Mod p Galois Reps and Abelian Varieties

Shiva Chidambaram

Junior Number Theory Days
December 4, 2020

Preliminaries

A – principally polarized abelian variety over $\mathbb{Q}$ of dim g

Then, $A[p] \simeq \mathbb{F}_p^{2g}$ as a vector space.

The polarization $(\lambda : A \to A^\vee)$ induces a non-degenerate, alternating, bilinear pairing $A[p] \times A[p] \longrightarrow \mu_p$

Eg: $g = 1$. E – elliptic curve over $\mathbb{Q}$.

$E[p] \simeq (\mathbb{Z}/p)^2$

$\rho_{E,p} : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F}_p)$

$\det \rho_{E,p} = \chi_p$ = the mod-p cyclotomic character.

$\cancel{\rho_{E,p} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}}$

Galois action on the torsion subgroup $A[p]$ gives a mod-p rep

$$\rho_{A,p} : G_{\mathbb{Q}} \longrightarrow GSp(2g, \mathbb{F}_p)$$

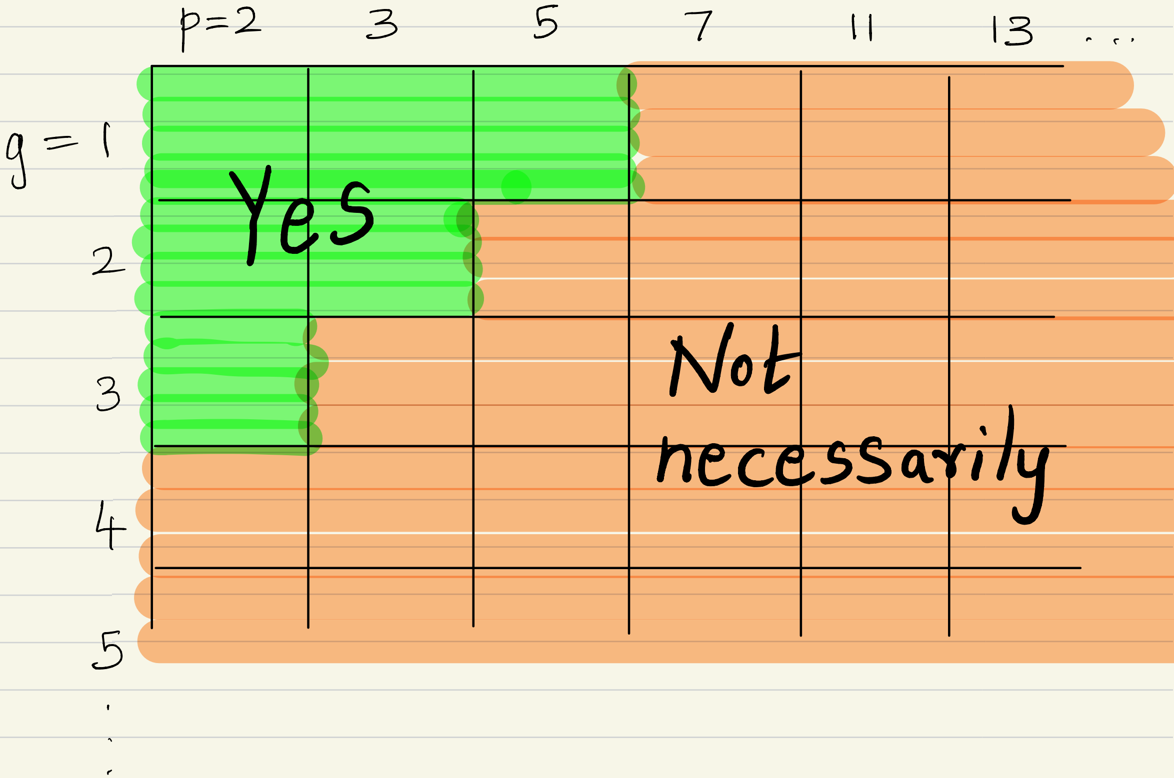
If $\chi_{sim} : GSp(2g, \mathbb{F}_p) \longrightarrow \mathbb{F}_p^{\times}$ is the similitude character, then

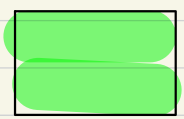
$$\chi_{sim} \circ \rho_{A,p} = \chi_p$$

because the pairing is equivariant wrt Galois action.

Question: Given a rep $\rho : G_{\mathbb{Q}} \to GSp(2g, \mathbb{F}_p)$ with $\chi_{sim} \circ \rho = \chi_p$, does it arise from an abelian variety over $\mathbb{Q}$?

If yes, can we find all such abelian varieties?

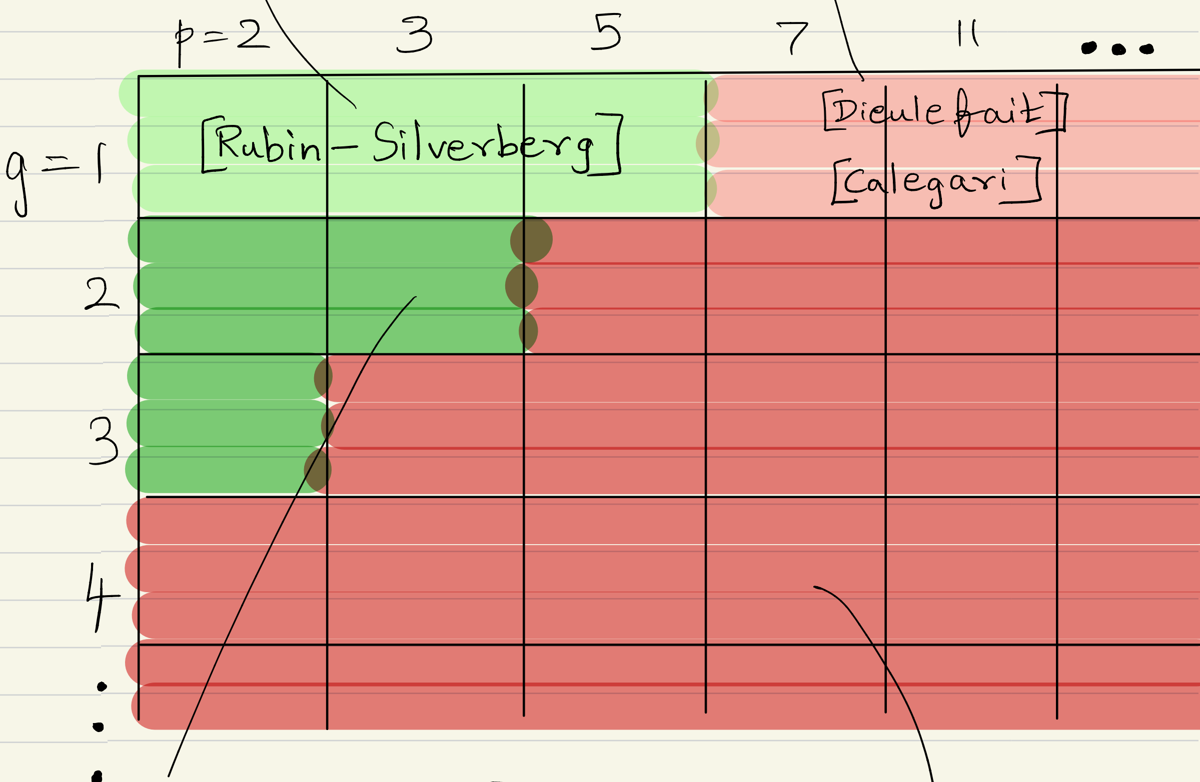




Exactly the pairs (g, p) for which $\mathcal{A}_g(p)$ is geometry rational.

$X(p)$ and all its twists $X(e)$ are $\simeq \mathbb{P}^1_{\mathbb{Q}}$.

Examples of modular Galois reps which fail Hasse bound $|a_p| \leq 2\sqrt{p}$



[Calegari–C–Roberts]

Explicit formulae describing all abelian surfaces with fixed 3-torsion

[C]

There exist mod-p Galois reps not arising from abelian varieties

Part I

$(g,p) = (1,3)$

$X(3)$ = modular curve for full 3-level structure, i.e., $\rho_0 = \mathbb{Z}/3 \oplus \mu_3$

$$\begin{array}{ccc} X(3) & \xrightarrow{\sim} & \mathbb{P}^1_{\mathbb{Q}} \\ \Psi & & \\ \tau & \longmapsto & (U(\tau) : V(\tau)) \end{array}$$

where $\{U, V\}$ is a basis of the space of modular forms of wt 1, level $\Gamma(3)$

For a given $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_3)$ with $\det \rho = \chi_3$, $X(\rho)$ is a twist of $X(3)$.

The coh. class $\in H^1(G_{\mathbb{Q}}, PGL(2,\overline{\mathbb{Q}}))$ representing the twist comes from a class $\in H^1(G_{\mathbb{Q}}, SL(2,\mathbb{F}_3))$ as

$$\begin{array}{ccc} & SL(2,\mathbb{F}_3) & \\ & \downarrow & \\ Aut(X(3)) = & PSL(2,\mathbb{F}_3) & \longrightarrow PGL(2,\overline{\mathbb{Q}}) \end{array}$$

So, by Hilbert 90, the class is trivial and

$$\begin{array}{ccc} X(\rho) & \xrightarrow{\sim} & \mathbb{P}^1_{\mathbb{Q}} \\ \psi & & \\ \tau & \longmapsto & (U'(\tau) : V'(\tau)) \end{array}$$

The new coordinates U', V' are $\overline{\mathbb{Q}}$-linear combinations of U and V.

i.e, $U', V' \in \overline{\mathbb{Q}} \otimes \{U, V\}$

By Weierstrass uniformization,

$$\mathcal{H} \ni \tau \longleftrightarrow \mathbb{C}/_{\mathbb{Z} \oplus \mathbb{Z} \cdot \tau} \xrightarrow{\sim} E_\tau : y^2 = x^3 + 432 E_4(\tau) x + 3456 E_6(\tau)$$

and the fact that $\mathbb{Q}[U, V]^{SL(2, \mathbb{F}_3)} = \mathbb{Q}[E_4, E_6]$
= modular forms of level 1,

we get

Thm (Lario-Rio) Let $E: y^2 = x^3 + ax + b$. Then for any $(s:t) \in \mathbb{P}^1(\mathbb{Q})$ the ell. curve $E_{s,t}: y^2 = x^3 + A(a,b,s,t)x + B(a,b,s,t)$ has isomorphic 3-torsion rep. for

$$3A(a,b,s,t) = 3as^4 + 18bs^3t - 6a^2s^2t^2 - 6abst^3 - (a^3 + 9b^2)t^4$$

$$9B(a,b,s,t) = 9bs^6 - 12a^2s^5t - 45abs^4t^2 - 90b^2s^3t^3 + 15a^2bs^2t^4 - 2a(2a^3 + 9b^2)st^5 - 3b(a^3 + 6b^2)t^6.$$

$(g,p)=(2,3)$: Let $\rho: G_{\mathbb{Q}} \to GSp(4,\mathbb{F}_3)$ with $\chi_{sim}\circ\rho = \chi_3$.

Even though $\mathcal{A}_2(3)$ is rational ($\simeq \mathbb{P}^1_{\mathbb{Q}}$),

Subtlety: we have to pass to a degree 6 cover $\mathcal{A}_2^w(3)$ to have equivariant rationality.

Take-aways from $(g,p)=(1,3)$:

- There is an analogous 4-dim irrep
$$\pi: Sp(4,\mathbb{F}_3) \longrightarrow GL(4,\overline{\mathbb{Q}})$$
- Let $L = \overline{\mathbb{Q}}^{\ker\rho}$. The new coordinates parametrizing $\mathcal{A}_2^w(\rho)$ are L-linear combinations of the coordinates parametrizing $\mathcal{A}_2^w(3)$.

This suggests that we try to find $\pi^\vee$-isotypical component inside L because for any G-irrep π, we have

$$\left(\mathbb{Q}[G]\otimes\pi\right)^G = \left[\begin{pmatrix}\pi^\vee\text{-isotypical comp.}\\ \text{of } \mathbb{Q}[G]\end{pmatrix}\otimes\pi\right]^G$$

Lucky coincidences

1. If $C: y^2 = x^5 + ax^3 + bx^2 + cx + d$ is a curve of genus 2 s.t. $\mathrm{Jac}(C)[3] \simeq \rho$, then Shioda's work on Mordell-Weil lattices gives a polynomial

$$P_{240}(x) = x^{240} + 15120\, a\, x^{228} + 2620800\, b\, x^{222} + \dots$$

whose roots generate a copy of $\pi^\vee \subset L$.

2. π and $\pi^\vee$ extend to complex reflection representations of $Sp(4, \mathbb{F}_3) \times \mathbb{Z}/3$.

This is good because invariant theory of complex reflection groups is very nice. If (G, V) is a complex reflection group, then $\mathrm{Sym}(V)^G$ is a polynomial algebra and

$$\mathrm{Sym}(V)/\mathrm{Sym}(V)^G \simeq \mathbb{C}[G].$$

Invariant theory $\Rightarrow$ The copies of $\pi^\vee$ inside $\mathrm{Sym}(\pi^\vee)$ are in degrees $1, 7, 13, 19$.

$\mathcal{M}_2^w(\rho)$ – moduli space of curves C of genus 2 with a Weierstrass point and a symplectic isomorphism $\rho \simeq \mathrm{Jac}(C)[3]$

Thm (Calegari–C–Roberts)

Let $C: y^2 = x^5 + ax^3 + bx^2 + cx + d$ be a smooth genus 2 curve over $\mathbb{Q}$. Let $\rho = \mathrm{Jac}(C)[3]$.

Then $\mathcal{M}_2^w(\rho) = \mathrm{Proj}\ \mathbb{Q}[s,t,u,v] \setminus Z_{a,b,c,d}$

a discriminant locus

Furthermore, there are explicit polynomials $A, B, C, D \in \mathbb{Q}[a,b,c,d,s,t,u,v]$ homogenous of degrees $12, 18, 24, 30$ in the variables s,t,u,v parametrizing all such curves giving rise to isomorphic 3-torsion representation.

$$\underset{\mathbb{P}^3(\mathbb{Q})}{\underset{\cap}{(s:t:u:v)}} \longleftrightarrow C_{new}: y^2 = x^5 + Ax^3 + Bx^2 + Cx + D.$$

Remarks:

1. This describes the universal curve over $\mathcal{M}_2^{w}(P)$.

2. When $(s:t:u:v) = (1:0:0:0)$, $C_{new} = C$.

3. The polynomials are homogenous of weight zero wrt the weight assignment

$$(12, 18, 24, 30, -1, -7, -13, -19) \text{ to } (a, b, c, d, s, t, u, v).$$

4. The polynomials are huge:
   - they have 14604, 112763, 515354 and 1727097 terms respectively.
   - largest absolute value of all numerators is $\approx 10^{45}$.
   - the coefficient are in $\mathbb{Z}[1/5]$.

Corollary:

Together with [Boxer-Calegari-Gee-Pilloni], this allows us to produce infinitely many examples of modular abelian surfaces with $\mathrm{End}_{\mathbb{C}} = \mathbb{Z}$

Part 2:

Thm (C): Let $g \geq 2$ and $(g,p) \neq (2,2),(2,3),(3,2)$.

Then there exists $\rho: G_{\mathbb{Q}} \to GSp(2g, \mathbb{F}_p)$ with $\chi_{sim} \circ \rho = \chi_p$ not arising from any abelian variety.

Proof Sketch: Step 1: Inertial condition.

A - g dim abelian variety $/\mathbb{Q}$.
$\rho = \rho_{A,p}$. $\ell \neq p$ is a prime.

Semistable reduction theorems:

* A attains semistable reduction at ℓ over $\mathbb{Q}(A[m])$ for $m > 2$ and $\ell \nmid m$.

* If A has semistable reduction at ℓ over the field K, then $I_{K,\ell}$ acts unipotently on $A[p]$

  In particular, $|\rho_{A,p}(I_{K,\ell})|$ is a power of p.

So, prime-to-p part of $|\rho(I_\ell)|$ must divide $|GSp(2g, \mathbb{F}_q)|$ for all primes $q > 2$, $q \neq \ell$.

So, prime-to-p part of $|\rho(I_\ell)|$ must divide $K_g = \gcd_{\substack{q \text{ prime} \\ q > 2}} |GSp(2g, \mathbb{F}_q)|$

Lemma: All the primes dividing K_g are less than or equal to $2g+1$.

Strategy:

Step 2: Construct small subgrps $G \subset GSp(2g, \mathbb{F}_p)$ with some large prime q dividing $|G|$.
$(> 2g+1)$

Step 3: Realize G as

$$G \xrightarrow{\sim} Gal(K|\mathbb{Q}) \quad \text{with}$$

$$|I_{K,\ell}| = q \text{ for some prime } \ell.$$

Step 2 $\quad \ell = \mathbb{F}_{p^{2g}} \qquad k = \mathbb{F}_{p^g} \qquad \ell \simeq k \oplus k$ as k-vector spaces.

$$\Lambda : \ell \times \ell = k^2 \times k^2 \longrightarrow k \xrightarrow{tr} \mathbb{F}_p$$
$$\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \longmapsto ad - bc$$

induces an inclusion $SL(2,k) \subset Sp(2g, \mathbb{F}_p)$.

Non-split Cartan:

$$\begin{array}{ccccc} \ell^\times & \subset & GL(2,k) & & \\ \cup & & & & \\ C = \ell^\times_{Nm_k \in \mathbb{F}_p^\times} & \subset & GL(2,k)_{\det \in \mathbb{F}_p^\times} & \subset & GSp(2g, \mathbb{F}_p) \\ \cup & & \cup & & \cup \\ \ell^\times_{Nm_k = 1} & \subset & SL(2,k) & \subset & Sp(2g, \mathbb{F}_p) \end{array}$$

C is cyclic of order $e = (p^g+1)(p-1)$.

$$N = \mathrm{Normalizer}(C) = \left\langle x, y \;\middle|\; \begin{array}{l} x^e = y^{4g} = 1, \; yxy^{-1} = x^p, \\ x^{e/2} = y^{2g} \end{array} \right\rangle$$

$$(*) \quad 0 \longrightarrow [N,N] = \mathbb{Z}/_{p^g+1} \longrightarrow N \longrightarrow N^{ab} = \mathbb{Z}/_{p-1} \times \mathbb{Z}/_{2g} \longrightarrow 0 \quad (*)$$

Since $GSp(2g, \mathbb{F}_p) \supset GSp(2d, \mathbb{F}_p)$ for $1 \leq d \leq g$, we actually have groups N of order $(p^d+1)(p-1)2d$ for each $1 \leq d \leq g$.

Zsigmondy's thm says that each number in the sequence $p+1, p^2+1, p^3+1, \ldots, p^g+1$ has a new prime factor (except for $p = 2, 3, 5, 9, 17, 33, \ldots$)

If $g > 6$, then $\pi(2g+1) < g$.
So, one of these p^d+1 has a prime factor $q > 2g+1$, and we proceed to Step 3 with the corresponding group N of order $(p^d+1)(p-1)2d$.

Step 3 We want $\rho : G_{\mathbb{Q}} \to N$ s.t.

$$\begin{tikzcd}
 & & & G_{\mathbb{Q}} \arrow[dl, dashed] \arrow[dd, bend left=60, "\chi_p"] & \\
0 \arrow[r] & \mathbb{Z}/p^{g+1} \arrow[r] & N \arrow[r] & \mathbb{Z}/p-1 \times \mathbb{Z}/2g \arrow[r] \arrow[d] & 0 \\
 & & & \mathbb{Z}/p-1 &
\end{tikzcd}$$

and s.t. $|\rho(I_\ell)| = q$.

<u>Embedding problem:</u>

Given
$$\begin{tikzcd}
 & & & G_{\mathbb{Q}} \arrow[d, "\phi"'] & \\
0 \arrow[r] & A \arrow[r] & G \arrow[r] & \Gamma \arrow[r] & 0
\end{tikzcd}$$
s.t. $\Gamma = \mathrm{Gal}(k|\mathbb{Q})$,

does there exist $\ell | k$ s.t.

$$\begin{tikzcd}
\mathrm{Gal}(\ell|\mathbb{Q}) \arrow[r, "\tilde{\phi}"] \arrow[d] \arrow[dr, phantom, "\circlearrowleft"] & G \arrow[d] \\
\mathrm{Gal}(k|\mathbb{Q}) \arrow[r] & \Gamma
\end{tikzcd}$$
?

If yes, $\tilde{\phi}$ is called a solution.
If $\mathrm{Gal}(\ell|\mathbb{Q}) \simeq G$, $\tilde{\phi}$ is called a proper solution.

General approach to embedding problems:

- The ses corresponds to a class $\xi \in H^2(\Gamma, A)$.
- A solution exists if and only if

$$\phi^* \xi = 0 \in H^2(G_{\mathfrak{P}}, A).$$

1. Choose a cyclic number field F of deg $2g$ s.t. $\phi : G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(F(\zeta_p)|\mathfrak{P}) \simeq \mathbb{Z}/_{p-1} \times \mathbb{Z}/_{2g}$
2. Choose F so that all local obstructions $\mathrm{res}_\ell(\phi^* \xi) \in H^2(G_{\mathfrak{P}_\ell}, A)$ are zero.
3. Show Hasse principle holds.

$$\ker\left(H^2(G_{\mathfrak{P}}, A) \longrightarrow \prod_\ell H^2(G_{\mathfrak{P}_\ell}, A)\right) = 0.$$

- Solution space is a homogenous space over $H^1(G_{\mathfrak{P}}, A)$. So, we twist using classes in $H^1(G_{\mathfrak{P}}, A)$ to try to obtain a proper solution.

Choose appropriate local classes $H^1(G_{\mathfrak{P}_v}, A)$ so that twisting gets us properness, and also $|\rho(I_\ell)| = q$

Thank You