) = L(f, s).$$

Theorem 1.8. *Let* $2 \leq k$ *and* Γ *a congruence subgroup. The is a Hecke equivaariant isomorphism*

$$H^1(\Gamma, V_{k-2}) \cong M_k(\Gamma) \oplus \overline{S_k}(\Gamma).$$

Definition 1.9. Let f be a weight two normalised newform of level $\Gamma_0(N)$ and character ϵ. Then we can attach to f a Galois representation by...

Definition 1.10. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. The Tate module of E is

$$T_p(E) := \varprojlim E[p^n].$$

Lemma 1.11. *Let* $E/\mathbb{Q}$ *be an elliptic curve and* p *a prime. The*

$$T_p(E) \cong \mathbb{Z}_p^2.$$

Definition 1.12. Let $E/\mathbb{Q}$ be an elliptic curve. This define a p-adic Galois representation $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ as the one coming from the action of $G_{\mathbb{Q}}$ on the Tate module $T_p(E)$.

Definition 1.13. A Galois representation is unramified if...

Definition 1.14. Let $0 < N$ be an integer. Then the Hecke algebra $\mathbb{T}'(N)$ is defined as...

Definition 1.15. An abelian variety is...

Definition 1.16. Let f be a modular form of weight 2. Then attached to f is an abelian variety A_f such that...

Definition 1.17. Let $0 < N$ be an integer. Let $X_0(N)$ denote the modular curve....

Fix a prime p.

Definition 1.18. A coefficient ring A is a complete noetherian local ring with finite residue field of characteristic p.

Definition 1.19. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(A)$ be a Galois representation over a coefficient ring A. Then ρ is modular if there exists some integer $0 < N$ and a homomorphism $\pi : \mathbb{T}'(N) \to A$ such that ρ is unramified outside Np and for every $\ell \nmid pN$, we have

$$\mathrm{Trace}(\rho(\mathrm{Fr}_\ell)) = \pi(T_\ell) \qquad \det(\rho(\mathrm{Fr}_\ell)) = \pi(\langle \ell \rangle)\ell$$

Definition 1.20. An elliptic curve is semistable if....

Definition 1.21. A Galois representation is irreducible if...

Lemma 1.22. *Let* $E/\mathbb{Q}$ *be a semistable elliptic curve and suppose* $\overline{\rho}_{E,p}$ *is both modular and irreducible for some prime* $3 \leq p$. *Then* E *is modular.*

Theorem 1.23. *Let* E *be an arbitrary elliptic curve and suppose* $\overline{\rho}_{E,3}$ *is irreducible. Then* $\overline{\rho}_{E,3}$ *is modular.*

Theorem 1.24. *Let* E *be a semistable elliptic curve and suppose* $\overline{\rho}_{E,5}$ *is irreducible. Then there is another semistable elliptic curve* $E'/\mathbb{Q}$ *for which:*

(1) $\overline{\rho}_{E',3}$ *is irreducible and;*
(2) $\overline{\rho}_{E',5} \cong \overline{\rho}_{E,5}$.

Theorem 1.25. *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then at least one of the representations $\overline{\rho}_{E,3}$ or $\overline{\rho}_{E,5}$ is irreducible.*

Theorem 1.26. *Every semi-stable elliptic curve over $\mathbb{Q}$ is modular.*

Proof. Let $E/\mathbb{Q}$ be a semi-stable elliptic curve. If $\overline{\rho}_{E,3}$ is irreducible then by 1.23 it is modular and hence by 1.22 E is modular. If $\overline{\rho}_{E,3}$ is not irreducible, then by 1.25, $\overline{\rho}_{E,5}$ is irreducible. Now using 1.24, we find another semistable elliptic curve E' such that $\overline{\rho}_{E',3}$ is irreducible and hence E' is modular. Therefore $\overline{\rho}_{E',5}$ is modular, making $\overline{\rho}_{E,5}$ modular and hence E is modular. □

Definition 1.27. A Galois representation is continuous if...

Theorem 1.28. *If $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_5)$ is an irreducible continuous representation with cyclotomic determinant, then $\overline{\rho}$ is modular.*

Theorem 1.29. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E is modular, equivalently:*

1. *Theorem 1.2 holds for E.*
2. *For some prime p, $\rho_{E,p}$ is modular.*
3. *For every prime p, $\rho_{E,p}$ is modular.*
4. *There is a non-constant morphism $\pi : X_0(N_E) \to E$ of algebraic curves defined over $\mathbb{Q}$.*
5. *E is isogenous to the modular abelian variety A_f associated to some weight 2 newform f of level $\Gamma_0(N_E)$.*

References

[CSS13] G. Cornell, J.H. Silverman, and G. Stevens. *Modular Forms and Fermat's Last Theorem.* Springer New York, 2013.