Choices of invariants for modular polynomials

Introduction

Ilan Ehrlich
Under the supervision of Jean Kieffer

January 2026

Often, one would like to know whether two elliptic curves are ℓ-isogenous, for a fixed number ℓ. For this, let us construct a classification of pairs of elliptic curves that are. First, consider the case over $\mathbb{C}$. We can classify elliptic curves in the following way. A elliptic curve E is always isomorphic to the quotient $E_\tau := \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ for some number τ with positive imaginary part. Let us then define the set

$$\mathbb{H} := \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$$

called the *upper-half plane*. The set of elliptic curves of the form E_τ for $\tau \in \mathbb{H}$ then provides all isomorphism classes of elliptic curves. On the other hand, we may observe that two elliptic curves E_τ, $E_{\tau'}$ of this form are isomorphic if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$, for $a, b, c, d \in \mathbb{Z}$ satisfying $ad-bc = 1$. This motivates to define an action $\mathrm{SL}_2(\mathbb{Z}) \curvearrowright \mathbb{H}$ given by the Möbius transformations $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau+b}{c\tau+d}$. Define

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

By construction, there exists a surjective map f that assigns to each elliptic curve a point in $Y(1)$. This function satisfies for any two elliptic curves

$$E \cong E' \iff f(E) = f(E').$$

Therefore, the points in $Y(1)$ are in bijection with the isomorphism classes of elliptic curves. In that case, $Y(1)$ is informally designated as a *moduli space* of elliptic curves.

We can adapt this construction to isogenies. We say that two isogenies are isomorphic if they are as objects in the arrow category of the category of elliptic curves with isogenies as morphisms. Similarly to elliptic curves, one can show that every ℓ-isogeny is isomorphic to the quotient isogeny $\phi_\tau : E_{\ell\tau} \to E_\tau$ for some $\tau \in \mathbb{H}$. In addition, two isogenies $\phi_\tau, \phi_{\tau'}$ of this form are isomorphic if and only if $\tau' = \gamma\tau$, for some γ in the subgroup

$$\Gamma_0(\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod l \right\}.$$

Consequently, the quotient $Y_0(\ell) := \Gamma_0(\ell) \setminus \mathbb{H}$ is a moduli space of ℓ-isogenies.

Define similarly

$$\Gamma(n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod n \right\},$$

where the equivalence is considered entry-wise. When a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ contains $\Gamma(n)$ for some n, then it is called a *congruence subgroup*. The subgroup $\Gamma_0(\ell)$ is then a congruence subgroup for $n = \ell$. The smallest n such that this inclusion holds is called the *level* of the congruence subgroup in question. A quotient of $\mathbb{H}$ by a congruence subgroup, such as $Y_0(\ell)$, is called a *modular curve*. Modular curves are notably Riemann surfaces, but they are also algebraic curves, as we explain further.

Let us now classify pairs of ℓ-isogenous elliptic curves. Note that the classification in which we are interested is slightly weaker than the one provided by $Y_0(\ell)$. We do not focus on the precise isogenies, but we solely focus on the property of being isogenous. Thus, we would like to confound all of the potential distinct ℓ-isogenies connecting two given elliptic curves. The isomorphism class $[\phi]$ of an isogeny $\phi : E \to E'$ defines two maps $[\phi] \mapsto [E]$, $[\phi] \mapsto [E']$ of domain and codomain respectively. Each of these induces, in turn, a map $Y_0(\ell) \to Y(1)$:

$$\begin{array}{ccc} & Y_0(\ell) & \\ \overset{\text{Domain}}{\swarrow} & & \overset{\text{Codomain}}{\searrow} \\ Y(1) & & Y(1). \end{array} \tag{1}$$

Consider the pair $Y_0(\ell) \to Y(1) \times Y(1)$ of these maps and denote its image $\tilde{Y}_\ell := \mathrm{Im}(Y_0(\ell) \to Y(1) \times Y(1))$. By construction, the moduli space classifying pairs of ℓ-isogenous elliptic curves is then precisely $\tilde{Y}_\ell$:

$$E \sim_\ell E' \iff ([E], [E']) \in \tilde{Y}_\ell,$$

where $\sim_\ell$ denotes the equivalence relation of being ℓ-isogenous. For reasons we do not explain here, $\tilde{Y}$ is an affine variety. Therefore, if we choose coordinates on it, we can describe it as the locus of polynomials.

The classical choice for a coordinate on $Y(1)$ is the *j-invariant* $Y(1) \to \mathbb{A}^1_{\mathbb{C}}$, defined on elliptic curves as

$$(E : y^2 = x^3 + ax + b) \mapsto \frac{4a^3}{4a^3 + 27b^2}.$$

Note that j is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, i.e., $j(\gamma\tau) = j(\tau)$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Thus, j defines a map on $Y(1)$, and by extension also defines a map on the set of elliptic curves. In particular, it is injective as a map on $Y(1)$, which means that

$$E \cong E' \iff j(E) = j(E').$$

Under this choice of coordinate, a single polynomial $\Phi_\ell \in \mathbb{Z}[x, y]$ suffices to describe $\tilde{Y}_\ell$. It is called the *classical modular polynomial* and is the main object of interest in this dissertation. At this stage, we then have

$$\begin{aligned} E \sim_\ell E' &\iff ([E], [E']) \in \tilde{Y}_\ell \\ &\iff (j[E], j[E']) \in (j \times j)(\tilde{Y}_\ell) = V(\Phi_\ell) \\ &\iff \Phi_\ell(j(E), j(E')) = 0. \end{aligned}$$

Thus, Φ_ℓ is the encapsulation in a polynomial of the exact piece of information we are seeking, that of when two elliptic curves are ℓ-isogenous. One of the major flaws of Φ_ℓ is the complexity of its coefficients. For example, when $\ell = 2$,

$$\begin{aligned} \Phi_2(x, y) = {} & x^3 - 162\,000x^2 + 8\,748\,000\,000x + 1\,488x^2y \\ & + y^3 - 162\,000y^2 + 8\,748\,000\,000y + 1\,488xy^2 \\ & - x^2y^2 + 40\,773\,375xy - 157\,464\,000\,000\,000. \end{aligned}$$

The symmetry of this polynomial is not hazardous, it corresponds to the symmetry of the relation of being isogenous. It is also an integer polynomial, which is a non-trivial fact that comes from theorems from the theory of moduli spaces, which we soon introduce. The fact that its coefficients are integers, or more generally elements in a number field, can be leveraged to use a concrete *height* function H, one that describes their complexity. We usually take $H(\Phi_\ell) = \max_c \log |c|$, where c ranges over the coefficients of Φ_ℓ. Therefore, a first natural question that arises is:

How can we replicate this construction in order to obtain a modular polynomial with coefficients of smallest possible height?

We may calculate that given a curve E_τ, the j-invariants of all of its ℓ-isogenous curves are the values $j_\ell \circ \gamma(\tau)$, where j_ℓ is the function $\tau \mapsto j(\ell\tau)$ and the elements γ are representatives of the right cosets of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$. We then have an explicit formula for Φ_ℓ : it is the unique polynomial satisfying

$$\Phi_\ell(j, y) = \prod_{\gamma \in R} (y - j_\ell \circ \gamma).$$

Intuitively, this formula suggests that the complexity of the coefficients depends on that of j. We are then inclined to think that if we were to take a "smaller" invariant, then the coefficients would be simpler. For example, one may consider the cube root γ_2 of j. Here, the degree-2 modular polynomial looks like

$$\Phi_2^{\gamma_2}(x, y) = x^3 + y^3 - (xy)^2 + 495xy - 54\,000.$$

However, γ_2 no longer defines an injective map $Y(1)$ into $\mathbb{A}^1_{\mathbb{C}}$. Instead, it defines one for another curve $Y_\Gamma := \Gamma \setminus \mathbb{H}$, for some congruence subgroup Γ. In other words, γ_2 is not an invariant for elliptic curves like j; as Γ is only a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, Y_Γ contains more data than $Y(1)$. It classifies *enhanced elliptic curves*,

i.e. elliptic curves endowed with additional data, called *level structures*. They should be thought of as objects emanating from $E[\ell]$, the ℓ-torsion subgroup of E, such as a point or a cyclic subgroup in $E[\ell]$. One can also define the isogenies that respect this level structure, and their moduli space is also a modular curve. We can then entirely describe the situation in terms of moduli spaces of enhanced elliptic curves. As the data of level structures is stronger, we can always recover the property of being isogenous with the result we obtain. We can then study the question more generally by classifying enhanced complex elliptic curves instead of simple ones. Moreover, the latter example gives the heuristic for a general motto, whose formalization and proof are precisely the aim of this dissertation:

The richer the level structure and the smaller the invariant,
the more compact the modular polynomial.

From here, if we want to frame this construction rigorously, a few questions arise:

1. To what extent can we generalize this approach beyond $\mathbb{C}$?
2. How to construct those invariants?
3. How can we ensure that we have a notion of height?

To answer the first question, note that level structures can be defined on any elliptic curve E defined over any scheme S, and of any level Γ. Consequently, viewing the situation conceptually as a classification problem of general enhanced elliptic curves opens the way to using the theory of moduli spaces developed by Deligne and Rapoport in *Les Schémas de Modules de Courbes elliptiques* (1973). We are now perceiving moduli curves first and foremost as moduli spaces, rather than quotients of the upper half plane. In particular, this theory shows that the moduli spaces of interest are algebraic curves. A *model* for a scheme is a scheme whose base change yields the original one. One of Deligne and Rapoport's prominent results provides a model for any moduli space of enhanced elliptic curves, that is defined over a number field $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_\ell)$, where ℓ denotes the level of Γ and $\zeta_\ell = e^{2\pi i/\ell}$. This allows us to introduce the investigation over any F-scheme, by replacing $\mathbb{C}$ by F and considering moduli spaces of enhanced elliptic curves over F. Note that we can still replicate the construction based on diagrams of schemes analogous to 1. Moreover, in favorable cases, the image of the pairs of maps from this diagram is again an affine variety. If the curve has genus 0, a single invariant suffices, and in favorable cases, this image is again given by a single polynomial. Thus, the concept of modular polynomials makes sense in this setting too.

The definition of the base scheme over a number field F also helps us answer the last question. Since we know that all the schemes under consideration are defined over F, if our invariants were also defined over F, then so would their image, namely the moduli space of isogenous pairs. In turn, this would imply that the modular polynomial itself has coefficients in F, which would suffice to define a computationally suitable notion of height.

We now need to address the second question, adding the condition that the invariant we obtain is also defined over F. For this we use the *Baily-Borel theorem*, which provides an "injective" (a degree-1) map into $\mathbb{P}^1$ using modular forms. We then use this map to generate general invariants. To address the question of the field of definition of the invariant, we use the *q-expansion principle*. This theorem provides a criterion to know when modular forms induce invariants defined over the subfield $F \subseteq \mathbb{C}$. We explain this tool and further use it to generate invariants over F with desired properties. Those can then be pulled back to yield ones over any F-scheme. Using this method, we can then restrict our attention to the situation over $\mathbb{C}$, making sure it descends to F.

Once the problem is well-defined, we may ask:

- How does the choice of level structure impact the size of the coefficients?

  Under conditions to be explained in the dissertation, there exists a polynomial P of degree $d = [\Gamma(1) : \Gamma]$ satisfying $j = P(h)$, where h is a new invariant. Our conjecture is that given h and P, the coefficients of Φ^h are $O(|\Phi^j| \cdot (\deg P)^{-2})$.

- Given a level structure, which choice of invariant induces the most compact modular polynomial?

- Given a choice of level structure Γ and invariant h such that $j = P(h)$, can we recover Φ_ℓ in terms of Φ_ℓ^h?