Explicit Arithmetic of Modular Curves
Lecture III: Eichler–Shimura and Modular Jacobians

Samir Siksek (Warwick/IHÉS/IHP)

19 June 2019

Notation

H	subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfying $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$.
Γ_H	$\{A \in \mathrm{SL}_2(\mathbb{Z}) \,:\, (A \mod N) \in H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\}$, congruence subgroup associated to H.
X_H	modular curve associated to H $\qquad (X_H(\mathbb{C}) \cong \Gamma_H \backslash \mathbb{H}^*)$.
J_H	Jacobian of H. X_H and J_H have models over $\mathrm{Spec}(\mathbb{Z}[1/N])$, so makes sense to talk about reduction at $\ell \nmid N$.
$\Omega(H)$	space of regular differentials on X_H.
$S_2(\Gamma_H)$	space of weight 2 cuspforms for Γ_H.

There is an isomorphism

$$S_2(\Gamma_H) \cong \Omega(X_H), \qquad f(q) \mapsto f(q)\frac{dq}{q}.$$

In particular,

$$\mathrm{genus}(X_H) \;:=\; \dim(\Omega(X_H)) \;=\; \dim(S_2(\Gamma_H)).$$

Eichler–Shimura

There is an action of the Hecke algebra on $S_2(\Gamma_H)$. Let $f_1, \ldots, f_n$ be representatives of Galois orbits of Hecke eigenforms.

Theorem (Eichler–Shimura)

Let $f \in \{f_1, \ldots, f_n\}$ be some representative of the Galois orbits of the eigenforms.

- *Associated to f is an abelian variety $\mathcal{A}_f/\mathbb{Q}$.*
- $\dim(\mathcal{A}_f) = [K_f : \mathbb{Q}]$ *where K_f is the Hecke eigenvalue field of f.*
- *Moreover,* $\mathrm{End}_{\mathbb{Q}}(\mathcal{A}_f)$ *is an order in K_f (we say that $\mathcal{A}_f$ is of* GL_2*-type).*
- *In particular* $\mathrm{rank}(\mathcal{A}_f(\mathbb{Q}))$ *is a multiple of $[K_f : \mathbb{Q}]$.*

Finally,

$$J_H \sim \mathcal{A}_{f_1} \times \mathcal{A}_{f_2} \times \cdots \times \mathcal{A}_{f_n},$$

where $\sim$ denotes isogeny over $\mathbb{Q}$.

Example $J_0(43)$

Let us consider $X_0(43)$ and its Jacobian $J_0(43)$. i.e. we're taking $H = B_0(43) \subset \mathrm{GL}_2(\mathbb{F}_{43})$ and $\Gamma_H = \Gamma_0(43)$.

Using `Magma` or `SAGE`: eigenforms of $S_2(\Gamma_0(43))$ are

$$f = q - 2q^2 - 2q^3 + 2q^4 - 4q^5 + \cdots$$
$$g_1 = q + \sqrt{2} \cdot q^2 - \sqrt{2} \cdot q^3 + (2 - \sqrt{2}) \cdot q^5 + \cdots$$
$$g_2 = q - \sqrt{2} \cdot q^2 + \sqrt{2} \cdot q^3 + (2 + \sqrt{2}) \cdot q^5 + \cdots$$

The Hecke eigenvalue field for f is $\mathbb{Q}$. The eigenform f corresponds to a dimension 1 abelian variety, which is the elliptic curve 43A1 with Weierstrass model

$$\mathcal{A}_f \ : \ y^2 + y = x^3 + x^2.$$

Note that g_1, g_2 form a single Galois orbit, with Hecke eigenvalue field $\mathbb{Q}(\sqrt{2})$ of degree 2. The abelian variety $\mathcal{A}_{g_1} = \mathcal{A}_{g_2}$ has dimension 2. Moreover,

$$J_0(43) \sim \mathcal{A}_f \times \mathcal{A}_{g_1}$$

has dimension 3 and so $X_0(43)$ has genus 3. What can we say about the Mordell–Weil group $J_0(43)(\mathbb{Q})$?

Kolyvagin–Logachev

Now let $g \in \{f_1, \ldots, f_n\}$, let K_g be the Hecke eigenvalue field of g, and let $\sigma_1, \ldots, \sigma_d : K_g \hookrightarrow \mathbb{C}$ be the embeddings of $\mathbb{C}$ (here $d = [K_g : \mathbb{Q}] = \dim(\mathcal{A}_g)$). Let $g_i = \sigma(g)$ be the conjugates of g. Then we have an equality of L-functions

$$L(\mathcal{A}_g, s) = \prod_{i=1}^{d} L(g_i, s) \qquad (g = \sum a_n q^q \implies L(g, s) = \sum \frac{a_n}{n^s}).$$

We have the following famous theorem, which is a version of weak BSD for modular Jacobians.

Theorem (Kolyvagin and Logachev)

Suppose $\mathcal{A}_g$ is a factor of $J_0(M)$ for some M.

(i) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for some i then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for all i and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = 0$.

(ii) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for some i then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for all i and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = \dim(\mathcal{A}_g) = [K_g : \mathbb{Q}]$.

$$L(\mathcal{A}_g, s) = \prod_{i=1}^{d} L(g_i, s) \qquad (g = \sum a_n q^q \implies L(g, s) = \sum \frac{a_n}{n^s}).$$

Theorem (Kolyvagin and Logachev)

Suppose $\mathcal{A}_g$ is a factor of $J_0(M)$ for some M.

(i) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for some* i *then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 0$ *for all* i *and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = 0$.

(ii) *If* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for some* i *then* $\mathrm{ord}_{s=1}(L(g_i, s)) = 1$ *for all* i *and* $\mathrm{rank}(\mathcal{A}_g(\mathbb{Q})) = \dim(\mathcal{A}_g) = [K_g : \mathbb{Q}]$.

Fact. $L(\mathcal{A}_g, 1)/\Omega_g \in \mathbb{Q}$ is a rational number, where Ω_g is integral of the Néron differential over $\mathcal{A}_g(\mathbb{R})$.

The modular symbols algorithm can in fact compute $L(\mathcal{A}_g, 1)/\Omega_g$ exactly.

Values $L^{(r)}(\mathcal{A}_g, 1)$ can only be computed numerically for $r \geq 1$.

$X_0(43)$ continued.

Recall

$$J_0(43) \sim \mathcal{A}_f \times \mathcal{A}_{g_1} \qquad \dim(\mathcal{A}_f) = 1, \quad \dim(\mathcal{A}_{g_1}) = 2.$$

What can we say about the Mordell–Weil group $J_0(43)(\mathbb{Q})$?

In fact

$$\frac{L(\mathcal{A}_f, 1)}{\Omega_{\mathcal{A}_f}} = 0, \qquad \frac{L(\mathcal{A}_{g_1}, 1)}{\Omega_{\mathcal{A}_g}} = \frac{2}{7}.$$

So we know that $\mathcal{A}_{g_1}(\mathbb{Q})$ has rank 0 from the Kolyvagin–Logachev theorem. What about $\mathcal{A}_f(\mathbb{Q})$?

We find that

$$L'(f, 1) = 0.34352\ldots$$

so by the Kolyvagin–Logachev theorem, $\mathcal{A}_f(\mathbb{Q})$ has rank 1. Hence $J_0(43)(\mathbb{Q})$ has rank 1.

Injectivity of Torsion

Let $\mathcal{A}$ be an abelian variety over $\mathbb{Q}$. We know $\mathcal{A}(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Let p be a prime of good reduction for $\mathcal{A}$. Then we have a natural homomorphism

$$\mathrm{red}_p \;:\; \mathcal{A}(\mathbb{Q}) \to \mathcal{A}(\mathbb{F}_p), \qquad P \mapsto \tilde{P}.$$

Theorem (Katz)

Let $\mathcal{A}$ be an abelian variety over $\mathbb{Q}$. Let $p \geq 3$ be a prime of good reduction. Then red_p is injective when restricted to the torsion subgroup $\mathcal{A}(\mathbb{Q})_{\mathrm{tors}}$.

$X_0(31)$ and $X_1(31)$

Let's consider $J_0(31)$ instead. There is only one Galois orbit of eigenforms of weight 2 for $\Gamma_0(31)$:

$$f_1 = q + \alpha q^2 - 2\alpha q^3 + (\alpha - 1)q^4 + q^5 + \cdots, \qquad \alpha = \frac{1+\sqrt{5}}{2}$$

$$f_2 = q + \beta q^2 - 2\beta q^3 + (\beta - 1)q^4 + q^5 + \cdots, \qquad \beta = \frac{1-\sqrt{5}}{2}.$$

$\therefore X_0(31)$ has genus 2.

And $J_0(31)$ is a simple 2-dimensional abelian variety.

We find that

$$L(J_0(31), 1)/\Omega = 2/5, \qquad \therefore \operatorname{rank}(J_0(31)(\mathbb{Q})) = 0.$$

Objective. Use fact $\text{rank}(J_0(31)(\mathbb{Q})) = 0$ to show that are no elliptic curves over $\mathbb{Q}$ with a point of order 31.

Work by contradiction. Suppose $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational point Q of order 31. Then $P = [(E, Q)]$ is a non-cuspidal rational point $P \in X_1(31)(\mathbb{Q})$.

We consider this commutative diagram.

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\pi} & X_0(31)(\mathbb{Q}) & \longrightarrow & X(1)(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \longrightarrow & X_0(31)(\mathbb{F}_3) & \longrightarrow & X(1)(\mathbb{F}_3). \end{array}$$

Note that $\pi(P) = [(E, \langle Q \rangle)]$.

Assumption: $E/\mathbb{Q}$ has a point Q of order 31.

Question: Can E has good reduction at 3? Suppose it does. Then, by the injectivity of torion, $E(\mathbb{F}_3)$ has a point of order 31, which is impossible because $\#E(\mathbb{F}_3) \leq 7$ by the Hasse–Weil bounds.
$\therefore$ E cannot have good reduction at 3.

Question: Can E have potentially good reduction at 3? Suppose it does. We consider the filtration

$$E(\mathbb{Q}_3) \supset E_0(\mathbb{Q}_3) \supset E_1(\mathbb{Q}_3) \supset E_2(\mathbb{Q}_3) \cdots$$

Theory of the formal group tells us $E_1(\mathbb{Q}_3) \cong \mathbb{Z}_3$ which has no torsion. Moreover,

$$[E(\mathbb{Q}_3) : E_0(\mathbb{Q}_3)] \leq 4, \qquad [E_0(\mathbb{Q}_3) : E_1(\mathbb{Q}_3)] = \#\tilde{E}_{ns}(\mathbb{F}_3) = 3$$

as E has additive reduction.
$\therefore$ $E(\mathbb{Q}_3)$ does not have 31 torsion. Contradiction.

Assumption: $E/\mathbb{Q}$ has a point Q of order 31.
$\therefore$ E has potentially multiplicative reduction at 3.

$$\therefore \quad \mathrm{ord}_3(j(E)) < 0.$$

Recall $P = [(E, Q)] \in X_1(31)(\mathbb{Q})$, $\pi(P) = [(E, \langle Q \rangle)] \in X_0(31)(\mathbb{Q})$ and

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\pi} & X_0(31)(\mathbb{Q}) & \longrightarrow & X(1)(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \longrightarrow & X_0(31)(\mathbb{F}_3) & \longrightarrow & X(1)(\mathbb{F}_3). \end{array}$$

$\mathrm{ord}_3(j(E)) < 0 \implies$ image of P in in $X(1)(\mathbb{F}_3)$ is the cusp.

$$\therefore \pi(P) \equiv c \pmod 3 \qquad c \in \{\text{cusps of } X_0(31)\}.$$

Consider $[\pi(P) - c] \in J_0(31)(\mathbb{Q})$.

This is a torsion point as $J_0(31)(\mathbb{Q})$ has rank 0.

Recall $P = [(E, Q)] \in X_1(31)(\mathbb{Q})$, $\pi(P) = [(E, \langle Q \rangle)] \in X_0(31)(\mathbb{Q})$ and

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\pi} & X_0(31)(\mathbb{Q}) & \longrightarrow & X(1)(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \longrightarrow & X_0(31)(\mathbb{F}_3) & \longrightarrow & X(1)(\mathbb{F}_3). \end{array}$$

$$\mathrm{ord}_3(j(E)) < 0 \implies \text{image of } P \text{ in in } X(1)(\mathbb{F}_3) \text{ is the cusp.}$$

$$\therefore \pi(P) \equiv c \pmod 3 \qquad c \in \{\text{cusps of } X_0(31)\}.$$

Consider $[\pi(P) - c] \in J_0(31)(\mathbb{Q})$. This is a torsion point as $J_0(31)(\mathbb{Q})$ has rank 0.

But $[\widetilde{\pi(P) - c}] = 0 \in J_0(31)(\mathbb{F}_3)$. **By injectivity of reduction modulo** 3 **on torsion** $[\pi(P) - c] = 0 \in J_0(31)(\mathbb{Q})$. $\qquad \therefore \pi(P) = c$.

$$\therefore X_1(31)(\mathbb{Q}) \subset \{\text{cusps}\}.$$

- We only needed the fact that the point comes from $X_1(31)$ to make sure it reduces to a cusp modulo 3.
- In fact if $R \in X_0(31)(\mathbb{Q})$ reduces to a cusp modulo any prime $p \neq 2$, 31 then R must equal that cusp, by the above argument.
- i.e. if $R \in X_0(31)(\mathbb{Q})$ then $j(R) \in \mathbb{Z}[1/62]$. So problem of determining the rational points on $X_0(31)$ is essentially reduced to a problem about integral points.
- Determining $X_0(31)(\mathbb{Q})$ is easier if we know the whole of $J_0(31)(\mathbb{Q})$.

Theorem (Mazur)

Let p be a prime. Then

$$J_0(p)(\mathbb{Q})_{\mathrm{tors}} \;=\; (\mathbb{Z}/d_p\mathbb{Z}) \cdot [c_1 - c_2], \qquad d_p = \mathrm{num}\left(\frac{p-1}{12}\right)$$

where c_1, c_2 are the two cusps of $X_0(p)$.

$J_0(31)(\mathbb{Q})$

Theorem (Mazur)

Let p be a prime. Then

$$J_0(p)(\mathbb{Q})_{\mathrm{tors}} = (\mathbb{Z}/d_p\mathbb{Z}) \cdot [c_1 - c_2], \qquad d_p = \mathrm{num}\left(\frac{p-1}{12}\right)$$

where c_1, c_2 are the two cusps of $X_0(p)$.

In our case $\quad J_0(31)(\mathbb{Q}) = \dfrac{\mathbb{Z}}{5\mathbb{Z}} \cdot [c_1 - c_2].$

Goal. Determine $X_0(31)(\mathbb{Q})$.

- Let $Q \in X_0(31)(\mathbb{Q})$. Then $[Q - c_2] = n \cdot [c_1 - c_2]$ for $n = 0, 1, \ldots, 4$.
- $Q \sim n \cdot c_1 + (1 - n) \cdot c_2$ for $n \in \{0, \ldots, 4\}$.
- If $n = 0$ then $Q = c_2$ and $n = 1$ then $Q = c_1$. What about $n = 2, 3, 4$? Write $D_n = c_1 + (1 - n)c_2$.
- $\therefore Q \sim D_n$. i.e. $Q = D_n + \mathrm{div}(f)$ where $f \in \mathbb{Q}(X_0(31))^*$.

In our case $$J_0(31)(\mathbb{Q}) = \frac{\mathbb{Z}}{5\mathbb{Z}} \cdot [c_1 - c_2].$$

Goal. Determine $X_0(31)(\mathbb{Q})$.

- Let $Q \in X_0(31)(\mathbb{Q})$. Then $[Q - c_2] = n \cdot [c_1 - c_2]$ for $n = 0, 1, \ldots, 4$.
- $Q \sim n \cdot c_1 + (1-n) \cdot c_2$ for $n \in \{0, \ldots, 4\}$.
- If $n = 0$ then $Q = c_2$ and $n = 1$ then $Q = c_1$. What about $n = 2, 3, 4$? Write $D_n = c_1 + (1-n)c_2$.
- $\therefore Q \sim D_n$. i.e. $Q = D_n + \mathrm{div}(f)$ where $f \in \mathbb{Q}(X_0(31))^*$.
- $f \in L(D_n)$. To compute Riemann–Roch space need a model.

A model for $X_0(31)$ was worked out by Galbraith:

$$X_0(31) \quad : \quad y^2 = \underbrace{x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3}_{h}.$$

Here c_1, c_2 are the two points at ∞ on this model. We find that $\dim(L(D_n)) = 1,\ 1,\ 0,\ 0,\ 0$ for $n = 0, 1, 2, 3, 4$ respectively. Thus there is no point $Q \sim D_n$ for $n = 2,\ 3,\ 4$. Hence $X_0(31)(\mathbb{Q}) = \{c_1,\ c_2\}$. In particular, there are no elliptic curves over $\mathbb{Q}$ with a 31-isogeny.

Sketch of Mazur's Theorem for $X_1(p)$

Defn. A morphism of schemes $\theta : X \to Y$ over $\mathrm{Spec}(\mathbb{Z}[1/p])$ is a **formal immersion** at $x \in X(\mathbb{Q})$ if the induced map

$$\hat{\mathcal{O}}_{Y,f(x)} \to \hat{\mathcal{O}}_{X,x}$$

is surjective.

Remark. Let $q \neq p$ be a prime. Let

$$\mathrm{res}_q(x) \ := \ \{x' \in X(\mathbb{Q}_q) \ : \ x' \equiv x \pmod{q}\}$$

which is called the q-adic residue disc of x. If θ is a formal immersion at x then the map

$$\theta \ : \ \mathrm{res}_q(x) \to Y(\mathbb{Q}_q)$$

is an injection.

Proposition

Let $Y = \mathcal{A}$ *be an abelian variety such that* $\mathcal{A}(\mathbb{Q})$ *has rank* 0*. Let* $\theta : X \to \mathcal{A}$ *be a morphism over* $\mathrm{Spec}(\mathbb{Z}[1/p])$ *that is formal immersion at* $x \in X(\mathbb{Q})$*. Then*

$$X(\mathbb{Q}) \cap \mathrm{res}_q(x) = \{x\}$$

for all primes $q \notin \{2, p\}$*.*

Proof.

- Let $x' \in X(\mathbb{Q}) \cap \mathrm{res}_q(x)$.
- Then $x' \equiv x \pmod{q}$.
- Thus $\theta(x') - \theta(x)$ is an element of $\mathcal{A}(\mathbb{Q})$ that reduces to 0 modulo q.
- But $\mathcal{A}(\mathbb{Q})$ is torsion. By the injectivity of torsion $\theta(x') - \theta(x) = 0$. Thus $\theta(x') = \theta(x)$.
- However, as θ is a formal immersion at x, and x' belong to $\mathrm{res}_q(x)$ we have $x = x'$.

□

Mazur's Theorem for $X_1(p)$

Theorem

Let $p \geq 11$ prime. Then there is no elliptic curve $E/\mathbb{Q}$ with a rational point of order p. Equivalently, $X_1(p)(\mathbb{Q}) \subset \{cusps\}$.

Sketch.

- Suppose $z \in X_1(p)(\mathbb{Q})$ is not a cusp.
- Then $z = [(E, P)]$ where E is an elliptic curve defined over $\mathbb{Q}$ and P is a rational point of order p.
- Then E has potentially multiplicative reduction at 3.

  Let $y = \pi(z)$ where $\pi : X_1(p) \to X_0(p)$ is the degeneracy map. In particular z reduces mod 3 to one of the cusps on X_0.

  The Atkin-Lehner involution swaps the cusps. Thus we can suppose that y reduces to the infinity cusp on X_0 which we denote by $\infty \in X_0(p)(\mathbb{Q})$.

Sketch.

- Suppose $z \in X_1(p)(\mathbb{Q})$ is not a cusp.
- Then $z = [(E, P)]$ where E is an elliptic curve defined over $\mathbb{Q}$ and P is a rational point of order p.
- Then E has potentially multiplicative reduction at 3.

  Let $y = \pi(z)$ where $\pi : X_1(p) \to X_0(p)$ is the degeneracy map. In particular y reduces mod 3 to one of the cusps on X_0.

  The atkin-Lehner involution swaps the cusps. Thus we can suppose that y reduces to the infinity cusp on X_0 which we denote by $\infty \in X_0(p)(\mathbb{Q})$.
- We let $J_e(p)$ be the largest quotient of J that has analytic rank 0. This **Merel's winding quotient**. We know by Kolyvagin–Logachev that this has rank 0. We take θ to be the map $X_0(p) \to J_0(p) \to J_e(p)$.
- Highly non-trivial fact: this is a formal immersion at ∞. Now

$$y \in \mathrm{res}_3(\infty) \cap X_0(3)(\mathbb{Q}).$$

  Hence by previous proposition $y = \infty$. Thus z is a cusp. ∎

Other modular curves

- Proofs of
  - Mazur's theorem for $X_0(p)$;
  - Merel's Uniform Boundedness theorem;
  - the theorem of Bilu, Parent and Rebolledo for $X_s^+(p)$;

  all crucially depend on the existence of a rank 0 quotient of the modular Jacobian.
- However, for $X_{ns}^+(p)$ it is known that every factor of the Jacobian has odd analytic rank, and so assuming BSD has non-zero rank. This is the reason why Serre's uniformity conjecture is still an open problem.