Langlands-Rapoport for the Modular Curve

S. M.-C.

8 May 2018

Abstract

We discuss a concrete version of the Langlands-Rapoport conjecture in the case of the modular curve, and use this case to illuminate some of the more abstract features of the Langlands-Rapoport conjecture for general (abelian type) Shimura varieties.

1 Motivation

The Langlands-Rapoport conjecture is all about counting mod-p points on Shimura varieties. So to start, let's give some quick motivation for why we want to do this.

Say we're interested in the Langlands program, whose goal is roughly to relate Galois representations to automorphic representations. The main source of Galois representation is the cohomology of varieties over number fields. The main source of automorphic representations is constructions with adele groups. Shimura varieties live in both worlds: they are constructed from adele groups, and also have the structure of varieties over number fields, so their cohomology carries both Galois and automorphic representations. In short, we expect the global Langlands correspondence to be realized in the cohomology of Shimura varieties (at least for representations accessible from such cohomology). The Grothendieck-Lefschetz trace formula philosophy tells us that we can understand the cohomology of Shimura varieties in terms of their mod-p points.

The Langlands-Rapoport conjecture describes the set of $\overline{\mathbb{F}}_p$-points of a Shimura variety in a purely group-theoreic way that is suitable for applications to cohomology. The general formulation is quite abstract, so our goal is to work through a simple case, and use it to help understand the general statement.

2 Counting Points on Modular Curves

The most basic examples of Shimura varieties are modular curves. There are many ways to define modular curves; we'll define them by their moduli structure, since this is the description which will be useful for point counting.

2.1 Definition of Modular Curves

Fix a positive integer m and consider the moduli problem over $\mathbb{Z}[\frac{1}{m}]$ of elliptic curves with level-m-structure,

$$T \mapsto \{(E, \alpha) : E \text{ an elliptic curve over } T \text{ and } \alpha : (\mathbb{Z}/m\mathbb{Z})^2_T \xrightarrow{\sim} E[m]\}.$$

For $m \geq 3$, this is representable by a smooth affine curve $\mathcal{M}_m/\mathbb{Z}[\frac{1}{m}]$, which we call the *modular curve of level m*.

If p is a prime not dividing m, then we can consider the points $\mathcal{M}_m(\mathbb{F}_q)$ of our modular curve over a finite field with $q = p^r$ elements. Our goal is a concrete group-theoretic expression for the set of these points. We will find such an expression by making use of the moduli interpretation. That is, we will count elliptic curves with level-m structure over $\mathbb{F}_q$.

It is helpful to break the problem down into two main steps:

1. Count isogeny classes of elliptic curves over $\mathbb{F}_q$;

2. Count elliptic curves in a fixed isogeny class.

2.2 Honda-Tate Theory

The first step is to describe the set of isogeny classes of elliptic curves over $\mathbb{F}_q$. Honda-Tate theory does this by showing that the isogeny class of an elliptic curve (or more generally, abelian variety) over a finite field is determined by its characteristic polynomial of Frobenius. For a more thorough survey of Honda-Tate theory, see II.2 of [Mil08].

First we need some facts about (geometric) Frobenius, which are essentially given by the Weil conjectures.

Theorem 1. *Let A be abelian varieties over $\mathbb{F}_q$. Then the characteristic polynomial p_A of (geometric) Frobenius acting on $H^1_{\acute{e}t}(A_{\overline{\mathbb{F}}_p}, \mathbb{Q}_\ell)$ has coefficients in $\mathbb{Z}$ and is independent of ℓ. Furthermore, the roots of p_A are Weil integers of weight q, meaning they are algebraic integers satisfying $|\sigma(\alpha)|^2 = q$ for any embedding $\overline{\mathbb{Q}} \to \mathbb{C}$.*

With this setup, we can state the main theorem of Honda-Tate theory.

Theorem 2 (Honda-Tate)**.** *A and B are isogenous exactly when $p_A = p_B$. More precisely, the map sending A to a root of p_A (i.e. Frobenius eigenvalue) defines a bijection*

$$\{\textit{simple abelian varieties over } \mathbb{F}_q\}/\textit{isogeny} \xleftrightarrow{\sim} \{\textit{Weil integers of weight } q\}/\operatorname{Gal}_{\mathbb{Q}}$$

(here $\operatorname{Gal}_{\mathbb{Q}}$ denotes the absolute Galois group of $\mathbb{Q}$, which has a natural action on the set of Weil q-integers).

The injectivity of this map follows from Tate's isogeny theorem [Tat66]

$$\operatorname{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \operatorname{Hom}_{\operatorname{Gal}_{\mathbb{F}_q}}(T_\ell A, T_\ell B)$$

(using the fact that $T_\ell A$ is a semisimple $\operatorname{Gal}_{\mathbb{F}_q}$-representation, thus determined by Frobenius eigenvalues, and that for simple abelian varieties $\operatorname{Hom}(A, B) \neq 0$ iff A, B are isogenous).

Surjectivity was shown by Honda [Hon68]. For this direction we need to produce an abelian variety from a Weil integer. In fact the Weil integer is used to construct a CM abelian variety in characteristic zero, which is then reduced to characteristic p to get the desired abelian variety over $\mathbb{F}_q$. As a corollary, we see that every isogeny class of abelian varieties over a finite field contains the reduction of a CM abe;ilan variety from characteristic zero.

We can rephrase this parametrization of isogeny class purely group-theoretically. We'll restrict to the case of elliptic curves. An elliptic curve, being 1-dimensional, has p_A a monic integral polynomial of degree 2. This determines a semisimple conjugacy class in $\mathrm{GL}_2(\mathbb{Q})$, the class of which it is the characteristic polynomial. The conditions of Honda-Tate theory can be translated to group theoretic conditions, cf. Theorem 10.4 of [Sch11]. Namely, we require that our conjugacy class has trace in $\mathbb{Z}$ and determinant q (so that its eigenvalues are Weil q-integers), and is elliptic in $\mathrm{GL}_2(\mathbb{R})$ (so that it corresponds to an elliptic curve, rather than a higher-dimensional abelian variety). *Elliptic* is a technical condition which in this case means the two eigenvalues are complex conjugates, including the case that they are real and identical.

The result is that isogeny classes of elliptic curves over $\mathbb{F}_q$ are in bijection with semisimple conjugacy classes of $\mathrm{GL}_2(\mathbb{Q})$ which are elliptic in $\mathrm{GL}_2(\mathbb{R})$ and which have determinant equal to q and trace in $\mathbb{Z}$. This is a purely group-theoretic description of the sort we're looking for.

2.3 Points in an Isogeny Class

Now that we have a satisfactory expression for isogeny classes, we want to count elliptic curves (with level structure) isogenous to a fixed elliptic curve E_0 over $\mathbb{F}_q$. We do this by using cohomology to count isogenies. For more details see §5 of [Sch11], or Part III of [Kot90] for a similar discussion in the case of Siegel modular varieties.

Define

$$H^p = H^1_{\text{ét}}(E_{0,\overline{\mathbb{F}}_p}, \mathbb{A}_f^p)$$

and

$$H_p = H^1_{\text{crys}}(E_0/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

(for ease of notation we write $\mathbb{Z}_q := W(\mathbb{F}_q)$ and $\mathbb{Q}_q := W(\mathbb{F}_q)[\frac{1}{p}]$). If $f : E_0 \to E$ is an isogeny, then we obtain lattices by pulling back the integral cohomology groups:

$$\Lambda^p = f^*(H^1_{\text{ét}}(E_{0,\overline{\mathbb{F}}_p}, \hat{\mathbb{Z}}^p)) \subset H^p$$

and

$$\Lambda_p = f^*(H^1_{\text{crys}}(E_0/\mathbb{Z}_q)) \subset H_p.$$

In fact, the isogeny f is determined by the pair (Λ^p, Λ_p), and such a pair arises from an isogeny exactly when Λ^p (resp. Λ_p) is stable under the Galois (resp. Frobenius/Verschiebung) action. This lets us express isogenies in a linear algebraic form; modding out by the choice of isogeny (to be precise, by a group of self-isogenies) gives an expression for the set of elliptic curves with level structure in a fixed isogeny class.

Define

$$\begin{aligned} Y^p &= \{(\Lambda^p, \phi) : \Lambda^p \subset H^p \text{ a } \mathrm{Gal}_{\mathbb{F}_q}\text{-stable } \hat{\mathbb{Z}}^p\text{-lattice}, \\ &\qquad \phi : (\mathbb{Z}/m\mathbb{Z})^2 \xrightarrow{\sim} \Lambda^p \otimes_{\hat{\mathbb{Z}}^p} \mathbb{Z}/m\mathbb{Z} \text{ a } \mathrm{Gal}_{\mathbb{F}_q}\text{-equivariant isomorphism}\}, \\ Y_p &= \{\Lambda_p : \Lambda_p \subset H_p \text{ a } F, V\text{-stable } \mathbb{Z}_q\text{-lattice}\}, \\ I &= (\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q})^\times \end{aligned}$$

(here $\mathrm{Gal}_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$). Note that I acts on Y^p and Y_p via its actions on H^p and H_p.

Proposition 3. *The association described above gives a bijection*

$$\{(E, \phi) \in \mathcal{M}_m(\mathbb{F}_q) : E \text{ isogenous to } E_0\} \xrightarrow{\sim} I \backslash Y^p \times Y_p.$$

2.4 Points on the Modular Curve

We can go further to describe the points in an isogeny class purely group-theoretically.

As H^p is a rank-2 $\mathbb{A}_f^p$-module, the group $\mathrm{GL}_2(\mathbb{A}_f^p)$ acts transitively on Y^p, and the subgroup stabilizing a point (Λ^p, ϕ) is

$$K_m^p = \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}^p) : g \equiv \mathrm{id} \bmod m\} \subset \mathrm{GL}_2(\mathbb{A}_f^p).$$

Thus the set of pairs (Λ^p, ϕ) is identified with the quotient $\mathrm{GL}_2(\mathbb{A}_f^p)/K_m^p$. To detect the $\mathrm{Gal}_{\mathbb{F}_q}$ action, consider the action of $\mathrm{Frob}_q \in \mathrm{Gal}_{\mathbb{F}_q}$ on H^p, and let $\gamma \in \mathrm{GL}_2(\mathbb{A}_f^p)$ be the corresponding element. A bit of work shows that we can rewrite Y^p as

$$Y^p(\gamma) = \{g \in \mathrm{GL}_2(\mathbb{A}_f^p)/K_m^p : g^{-1}\gamma g \in K_m^p\}.$$

Likewise we can rewrite Y_p group-theoretically. The group $\mathrm{GL}_2(\mathbb{Q}_q)$ acts transitively on lattices $\Lambda_p \subset H_p$, and the stabilizer of a lattice is $\mathrm{GL}_2(\mathbb{Z}_q)$. The set of lattices is identified with the quotient. Consider the action of F on H_p: since it is σ-linear, we can write it as $\delta\sigma$, where σ is the lift of Frobenius on $\mathbb{Q}_q$ and $\delta \in \mathrm{GL}_2(\mathbb{Q}_q)$. With a bit of work we see that Y_p can be rewritten

$$Y_p(\delta) = \{h \in \mathrm{GL}_2(\mathbb{Q}_q)/\,\mathrm{GL}_2(\mathbb{Z}_q) : h^{-1}\delta h^\sigma \in \mathrm{GL}_2(\mathbb{Z}_q)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\mathrm{GL}_2(\mathbb{Z}_q)\}.$$

We can now write the $\mathbb{F}_q$-points of our modular curve as

$$\mathcal{M}_m(\mathbb{F}_q) = \coprod_{(\gamma_0,\gamma,\delta)} I\backslash Y^p(\gamma) \times Y_p(\delta),$$

where $(\gamma_0, \gamma, \delta)$ runs over tuples where: γ_0 is a conjugacy class of semisimple elements of $\mathrm{GL}_2(\mathbb{Q})$ corresponding to an isogeny class of elliptic curves as explained above, and $\gamma \in \mathrm{GL}_2(\mathbb{A}_f^p)$, $\delta \in \mathrm{GL}_2(\mathbb{Q}_q)$ are the elements corresponding to Frobenius on étale and crystalline cohomology as above. The triples appearing in this disjoint union can be described purely in terms of group theory; this is the notion of a Kottwitz triple. The result is a purely group-theoretic expression for the set $\mathscr{M}_m(\mathbb{F}_q)$, ready for applications to cohomology.

3 The Langlands-Rapoport Conjecture

We would like to be able to perform this type of point counting on general Shimura varieties. There are two main obstacles to generalizing.

First, general Shimura varieties have more complicated moduli data. The modular curve simply parametrized elliptic curves with level structure, but for example in the case of Hodge type our Shimura variety parametrizes abelian varieties with a polarization, a set of tensors, and level structure. This makes it much more difficult to work with these objects concretely.

Second, most Shimura varieties are not honest moduli spaces at the integral or mod p level (or even rationally). Our modular curve has a moduli interpretation over $\mathbb{Z}[\frac{1}{m}]$, so the mod p points can be literally interpreted as elliptic curves with level structure over finite fields. Integral models of Hodge type Shimura varieties are embedded in integral models of Siegel modular varieties (up to a normalization, which is an important detail that we will ignore). The latter do have a moduli structure, so we can still associate abelian varieties (with various extra structures) to points on our Hodge type integral model. But the image is not well understood, so there is no complete description of points in terms of abelian varieties. This makes it nearly impossible to work with these objects concretely.

Nonetheless, at the cost of some abstraction, we do have a satisfactory description of the mod p points of Shimura varieties. We'll give the statement (without any detail), and then see how it relates to the more familiar case of the modular curve.

Conjecture 4. *Let $\mathscr{S}_p(G, X)$ be a suitable integral model of a Shimura variety of Hodge (or abelian) type arising from a Shimura datum (G, X). There is a bijection*

$$\mathscr{S}_p(G, X)(\overline{\mathbb{F}}_p) \xrightarrow{\sim} \coprod_{[\phi]} \varprojlim_{K^p} I_\phi(\mathbb{Q})\backslash X_p(\phi) \times X^p(\phi)/K^p$$

equivariant for the action of $G(\mathbb{A}_f^p)$ *and the Frobenius* Φ*, where*

- ϕ *varies over conjugacy classes of admissible morphisms* $\mathfrak{Q} \to G(\overline{\mathbb{Q}}) \rtimes \mathrm{Gal}_{\mathbb{Q}}$,
- K^p *varies over compact open subgroups of* $G(\mathbb{A}_f^p)$*, and*
- $X_p(\phi) \subset G(\overline{\mathbb{A}}_f^p)$, $X^p(\phi) \subset G(\hat{\mathbb{Q}}_p^{\mathrm{ur}})/G(\hat{\mathbb{Z}}_p^{\mathrm{ur}})$ *are subsets defined explicitly in terms of* ϕ.

This has been proven in many cases by Kisin [Kis17] (up to a twist in the action of $I_\phi(\mathbb{Q})$ on $X_p(\phi) \times X^p(\phi)$).

It is clear that the basic form of this expression is similar to the case of the modular curve. Indeed, we can understand it the same way: as a disjoint union over isogeny classes, and within each isogeny class is a set parametrizing prime-to-p isogenies and a set parametrizing p-power isogenies quotiented by a group of self-isogenies (the limit over K^p is a technical detail and should not damage the intuition).

The core of the difference between the statement for modular curves and this general one is the parametrization of isogeny classes. The disjoint union in this case is parametrized by admissible morphisms from the quasi-motivic Galois gerb $\mathfrak{Q}$ to G (or more precisely, the neutral Galois gerb $G(\overline{\mathbb{Q}}) \rtimes \mathrm{Gal}_{\mathbb{Q}}$ associated to G). To give a vague idea, a Galois gerb (over $\mathbb{Q}$) consists of the data of an algebraic group H over $\overline{\mathbb{Q}}$ and an extension of groups

$$1 \to H(\overline{\mathbb{Q}}) \to \mathfrak{H} \to \mathrm{Gal}_{\mathbb{Q}} \to 1$$

satisfying some axioms. The quasi-motivic Galois gerb $\mathfrak{Q}$ is a certain Galois gerb which is an extension of $\mathrm{Gal}_{\mathbb{Q}}$ by a certain pro-torus. Rather than going into more detail about the definition, we'll try to give an idea of the role it plays.

The idea is that $\mathfrak{Q}$ is (a good enough replacement for) the Tannakian fundamental group of the category of motives over $\overline{\mathbb{F}}_p$. (See §15 of [Mil17] for a discussion of the "fake" category of motives over $\overline{\mathbb{F}}_p$ and its fundamental group). For those unfamiliar, a Tannakian category is a category with particular nice "linear-algebraic" properties, and which is (by some abstract theoy) therefore equivalent to the category of representations of some group, which we call its fundamental group. Though we don't know what the category of motives is, we know enough about what it "should be" (in particular, it should be a Tannakian category) that we can define its fundamental group in a way that is useful to work with; namely, the quasi-motivic Galois gerb $\mathfrak{Q}$. But how does this fundamental group fit into our framework?

As a first step, Honda-Tate theory tells us that the motive associated to an abelian variety is its isogeny class. As a vague justification, the étale cohomology of an abelian variety is given by exterior powers of $H^1_{\text{ét}}$, and therefore determined by $H^1_{\text{ét}}$. This in turn is determined by the characteristic polynomial of Frobenius, and Honda-Tate theory says that the abelian varieties sharing a common characteristic polynomial of Frobenius are precisely the isogeny classes. So parametrizing isogeny classes of abelian varieties over $\overline{\mathbb{F}}_p$ is the same as parametrizing motives of abelian varieties over $\overline{\mathbb{F}}_p$.

Now to say that $\mathfrak{Q}$ is the Tannakian fundamental group of motives over $\overline{\mathbb{F}}_p$ is to say that the category of motives is equivalent to the category of representations of $\mathfrak{Q}$. Thus to give a motive over $\overline{\mathbb{F}}_p$ is the same as giving a representation $\mathfrak{Q} \to \mathrm{GL}(V)$. (The notion of a representation actually requires a slight adaptation to the setting of Galois gerbs, but we'll ignore this). A morphism $\mathfrak{Q} \to G$, i.e. a representation factoring through G, can then be thought of as a "motive with G-structure".

Finally, we don't want all motives with G-structure, only those of abelian varieties, and only abelian varieties suitable to contribute to our "moduli problem". This is the content of the condition that our morphism be *admissible*. Admissibility includes a condition at each prime and a global condition; for example, the condition at p can be understood as saying that the isocrystal associated to our motive is among the isocrystals we expect to see arising from an abelian variety on our Shimura variety.

So an admissible morphism $\phi : \mathfrak{Q} \to G$ can be thought of as a "motive of an abelian variety with G-strurcture" contributing to our Shimura variety, and we can imagine that this is a suitable replacement for an isogeny class. And the sets $X_p(\phi), X^p(\phi)$, though indirectly, can be thought of as parametrizing prime-to-p and p-power isogenies, and $I_\phi(\mathbb{Q})$ as a group of self-isogenies.

One may wonder, still, how any of this can be made precise without a tractable moduli description of our Shimura variety. Recall the theorem of Honda-Tate theory that every isogeny class of abelian varieties over $\mathbb{F}_q$ contains the reduction of a CM abelian variety from characteristic zero. One of the essential parts of Kisin's work is a generalization of this: after defining a notion of isogeny class on the mod-p points of our Shimura variety, he shows that every isogeny class contains the reduction of a "special point" from characteristic zero. One also shows that all admissible morphisms $\mathfrak{Q} \to G$ arise from special points, and this is what allows the two sides to be related.

References

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[Kis10] Mark Kisin. Integral models for Shimura varieties of abelian type. *J. Amer. Math. Soc.*, 23(4):967–1012, 2010.

[Kis17] Mark Kisin. mod p points on Shimura varieties of abelian type. *J. Amer. Math. Soc.*, 30(3):819–914, 2017.

[Kot90] Robert E. Kottwitz. Shimura varieties and λ-adic representations. In *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988)*, volume 10 of *Perspect. Math.*, pages 161–209. Academic Press, Boston, MA, 1990.

[Mil92] James S. Milne. The points on a Shimura variety modulo a prime of good reduction. In *The zeta functions of Picard modular surfaces*, pages 151–253. Univ. Montréal, Montreal, QC, 1992.

[Mil08] James S. Milne. Abelian varieties (v2.00). pages 166+vi, 2008.

[Mil17] James S. Milne. Introduction to shimura varieties. page 172, 2017.

[Sch11] Peter Scholze. The Langlands-Kottwitz approach for the modular curve. *Int. Math. Res. Not. IMRN*, (15):3368–3425, 2011.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.