This is page 1
Printer: Opaque this

1
Modularity of Abelian Varieties

1.1 Modularity Over $\mathbf{Q}$

Definition 1.1.1 (Modular Abelian Variety). Let A be an abelian variety over $\mathbf{Q}$. Then A is *modular* if there exists a positive integer N and a surjective map $J_1(N) \to A$ defined over $\mathbf{Q}$.

The following theorem is the culmination of a huge amount of work, which started with Wiles's successful attack [7] on Fermat's Last Theorem, and culminated with [1].

Theorem 1.1.2 (Breuil, Conrad, Diamond, Taylor, Wiles). *Let E be an elliptic curve over $\mathbf{Q}$. Then E is modular.*

We will say nothing about the proof here.

If A is an abelian variety over $\mathbf{Q}$, let $\mathrm{End}_{\mathbf{Q}}(A)$ denote the ring of endomorphisms of A that are defined over $\mathbf{Q}$.

Definition 1.1.3 (GL_2-type). An abelian variety A over $\mathbf{Q}$ is of GL_2*-type* if the endomorphism algebra $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$ contains a number field of degree equal to the dimension of A.

For example, every elliptic curve E over $\mathbf{Q}$ is trivially of GL_2-type, since $\mathbf{Q} \subset \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(E)$.

Proposition 1.1.4. *If A is an abelian variety over $\mathbf{Q}$, and $K \subset \mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$ is a field, then $[K : \mathbf{Q}]$ divides $\dim A$.*

Proof. As discussed in [4, §2], K acts faithfully on the tangent space $\mathrm{Tan}_0(A/\mathbf{Q})$ over $\mathbf{Q}$ to A at 0, which is a $\mathbf{Q}$ vector space of dimension $\dim(A)$. Thus $\mathrm{Tan}_0(A/\mathbf{Q})$ is a vector space over K, hence has $\mathbf{Q}$-dimension a multiple of $[K : \mathbf{Q}]$. $\square$

Proposition 1.1.4 implies, in particular, that if E is an elliptic curve over $\mathbf{Q}$, then $\mathrm{End}_{\mathbf{Q}}(E) = \mathbf{Q}$. Recall that E *has CM* or is a *complex multiplication* elliptic curve if $\mathrm{End}_{\overline{\mathbf{Q}}}(E) \neq \mathbf{Z}$). Proposition 1.1.4 implies that if E is a CM elliptic curve, the extra endomorphisms are *never* defined over $\mathbf{Q}$.

Proposition 1.1.5. *Suppose $A = A_f \subset J_1(N)$ is an abelian variety attached to a newform of level N. Then A is of GL_2-type.*

Proof. The endomorphism ring of A_f contains $\mathcal{O}_f = \mathbf{Z}[\ldots, a_n(f), \ldots]$, hence the field $K_f = \mathbf{Q}(\ldots, a_n(f), \ldots)$ is contained in $\mathbf{Q} \otimes \mathrm{End}_{\mathbf{Q}}(A)$. Since $A_f = n\pi J_1(N)$, where π is a projector onto the factor K_f of the anemic Hecke algebra $\mathbf{T}_0 \otimes_{\mathbf{Z}} \mathbf{Q}$, we have $\dim A_f = [K_f : \mathbf{Q}]$. (One way to see this is to recall that the tangent space $T = \mathrm{Hom}(S_2(\Gamma_1(N)), \mathbf{C})$ to $J_1(N)$ at 0 is free of rank 1 over $\mathbf{T}_0 \otimes_{\mathbf{Z}} \mathbf{C}$.) $\square$

Conjecture 1.1.6 (Ribet). *Every abelian variety over $\mathbf{Q}$ of GL_2-type is modular.*

Suppose

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

is an odd irreducible continuous Galois representation, where odd means that

$$\det(\rho(c)) = -1,$$

where c is complex conjugation. We say that ρ is *modular* if there is a newform $f \in S_k(\Gamma_1(N))$, and a prime ideal $\wp \subset \mathcal{O}_f$ such that for all $\ell \nmid Np$, we have

$$\begin{aligned} \mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) &\equiv a_\ell \pmod{\wp}, \\ \mathrm{Det}(\rho(\mathrm{Frob}_\ell)) &\equiv \ell^{k-1} \cdot \varepsilon(\ell) \pmod{\wp}. \end{aligned}$$

Here χ_p is the p-adic cyclotomic character, and ε is the (Nebentypus) character of the newform f.

Conjecture 1.1.7 (Serre). *Every odd irreducible continuous representation*

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

is modular. Moreover, there is a formula for the "optimal" weight $k(\rho)$ and level $N(\rho)$ of a newform that gives rise to ρ.

In [6], Serre describes the formula for the weight and level. Also, it is now known due to work of Ribet, Edixhoven, Coleman, Voloch, Gross, and others that if ρ is modular, then ρ arises from a form of the conjectured weight and level, except in some cases when $p = 2$. (For more details see the survey paper [5].) However, the full Conjecture 1.1.7 is known in very few cases.

Remark 1.1.8. There is interesting recent work of Richard Taylor which connects Conjecture 1.1.7 with the open question of whether every variety of a certain type has a point over a solvable extension of $\mathbf{Q}$. The question of the existence of solvable points ("solvability of varieties in radicals") seems very difficult. For example, we don't even know the answer for genus one curves, or have a good reason to make a conjecture either way (as far as I know). There's a book of Mike Fried that discusses this solvability question.

Serre's conjecture is very strong. For example, it would imply modularity of all abelian varieties over $\mathbf{Q}$ that could possibly be modular, and the proof of this implication does not rely on Theorem 1.1.2.

Theorem 1.1.9 (Ribet). *Serre's conjectures on modularity of all odd irreducible mod p Galois representations implies Conjecture 1.1.6.*

To give the reader a sense of the connection between Serre's conjecture and modularity, we sketch some of the key ideas of the proof of Theorem 1.1.9; for more details the reader may consult Sections 1–4 of [4].

Without loss, we may assume that A is $\mathbf{Q}$-simple. As explained in the not trivial [4, Thm. 2.1], this hypothesis implies that

$$K = \mathbf{Q} \otimes_{\mathbf{Z}} \mathrm{End}_{\mathbf{Q}}(A)$$

is a number field of degree $\dim(A)$. The Tate modules

$$\mathrm{Tate}_\ell(A) = \mathbf{Q}_\ell \otimes \varprojlim_{n\geq 1} A[\ell^n]$$

are free of rank two over $K \otimes \mathbf{Q}_\ell$, so the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $\mathrm{Tate}_\ell(A)$ defines a representation

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(K \otimes \mathbf{Q}_\ell).$$

Remarks 1.1.10. That these representations take values in GL_2 is why such A are said to be "of GL_2-type". Also, note that the above applies to $A = A_f \subset J_1(N)$, and the ℓ-adic representations attached to f are just the factors of $\rho_{A,\ell}$ coming from the fact that $K \otimes \mathbf{Q}_\ell \cong \prod_{\lambda|\ell} K_\lambda$.

The deepest input to Ribet's proof is Faltings's isogeny theorem, which Faltings proved in order to prove Mordell's conjecture (there are only a finite number of L-rational points on any curve over L of genus at least 2).

If B is an abelian variety over $\mathbf{Q}$, let

$$L(B,s) = \prod_{\text{all primes } p} \frac{1}{\det\left(1 - p^{-s} \cdot \mathrm{Frob}_p \,|\, \mathrm{Tate}_\ell(A)\right)} = \prod_p L_p(B,s),$$

where ℓ is a prime of good reduction (it makes no difference which one).

Theorem 1.1.11 (Faltings). *Let A and B be abelian varieties. Then A is isogenous to B if and only if $L_p(A,s) = L_p(B,s)$ for almost all p.*

Using an analysis of Galois representations and properties of conductors and applying results of Faltings, Ribet finds an infinite set Λ of primes of K such that all $\rho_{A,\lambda}$ are irredudible and there only finitely many Serre invariants $N(\rho_{A,\lambda})$ and $k(\rho_{A,\lambda})$. For each of these λ, by Conjecture 1.1.7 there is a newform f_λ of level $N(\rho_{A,\lambda}))$ and weight $k(\rho_{A,\lambda})$ that gives rise to the mod ℓ representation $\rho_{A,\lambda}$. Since Λ is infinite, but there are only finitely many Serre invariants $N(\rho_{A,\lambda}))$, $k(\rho_{A,\lambda})$, there must be a single newform f and an infinite subset Λ' of Λ so that for every $\lambda \in \Lambda'$ the newform f gives rise to $\rho_{A,\lambda}$.

Let $B = A_f \subset J_1(N)$ be the abelian variety attached to f. Fix any prime p of good reduction. There are infinitely many primes $\lambda \in \Lambda'$ such that $\rho_{A,\lambda} \cong \rho_{B,\tilde{\lambda}}$ for some $\tilde{\lambda}$, and for these λ,

$$\det\left(1 - p^{-s} \cdot \mathrm{Frob}_p \,|A[\lambda]\right) = \det\left(1 - p^{-s} \cdot \mathrm{Frob}_p \,|B[\tilde{\lambda}]\right).$$

This means that the degree two polynomials in p^{-s} (over the appropriate fields, e.g., $K \otimes \mathbf{Q}_\ell$ for A)

$$\det\left(1 - p^{-s} \cdot \mathrm{Frob}_p \,|\, \mathrm{Tate}_\ell(A)\right)$$

and

$$\det\left(1 - p^{-s} \cdot \mathrm{Frob}_p \mid \mathrm{Tate}_\ell(B)\right)$$

are congruent modulo infinitely many primes. Therefore they are equal. By Theorem 1.1.11, it follows that A is isogenous to $B = A_f$, so A is modular.

1.2 Modularity of Elliptic Curves over $\overline{\mathbf{Q}}$

Definition 1.2.1 (Modular Elliptic Curve). An elliptic curve E over $\overline{\mathbf{Q}}$ is *modular* if there is a surjective morphism $X_1(N) \to E$ for some N.

Definition 1.2.2 (Q-curve). An elliptic curve E over **Q**-bar is a **Q**-*curve* if for every $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ there is an isogeny $E^\sigma \to E$ (over $\overline{\mathbf{Q}}$).

Theorem 1.2.3 (Ribet). *Let E be an elliptic curve over $\overline{\mathbf{Q}}$. If E is modular, then E is a* **Q**-*curve, or E has CM.*

This theorem is proved in [4, §5].

Conjecture 1.2.4 (Ribet). *Let E be an elliptic curve over $\overline{\mathbf{Q}}$. If E is a* **Q**-*curve, then E is modular.*

In [4, §6], Ribet proves that Conjecture 1.1.7 implies Conjecture 1.2.4. He does this by showing that if a **Q**-curve E does not have CM then there is a **Q**-simple abelian variety A over **Q** of GL_2-type such that E is a simple factor of A over $\overline{\mathbf{Q}}$. This is accomplished finding a model for E over a Galois extension K of **Q**, restricting scalars down to **Q** to obtain an abelian variety $B = \mathrm{Res}_{K/\mathbf{Q}}(E)$, and using Galois cohomology computations (mainly in H^2's) to find the required A of GL_2-type inside B. Then Theorem 1.1.9 and our assumption that Conjecture 1.1.7 is true together immediately imply that A is modular.

Ellenberg and Skinner [3] have recently used methods similar to those used by Wiles to prove strong theorems toward Conjecture 1.2.4. See also Ellenberg's survey [2], which discusses earlier modularity results of Hasegawa, Hashimoto, Hida, Momose, and Shimura, and gives an example to show that there are infinitely many **Q**-curves whose modularity is not known.

Theorem 1.2.5 (Ellenberg, Skinner). *Let E be a* **Q**-*curve over a number field K with semistable reduction at all primes of K lying over* 3*, and suppose that K is unramified at* 3*. Then E is modular.*

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 2002d:11058

[2] J. Ellenberg, $\mathbf{q}$-*curves and Galois Representations*, `http://www.math.princeton.edu/ ellenber/papers.html#MCAV` (2002).

[3] J. Ellenberg and C. Skinner, *On the Modularity of* $\mathbf{Q}$*-curves*, `http://www.math.princeton.edu/ ellenber/papers.html#QCURVE` (2000).

[4] K. A. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79. MR 94g:11042

[5] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232. MR 2002h:11047

[6] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[7] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.