ON TWISTED MODULAR CURVES

FRANCISZEK KNYSZEWSKI

Abstract. This is an informal set of notes accompanying a talk given at University of Oxford's Junior Number Theory Seminar in May 2024.

Modular curves are moduli spaces of elliptic curves equipped with certain level structures. This talk will be concerned with how the attendant theory has been used to answer questions about the modularity of elliptic curves over $\mathbb{Q}$ and over quadratic fields. In particular, we will outline two instances of the modularity switching technique over totally real fields: the 3-5 trick of Wiles and the 3-7 trick of Freitas, Le Hung and Siksek. The recent work of Caraiani and Newton over imaginary quadratic fields naturally leads one to consider the decent theory of 'twisted' modular curves, and this will be the focus of the final part of the talk.

Contents

1. Pre-classical theory

We start with the familiar complex picture. Elliptic curves over $\mathbb{C}$ (i.e., smooth projective curves of arithmetic genus 1 equipped with a structure of a group scheme) are complex tori, as follows from the degree-genus formula and from the theory of the Weierstrass $\wp$-function, and these have the form $\mathbb{C}/\Lambda$ for $\Lambda \subseteq \mathbb{C}$ a lattice.

Now holomorphic maps $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ are all of type $x \mapsto mz + c$ where $m\Lambda \subseteq \Lambda'$ (to prove this: $\mathbb{C}$ is the universal analytic cover of any complex torus). These are homomorphisms iff $b = 0$ and so to classify elliptic curves over $\mathbb{C}$ it suffices to classify orbits of lattices in $\mathbb{C}$ under dilatations.

Let $\mathfrak{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ be the complex upper half-plane. Then we need only consider lattices of type $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ where $\tau \in \mathfrak{H}$. $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{H}$ via Mobius transformations, and in fact $\Lambda_\tau = \Lambda_{\tau'}$ iff τ and τ' are equal modulo $\mathrm{SL}_2(\mathbb{Z})$. Therefore we have an equality between

$$\mathcal{M}^{1,1} = \{\text{complex elliptic curves over } \mathbb{C}\},$$

and

$$Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}.$$

Date: May 5, 2024.

More generally one would like to consider elliptic curves with a level structure (motivation: Galois representations, to be discussed momentarily). Let $E/\mathbb{C}$ be an elliptic curve and $N \geq 1$ an integer. Then

$$E[N] = \{x \in E \mid Nx = 0\}$$

is isomorphic to $(\mathbb{Z}/N)^2$. We let $\mathcal{M}^{1,1}(N)$ – nonstandard notation! – be the moduli stack of elliptic curves E equipped with a symplectic isomorphism $(\mathbb{Z}/N)^2 \xrightarrow{\sim} E[N]$. (There is a notion of the determinant on $E[N]$, the Weil pairing, and a symplectic isomorphism is by definition required to identify the determinant on each side.) Question: is this representable?

The answer is yes, and can show this in a manner analogous to the above. Let

$$\Gamma(N) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N))$$

be the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level N. If

$$Y(N) = \Gamma(N)\backslash\mathfrak{H}$$

then we have $\mathcal{M}^{1,1}(N) = Y(N)$. Here is how this works: take $E = \mathbb{C}/\Lambda_\tau$ as your elliptic curve. Then massaging the isomorphism $(\mathbb{Z}/N)^2 \cong E[N]$ slightly, we may assume it is given by $(1,0) \mapsto 1/N$, $(0,1) \mapsto \tau/N$. Conversely can check that $\Gamma(N)\tau = \Gamma(N)\tau'$ iff τ and τ' define the same class in $\mathcal{M}^{1,1}(N)$, as required.

Remark. One can also consider other modular problems: e.g., prescribing a cyclic subgroup of $E[N]$ or order N or a point in $E[N]$ of order N. These give the moduli stacks $\mathcal{M}_0^{1,1}(N)$ and $\mathcal{M}_1^{1,1}(N)$, represented by quotients of $\mathfrak{H}$ by

$$\Gamma_0(N) = \mathrm{SL}_2(\mathbb{Z}) \cap B_2(\mathbb{Z}/N)$$

and

$$\Gamma_1(N) = \mathrm{SL}_2(\mathbb{Z}) \cap U_2(\mathbb{Z}/N)$$

respectively. For simplicity of the exposition, we will not be concerned with these, though they are equally as important.

The $Y(N)$ are noncompact Riemann surfaces and so we cannot use algebraic geometry to study them. We must therefore compactify them to obtain $X(N)$, the principal modular curve of level N. The terminology is justified: any compact Riemann surface arises as the analytification of a unique smooth projective curve over $\mathbb{C}$. As a set, $X(N) = \Gamma(N)\backslash\overline{\mathfrak{H}}$ where

$$\overline{\mathfrak{H}} = \mathfrak{H} \sqcup \mathbb{QP}^1 \subseteq \mathbb{CP}^1$$

is acted upon by $\Gamma(N)$ via Mobius maps. The points of $X(N) \setminus Y(N)$ are called the cusps of the modular curve/congruence subgroup. The topology on $X(N)$ is not the one inherited from $\mathbb{CP}^1$ as then we do not obtain a Hausdorff space. Instead, define a topology using charts in such a way that everything works out: the underlying idea is to concentrate the topology of $\mathfrak{H}$ near the real line. This can be a bit tricky, as there are points of $\mathfrak{H}$ having large stabiliser under $\Gamma(N)$ (these are the so called 'elliptic points'). See Diamond and Shurman, Chapter 2.

Remark. The points of $X(N)$ also represent a a moduli problem, which is given by a 'compactification' of $\mathcal{M}^{1,1}(N)$. The point is that one considers generalised elliptic curves. These are no longer required to be smooth but can have at worst a nodal singularity, among some other conditions.

In fact, generalised elliptic curves which are not elliptic curves already turn out to just be Neron polygons, i.e., a bunch of copies of $\mathbb{P}^1$ glued together into a link. The unique cusp of $X(1) \cong \mathbb{CP}^1$, for example, corresponds to the nodal cubic.

It is easy to compute the genus of $X(N)$, by applying the Riemann-Hurwitz formula to the Galois covering

$$(*) \qquad X(N) \to X(1).$$

For example, $X(5)$ has genus 0, whereas $X(7)$ has genus 3.

2. Twists of modular curves

We would now like to descend down to the world of number fields. There is a (limited) classical approach which achieves this, the point being to realise $(*)$ over a number field, using Galois theory. There is a 'universal elliptic surface'

$$\mathcal{E} \to Y(1)$$

whose fibres classify isomorphism classes of elliptic curves over $\mathbb{C}$. But $\mathcal{E}$ is defined over $\mathbb{Q}(j)$ not just $\mathbb{C}(j)$. So for instance once we know that the function field of $X(N)$ is $\mathbb{C}(j, x(\mathcal{E}[N]))$, and that this has Galois group $\mathrm{SL}_2(\mathbb{Z}/N)/\{\pm 1\}$ over $\mathbb{C}(j)$, we can ask when the Galois group of $F(j, x(\mathcal{E}[N]))$ over $F(j)$ is $\mathrm{SL}_2(\mathbb{Z}/N)/\{\pm 1\}$ and also when this field is in fact a function field of an algebraic curve over F. (Here, F is a number field.) It turns out that this is the case provided F contains a primitive N-th root of unity, so at least $X(N)$ is defined over $\mathbb{Q}(\zeta_N)$.

Much more successful is the moduli approach of Deligne-Rapoport. This is rather involved, but the idea is to consider the compactified stack $\overline{\mathcal{M}^{1,1}(N)}$ and prove that it is representable. This leads to the following result.

Theorem 1 (Deligne-Rapoport)**.** *There is a curve $X(N)$ over $\mathbb{Z}[1/N]$ whose points over $\mathbb{C}$ are in bijection with the points of $\Gamma(N)\backslash\overline{\mathfrak{H}}$.*

For the purpose of this talk, it suffices to know that the modular curve is defined over your favourite number field F. There is of course the question of uniqueness.

Let X for now denote a smooth projective curve over F. Then a twist X' of X over F is another smooth projective curve which becomes isomorphic to X over $\overline{F}$. How do we classify twists? Let

$$\phi : X' \to X$$

be an isomorphism defined over $\overline{F}$. To measure the failure of this being defined over F, we consider the function

$$G_F \to \mathrm{Aut}_{\overline{F}}(X), \quad \sigma \mapsto \sigma \circ \phi \circ \sigma^{-1} \circ \phi^{-1}.$$

This is easily seen to be a 1-cocycle, and in fact our construction furnishes a bijection

$$\{F\text{-twists of } X \text{ up to isomorphism}\} \cong H^1(G_F, \mathrm{Aut}_{\overline{F}}(X))$$

(see Silverman, Chapter X). It is in general hard to give an explicit description of the inverse of this map, as the proof of its surjectivity relies on the correspondence between smooth projective curves and their function fields.

We will see in the next couple of sections that the non-uniqueness of the model for $X(N)$ over F is a benefit rather than a draw-back: indeed, this will allow us to consider modified moduli problems without changing the geometry of $X(N)$!

For instance if E is an elliptic curve over F then there is a twist $X_E(N)$ of $X(N)$ over F whose non-cuspidal rational points parameterise elliptic curves A equipped with a Galois-equivariant isomorphism $A[N] \cong E[N]$. The cocycle is constructed as follows: fix an symplectic isomorphism

$$\psi : E[N] \to (\mathbb{Z}/N)^2 \to \mathbb{Z}/N \times \mathbb{C}^\times[N],$$

which is also G_F-equivariant. Then we have a cocycle

$$G_F \to \mathrm{Sp}(\mathbb{Z}/N \times \mathbb{C}^\times[N]), \quad \sigma \mapsto \sigma \circ \psi \circ \sigma^{-1} \circ \psi^{-1}$$

and $\mathrm{Sp}(\mathbb{Z}/N \times \mathbb{C}^\times[N])$ acts on $X(N)$ so that there is a homomorphism

$$\mathrm{Sp}(\mathbb{Z}/N \times \mathbb{C}^\times[N]) \to \mathrm{Aut}_{\overline{F}}(X(N)).$$

We obtain the desired cocycle upon composition.

3. Modularity of semi-stable elliptic curves

Let us quickly prove Fermat's last theorem, modulo several very deep results. Precisely, we will demonstrate why any semi-stable elliptic curve $E/\mathbb{Q}$ is modular, which is a rather neat argument. (Semi-stable means it has at worst a multiplicative reduction everywhere.)

Let p be a prime number, and consider a continuous Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$$

of cyclotomic determinant, which is odd, irreducible, and which is unramified almost everywhere. We say ρ is modular if it arises as the p-adic representation attached to a modular eigenform. We can also reduce ρ mod p (and semi-simplify) to obtain

$$\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p);$$

we say a mod-p Galois representation $\overline{\rho}$ is modular if it arises as a semi-simplification of the mod-p reduction of a modular Galois representation.

The first ingredient is the modularity lifting theorem of Wiles and Taylor-Wiles.

Theorem 2. *Suppose that $p > 2$, that $\overline{\rho}$ is irreducible, and that ρ is semi-stable. If $\overline{\rho}$ is modular then so is ρ.*

(The semi-stability assumption is slightly technical, and in fact can be discarded by the subsequent work of Breuil, Conrad, Diamond, Taylor: it essentially means that ρ looks like a representation arising from the étale cohomology of a variety with semi-stable reduction.)

Accordingly, our focus shifts towards proving that the $\overline{\rho}$ of interest are modular. This is the content of a conjecture of Serre, now a theorem due to Khare and Wintenberger. It says that if $\overline{\rho}$ is continuous odd and absolutely irreducible then it must be modular. In the 1990s, however, this was still an open problem, with only the following special case known to hold.

Theorem 3 (Langlands-Tunnell)**.** *If $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_3)$ is continuous odd and irreducible, then it is modular.*

This is a very deep, analytic theorem: indeed, it relies on the non-compact trace formula developed by Arthur. (To link this with Serre's conjecture, we note that irreducibility and absolute irreducibility are equivalent for odd representations in odd characteristic, seeing as complex conjugation acts diagonalisably.)

So let E be a semi-stable modular curve and let $\overline{\rho}$ be the representation of $G_{\mathbb{Q}}$ arising from the 3-adic Tate module of E. Then $\overline{\rho}$ is continuous, odd, irreducible, unramified outside a finite set of places, and it has cyclotomic determinant. If $E[3]$ is irreducible, then $\overline{\rho}$ is modular by the Langlands-Tunnell theorem, so ρ is modular by the modularity lifting theorem, and we win.

Suppose on the other hand that $E[3]$ is reducible. If $E[5]$ were also reducible then E would define a rational point on $X_0(15)$. The latter has genus 1 and admits finitely many such points; one can check explicitly that none of these come from a semi-stable elliptic curve (and in fact all of these points are modular anyway). Okay, so $E[5]$ must be irreducible.

Consider now $X_E(5)$. This has genus 0 and and admits a rational point, so must be isomorphic to $\mathbb{P}^1$. We can now find a semi-stable elliptic curve $E'/\mathbb{Q}$ defining a point on $X_E(5)$ such that $E'[3]$ is irreducible: to find it, we need to look for points on $X_E(5)$ 3-adically very far away from E (so as to guarantee irreducibility) and 5-adically very close to E (so as to guarantee semi-stability), and such a point exists by Hilbert's irreducibility theorem. By Langlands-Tunnell, $E'[3]$ is modular so E' is modular so $E'[5] \cong E[5]$ is modular so E itself must be modular.

4. Modularity over real quadratic fields

Freitas, Le Hung and Siksek recently proved that all elliptic curves over real quadratic fields are modular. Their proof invariably draws upon the strategy we saw in the previous section, generalising appropriate bits. Let us outline how the 3-5 trick adapts to this setting. This should in particular shed a little bit more light on how Hilbert irreducibility was used by Wiles.

Let F be a number field (say, an RQF). By a thin subset of $\mathbb{P}^n(F)$ we understand a subset of finitely many principal thin subset. Principal thin subsets T of $\mathbb{P}^n(F)$ fall into two categories (sometimes called Type I and Type II respectively):

- $T = V(F)$ where V is a proper Zaryski-closed F-subvariety of $\mathbb{P}^n(F)$;
- $T = \pi(V(F))$ where $\pi : V \to \mathbb{P}^n$ is a generically surjective F-morphism of degree at least 2, and V is an irreducible n-dimensional F-variety.

Then Hilbert's irreducibility theorem says that $\mathbb{P}^n(F)$ is not thin.

Here is the modularity switching result we need over real quadratic fields.

Lemma 4. *Let E be an elliptic curve over the totally real field F. There is a degree-4 totally real extension K/F and an elliptic curve E'/K such that*

(i) $K \cap F(E[7]) = F$;
(ii) $E[7] \cong E'[7]$ *as G_K-modules;*
(iii) $\mathrm{SL}_2(\mathbb{F}_3) \subseteq \overline{\rho}_{E',3}(G_K)$.

Proof. Fix an embedding $X_E(7) \hookrightarrow \mathbb{P}^2$. Let $\mathbb{P}^{2,\vee}$ be the dual projective plane parametrising lines in $\mathbb{P}^2$. By Bézout, it makes sense to consider the map

$$\iota : \mathbb{P}^{2,\vee} \hookrightarrow \mathrm{Sym}^4 X_E(7), \quad \ell \mapsto \ell \cdot X_E(7)$$

We now wish to produce a line ℓ outside a cleverly chosen thin subset of $\mathbb{P}^{2,\vee}$.

Let S_1 be the set of all lines passing through either a (geometric) cusps of $X_E(7)$ or through a point of $X_E(7)$ defined over $F(E[7])$. The former set is clearly finite; the latter is finite by Faltings' theorem since $X(7)$ has genus 3. So S_1 is thin.

Let S_2 be the set of lines tangent to $X_E(7)$. These are parameterised by the curve dual to $X_E(7)$, and therefore S_2 is thin.

What have we got so far? Any line ℓ not lying in $S_1 \cup S_2$ must intersect $X_E(7)$ in an irreducible degree 4 divisor, or in a sum of two irreducible degree 2 divisors. We wish to get rid of the latter possibility. This will be so once we show that the set S_3 of all those ℓ for which $\iota(\ell)$ lies in the image of

$$\mathrm{Sym}^2 X_E(7) \times \mathrm{Sym}^2 X_E(7) \to \mathrm{Sym}^4 X_E(7), \quad (D_1, D_2) \mapsto D_1 + D_2$$

is a thin subset of $\mathbb{P}^{2,\vee}$. This can be done by embedding $\mathrm{Sym}^2 X_E(7)$ in its Jacobian via the Abel-Jacobi map, and noting that the F-rational points of its image can be written as $\{D_i, E_j(F)\}_{i,j}$ for finitely many divisors D_i over F and finitely many elliptic curves E_j over F (this follows from Faltings' theorem).

For ℓ not in $S_1 \cup S_2 \cup S_3$ we get a point on $X_E(7)$ defined over some degree 4 extension K/F. This point is non-cuspidal, and therefore defines an elliptic curve E' over K satisfying (ii). To ensure that (i) holds we need to remove another thin set S_4. Note that $F(E[7]) \cap K$ can be either F or a quadratic extension M thereof, by choice of S_1. There are only finitely many such $M \subseteq F(E[7])$, and for each of these we want $\iota(\ell)$ to avoid the image of

$$\mathrm{Sym}^2 X_E(7) \to \mathrm{Sym}^4 X_E(7), \quad D \mapsto D + D^{\sigma_M}$$

where $\sigma_M \in \mathrm{Gal}(M/F)$ is conjugation. Using the Abel-Jacobi map again, this can be ensured outside of a thin set S_4.

We may remove another thin set S_5 to ensure (iii); this follows by classifying maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$, and looking at points of attendant modular curves.

So it remains to prove that we can take K to be totally real. For this, let σ_i be the (real) embeddings of F. Write X_i for the base change of $X_E(7)$ along $\sigma_i : F \hookrightarrow \mathbb{R}$. Then each X_i is isomorphic to a real twist of the Klein quartic $X(7)$, and hence must itself be the Klein quartic (look at conjugacy classes in $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \ltimes \mathrm{Aut}_{\mathbb{C}}(X(7))$; it's an explicit calculation to show $H^1 = *$). This has equation $x^3y + y^3z + z^3x = 0$. The line $2y + z = 0$ meets this in four distinct real points, and so there are open subsets $U_i \subseteq \mathbb{P}^{2,\vee}(\mathbb{R})$, one for each embedding, such that any $\ell \in U_i$ meets X_{σ_i} in four distinct real points. Consider

$$U = \{\ell \in \mathbb{P}^{2,\vee}(F) \mid \sigma_i(\ell) \in U_i\}.$$

All that is left is to show that $U \setminus \cup S_i$ is nonempty. But U is not thin, as $\mathbb{P}^{2,\vee}(F)$ is given by finitely many translates of $\prod_i U_i$ by elements of $\mathrm{PGL}_2(F)$ (since $\prod_i \mathbb{P}^{2,\vee}(\mathbb{R})$ is compact, and since $\mathrm{PGL}_2(F)$ is dense in $\prod_i \mathrm{PGL}_2(\mathbb{R})$ by weak approximation) and Hilbert irreducibility says that $\mathbb{P}^{2,\vee}(F)$ is not thin! □

Given the previous section, it should not be too surprising to see condition (ii), but what about (i) and (iii)? Well (iii) is needed for an appropriate generalisation of Langlands-Tunnell to totally real fields: instead of absolutely irreducible we can get away with the restriction to the $G_{K(\zeta_3)}$ to be so, and this is guaranteed by (iii). So we know E' is modular and hence that $\mathrm{Res}_{K/F} E[7]$ is modular.

In fact, it is possible to show (with some amount of effort, taking F to be an RQF and analysing rational points on many different modular curves) that we can assume $\mathrm{Res}_{F(\zeta_7)/F} E[7]$ to be absolutely irreducible. We thus come to the purpose of condition (i): it guarantees that $\mathrm{Res}_{K/F} E[7]$ is absolutely irreducible. Indeed,

$$\overline{\rho}_{E,7}(G_{L(\zeta_7)}) = \overline{\rho}_{E,7}(G_L) \cap \mathrm{SL}_2(\mathbb{F}_7)$$

for $L = F$ or $L = K$, and we know that the images of G_F and G_K coincide by Galois theory and by (i), since $\overline{\rho}_{E,7}(G_L)$ is the Galois group of $L(E[7])/L$.

We know that $\mathrm{Res}_{K/F} E[7]$ is modular and also absolutely irreducible, so E_K is modular by an appropriate generalisation of modularity lifting. However K/F has degree 4 so is solvable; therefore cyclic base implies that E is modular.

5. Projective twists

The recent work of Caraiani and Newton aims to tackle modularity of elliptic curves over imaginary quadratic fields. This is really serious stuff as we are no longer in the totally real world. The difficulty is that the relevant Hecke eigenvalues come from the cohomology of locally symmetric spaces which are harder to handle than Shimura varieties; in particular, one works with real, and not complex, manifolds.

They prove that, statistically, all elliptic curves defined over F are modular, where F belongs to a certain infinite family of IQFs satisfying a technical condition.

The implementation of a 3-7 switch in the setting of IQFs seems rather subtle. The totally real condition should be replaced by the field in question being CM. One solution is to look for totally real points on the Weil restriction $\mathrm{Res}_{F/\mathbb{Q}} X_E(7)$ but this is a surface rather than a curve. Nevertheless, one can use this to produce CM points on $X_E(7)$ but it is then hard to guarantee that they are solvable.

A shortcut is to consider when $X_E(7)$ is already defined over $\mathbb{Q}$, as then we can find loads of such points. This is where some of my own work comes in.

Given an elliptic curve E/F, we have looked at the mod-p representation

$$\overline{\rho}_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{F}_p).$$

Composing with the natural projection

$$\mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$$

we obtain the projective Galois representation $\overline{\rho}^{\mathrm{pr}}_{E,p}$. By class field theory, we really only care about $E[p]$ up to a character when it comes to modularity, and therefore it is natural to look for analogues of $X_E(p)$ parametrising elliptic curves with a given projective representation at p.

For this we need to consider a particular model of $X(p)$, which is something we glossed over previously. This is defined by the subgroup

$$\mathbb{F}_p^\times \cup V\mathbb{F}_p^\times \subseteq \mathrm{GL}_2(\mathbb{F}_p)$$

where

$$V = \begin{pmatrix} 0 & v \\ -1 & 0 \end{pmatrix}$$

and where $v \in \mathbb{F}_p^\times$ is a quadratic non-residue. The point is that this subgroup has full determinant and so our model $X(p)$ is defined over $\mathbb{Q}$. It is also possible to explicitly describe the Galois action on $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X(p))$, something we will need for cohomology and twisting. Provided $p \geq 7$, we have that $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X(p)) \cong \mathrm{PSL}_2(\mathbb{F}_p)$ (essentially by the Hurwitz automorphism theorem) and $G_{\mathbb{Q}}$ acts on the latter via conjugation through

$$\eta : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(p)/\mathbb{Q}) \xrightarrow{\sim} \langle V \rangle \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

where $\mathbb{Q}(p)$ is the unique quadratic field inside $\mathbb{Q}(\zeta_p)$. This is also the field defined by the projective cyclotomic character.

Let F be any number field and fix a projective Galois representation

$$\overline{\rho} : G_F \to \mathrm{PGL}_2(\mathbb{F}_p)$$

with cyclotomic determinant. Let $\overline{\rho}^\vee$ be the contragredient of $\overline{\rho}$; the former is obtained from the latter by tasking the inverse-transpose. Then $\eta\overline{\rho}^\vee$ is a cocycle with values in $\mathrm{PSL}_2(\mathbb{F}_p)$, and hence defines a twist $X_{\overline{\rho}}(p)$ of $X(p)$. This construction first appears in a paper of Fernandez, Lario and Rio, and what is important for us is that they prove that the non-cuspidal non-CM F-rational points of $X_{\overline{\rho}}(p)$ correspond to elliptic curves over F whose projective representation is given by $\overline{\rho}$.

6. Descent theory

We conclude by discussing the following result.

Theorem 5 (Knyszewski)**.** *The curve $X_{\overline{\rho}}(p)$ is defined over $\mathbb{Q}$ if and only if $\overline{\rho}$ extends to a representation $\overline{r} : G_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_p)$ with cyclotomic determinant.*

We sketch how the proof of Theorem 5 proceeds. We look at the when $\overline{\rho}$ extends to $G_{\mathbb{Q}}$. (Chronologically, this in fact came last as a thing to think about, but maybe it makes more sense to explain the proof in the backward direction!) For $F/\mathbb{Q}$ cyclic there is a fairly straightforward criterion for when $\overline{\rho}$ extends to $G_{\mathbb{Q}}$.

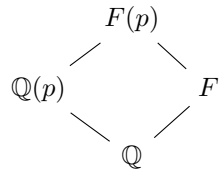
Let $K \subseteq F$ be a subfield and suppose that F is Galois over K. We say $\overline{\rho}$ is compatible with F/K if for all $\tau \in G_K$ there is some $g_\tau \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that:

- $\overline{\rho}(\tau\sigma\tau^{-1}) = g_\tau\overline{\rho}(\sigma)g_\tau^{-1}$ for all $\sigma \in \sigma \in G_F$;
- $\overline{\rho}(\tau^d) = g_\tau^d$ for d the least positive integer such that $\tau^d \in G_K$.

If additionally $\det(g_\tau)$ coincides with the projective cyclotomic character evaluated at τ, we speak of strong compatibility.

It is not too hard to prove that if F/K is cyclic then $\overline{\rho}$ extends to G_K iff it is compatible with F/K, and that this extension moreover has cyclotomic determinant iff the compatibility with F/K is in fact strong.

The caveat is that $F/\mathbb{Q}$ need not be cyclic, or indeed even Galois. Here is how we fix this. Let $F(p)$ be the compositum of F with $\mathbb{Q}(p)$. Consider the lattice of field extensions



Then instead of looking at $\overline{\rho}$ directly, we first restrict it to $F(p)$. Using cohomology, we can prove that $X_{\overline{\rho}}(p)$ is defined over $\mathbb{Q}$ iff $\overline{\rho}|_{G_{F(p)}}$ extends to a representation of $G_{\mathbb{Q}(p)}$ with cyclotomic determinant which also satisfies some auxiliary conditions. One of these conditions implies that this extension of $\overline{\rho}|_{G_{F(p)}}$ is strongly compatible with $\mathbb{Q}(p)/\mathbb{Q}$ and hence extends to $G_{\mathbb{Q}}$. Another guarantees that this extension agrees with $\overline{\rho}$ on F. The cohomological argument we allude to requires one to distinguish between two cases, namely $\mathbb{Q}(p) \nsubseteq F$ and $\mathbb{Q}(p) \subseteq F$.

Remark. Elliptic curves over number fields correspond to rank-1 Drinfeld modules over function field. One can define analogous moduli problem as for elliptic curves, the level structures being given by the ideals in the ring of integers of our fields. This lends itself to the notion of a Drinfeld modular curve, which in the situation of sections 5 and 6 would not be a curve as such, but rather an Artin stack: prime ideals in the ring of integers are somehow too small to guarantee representability. It would be interesting to see if Theorem 5 admits an analogue for function fields.

Here is something which might be relevant to the modularity story.

Corollary 6. *Suppose that F is a cyclic number field of degree d, and pick a $\tau \in G_{\mathbb{Q}}$ which restricts to a generator of $\mathrm{Gal}(F/\mathbb{Q})$. Let E/F be an elliptic curve, and put $X_E^{\mathrm{pr}}(p)$ for the twist of $X(p)$ by $\overline{\rho}_{E,p}^{\mathrm{pr}}$. Then $X_E^{\mathrm{pr}}(p)$ is defined over $\mathbb{Q}$ if and only if there exists a continuous character $\overline{\chi} : G_F \to \mathbb{F}_p^\times$ and a symplectic isomorphism*

$$\varphi : \tau(E)[p] \xrightarrow{\sim} E[p] \otimes \overline{\chi}$$

of G_F-representations such that $(\varphi \circ \tau)^d = \pm \tau^d$ as maps on $E[p]$.

If F is an imaginary quadratic field then choosing τ to be a complex conjugation, the above condition on $\varphi \circ \tau$ is equivalent to: $\varphi \circ \tau$ is represented by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ or } \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

with respect to some basis for $E[p]$, where $i \in \mathbb{F}_p^\times$ has $i^2 = -1$ (if such an i exists).

Corollary 6 can be obtained using Theorem 5 and the strong compatibility stuff we mentioned above. Anyway, this is probably a good place to stop.

Email address: franciszek.knyszewski@stcatz.ox.ac.uk

St Catherine's College, University of Oxford, Oxford OX1 3UJ, United Kingdom