Explicit Arithmetic of Modular Curves
Lecture I: Galois Properties of Torsion of Elliptic Curves

Samir Siksek (Warwick/IHÉS/IHP)

17 June 2019

Notation

K	a perfect fields
G_K	$= \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K
N	a positive integer, if $\mathrm{char}(K) > 0$ then want $\mathrm{char}(K) \nmid N$.
E	an elliptic curve defined over K.
$E[N]$	the N-torsion subgroup of $E(\overline{K})$.

$E[N]$ is stable under the action of G_K.

For $\sigma \in G_K$,

$$E[N] \to E[N], \qquad P \mapsto P^\sigma$$

is an automorphism.

Mod N Galois Representation of E

Obtain a representation

$$\overline{\rho}_{E,N} \;:\; G_K \to \mathrm{Aut}(E[N]).$$

This is known as the mod N Galois representation attached to E.

- $\ker(\overline{\rho})$ is normal of finite index.
- $\sigma \in \ker(\overline{\rho}) \iff P^\sigma = P$ for all $P \in E[N]$.
- $\therefore \ker(\overline{\rho}) = G_{K(E[N])}$.
- $\overline{\rho}(G_K) \;\cong\; G_K/G_{K(E[N])} \;\cong\; \mathrm{Gal}(K(E[N])/K)$.

$E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2 \qquad (\mathbb{Z}/N\mathbb{Z}$-module of rank 2).

Automorphism of $E[N] = \mathbb{Z}/N\mathbb{Z}$ linear isomorphism $E[N] \to E[N]$.

Choosing an basis for $E[N]$ we can identify $\overline{\rho}_{E,N}$ as a representation

$$\overline{\rho}_{E,p} \ : \ G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

An Example: $\overline{\rho}_{E,2}$

Suppose $\mathrm{char}(K) \neq 2$.

$$E \ : \ Y^2 = f(X), \qquad f(X) = X^3 + aX^2 + bX + c \in K[X], \quad \Delta(f) \neq 0.$$

Write

$$f = (X - \theta_1)(X - \theta_2)(X - \theta_3), \qquad \theta_i \in \overline{K}.$$

$$E[2] = \{0, P_1, P_2, P_3\}, \qquad P_i = (\theta_i, 0), \qquad P_3 = P_1 + P_2.$$

$$K(E[2]) = K(\theta_1, \theta_2, \theta_3), \qquad \mathrm{Gal}(K(E[2])/K) = \mathrm{Gal}(f).$$

Choose P_1, P_2 as basis.

Case 1: If θ_1, θ_2, $\theta_3 \in K$, then $\overline{\rho} = 1$ (the trivial homomorphism).

An Example: $\overline{\rho}_{E,2}$ (continued)

$$E[2] = \{0, P_1, P_2, P_3\}, \qquad P_i = (\theta_i, 0), \qquad P_3 = P_1 + P_2.$$

Case 2: $\quad \theta_1 \in K, \qquad K(\theta_2) = K(\theta_3) = K(\sqrt{d}), \quad d \in K^* \setminus (K^*)^2.$

Let $\sigma \in G_K$.

$$\sigma(\sqrt{d}) = \sqrt{d} \implies \sigma(P_1) = P_1, \quad \sigma(P_2) = P_2,$$

$$\implies \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$$

$$\sigma(\sqrt{d}) = -\sqrt{d} \quad (\sigma \text{ swaps } \theta_2,\, \theta_3)$$

$$\sigma(P_1) = P_1, \quad \sigma(P_2) = P_3 = P_1 + P_2 \implies \overline{\rho}(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2).$$

$$\overline{\rho}(G_K) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \cong \mathrm{Gal}(K(\sqrt{d})/K) = \mathrm{Gal}(K(E[2])/K).$$

An Example: $\overline{\rho}_{E,2}$ (continued)

$$E[2] = \{0, P_1, P_2, P_3\}, \qquad P_i = (\theta_i, 0), \qquad P_3 = P_1 + P_2.$$

Case 3: $\mathsf{Gal}(f) = A_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$.
e.g.

$$(\theta_1, \theta_2, \theta_3)^\sigma = (\theta_2, \theta_3, \theta_1) \implies P_1^\sigma = P_2, \quad P_2^\sigma = P_3 = P_1 + P_2$$
$$\implies \overline{\rho}(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\overline{\rho}(G_K) \;=\; \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \cong A_3 \cong \mathsf{Gal}(K(E[2])/K).$$

Case 4: $\mathsf{Gal}(f) = S_3$, find

$$\overline{\rho}(G_K) \;=\; \mathsf{GL}_2(\mathbb{F}_2) \cong S_3 \cong \mathsf{Gal}(K(E[2])/K).$$

Important Remark: Image Upto Conjugation

- $\overline{\rho}(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ depends on a choice of basis for $E[N]$.
- If we change basis then we conjugate $\overline{\rho}$ by the change-of-basis matrix, which is an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
- $\therefore$ image is only defined up to conjugation.

The mod N-Cyclotomic Character

Let ζ_N be a primitive N-th root of 1.

Define **the mod N-cyclotomic character**

$$\chi_N \ : \ G_K \to (\mathbb{Z}/N\mathbb{Z})^*, \qquad \zeta_N^\sigma = \zeta_N^{\chi_N(\sigma)}.$$

Theorem

If $\tau \in G_{\mathbb{Q}}$ denotes any complex conjugation then $\chi_N(\tau) = -1$.

Proof.

Complex conjugation takes ζ_N to ζ_N^{-1}. □

Theorem

$$\det \overline{\rho}_{E,N} = \chi_N \qquad \left(G_K \xrightarrow{\overline{\rho}} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\det} (\mathbb{Z}/N\mathbb{Z})^* \right).$$

Cyclotomic Character (continued)

Theorem

$\det \overline{\rho}_{E,N} = \chi_N$.

Proof.

Recall that the Weil pairing $e_N : E[N] \times E[N] \to \mu_N = \langle \zeta_N \rangle$ is bilinear, alternating, non-degenerate, and Galois invariant.

Alternating: $e_N(S,S) = 1$ for all $S \in E[N]$.

Alternating implies skew-symmetric:

$$\begin{aligned} 1 &= e_N(S+T, S+T) \\ &= e_N(S,S)e_N(S,T)e_N(T,S)e_N(T,T) \\ &= e_N(S,T)e_N(T,S). \end{aligned}$$

$$\therefore e_N(T,S) = e_N(S,T)^{-1} \qquad \text{(skew-symmetric)}$$

□

Cyclotomic Character (continued)

Proof.

$$e_N \text{ non-degenerate} \implies \exists \text{ basis } S,\ T \text{ such that } e_N(S,T) = \zeta_N.$$

$$\text{Let } \sigma \in G_K, \qquad \overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \qquad \therefore \begin{cases} S^\sigma = aS + cT, \\ T^\sigma = bS + dT. \end{cases}$$

$$\begin{aligned}
\zeta_N^{\chi_N(\sigma)} &= \zeta_N^\sigma && \text{by definition of } \chi_N \\
&= e_N(S,T)^\sigma && \text{by choice of } S,\ T \\
&= e_N(S^\sigma, T^\sigma) && \text{Galois invariance} \\
&= e_N(aS + cT, bS + dT) \\
&= e_N(S,S)^{ac} e_N(S,T)^{ad} e_N(T,S)^{bc} e_N(T,T)^{cd} && \text{bilinearity} \\
&= e_N(S,T)^{ad-bc} && e_N \text{ alternating} \\
&= \zeta_N^{ad-bc} && \text{by choice of } S,\ T.
\end{aligned}$$

$$\therefore \qquad \chi_N(\sigma) = ad - bc = \det \overline{\rho}_{E,N}(\sigma).$$

□

Torsion and Isogenies

Theorem

The following are equivalent:

(a) *E has a K-rational point of order N;*

(b) $\overline{\rho}_{E,N} \sim \begin{pmatrix} 1 & * \\ 0 & \chi_N \end{pmatrix}$.

(c) $\overline{\rho}_{E,N}(G_K)$ *is conjugate inside* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *to a subgroup of*

$$B_1(N) := \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z},\ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Theorem

The following are equivalent:

(a) *E has a cyclic K-rational N-isogeny;*

(b) $\overline{\rho}_{E,N} \sim \begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix}$*, where $\phi, \psi : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ are characters satisfying $\phi\psi = \chi_N$.*

(c) $\overline{\rho}_{E,N}(G_K)$ *is conjugate inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of*

$$B_0(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : b \in \mathbb{Z}/N\mathbb{Z}, \quad a,\ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

Proof. (a) $\implies$ (b). Let $\theta : E \to E$ be a cyclic N isogeny, defined over K.

$$\ker(\theta) = \langle P \rangle, \qquad P \in E[N] \text{ has order } N.$$

$$\theta \text{ defined over } K \implies \langle P \rangle^\sigma = \langle P \rangle.$$

Theorem

The following are equivalent:

(a) *E has a cyclic K-rational N-isogeny;*

(b) $\overline{\rho}_{E,N} \sim \begin{pmatrix} \phi & * \\ 0 & \psi \end{pmatrix}$, *where $\phi, \psi : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ are characters satisfying $\phi\psi = \chi_N$.*

Proof. (a) $\implies$ (b). Let $\theta : E \to E$ be a cyclic N isogeny, defined over K.

$$\ker(\theta) = \langle P \rangle, \qquad P \in E[N] \text{ has order } N.$$

$$\theta \text{ defined over } K \implies \langle P \rangle^\sigma = \langle P \rangle.$$

Choose $Q \in E[N]$ such that P, Q is a basis.

$$P^\sigma = a_\sigma P, \qquad Q^\sigma = b_\sigma P + d_\sigma Q \qquad \forall \sigma \in G_K$$

$$\therefore \qquad \overline{\rho}_{E,N}(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ 0 & d_\sigma \end{pmatrix}.$$

Exercise: Complete the proof.

Quadratic Twisting

Lemma

Let $d \in K^*$. Suppose $\mathrm{char}(K) \neq 2$. Let E' be the quadratic twist of E by d. Let $\psi : G_K \to \{1, -1\}$ be the quadratic character defined by $\sqrt{d}^{\sigma} = \psi(\sigma) \cdot \sqrt{d}$. Then $\overline{\rho}_{E,N} \sim \psi \cdot \overline{\rho}_{E',N}$.

Proof. E, E' have models

$$E \;:\; Y^2 \;=\; X^3 + aX^2 + bX + c, \qquad E' \;:\; Y^2 \;=\; X^3 + daX^2 + d^2bX + d^3c.$$

The map $\quad \phi : E(\overline{K}) \to E'(\overline{K}), \quad \phi(x, y) \;=\; \left(\frac{x}{d}, \; \frac{y}{d\sqrt{d}}\right)$ is an isomorphism. Induces isomorphism $\phi : E[N] \to E'[N]$.

Let $P = (x, y) \in E[N]$. Note that $\pm P = (x, \pm y)$. Thus,

$$\begin{aligned} \phi(P)^{\sigma} \;&=\; \left(\frac{x^{\sigma}}{d}, \; \frac{y^{\sigma}}{d\sqrt{d}^{\sigma}}\right) \;=\; \left(\frac{x^{\sigma}}{d}, \; \psi(\sigma) \cdot \frac{y^{\sigma}}{d\sqrt{d}}\right) \\ &=\; \psi(\sigma) \cdot \left(\frac{x^{\sigma}}{d}, \; \frac{y^{\sigma}}{d\sqrt{d}}\right) \;=\; \psi(\sigma) \cdot \phi(P^{\sigma}). \end{aligned}$$

Exercise: complete the proof.

Theorem

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Suppose that $\overline{\rho}_{E,N}(G_K)$ is contained in H. Let E' be a quadratic twist of E. If $-I \in H$, then $\overline{\rho}_{E',N}(G_K)$ is contained in H (up to conjugation).

Corollary

If E has a cyclic K-rational N isogeny, then so does any quadratic twist.

Recall

$$E \text{ has point of order } N \iff \text{image } \subset B_1(N) := \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \right\}$$

$$E \text{ has cyclic } N \text{ isogeny } \iff \text{image } \subset B_0(N) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\}.$$

Note $-I \in B_0(N)$ but $-I \notin B_1(N)$ (for $N \geq 3$).

Serre's Uniformity Conjecture

Conjecture (Serre's Uniformity Conjecture)

Let $E/\mathbb{Q}$ be without CM. Let $p > 37$. Then $\overline{\rho}_{E,p}$ is surjective.

Note: $\overline{\rho}$ surjective $\iff$ image contains $\mathrm{SL}_2(\mathbb{F}_p)$.

Theorem (Dickson)

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ not containing $\mathrm{SL}_2(\mathbb{F}_p)$. Then (up to conjugation)

(i) *either* $H \subseteq B_0(p) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ *(Borel subgroup)*

(ii) *or* $H \subseteq N_s^+(p) := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p^* \right\}$ *(normalizer of split Cartan)*

(iii) *or* $H \subseteq N_{ns}^+(p)$ *(normalizer of non-split Cartan).*

(iv) *or the image of* H *in* $\mathrm{PGL}_2(\mathbb{F}_p)$ *is isomorphic to* A_4, S_4 *or* A_5 *(these are called the exceptional subgroups of* $\mathrm{GL}_2(\mathbb{F}_p)$*).*

Conjecture (Serre's Uniformity Conjecture)

Let $E/\mathbb{Q}$ be without CM. Let $p > 37$. Then $\overline{\rho}_{E,p}$ is surjective.

Theorem (Dickson)

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ not containing $\mathrm{SL}_2(\mathbb{F}_p)$. Then (up to conjugation)

(i) *either $H \subseteq B_0(p) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$ (Borel subgroup)*

(ii) *or $H \subseteq N_s^+(p) := \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \ : \ \alpha,\ \beta \in \mathbb{F}_p^* \right\}$ (normalizer of split Cartan)*

(iii) *or $H \subseteq N_{ns}^+(p)$ (normalizer of non-split Cartan)[a]*

(iv) *or the image of H in $\mathrm{PGL}_2(\mathbb{F}_p)$ is isomorphic to A_4, S_4 or A_5 (these are called the exceptional subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$).*

---

[a] $N_{ns}^+(p)$ can be conjugated inside $\mathrm{GL}_2(\mathbb{F}_{p^2})$ to

$$\left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \alpha^p & 0 \end{pmatrix} \ : \ \alpha \in \mathbb{F}_p^{2\,*} \right\}.$$