Ideas

Simon Pohmann

April 27, 2022

1 (d, ϵ)-structures

Let p be a prime. Consider the category EC defined by

$$\begin{aligned} \mathrm{Ob}(\mathrm{EC}) &:= \{E \text{ elliptic curve over } \mathbb{F}_{p^2}\} \\ \mathrm{Hom}_{\mathrm{EC}}(E, E') &:= \{\psi : E \to E' \text{ isogeny}\} \end{aligned}$$

Have a functor

$$\begin{aligned} \cdot^{(p)} : \mathrm{EC} &\to \mathrm{EC} \\ E \text{ defined by } y^2 = x^3 + Ax + B &\mapsto E' \text{ defined by } y^2 = x^3 + A^p x + B^p \\ \left[\sum_{i,j} a_{ij} x^i y^j : \sum_{i,j} b_{ij} x^i y^j : \sum_{i,j} c_{ij} x^i y^j \right] &\mapsto \left[\sum_{i,j} a_{ij}^p x^i y^j : \sum_{i,j} b_{ij}^p x^i y^j : \sum_{i,j} c_{ij}^p x^i y^j \right] \end{aligned}$$

and a functor

$$\hat{\cdot} : \mathrm{EC} \to \mathrm{EC}^{\mathrm{op}}, \quad E \mapsto E, \quad \phi \mapsto \hat{\phi}$$

(d, ϵ)-structures and their isogenies are given by the category $\mathrm{ES}_{d,\epsilon}$ defined by

$$\begin{aligned} \mathrm{Ob}(\mathrm{ES}) &:= \{(E, \psi) \mid E \in \mathrm{EC},\ \psi : E \to E^{(p)},\ \hat{\psi} = \epsilon \psi^{(p)}\} \\ \mathrm{Hom}_{\mathrm{ES}}((E, \psi), (E', \psi')) &:= \{\phi : E \to E' \mid \psi' \circ \phi = \phi^{(p)} \circ \psi\} \end{aligned}$$

2 j-invariant and modular polynomials

Consider the j-invariant

$$j : \mathcal{H} \to \mathbb{C}$$

that assigns to a complex elliptic curve given by a lattice $\mathcal{L}\{\tau, 1\}$ its j-invariant $j(\tau)$. Then it is a fact that for $N \in \mathfrak{N}$ the map

$$j_N : \mathcal{H} \to \mathbb{C}, \quad \tau \mapsto j(N\tau)$$

is algebraic over $\mathbb{C}(j)$ and its minimal polynomial is $\Phi_N(X, j)$. This Φ_N is called modular polynomial, and we have $\Phi_N \in \mathbb{Q}[X, Y]$ and furthermore $\Phi_N(X, Y) = \Phi_N(Y, X)$.

Furthermore, it holds that

$$\Phi_N(j(E), j(E')) = 0$$

for any E' such that there is an N-isogeny $E \to E'$ (No idea how to prove that).

We see then that for all primes p, have

$$\Phi_N(j(E), j(E')) = 0$$

for elliptic curves E, E' defined over $\bar{\mathbb{F}}_p$ such that there is an N-isogeny $E \to E'$.

This shows that if we have a (d, ϵ)-structure (E, ψ) then

$$\Phi_d(j(E), j(E^{(p)})) = \Phi_d(j(E), j(E)^p) = 0$$

as there is the d-isogeny $\psi : E \to E^{(p)}$.

3 My first idea

As usual, let p be a (big) prime and consider $q := p^2$. Consider a (small) prime l. Then every supersingular Elliptic Curve $E/\mathbb{F}_q$ satisfies $\Phi_n(j(E), j(E)^p) = 0$ with $n = l^{O(\log(p))}$, as the supersingular l-isogeny graph is an expander with mixing length $O(\log(p))$, hence there is a path from E to $E^{(p)}$ of length $O(\log(p))$.

Now we analyze when $\Phi_n(j(E), j(E)^p) = 0$ for an ordinary Elliptic Curve $E/\mathbb{F}_q$.

Using the isogeny graph

Since the connected component of E in the l-isogeny graph is a vulcano, we can find a path (of length $O(\log(p))$) to an Elliptic Curve in the crater, say E_0. Hence there are ascending l-isogenies

$$E \to \dots \to E_0$$

Let $K := \mathrm{End}^0(E_0)$ and consider the maximal order $\mathcal{O}_K \subseteq K$, $\mathcal{O}_0 := \mathrm{End}(E_0)$ and $\mathcal{O} := \mathrm{End}(E)$. Then have that $\mathcal{O} \subseteq \mathcal{O}_0 \subseteq \mathcal{O}_K$ with $[\mathcal{O}_0 : \mathcal{O}] = l^{O(\log(p))}$ and $l \nmid [\mathcal{O}_K : \mathcal{O}_0]$.

Now we are in one of the following cases:

(I) E_0 is defined over $\mathbb{F}_p$, i.e. $E_0^{(p)} = E_0$; Then $\Phi_n(j(E), j(E)^p) = 0$

(II) $E_0^{(p)}$ is (nontrivially) l-isogeneous to E_0, i.e. they are two distinct vertices on the crater; Then it is likely that $\Phi_n(j(E), j(E)^p) \neq 0$, but that depends on the distance in the crater

(III) $E_0^{(p)}$ is not l-isogeneous to E_0; Then $\Phi_n(j(E), j(E)^p) \neq 0$

Analyzing (III)

Now consider only E_0 and denote $\mathcal{O} := \mathcal{O}_0$ and $E := E_0$.

Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that $[\mathfrak{a}].E = E^{(p)}$. We have (III) if and only if $[\mathfrak{a}]$ contains no integral ideal of index l^r, for any $r \in \mathfrak{N}$. Assume it does, say $\mathfrak{b}$. Then $\mathfrak{b} = \alpha\mathfrak{a}$ for some $\alpha \in \mathfrak{a}^{-1}$ with

$$\mathfrak{N}(\alpha) = \frac{\mathfrak{N}(\mathfrak{b})}{\mathfrak{N}(\mathfrak{a})} = \frac{l^r}{\mathfrak{N}(\mathfrak{a})}$$

Since we do not require α to be integral, we can substitute α by α/l and so find that

$$\mathfrak{N}(\alpha) = \mathfrak{N}(\mathfrak{a})^{-1} \quad \text{or} \quad \mathfrak{N}(\alpha) = l\mathfrak{N}(\mathfrak{a})^{-1}$$

This leads us to the interesting (slightly weaker) question: When does there exist some $\alpha \in K$ with $\mathfrak{N}(\alpha) = N$ for some (square-free) N?