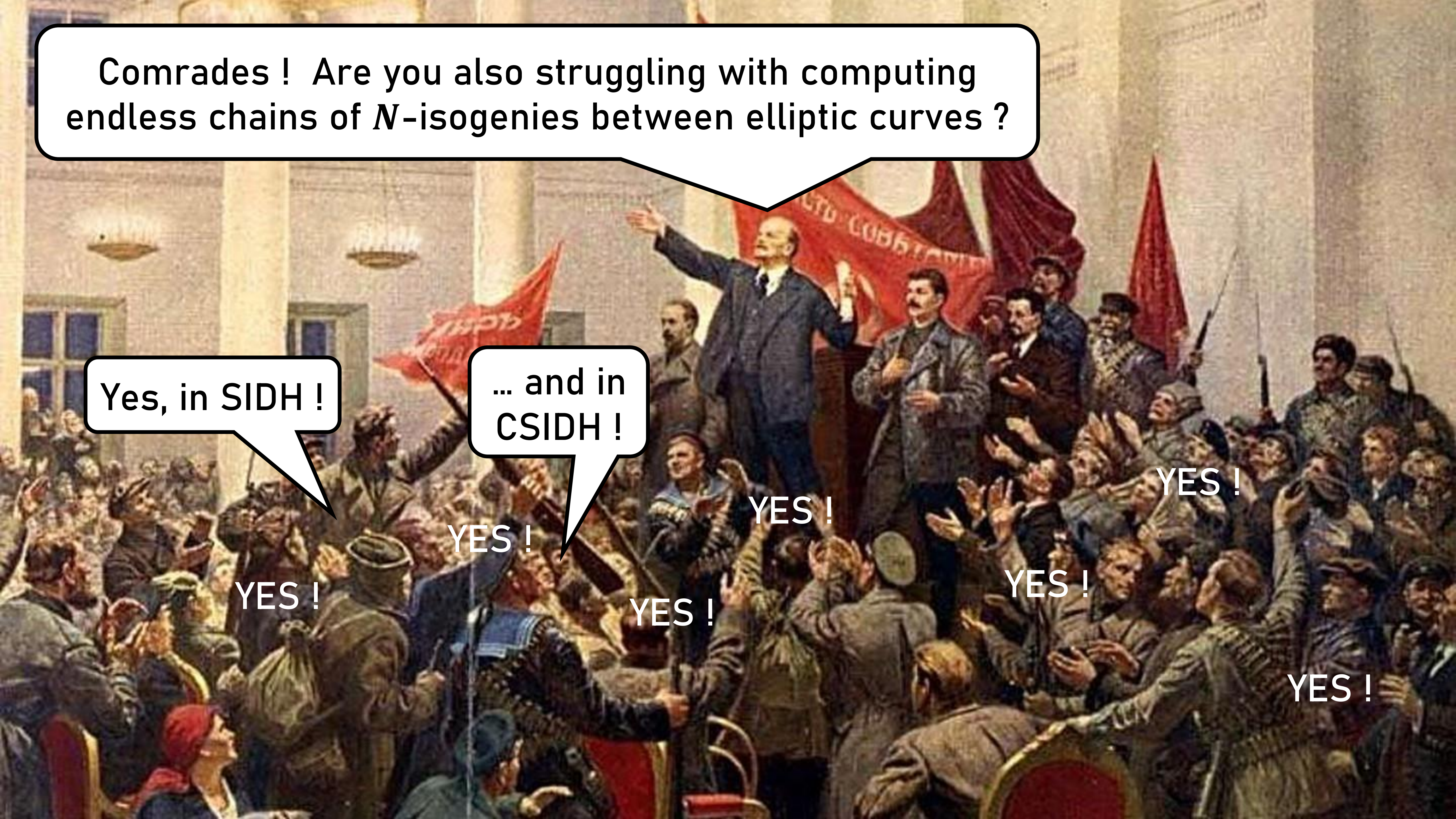
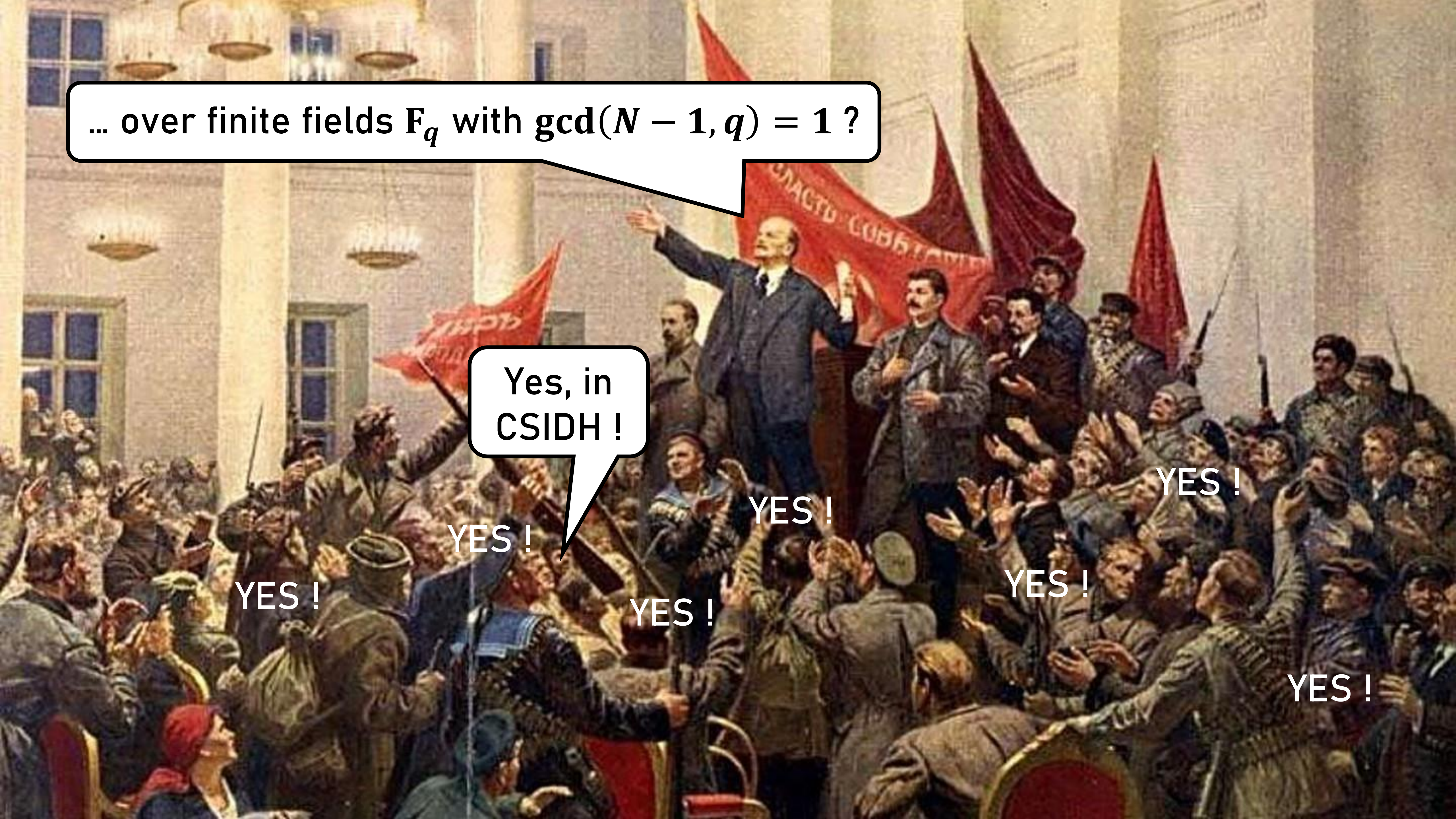
RADICAL ISOGENIES !

Wouter Castryck, Thomas Decru, Frederik Vercauteren

Rump session ANTS-XIV, New Zoomland, 1 July 2020


Comrades ! Are you also struggling with computing endless chains of N-isogenies between elliptic curves ?
Yes, in SIDH !
... and in CSIDH !
YES !
YES !
YES !
YES !
YES !
YES !
YES !


… over finite fields $\mathbf{F}_q$ with $\mathbf{gcd}(N-1, q) = 1$?
Yes, in CSIDH !
YES !
YES !
YES !
YES !
YES !
YES !
YES !


Are you also fed up with sampling random $\mathbf{F}_q$-rational points and multiplying by $\#E(\mathbf{F}_q)/N$, before applying Vélu, at each step ?
YES !
YES !
YES !
YES !
YES !
YES !
YES !


Behold, we present to you:
RADICAL ISOGENIES !
RADICAL ISOGENIES !
RADICAL ISOGENIES !
RADICAL ISOGENIES !
RADICAL ISOGENIES !

Observation: for each $N \geq 2$ there exist concrete radical formulas

$$x_1\left(a_1, a_2, a_3, a_4, a_6, x_0, y_0, \sqrt[N]{\rho(a_1, a_2, a_3, a_4, a_6, x_0, y_0)}\right)$$
$$y_1\left(a_1, a_2, a_3, a_4, a_6, x_0, y_0, \sqrt[N]{\rho(a_1, a_2, a_3, a_4, a_6, x_0, y_0)}\right)$$

such that for whatever cyclic N-isogeny we computed using Vélu

$$E_0\colon\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad P_0 = (x_0, y_0)$$

$$\Big\downarrow \varphi$$

$$E_1 = {}^{E_0}/_{\langle P_0\rangle} \longrightarrow E_2 = {}^{E_1}/_{\langle P_1\rangle}$$

these produce a point $P_1 = (x_1, y_1) \in E_1$ extending φ to a cyclic N^2-isogeny.

Proof 1:

➢ Forgetful map between modular curves

$$
\begin{array}{c}
X_1'(N) = \{(E_0, P_0, P_1)\} \\
\downarrow \\
X_1(N) = \{(E_0, P_0)\}
\end{array}
$$

is a simple radical extension (analysis of Galois groups).

Proof 2 (in progress, but more explicit):

➢ Conjectural formula that will be discussed in next week's workshop.

➢ Leads to concrete formula for ρ in terms of well-known modular units.

Example: for $N = 5$, assume w.l.o.g. that we are in Tate normal form:

$$E_0\colon\ y^2 + (1-b)xy - by = x^3 - bx^2, \qquad P_0 = (0,0).$$

Then Vélu produces

$$E_1\colon\ y^2 + (1-b)xy - by = x^3 - bx^2 - \left(5b^3 + 10b^2 - 5b\right)x$$
$$-\left(b^5 + 10b^4 - 5b^3 + 15b^2 - b\right).$$

We can take

$$x_1 = \left(\sqrt[5]{b}^3 + \sqrt[5]{b}^2 + 2\sqrt[5]{b} - 2\right)b + 5\sqrt[5]{b}^4 - 3\sqrt[5]{b}^3 + 2\sqrt[5]{b}^2 - \sqrt[5]{b}$$

$$y_1 = \left(\sqrt[5]{b}^2 - \sqrt[5]{b} - 1\right)b^2 + \left(\sqrt[5]{b}^3 - 10\sqrt[5]{b}^2 + 13\sqrt[5]{b} - 11\right)b$$
$$+5\sqrt[5]{b}^4 - 3\sqrt[5]{b}^3 + \sqrt[5]{b}^2.$$

Putting (E_1, P_1) back into Tate normal form yields recursive formulas.

If our field contains all $\boldsymbol{N}^{\mathbf{th}}$ roots of unity, then: $\boldsymbol{N}$ options for $\sqrt[N]{\boldsymbol{\rho}}$. This gives generators for all cyclic subgroups of $\boldsymbol{E_1}$ that extend $\boldsymbol{\varphi}$ to a cyclic $\boldsymbol{N^2}$-isogeny.

Over $\mathbf{F}_{\boldsymbol{q}}$ with $\mathbf{gcd}(\boldsymbol{q}-\mathbf{1}, \boldsymbol{N}) = \mathbf{1}$ there is a unique choice for $\sqrt[N]{\boldsymbol{\rho}}$, which can be computed by mere exponentiation:

- costs $\approx \frac{\mathbf{3}}{\mathbf{2}} \mathbf{log}(\boldsymbol{q})$
- scalar multiplication costs $\approx \mathbf{11}\,\mathbf{log}(\boldsymbol{q})$

Leads to speed-up factor of up to $\mathbf{50}$ for chains of $\boldsymbol{N}$-isogenies (decays with $\boldsymbol{N}$).

Speeds up CSIDH-512 by about 18%.