# On prime degree twisting endomorphisms of supersingular elliptic curves

Jordi Pujolàs, Universitat de Lleida
together with Josep M. Miret and Javier Valera

Escola Politècnica, Universitat de Lleida
wednesday april 30th, 2025

Financiado por la Unión Europea NextGenerationEU
Gobierno de España
Ministerio para la Transformación Digital y de la Función Pública
Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

# Index

# Elliptic curves, j-invariant, Frobenius

$$p \text{ any prime} > 3, q = p^n, a, b \in \mathbb{F}_q$$

$$E : y^2 = x^3 + ax + b, \quad \mathbf{j_E} = 1728\frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_q$$

$$E^p : y^2 = x^3 + a^p x + b^p, \quad {j_E}^p = j_{E^p}$$

$$\phi_p : E(\overline{\mathbb{F}}_q) \longrightarrow E^p(\overline{\mathbb{F}}_q) \quad \text{If } a, b \in \mathbb{F}_p \text{ then } \phi_p = \pi_E \in End_{\mathbb{F}_p}(E)$$

$$(x, y) \longmapsto (x^p, y^p)$$

**Example** : $p \equiv 2 \mod 3, E : y^2 = x^3 + 1_{|\mathbb{F}_p}, j_E = 0$

$1 \neq$ cube $\mod p$. If $\xi \in \mathbb{F}_{p^2}$ with $\xi^2 + \xi + 1 = 0$ then $\xi^p = \xi^2$

$\Rightarrow \xi(x, y) = (\xi x, y) \in End(E)$ satisfies $\pi_E \xi = \xi^2 \pi_E \Rightarrow E$ supersingular

# Isomorphisms and Quadratic Twists

$$\textbf{Isomorphisms}: E^{'} : Y^2 = X^3 + a^{'}X + b^{'}, \quad a^{'}, b^{'} \in \mathbb{F}_q$$

$$E^{'} \in Isom_k(E) \Longleftrightarrow (X, Y) = (v^2x, v^3y) \text{ for } v \in k \mid a^{'} = av^4,\ b^{'} = bv^6$$

$$\textbf{Twists}: E^{t} : Y^2 = X^3 + au^2X + bu^3{}_{|\mathbb{F}_p}$$

$$E^{t} \in Twist(E) \Longleftrightarrow E^{t} \in Isom_k(E),\ k \text{ extension of } \mathbb{F}_q. \text{Then } j_E = j_{E^t}.$$

*Beware* : ([CPV, Lemma 1]) if $p \equiv 3 \mod 4$ and $b = 0$ and $u \in \mathbb{F}_p$

$$\Longrightarrow E^{t} \in Isom_{\mathbb{F}_p}(E) \text{ regardless of} \left(\frac{u}{p}\right) = \pm 1$$

because $u^2$ is always a square of $\mathbb{F}_p \Longrightarrow u^2 = v^4$ for some $v \in \mathbb{F}_p$

$$\Longrightarrow (X, Y) = (v^2x, v^3y) \text{ isomorphism defined over } \mathbb{F}_p$$

Non trivial twist: $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \mid \omega^2 = u,\ E^{t} : Y^2 = X^3 + auX_{|\mathbb{F}_p}$

isomorphism $(X, Y) = (ux, u\omega y)$ now defined over $\mathbb{F}_{p^2}$

# j-invariant 1728

$$\textbf{Example :} \quad p \equiv 3 \mod 4$$

$$E_1 : y^2 = x^3 + x_{|\mathbb{F}_p}, \quad E_2 : y^2 = x^3 - x_{|\mathbb{F}_p}, \quad j_{E_1} = j_{E_2} = 1728$$

- $E_1, E_2$ are non-trivial quadratic twists one of each other
- $E_1^t = E_2$ with an isomorphism

$$(X, Y) = (ix, i(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})y)$$

- $E_1, E_2$ are 2-isogenous: $E_1 \in Isom_{\mathbb{F}_p}(E_2/[2]E_2)$
- If $j = 1728$ then $E_1 \xrightarrow{\varphi} {E_1}^t$, $\varphi$ isogeny with coefficients in $\mathbb{F}_p$

# j-invariant 1728

**Example** (*continued*) : $p \equiv 3 \mod 4$

$$E_1 : y^2 = x^3 + x_{|\mathbb{F}_p}, \quad E_2 : y^2 = x^3 - x_{|\mathbb{F}_p}, \quad j_{E_1} = j_{E_2} = 1728$$

- $i^p = -i$ so $\iota(x, y) = (-x, iy) \in End(E_1) \cap End(E_2)$ satisfies

$$\pi_E \iota = -\iota \pi_E$$

- Hence $E_1$ and $E_2$ are supersingular over $\mathbb{F}_p$
- Is $\iota$ related to $E_1 \xrightarrow{\varphi_{|\mathbb{F}_p}} {E_1}^t$?
- Is this situation holding for other $j_E$ ? We follow [CPV, Sect. 3] and ask for other $E$ and $\alpha \in End(E)$ such that

$$\pi_E \circ \alpha = -\alpha \circ \pi_E$$

# Quotient isogenies

- $\mathcal{I}_G : E \to E/G$ defined over $\mathbb{F}_p$ if and only if $\pi_E(G) \subseteq G$.
- $G_1, \ldots, G_{\ell+1}$ the $\ell + 1$ subgroups of order $\ell$ in $E(\overline{\mathbb{F}}_q)$
- $E/G_i$ the $\ell + 1$ curves adjacent to $E$ by $\ell$-isogenies $\mathcal{I}_{G_i}$ with coefficients in any extension of $\mathbb{F}_q$
- $\Phi_\ell(X, Y)$ the classical modular polynomial w.r.t. $\ell$
- $j(E/G_1), \ldots, j(E/G_{\ell+1})$ are roots of $\Phi_\ell(X, j(E))$.
- Solution of $\Phi_\ell(X, X) \mod p = 0$ represent $\overline{\mathbb{F}}_q$-isomorphism classes of curves with the same $j$-invariant ( so twists ) with isogenies of degree $\ell$ and coefficients over any extension.
- Our algorithm identifies the roots of $\Phi_\ell(X, X) \mod p$ where the "1728 scenario $E \xrightarrow{\varphi_{|\mathbb{F}_p}} E^t$ " takes place.

# 1728 scenario for other $j$

## Proposition

*If $E_{|\mathbb{F}_p}$ with $j(E) \neq 1728$, and $E^t$ non trivial $E^t \in Twist(E)$ s.t. $\varphi_{|\mathbb{F}_p} : E \to E^t$ isogeny over $\mathbb{F}_p$, then $\exists\, \alpha \in End(E)$ such that*

$$\pi_E \circ \alpha = -\alpha \circ \pi_E$$

$$\varphi_{|\mathbb{F}_p} \Rightarrow E^t_{|\mathbb{F}_p}$$

$$E^t \text{non trivial} \Rightarrow \exists u \notin \mathbb{F}_p \mid (X, Y) = (u^2 x, u^3 y),\ a' = u^4 a,\ b' = u^6 b$$

$$\Rightarrow u^2 \in \mathbb{F}_p \Rightarrow (u^2)^{(p-1)/2} = -1 \Rightarrow u^p = (u^2)^{(p-1)/2} u = -u$$

# twisting endos

$$\begin{array}{ccccc}
E & \xrightarrow{\varphi} & E^t & \xrightarrow{\psi_u} & E \\
\downarrow \pi_E & & \downarrow \pi_{E^t} & & \downarrow \pi_E \\
E & \xrightarrow[\varphi]{} & E^t & \xrightarrow[-\psi_u]{} & E
\end{array}$$

$$\alpha = \psi_u \circ \varphi \Longrightarrow \pi_E \circ \alpha = -\alpha \circ \pi_E$$

# Isogenies not defined in $\mathbb{F}_p$ come in pairs

$$\mathcal{Q}(E) = \{\mathcal{I}_{\langle P\rangle} : E \longrightarrow E/\langle P\rangle \mid \pi_E(P) \notin \langle P\rangle, ord(P) = \ell\}$$

$$\mathcal{T}(E, C) = \{\mathcal{I} : E \to E' \mid \mathcal{I} \in \mathcal{Q}(E), E' \in Twist(C)\}$$

**Lemma**

*If $E, C$ supersingular over $\mathbb{F}_p$ then $\#\mathcal{T}(E, C)$ is even.*

Let $P_1 \in E(\overline{\mathbb{F}}_p)$ of order $\ell$ such that $\mathcal{I}_{\langle P_1\rangle} \in \mathcal{Q}(E)$. Assume

$$C \cong E/\langle P_1\rangle = E_1$$

Then $j_{E_1} \in \mathbb{F}_p$. We will find another isogeny $\in \mathcal{Q}(E)$ different from $\mathcal{I}_{\langle P_1\rangle}$.

# Isogenies not defined in $\mathbb{F}_p$ come in pairs

Let $P_2 = \pi_E(P_1)$, $E_2 = E/\langle P_2\rangle$. Then $E_2 = {E_1}^p$.

But $j(E_1) \in \mathbb{F}_p$, so $j(E_2) = j({E_1}^p) = j(E_1)^p = j(E_1)$

$$\Rightarrow E_2 \in Twist(E_1)$$

$E$ supersingular $\Rightarrow \pi_E^2 = -[p]_E$

Hence $\pi_E(P_2) = \pi_E^2(P_1) \in \langle P_1\rangle \notin \langle P_2\rangle$

Therefore $\mathcal{I}_{\langle P_2\rangle} : E \to E_2 \in \mathcal{T}(E, C)$

# $\mathcal{G}_i(\mathbb{F}_p, \ell)$

- If $p \equiv 3 \mod 4$ then $K = \mathbb{Q}(\sqrt{-p})$ has discriminant $d_K = -p$
- $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, $\mathbb{Z}[\pi_E] \subseteq \mathcal{O}_K$ with index 2
- $$\mathbb{Z}[\pi] \subseteq End_{\mathbb{F}_p}(E) \subseteq \mathcal{O}_K$$
  one = one $\subset$ because of index constrain [K, DG]
- $\mathbb{Z}[\pi] = End_{\mathbb{F}_p}(E) \Longleftrightarrow E[2](\mathbb{F}_p)$ rank 1 [CPV, DG]
- Example $E_1, E_2$ with $j = 1728$.
- If $j_E \neq 1728$ then $End_{\mathbb{F}_p}(E) = End_{\mathbb{F}_p}(E^t)$ [ACLLNSS, Corollary 3.7]
- Write $O_2 = \mathbb{Z}[\pi_E]$ and $O_1 = \mathcal{O}_K$ and class numbers $h_1, h_2$

# $\mathcal{G}_i(\mathbb{F}_p, \ell)$

- The nodes of $\mathcal{G}(\overline{\mathbb{F}}_p, \ell)$ are $j$-invariants, and the arcs are $\ell$-isogenies defined over $\overline{\mathbb{F}}_p$
- The 1728 scenario $E \xrightarrow{\varphi_{|\mathbb{F}_p}} E^t$ becomes a node with a loop in $\mathcal{G}(\overline{\mathbb{F}}_p, \ell)$, hence a zero of $\Phi_\ell(X, X) \mod p$
- The 1728 scenario in $\mathcal{G}_i(\mathbb{F}_p, \ell)$ corresponds to

$$[\mathfrak{a}]^{-1}\mathcal{E} = ([\mathfrak{a}]\mathcal{E}^t)^t \text{ ([CPV, Lemma 5])}$$

- and an endomorphism $\alpha \in End(E)$ to a principal ideal in the maximal quaternionic order
- $\mathcal{G}_i(\mathbb{F}_p, \ell)$ :

nodes: $\mathcal{E}\ell\ell_p(O_i)$ $(Isom_{\mathbb{F}_p}(E) \mid End_{\mathbb{F}_p}(E) \cong O_i)$

arcs: $\ell$-isogenies $|_{\mathbb{F}_p}$

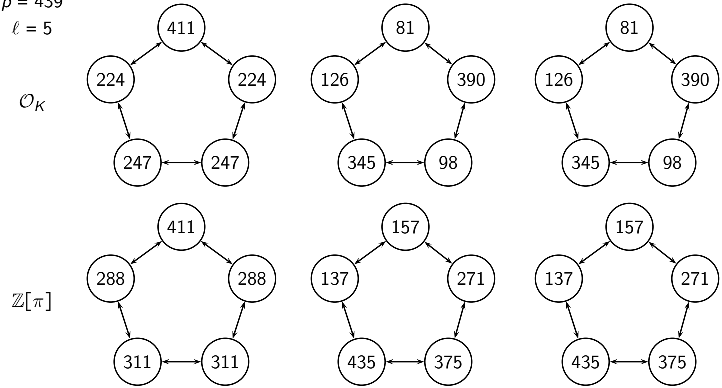
- Class group action on $\mathcal{E}\ell\ell_p(O_i)$ by ideal multiplication.

# $\mathcal{G}_i(\mathbb{F}_p, \ell)$

- $\ell \neq 2$ then a rational $\ell$-isogeny is ideal class of norm $\ell$ and order say $n_i$ in $\mathcal{C}\ell(O_i)$
- If $\left(\frac{-p}{\ell}\right) = 1$ then $(\ell)$ splits $\ell = \mathfrak{l}\bar{\mathfrak{l}}$ in $O_i$
- If also $\ell \neq 2$ and $p \equiv 3 \mod 4$ then $\mathcal{G}_1(\mathbb{F}_p, \ell)$, $\mathcal{G}_2(\mathbb{F}_p, \ell)$ are disconnected, so every node has just 2 horizontal arcs [K, DG]
- The $h_i$ classes in $\mathcal{G}_i(\mathbb{F}_p, \ell)$ are $\frac{h_i}{n_i}$ cycles of length $n_i$.
- If $p \equiv 3 \pmod 4$ then $h_i$ is odd, hence the length of both cycles $n_i$ is odd.
- If $n_i > 1$ then the 1728 scenario takes place for non principal ideals

# Example

$p = 439$
$\ell = 5$



# Algorithm

## Proposition

*If $p \equiv 3 \mod 4$ then the 1728 scenario $E \xrightarrow{\varphi_{|\mathbb{F}_p}} E^t$ takes place only in the cycle of $\mathcal{G}_i(\mathbb{F}_p, \ell)$ where $Isom_{\mathbb{F}_p}(C)$ with $j_C = 1728$ lies.*

Odd nodes + [CPV, Lemma 5]

## Proposition

*If $p \equiv 3 \mod 4$ and $E$ has a twisting endomorphism then the multiplicity of $j_E$ a zero of $\Phi_\ell(X, X) \mod p$ is odd.*

The 1728 scenario shows an arc joining $E$ and $E^t$ is $\varphi_{|\mathbb{F}_p}$. There might be more isogenies between them, but necessarily these are non-rational. By Lemma these come in pairs.

# Algorithm

## Proposition

- *If multiplicity of $j_E$ as a zero of $\Phi_\ell(X, X) \mod p$ is odd and $> 3$ then we found $j_E$ because then $E$ is necessarily supersingular.*
- *If multiplicity is 1 we have to sort supersingular $j$'s with factorization pattern of $\Phi_\ell(X, X) \mod p$ [BSS] (treat case $j = 0$ directly).*

# Algorithm

- set $c = 0$
- Find $\mathcal{O}_k, \mathbb{Z}[\pi]$ and find factorization of $\ell$ in both orders:
  1. $(\ell) = \mathfrak{e}_1\bar{\mathfrak{e}_1}$ in $O_1$
  2. $(\ell) = \mathfrak{e}_2\bar{\mathfrak{e}_2}$ in $O_2$
- If $\mathfrak{e}_1$ is ppal (in $O_1$) then add $j = 1728$ to list $J$
- If $\mathfrak{e}_2$ is ppal (in $O_2$) then add $j = 1728$ to $J$
- If both are ppal we are done

# Algorithm

- If $\mathfrak{c}_1$ is NOT ppal (in $O_1$) then all cycles have length $n_1 > 1$ and we are looking for a $j \neq 1728$
- The cycle $\mathcal{C}_1$ containing an isomorphism class with $j = 1728$ has the 1728 scenario. Put $c = c + 1$.
- If $\mathfrak{c}_2$ is NOT ppal (in $O_2$) then all cycles have length $n_2 > 1$ and we are looking for a $j \neq 1728$. Now $j$ can be $j = 0$.
- if $p \equiv 2 \mod 3$ and $\Phi_\ell(X, X) \mod p = X^k \cdot g(X) \mod p$ with $k$ odd then add $j = 0$ to the list
- else $j$ is $\neq 0$. Put $c = c + 1$

# Algorithm

- Set counter $r = 0$, and remove roots $0, 1728$ from $\Phi_\ell(X, X)$ mod $p$. Call it $f(X)$.
- While $r \neq c$ find root of $f(x)$ and check for odd multiplicity $m$.
- If $m \geq 3$ add the root to $J$ and set $r = r + 1$.
- If $m = 1$ the root may correspond to ordinary $j$ and rule out this case. If not, add the root to $J$ and $r = r + 1$
- return $J$

# More twisting endomorphisms

Examples given by our algorithm:

$$\mathbb{F}_{47}, \quad E: y^2 = x^3 + 16x + 15, \quad w^2 + 45w + 5 = 0$$

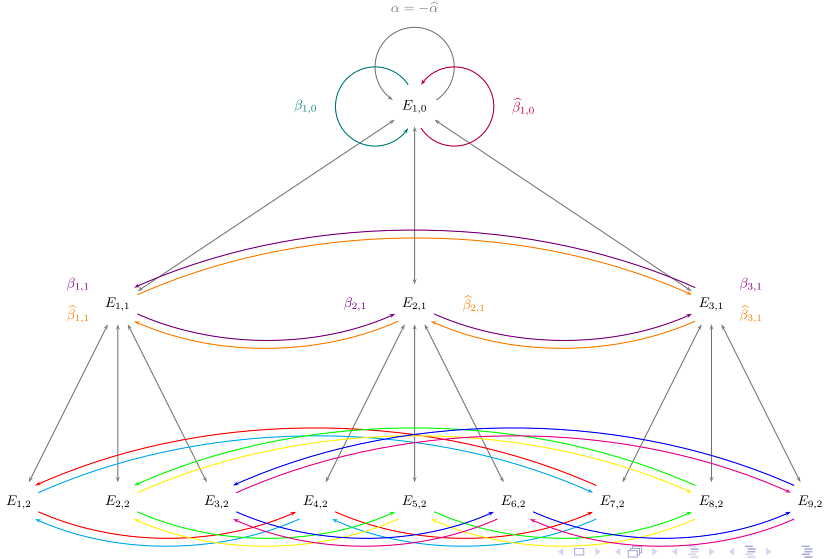
$$\alpha(x, y) = \Big(\frac{31x^3 + 7x^2 + 18x + 17}{x^2 + 26x + 28},$$

$$\frac{(32w + 15)x^3 + (26w + 21)x^2 + (w + 46)x + (23w + 24)}{x^3 + 39x^2 + 37x + 35}y\Big)$$

# Endomorphisms

- For $\alpha$ a twisting endomorphism of $E$ of order $\ell$ , let $\beta = r + s\alpha$ of prime degree $m = r^2 + s^2\ell$
- Then $\alpha$ spreads in the $\ell$-isogeny graph inducing endomorphisms of degree $m^{c_k}$ for $c_k \mid \ell^k$
- All elliptic curves $\ell^k$-isogenous to $E$ have an endomorphism of degree $m^{c_k}$

# Example $\ell = 3, r = 2, s = \pm 1, m = 7$



# Thank you!

- S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, J. Sotáková. "Adventures in Supersingularland". Experimental Mathematics 32(2), pp. 241-268, 2023.
- I. F. Blake, G. Seroussi, N. P. Smart. "Elliptic Curves in Cryptography". London Mathematical Society Lecture Note Series, vol. 265, 1999.
- W. Castryck, L. Panny, F. Vercauteren. "Rational Isogenies from Irrational Endomorphisms". EUROCRYPT 2020, LNCS, vol. 12106, pp. 523-548, 2020.
- C. Delfs, S. D. Galbraith. "Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$". Designs, Codes and Cryptography, vol. 78, pp. 425-440, 2016.
- D. Kohel. Endomorphism rings of elliptic curves over finite fields. PhD, University of California Berkeley, 1996.