Arpin + Martindale – Lecture II
Efficient Rep. + Eval. of Isogenies.

KLPT (abridged)

Given $\eta : E \to E'$ (as a quaternion ideal) find $\varphi : E \to E'$ with $\deg \varphi = \ell^e$ "unrelated" to η

Find $L \sim I_\eta$ of prime norm:

find $\alpha \in I_\eta$ w/ $N(\alpha) = q N(I_\eta)$

$L = I_\eta \frac{\bar{\alpha}}{N(I_\eta)}$ check: $L \sim I_\eta$, $N(L) = q$

Find $J \sim L$ of $N(J) = \ell^e$

using norm form eq'n and strong approximation.

Translate J to an isogeny φ_J.

More efficient rep + eval. of isogenies using abelian varieties

Def. An abelian variety X is a smooth, projective algebraic group variety. An isogeny $f: X \to X'$ is a hom. which is finite flat surjective.

$$\deg f = [k(X) : f^* k(X')]$$

An abelian variety is supersingular if it's isogenous to a product of supersingular e.c.'s and superspecial if the isogeny is an isom.

The dual of X is denoted

$$\hat{X} = \mathrm{Pic}^\circ(X)$$

$\mathrm{Pic}(X)$ = isom. classes of line bundles

$\mathrm{Pic}^\circ(X)$ = subgroup of lb's alg. equiv. to $\mathcal{O}$.

Proposition $\mathcal{L}$: line bundle on A/k

The map $\varphi_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A)$

$$x \longmapsto [T_x^* \mathcal{L} \otimes \mathcal{L}^{-1}]$$

is a group homomorphism.

(ample) line bundles $\to$ Projective Coord's

$\mathrm{Pic}^0(A) = \{\mathcal{L} \in \mathrm{Pic}(A) : \varphi_{\mathcal{L}} = 0\}$

If $\mathcal{L}$ is ample, then $\varphi_{\mathcal{L}}$ defines an isogeny.

A polarization is an isogeny $\varphi : A \to \hat{A}$ over k such that $\exists$ ample $\mathcal{L}$ of $A \otimes \bar{k}$ for which $\varphi \otimes \bar{k} = \varphi_{\mathcal{L}}$. If φ is an isom., (A, φ) is principally polarized a.v.

"line bundles" ~~~ divisors (formal sums of pts)

$\mathcal{L} \otimes \mathcal{L}'$ $\quad D + D'$

"ample" $\quad \deg D > 0$

Weierstrass equations "come from"

$$\mathcal{L}(3O_E) = \{f \in \bar{K}(E)^* : \operatorname{div}(f) + 3O_E \geq 0\} \cup \{0\}$$

$$\operatorname{Pic}^0(E) \cong E$$

$$[(P) - (O_E)] \longmapsto P$$

Theorem E: supersingular e.c /k with $\mathrm{End}(E) \cong \mathcal{O} \subseteq B_{p,\infty}$

A/k: superspecial a.v. of $\dim A = g$

The principal polarizations of A are in bijection with

$$S := \{M \in GL_g(\mathcal{O}) : M = \bar{M}^T\}$$

Dimension-2 Corollary:

$$S = \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \in M_2(\mathcal{O}) : \begin{matrix} s, t \in \mathbb{Z}_{>0} \\ st - r\bar{r} = 1 \end{matrix} \right\}$$

Def $(A, \lambda), (A', \lambda')$: ppav's of dim = g. A special class of polarization preserving isogenies "N-isog" or "$(N, \ldots, N)$"-isog. are $f : A \to A'$ such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle \lambda_0 [N]}\downarrow & & \downarrow{\scriptstyle \lambda'} \\ \hat{A} & \xleftarrow{\hat{f}} & \hat{A'} \end{array}$$

where $\deg f = N^g$

Theorem (Dim. 2 Torelli)

Every ppas is either

1) $J(C)$ Jacobian of genus 2 C

2) $E_1 \times E_2$: product of EC's

Flavors of pol. pres. isogeny:

1) $f : E_1 \times E_2 \to E_3 \times E_4$

2) $f : J(C) \to E_1 \times E_2$ "splitting"

3) $f : E_1 \times E_2 \to J(C)$ "gluing"

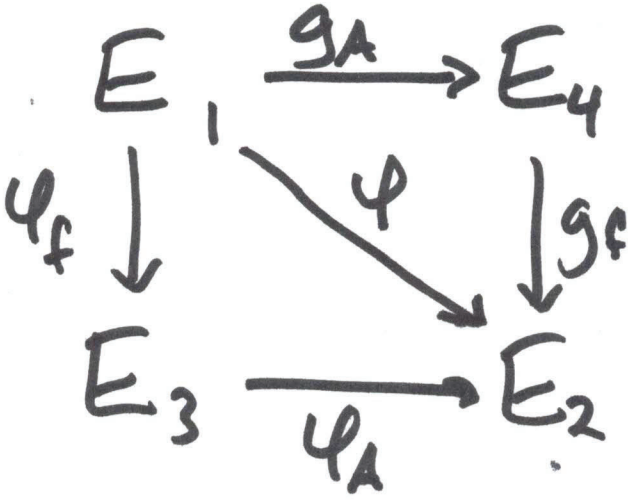
4) $f : J(C_1) \to J(C_2)$

Theorem Kani's Reducibility Criterion (= "Kani")

f, A, B : pairwise coprime, $\in \mathbb{Z}_{>0}$

$$f + A = B$$

E_i : elliptic curves



Then, the isog.

$$\Phi : E_1 \times E_2 \to E_3 \times E_4$$

$$\begin{pmatrix} \varphi_f & -\hat{\varphi}_A \\ g_A & \hat{g}_f \end{pmatrix}$$

is a (B, B) isogeny wrt the product polarizations and

$$\ker \Phi = \{ ([A]P, \varphi(P)) : P \in E_1[B] \}$$

Proof by direct computation.

Kani Consequences

1) Recares a factred isogeny:

$$\psi = \psi_A \circ \psi_f$$

2) Eff. rep of ψ:

If $E_1[B] = \langle P, Q \rangle$

$\rightarrow (\psi(P), \psi(Q))$

3) Ideals $\rightarrow$ isogenies more eff.