Ideas

Simon Pohmann

April 8, 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 $N \in \mathbb{N}$ 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 $\psi : E \to E^{(p)}$.

2.1 Supersingularity Polynomials

Let p be prime and consider

$$K = \mathbb{F}_p(A, B) \quad \text{and} \quad E : z = w^3 + Awz^2 + Bz^3$$

Now consider the local ring $R = K[\![t]\!]$ and the subring (in fact ideal) $R_t := tR$. Have

$$E(R_t) := E(R) \cap \mathbb{P}^2_{R_t} = \{(t, \omega(t)) \mid t \in R\}$$

where $\omega \in R_t$.

Now we analyse the group law $*$ on $E(R_t)$ given by

$$(u * v, \_) := (u, \omega(u)) +_E (v, \omega(v))$$

As e.g. discussed in Silverman, have

$$u * v = F(u, v)$$

where

$$\begin{aligned}
F &:= -T - S - \frac{2A\lambda(T,S)\nu(T,S) + 3B\lambda(T,S)^2\nu(T,S)}{1 + A\lambda(T,S)^2 + B\lambda(T,S)^3} \in K[\![T, S]\!], \\
\lambda &:= \frac{\omega(T) - \omega(S)}{T - S} \in K[\![T, S]\!], \\
\nu &:= \omega(T) - \lambda(T, S)T \in K[\![T, S]\!]
\end{aligned}$$

Note that F is a power series in T, S and so we can evaluate $F(u, v)$ in R_t as for $u, v \in R_t$ have that $|u|_t, |v|_t < 1$ have small t-adic valuation, so $F(u, v)$ converges.

Slightly different approach

Assume $x_1 = x, x_2 = \dots$ and

$$x_{n+1} = -x_n - x + \frac{q(x_n) + q(x) + 2yy_n}{(x_n - x)^2}$$

Polynomial division yields

$$\begin{aligned} x_{n+1} =& - x_n - x + x_n + 2x + \frac{(A + x^2)x_n - x^3 + Ax + 2B + 2yy_n}{(x_n - x)^2} \\ =& x + \frac{(A + x^2)x_n - x^3 + Ax + 2B + 2yy_n}{(x_n - x)^2} \end{aligned}$$

Substituting $w_n = x_n - x$ yields

$$w_{n+1} = \frac{(A + x^2)w_n + 2Ax + 2B + 2yy_n}{w_n^2} = \frac{A + x^2}{w_n} + \frac{2Ax + 2B}{w_n^2} + \frac{2yy_n}{w_n^2}$$