THE

Lattès club

PRESENTS

The Hessian as a Lattès map

Joint work with F. Pintore and D. Taufer

Marzio Mula • November 19, 2024

Research Institute
Cyber Defence
Universität der Bundeswehr München

Goals of this talk

- Define the Hessian of...

Goals of this talk

- Define the Hessian of...
  - ...a cubic

Goals of this talk

- Define the Hessian of...
  - ...a cubic
  - ...an element of the modular curve $X(3)$

Goals of this talk

- Define the Hessian of...
  - ...a cubic
  - ...an element of the modular curve $X(3)$
  - ...a j-invariant

Goals of this talk

- Define the Hessian of...
  - ...a cubic
  - ...an element of the modular curve $X(3)$
  - ...a j-invariant
- View the corresponding dynamical system as a Lattès map

Goals of this talk

- Define the Hessian of...
  - ...a cubic
  - ...an element of the modular curve $X(3)$
  - ...a j-invariant
- View the corresponding dynamical system as a Lattès map
- Draw Hessian graphs: graphs of j-invariants that are not isogeny graphs!

Hessian of a cubic curve

Main ingredients

$$\Bbbk = \text{(perfect) field of characteristic} \neq 2, 3$$

$$G(X, Y, Z) = \text{homogeneous cubic polynomial in } \Bbbk[X, Y, Z]$$

$$\mathcal{H}(G) = \text{Hessian matrix of } G = \begin{pmatrix} \frac{\partial^2 G}{\partial X^2} & \frac{\partial^2 G}{\partial X \partial Y} & \frac{\partial^2 G}{\partial X \partial Z} \\ \frac{\partial^2 G}{\partial Y \partial X} & \frac{\partial^2 G}{\partial Y^2} & \frac{\partial^2 G}{\partial Y \partial Z} \\ \frac{\partial^2 G}{\partial Z \partial X} & \frac{\partial^2 G}{\partial Z \partial Y} & \frac{\partial^2 G}{\partial Z^2} \end{pmatrix}$$

$$\Bbbk = \text{(perfect) field of characteristic} \neq 2, 3$$

$$G(X,Y,Z) = \text{homogeneous cubic polynomial in } \Bbbk[X,Y,Z]$$

$$\mathcal{H}(G) = \text{Hessian matrix of } G = \begin{pmatrix} \frac{\partial^2 G}{\partial X^2} & \frac{\partial^2 G}{\partial X \partial Y} & \frac{\partial^2 G}{\partial X \partial Z} \\ \frac{\partial^2 G}{\partial Y \partial X} & \frac{\partial^2 G}{\partial Y^2} & \frac{\partial^2 G}{\partial Y \partial Z} \\ \frac{\partial^2 G}{\partial Z \partial X} & \frac{\partial^2 G}{\partial Z \partial Y} & \frac{\partial^2 G}{\partial Z^2} \end{pmatrix}$$

Consider the (possibly singular) cubic

$$E\colon G(X,Y,Z) = 0.$$

The *Hessian of* E is the (possibly singular) cubic

$$\mathrm{Hess}(E)\colon \; \det(\mathcal{H}(G)) = 0.$$

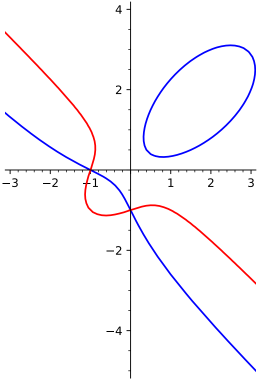
Geometric interpretation

$$
\begin{aligned}
E \cap \mathrm{Hess}(E) &= \textit{inflection points of } E \\
&= E[3] && \text{(when } E \text{ is an elliptic curve)} \\
&= \mathrm{Hess}(E)[3] && \text{(when } \mathrm{Hess}(E) \text{ is an elliptic curve)}
\end{aligned}
$$

$$E \cap \mathrm{Hess}(E) = \textit{inflection points} \text{ of } E$$
$$= E[3] \qquad \text{(when } E \text{ is an elliptic curve)}$$
$$= \mathrm{Hess}(E)[3] \qquad \text{(when } \mathrm{Hess}(E) \text{ is an elliptic curve)}$$

Example (over $\mathbb{Q}$):

$$E\colon x^3 + y^3 + 1 = 6xy$$
$$\mathrm{Hess}(E)\colon x^3 + y^3 + 1 = -xy$$



Geometric interpretation

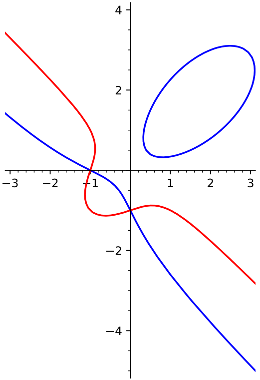
$$\begin{aligned} E \cap \mathrm{Hess}(E) &= \textit{inflection points of } E \\ &= E[3] && \text{(when } E \text{ is an elliptic curve)} \\ &= \mathrm{Hess}(E)[3] && \text{(when } \mathrm{Hess}(E) \text{ is an elliptic curve)} \end{aligned}$$

Example (over $\mathbb{Q}$):

$$E\colon x^3 + y^3 + 1 = 6xy$$

$$\mathrm{Hess}(E)\colon x^3 + y^3 + 1 = -xy$$

$$E \cap \mathrm{Hess}(E) = \Big\{ \left(\frac{1 \pm \sqrt{-3}}{2} : 0 : 1\right), \left(\frac{1 \pm \sqrt{-3}}{2} : 1 : 0\right), \left(0 : \frac{1 \pm \sqrt{-3}}{2} : 1\right), (-1 : 0 : 1), (0 : -1 : 1)\,(-1 : 1 : 0) \Big\}$$



The Hesse pencil

- Pick 9 (inflection) points
- Parametrize cubics through them

The Hesse pencil

- Pick 9 (inflection) points $\rightarrow$ the inflection points of $X^3 + Y^3 + Z^3 = 0$
- Parametrize cubics through them

The Hesse pencil

- Pick 9 (inflection) points $\rightarrow$ the inflection points of $X^3 + Y^3 + Z^3 = 0$
- Parametrize cubics through them $\rightarrow$ $\lambda \underbrace{XYZ}_{\text{(Hessian of } X^3+Y^3+Z^3)} + \mu(X^3 + Y^3 + Z^3) = 0$

for $[\lambda : \mu] \in \mathbb{P}^1(\Bbbk)$

The Hesse pencil

- Pick 9 (inflection) points $\rightarrow$ the inflection points of $X^3 + Y^3 + Z^3 = 0$
- Parametrize cubics through them $\rightarrow$ $\lambda \underbrace{XYZ}_{\text{(Hessian of } X^3+Y^3+Z^3\text{)}} + \mu(X^3 + Y^3 + Z^3) = 0$

(smooth iff $\mu \neq 0$ and $\left(\frac{\lambda}{3\mu}\right)^3 \neq -1$) for $[\lambda : \mu] \in \mathbb{P}^1(\Bbbk)$

The Hesse pencil

- Pick 9 (inflection) points $\rightarrow$ the inflection points of $X^3+Y^3+Z^3=0$
- Parametrize cubics through them $\rightarrow$ $\lambda \underbrace{XYZ}_{\text{(Hessian of } X^3+Y^3+Z^3)} + \mu(X^3+Y^3+Z^3)=0$

(smooth iff $\mu \neq 0$ and $\left(\frac{\lambda}{3\mu}\right)^3 \neq -1$) for $[\lambda : \mu] \in \mathbb{P}^1(\Bbbk)$

Fun facts:

- The Hesse pencil is a model for the modular curve $X(3)$:

$$[\lambda : \mu] \quad \leftrightarrow \quad (\text{Isomorphism class of elliptic curves, } 3\text{-torsion basis}).$$

The Hesse pencil

- Pick 9 (inflection) points $\rightarrow$ the inflection points of $X^3+Y^3+Z^3=0$
- Parametrize cubics through them $\rightarrow$ $\lambda \underbrace{XYZ}_{\text{(Hessian of } X^3+Y^3+Z^3)} + \mu(X^3+Y^3+Z^3)=0$

(smooth iff $\mu \neq 0$ and $\left(\frac{\lambda}{3\mu}\right)^3 \neq -1$) for $[\lambda : \mu] \in \mathbb{P}^1(\mathbb{k})$

Fun facts:

- The Hesse pencil is a model for the modular curve $X(3)$:

$$[\lambda : \mu] \quad \leftrightarrow \quad \text{(Isomorphism class of elliptic curves, 3-torsion basis).}$$

- The 'cubed' Hesse pencil is a model for the modular curve $X_0(3)$:

$$[\lambda^3 : \mu^3] \quad \leftrightarrow \quad \text{(Isomorphism class of elliptic curves, order-3 subgroup).}$$

Hessian map on $X(3)$

Weierstrass form

$$\boxed{X^3 + AXZ^2 + BZ^3 - Y^2Z = 0}$$

Hessian map on $X(3)$

Weierstrass form

Garbage form :-(

$$\boxed{X^3 + AXZ^2 + BZ^3 - Y^2Z = 0} \xrightarrow{\text{Hess}} \boxed{-8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0}$$

HESSIAN MAP ON $X(3)$

Weierstrass form

$$X^3 + AXZ^2 + BZ^3 - Y^2Z = 0 \xrightarrow{\text{Hess}} -8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0$$

Garbage form :(

$$\lambda XYZ + \mu(X^3 + Y^3 + Z^3) = 0$$

Hessian form

Hessian map on $X(3)$

Weierstrass form

$$X^3 + AXZ^2 + BZ^3 - Y^2Z = 0 \xrightarrow{\text{Hess}} -8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0$$

Garbage form

$$\lambda XYZ + \mu(X^3 + Y^3 + Z^3) = 0 \xrightarrow{\text{Hess}} (108\mu^3 + \lambda^3)XYZ + (-3\mu\lambda^2)(X^3 + Y^3 + Z^3) = 0$$

Hessian form

Hessian form

Hessian map on $X(3)$

Weierstrass form | Garbage form :(

$$X^3 + AXZ^2 + BZ^3 - Y^2Z = 0 \xrightarrow{\text{Hess}} -8(3XY^2 + 3AX^2Z + 9BXZ^2 - A^2Z^3) = 0$$

$$\lambda XYZ + \mu(X^3 + Y^3 + Z^3) = 0 \xrightarrow{\text{Hess}} (108\mu^3 + \lambda^3)XYZ + (-3\mu\lambda^2)(X^3 + Y^3 + Z^3) = 0$$

Hessian form | Hessian form :)

Bottom line

The Hessian map on the Hesse pencil can be viewed as a map on $\mathbb{P}^1(\overline{\mathbb{k}}) \cong X(3)$:

$$\Lambda : \quad [\lambda : \mu] \mapsto [108\mu^3 + \lambda^3 : -3\mu\lambda^2]$$

Hessian map on $X(1)$

What about j-invariants?

What about j-invariants?

Proposition

Let E be a cubic. If E is...

- *...nonsingular and $j(E) \neq 0$, then*

$$j\big(\mathrm{Hess}(E)\big) = \frac{(6912 - j(E))^3}{27(j(E))^2}.$$

Hessian map on $X(1)$

What about j-invariants?

Proposition

Let E be a cubic. If E is...

- *...nonsingular and $j(E) \neq 0$, then*

$$j\big(\mathrm{Hess}(E)\big) = \frac{(6912 - j(E))^3}{27(j(E))^2}.$$

- *...nonsingular and $j(E) = 0$, then $\mathrm{Hess}(E)$ is the union of three lines.*

What about j-invariants?

Proposition

Let E be a cubic. If E is...

- *...nonsingular and $j(E) \neq 0$, then*

$$j\big(\mathrm{Hess}(E)\big) = \frac{(6912 - j(E))^3}{27(j(E))^2}.$$

- *...nonsingular and $j(E) = 0$, then $\mathrm{Hess}(E)$ is the union of three lines.*
- *...the union of three lines, then $\mathrm{Hess}(E)$ is the union of three lines.*

Hessian map on $X(1)$

What about j-invariants?

Proposition

Let E be a cubic. If E is...

- *...nonsingular and $j(E) \neq 0$, then*

$$j\big(\mathrm{Hess}(E)\big) = \frac{(6912 - j(E))^3}{27(j(E))^2}.$$

- *...nonsingular and $j(E) = 0$, then $\mathrm{Hess}(E)$ is the union of three lines.*
- *...the union of three lines, then $\mathrm{Hess}(E)$ is the union of three lines.*

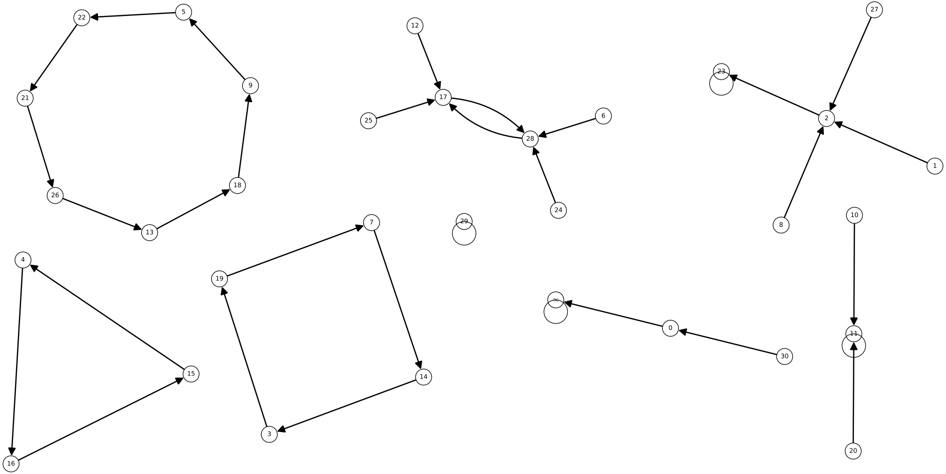
Bottom line

The Hessian map on the Hesse pencil can be viewed as a map on $\mathbb{P}^1(\overline{\Bbbk}) \cong X(1)$:

$$\mathrm{H}: \quad [j : w] \mapsto [(6912w - j)^3 : 27j^2 w]$$

What happens if we iterate H over $\mathbb{P}^1(\mathbb{k})$?

For $\mathbb{k} = \mathbb{F}_{31}$...



Functional graphs

Functional graphs

$$\mathbb{k} = \text{field of characteristic} \notin \{2, 3\}$$
$$\phi(x) = \text{rational function in } \mathbb{k}(x)$$

Functional graphs

$$\mathbb{k} = \text{field of characteristic} \notin \{2,3\}$$
$$\phi(x) = \text{rational function in } \mathbb{k}(x)$$

The *functional graph* of ϕ is the directed graph s.t.

- the vertices are the elements of $\mathbb{k}$;
- there is an edge $\alpha \to \beta$ iff $\beta = \phi(\alpha)$ (counted with multiplicity).

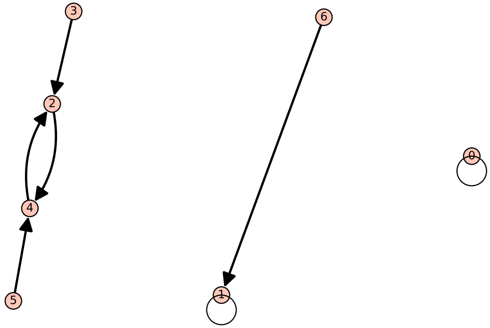
Functional graphs

$$\mathbb{k} = \text{field of characteristic} \notin \{2,3\}$$
$$\phi(x) = \text{rational function in } \mathbb{k}(x)$$

The *functional graph* of ϕ is the directed graph s.t.

- the vertices are the elements of $\mathbb{k}$;
- there is an edge $\alpha \to \beta$ iff $\beta = \phi(\alpha)$ (counted with multiplicity).

Example: $\phi(x) = x^2$ on $\mathbb{F}_7$



Functional graphs

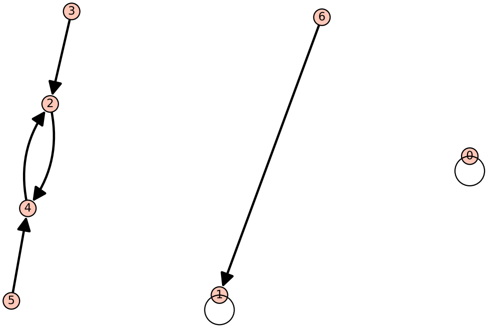
$$\mathbb{k} = \text{field of characteristic} \notin \{2,3\}$$
$$\phi(x) = \text{rational function in } \mathbb{k}(x)$$

The *functional graph* of ϕ is the directed graph s.t.

- the vertices are the elements of $\mathbb{k}$;
- there is an edge $\alpha \to \beta$ iff $\beta = \phi(\alpha)$ (counted with multiplicity).

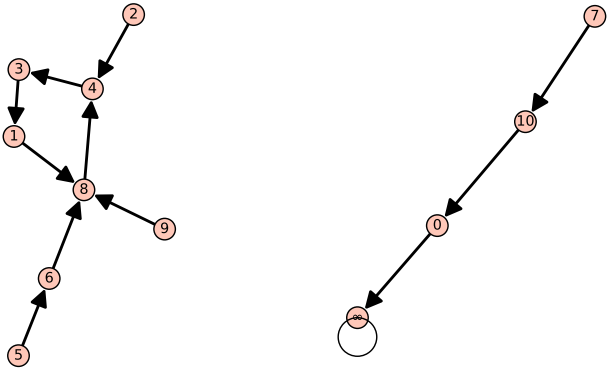
When $\phi(\alpha)$ is not defined, we set $\phi(\alpha) = \infty$.

Example: $\phi(x) = x^2$ on $\mathbb{F}_7$



Some general (obvious) remarks

Example: $\phi(x) = \frac{(x+1)^3}{x^2}$ on $\mathbb{F}_{11}$



- Each connected component of the graph has at most one cycle (exactly 1 if $\mathbb{k}$ is finite).
- The indegree of each vertex is at most the the maximum between the degree of the numerator and the degree of the denominator of $\phi(x)$.
- The outdegree of each vertex is (at least) 1.

$\mathbb{k}$ = field of characteristic $\neq 2, 3$

ϕ = rational map $\mathbb{P}^1(\overline{\mathbb{k}}) \to \mathbb{P}^1(\overline{\mathbb{k}})$ of degree $d \geq 2$

We say that ϕ is a *Lattès map* if there exist:

$$\mathbb{P}^1(\overline{\mathbb{k}}) \xrightarrow[\phi]{} \mathbb{P}^1(\overline{\mathbb{k}})$$

Lattès maps

$\mathbb{k} =$ field of characteristic $\neq 2, 3$

$\phi =$ rational map $\mathbb{P}^1(\overline{\mathbb{k}}) \to \mathbb{P}^1(\overline{\mathbb{k}})$ of degree $d \geq 2$

We say that ϕ is a *Lattès map* if there exist:

- an elliptic curve E over $\overline{\mathbb{k}}$,

$$E(\overline{\mathbb{k}})$$

$$\mathbb{P}^1(\overline{\mathbb{k}}) \xrightarrow[\phi]{} \mathbb{P}^1(\overline{\mathbb{k}})$$

Lattès maps

$\mathbb{k}$ = field of characteristic $\neq 2, 3$

ϕ = rational map $\mathbb{P}^1(\overline{\mathbb{k}}) \to \mathbb{P}^1(\overline{\mathbb{k}})$ of degree $d \geq 2$

We say that ϕ is a *Lattès map* if there exist:

- an elliptic curve E over $\overline{\mathbb{k}}$,
- a morphism $\psi\colon E \to E$,

$$E(\overline{\mathbb{k}}) \xrightarrow{\ \psi\ } E(\overline{\mathbb{k}})$$

$$\mathbb{P}^1(\overline{\mathbb{k}}) \xrightarrow[\ \phi\ ]{} \mathbb{P}^1(\overline{\mathbb{k}})$$

Lattès maps

$$\Bbbk = \text{field of characteristic} \neq 2, 3$$

$$\phi = \text{rational map } \mathbb{P}^1(\overline{\Bbbk}) \to \mathbb{P}^1(\overline{\Bbbk}) \text{ of degree } d \geq 2$$

We say that ϕ is a *Lattès map* if there exist:

- an elliptic curve E over $\overline{\Bbbk}$,
- a morphism $\psi\colon E \to E$,
- a finite separable covering $\pi\colon E \to \mathbb{P}^1(\overline{\Bbbk})$,

such that the following diagram is commutative:

$$\begin{array}{ccc} E(\overline{\Bbbk}) & \xrightarrow{\quad\psi\quad} & E(\overline{\Bbbk}) \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{P}^1(\overline{\Bbbk}) & \xrightarrow[\quad\phi\quad]{} & \mathbb{P}^1(\overline{\Bbbk}) \end{array}$$

THEOREM

A rational map $\phi\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a Lattès map if and only if:

1. *ϕ has no exceptional points.*
2. *There exists a ramification function $v\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{N}^*$ such that:*

$$v(\phi(P)) = e_P(\phi) \cdot v(P) \quad \textit{for all } P \in \mathbb{P}^1(\mathbb{C}).$$

The *set of exceptional points* of ϕ is the largest finite set $T \subseteq \mathbb{C}$ such that $\phi^{-1}(T) = T$.

THEOREM

A rational map $\phi\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a Lattès map if and only if:

1. *ϕ has no exceptional points.*
2. *There exists a ramification function $v\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{N}^*$ such that:*

$$v(\phi(P)) = e_P(\phi) \cdot v(P) \quad \text{for all } P \in \mathbb{P}^1(\mathbb{C}).$$

Theorem

A rational map $\phi\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ *is a Lattès map if and only if:*

1. ϕ *has no exceptional points.*
2. *There exists a ramification function* $v\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{N}^*$ *such that:*

$$v(\phi(P)) = e_P(\phi) \cdot v(P) \quad \text{for all } P \in \mathbb{P}^1(\mathbb{C}).$$

The *ramification index* of ϕ at P is:

$$e_P(\phi) = \operatorname{ord}_P(\phi(x) - \phi(P)).$$

A point P is a *critical point* if $e_P(\phi) \geq 2$.

THEOREM

A rational map $\phi\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is a Lattès map if and only if:

1. *ϕ has no exceptional points.*
2. *There exists a ramification function $v\colon \mathbb{P}^1(\mathbb{C}) \to \mathbb{N}^*$ such that:*

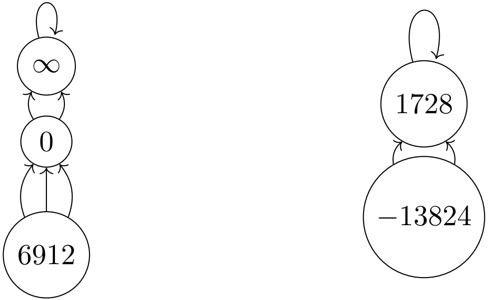
$$v(\phi(P)) = e_P(\phi) \cdot v(P) \quad \text{for all } P \in \mathbb{P}^1(\mathbb{C}).$$

Conclusion: to check if a map is Lattès, we only need to inspect its *post-critical portrait*, i.e. the points of the form $\phi^{(n)}(P)$, where P is critical.

The Hessian as a Lattès map

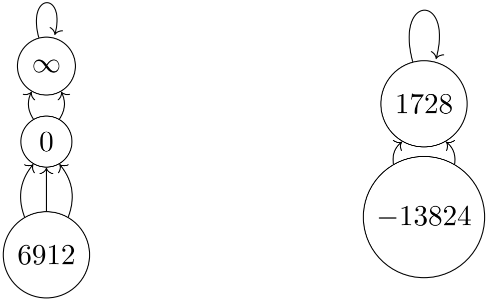
HESSIAN AS A LATTÈS MAP OVER $\mathbb{C}$

Post-critical portrait of H:



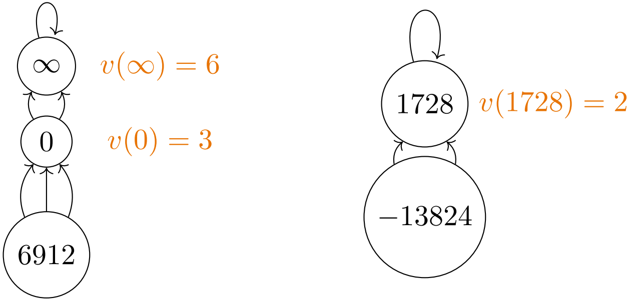
Post-critical portrait of H:

We can define a ramification function v that is 1 everywhere except from...



Post-critical portrait of H:

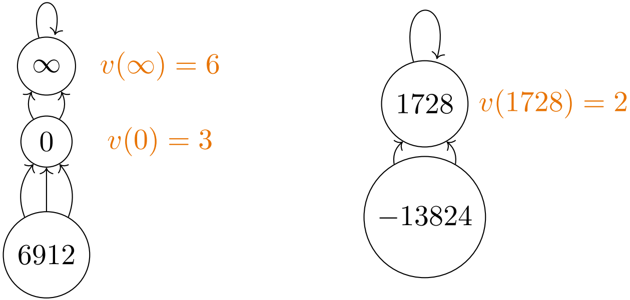
We can define a ramification function v that is 1 everywhere except from...



Hessian as a Lattès map over $\mathbb{C}$

Post-critical portrait of H:

We can define a ramification function v that is 1 everywhere except from...



Corollary

H *is a Lattès map over* $\mathbb{C}$.

Our contributions

- H and Λ are Lattès maps in any characteristic other than 2 and 3

Our contributions

- H and Λ are Lattès maps in any characteristic other than 2 and 3
- complete picture of Hessian graphs over number fields and finite fields

Our contributions

- H and Λ are Lattès maps in any characteristic other than 2 and 3
- complete picture of Hessian graphs over number fields and finite fields
- fast algorithms to compute iterated Hessian

Our contributions

- H and Λ are Lattès maps in any characteristic other than 2 and 3
- complete picture of Hessian graphs over number fields and finite fields
- fast algorithms to compute iterated Hessian
- algorithms to tell whether two j-invariants are in the same connected component

Our contributions

- H and Λ are Lattès maps in any characteristic other than 2 and 3
- complete picture of Hessian graphs over number fields and finite fields
- fast algorithms to compute iterated Hessian
- algorithms to tell whether two j-invariants are in the same connected component
- wishful thinking on finding supersingular j-invariants

The model curve/endomorphism

Ingredients for a Lattès map:

- Model elliptic curve
- Morphism on model curve
- Projection map

Let $k \in \mathbb{k}^*$.

The model curve/endomorphism

Ingredients for a Lattès map:
- Model elliptic curve ✓
- Morphism on model curve
- Projection map

$E_k(\bar{\mathbb{k}})$

Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$E_k\colon y^2 = x^3 + \frac{k}{4}.$$

Ingredients for a Lattès map:

- Model elliptic curve ✓
- Morphism on model curve ✓
- Projection map

$$E_k(\bar{\mathbb{k}}) \xrightarrow{\psi_k} E_k(\bar{\mathbb{k}})$$

Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$E_k : y^2 = x^3 + \frac{k}{4}.$$

- 3-endomophism on E_k:

$$\psi_k : E_k \to E_k \qquad \text{with } \ker(\psi_k) = \left\langle \left(0, \frac{\sqrt{k}}{2}\right) \right\rangle.$$

THE MODEL CURVE/ENDOMORPHISM

Ingredients for a Lattès map:
- Model elliptic curve ✓
- Morphism on model curve ✓
- Projection map ✓

$$\begin{array}{ccc} E_k(\overline{\mathbb{k}}) & \xrightarrow{\psi_k} & E_k(\overline{\mathbb{k}}) \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{P}^1(\overline{\mathbb{k}}) & \xrightarrow[\phi_k]{} & \mathbb{P}^1(\overline{\mathbb{k}}) \end{array}$$

Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$E_k : y^2 = x^3 + \frac{k}{4}.$$

- 3-endomophism on E_k:

$$\psi_k : E_k \to E_k \qquad \text{with } \ker(\psi_k) = \left\langle \left(0, \frac{\sqrt{k}}{2}\right) \right\rangle.$$

THEOREM (–, P., T.)

$$k = 108 \qquad \phi_{108} = \Lambda$$

$\rightsquigarrow$ *(Hesse pencil)*

$$(x, y) \overset{\pi}{\mapsto} [x : 1]$$

The model curve/endomorphism

Ingredients for a Lattès map:

- Model elliptic curve ✓
- Morphism on model curve ✓
- Projection map ✓

$$\begin{array}{ccc} E_k(\overline{\mathbb{k}}) & \xrightarrow{\psi_k} & E_k(\overline{\mathbb{k}}) \\ \downarrow \pi & & \downarrow \pi \\ \mathbb{P}^1(\overline{\mathbb{k}}) & \xrightarrow[\phi_k]{} & \mathbb{P}^1(\overline{\mathbb{k}}) \end{array}$$

Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$E_k : y^2 = x^3 + \frac{k}{4}.$$

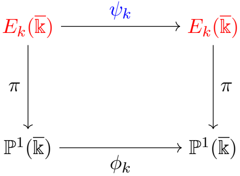
- 3-endomophism on E_k:

$$\psi_k : E_k \to E_k \qquad \text{with } \ker(\psi_k) = \left\langle \left(0, \frac{\sqrt{k}}{2}\right) \right\rangle.$$

Theorem (–, P., T.)

$k = 108$, $(x, y) \overset{\pi}{\mapsto} [x : 1]$ $\rightsquigarrow$ $\phi_{108} = \Lambda$ *(Hesse pencil)*	$k = -6912$, $(x, y) \overset{\pi}{\mapsto} [x^3 : 1]$ $\rightsquigarrow$ $\phi_{-6912} = \mathrm{H}$ *(j-invariants)*

Ingredients for a Lattès map:
- Model elliptic curve ✓
- Morphism on model curve ✓
- Projection map ✓



Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$\boxed{j(E_k) = 0}$$

$$E_k : y^2 = x^3 + \frac{k}{4}.$$

- 3-endomophism on E_k:

$$\psi_k : E_k \to E_k \qquad \text{with } \ker(\psi_k) = \left\langle \left(0, \frac{\sqrt{k}}{2}\right) \right\rangle.$$

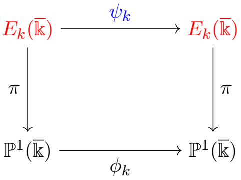
THEOREM (–, P., T.)

$k = 108$ $(x, y) \overset{\pi}{\mapsto} [x : 1]$	$\rightsquigarrow$	$\phi_{108} = \Lambda$ *(Hesse pencil)*
$k = -6912$ $(x, y) \overset{\pi}{\mapsto} [x^3 : 1]$	$\rightsquigarrow$	$\phi_{-6912} = \mathrm{H}$ *(j-invariants)*

The model curve/endomorphism

Ingredients for a Lattès map:

- Model elliptic curve ✓
- Morphism on model curve ✓
- Projection map ✓



Let $k \in \mathbb{k}^*$.

- Model elliptic curve E_k:

$$\boxed{j(E_k) = 0}$$

$$E_k : y^2 = x^3 + \frac{k}{4}.$$

- 3-endomophism on E_k:

$$\psi_k : E_k \to E_k \qquad \text{with } \ker(\psi_k) = \left\langle \left(0, \frac{\sqrt{k}}{2}\right) \right\rangle.$$

$$\boxed{{\psi_k}^2 = [-3]}$$

Theorem (–, P., T.)

$k = 108$ $\rightsquigarrow$ $\phi_{108} = \Lambda$ *(Hesse pencil)*	$k = -6912$ $\rightsquigarrow$ $\phi_{-6912} = \mathrm{H}$ *(j-invariants)*
$(x, y) \overset{\pi}{\mapsto} [x : 1]$	$(x, y) \overset{\pi}{\mapsto} [x^3 : 1]$

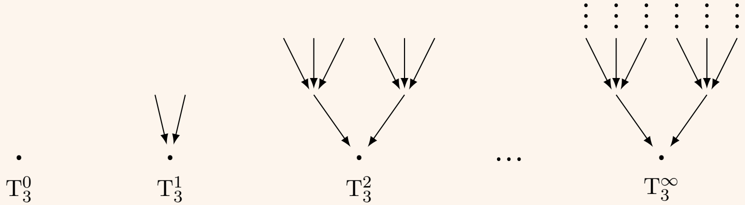
Drawing the Hessian graph

Dynamics of group endomorphisms with prime kernel I

Goal: Understanding the dynamics of the 3-endomorphism ψ_k.

Goal: Understanding the dynamics of the 3-endomorphism ψ_k.

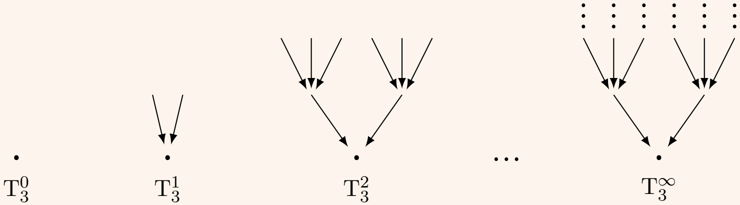
Main building block: the arborescence T_ℓ^m



- If $m < \infty$, then T_ℓ^m is finite and every leaf has depth m.

Goal: Understanding the dynamics of the 3-endomorphism ψ_k.

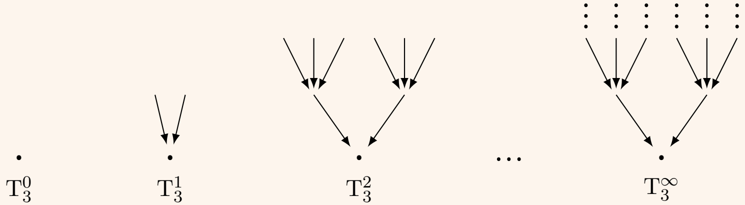
Main building block: the arborescence T_ℓ^m



- If $m < \infty$, then T_ℓ^m is finite and every leaf has depth m.
- T_ℓ^∞ has no leaves.

Goal: Understanding the dynamics of the 3-endomorphism ψ_k.

Main building block: the arborescence T_ℓ^m



- If $m < \infty$, then T_ℓ^m is finite and every leaf has depth m.
- T_ℓ^∞ has no leaves.
- Every non-leaf has indegree $\begin{cases} \ell - 1 & \text{if it is the root,} \\ \ell & \text{otherwise.} \end{cases}$

Dynamics of group endomorphisms with prime kernel II

$G =$ group with identity $\mathcal{O}$

$\psi =$ endomorphism of G with $|\ker \psi| = \ell$ prime

Given $P \in G$, let τ_P be the subgraph whose vertices are $\{Q \in G \mid \exists n \in \mathbb{N} : \psi^{(n)}(Q) = P\}$.

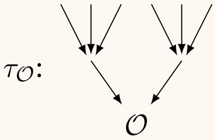
$$G = \text{group with identity } \mathcal{O}$$
$$\psi = \text{endomorphism of } G \text{ with } |\ker\psi| = \ell \text{ prime}$$

Given $P \in G$, let τ_P be the subgraph whose vertices are $\{Q \in G \mid \exists n \in \mathbb{N} : \psi^{(n)}(Q) = P\}$.

Theorem (Functional graph of ψ on G)

Let $m \in \mathbb{N}^* \cup \{\infty\}$ be the maximal depth in $\tau_{\mathcal{O}}$.

Then $\tau_{\mathcal{O}}$ is isomorphic to T_ℓ^m.



Dynamics of group endomorphisms with prime kernel II

G = group with identity $\mathcal{O}$

ψ = endomorphism of G with $|\ker\psi| = \ell$ prime

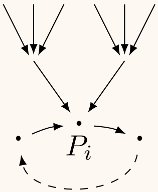
Given $P \in G$, let τ_P be the subgraph whose vertices are $\{Q \in G \mid \exists n \in \mathbb{N} : \psi^{(n)}(Q) = P\}$.

Theorem (Functional graph of ψ on G)

Let $m \in \mathbb{N}^* \cup \{\infty\}$ be the maximal depth in $\tau_{\mathcal{O}}$.

Then $\tau_{\mathcal{O}}$ is isomorphic to T_ℓ^m.
Every connected component is one of the following:

1. *a periodic cycle $\{P_1, \dots, P_r\}$, with $\tau_{P_i} \simeq \tau_{\mathcal{O}}$;*



Case 1

Dynamics of group endomorphisms with prime kernel II

$G =$ group with identity $\mathcal{O}$

$\psi =$ endomorphism of G with $|\ker \psi| = \ell$ prime

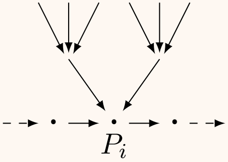
Given $P \in G$, let τ_P be the subgraph whose vertices are $\{Q \in G \mid \exists n \in \mathbb{N} : \psi^{(n)}(Q) = P\}$.

Theorem (Functional graph of ψ on G)

Let $m \in \mathbb{N}^* \cup \{\infty\}$ *be the maximal depth in* $\tau_{\mathcal{O}}$.

Then $\tau_{\mathcal{O}}$ *is isomorphic to* T_ℓ^m.
Every connected component is one of the following:

1. *a periodic cycle* $\{P_1, \ldots, P_r\}$, *with* $\tau_{P_i} \simeq \tau_{\mathcal{O}}$;
2. *an oriented line* $\{P_i\}_{i\in\mathbb{Z}}$, *with* $\tau_{P_i} \simeq \tau_{\mathcal{O}}$;



Case 2

$$G = \text{group with identity } \mathcal{O}$$
$$\psi = \text{endomorphism of } G \text{ with } |\ker\psi| = \ell \text{ prime}$$

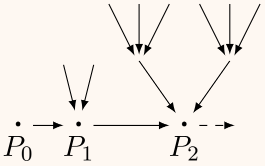
Given $P \in G$, let τ_P be the subgraph whose vertices are $\{Q \in G \mid \exists n \in \mathbb{N} : \psi^{(n)}(Q) = P\}$.

THEOREM (FUNCTIONAL GRAPH OF ψ ON G)

Let $m \in \mathbb{N}^* \cup \{\infty\}$ be the maximal depth in $\tau_{\mathcal{O}}$.

Then $\tau_{\mathcal{O}}$ is isomorphic to T_ℓ^m.
Every connected component is one of the following:

1. *a periodic cycle $\{P_1, \ldots, P_r\}$, with $\tau_{P_i} \simeq \tau_{\mathcal{O}}$;*
2. *an oriented line $\{P_i\}_{i\in\mathbb{Z}}$, with $\tau_{P_i} \simeq \tau_{\mathcal{O}}$;*
3. *an oriented semiline $\{P_i\}_{i\in\mathbb{N}}$, with $\tau_{P_i} \simeq \mathrm{T}_\ell^{\min(i,m)}$.*



Case 3

Bottom line

We know how ψ_k behaves on subgroups of E_k.

Back to the Hessian graph

Bottom line

We know how ψ_k behaves on <u>subgroups</u> of E_k.

Let us refine the Lattès diagram...

$$\begin{array}{ccc} E_k(\overline{\mathbb{k}}) & \xrightarrow{\psi_k} & E_k(\overline{\mathbb{k}}) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1(\overline{\mathbb{k}}) & \xrightarrow[\phi_k]{} & \mathbb{P}^1(\overline{\mathbb{k}}) \end{array}$$

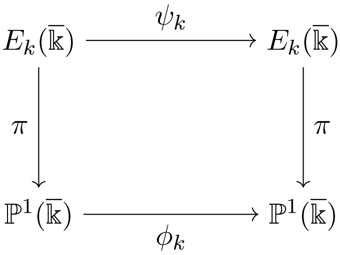
...to study the Hessian graph over $\mathbb{k}$

$$\mathbb{P}^1(\mathbb{k}) \xrightarrow[\phi_k]{} \mathbb{P}^1(\mathbb{k})$$

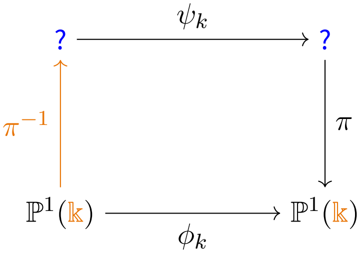
Bottom line

We know how ψ_k behaves on subgroups of E_k.

Let us refine the Lattès diagram...



...to study the Hessian graph over $\Bbbk$



Some ingredients

$$\begin{aligned} \mathcal{S}_k(\mathbb{k}) &= \{(x,y) \in E_k \mid x \in \mathbb{k}\} \cup \{\mathcal{O}\}, \\ \mathbb{k}_3 &= \mathbb{k}(\sqrt[3]{x})_{x \in \mathbb{k}}, \\ \mathcal{S}_k(\mathbb{k}_3) &= \{(x,y) \in E_k \mid x^3 \in \mathbb{k}\} \cup \{\mathcal{O}\}. \end{aligned}$$

Some ingredients

$$\mathcal{S}_k(\Bbbk) = \{(x,y) \in E_k \mid x \in \Bbbk\} \cup \{\mathcal{O}\},$$
$$\Bbbk_3 = \Bbbk(\sqrt[3]{x})_{x\in\Bbbk},$$
$$\mathcal{S}_k(\Bbbk_3) = \{(x,y) \in E_k \mid x^3 \in \Bbbk\} \cup \{\mathcal{O}\}.$$

THEOREM (–, P., T.)

The following diagram is commutative.

$$\begin{array}{ccccc}
(x,y) & & \mathcal{S}_k(\Bbbk) & \xrightarrow{\psi_k} & \mathcal{S}_k(\Bbbk) \\
\downarrow & & \pi \downarrow & & \downarrow \pi \\
[x:1] & & \mathbb{P}^1(\Bbbk) & \xrightarrow{\phi_k} & \mathbb{P}^1(\Bbbk)
\end{array}$$

$$[\lambda : \mu] \longmapsto [k\mu^3 + \lambda^3 : -3\mu\lambda^2]$$

Some ingredients

$$\begin{aligned}
\mathcal{S}_k(\mathbb{k}) &= \{(x,y) \in E_k \mid x \in \mathbb{k}\} \cup \{\mathcal{O}\},\\
\mathbb{k}_3 &= \mathbb{k}(\sqrt[3]{x})_{x\in\mathbb{k}},\\
\mathcal{S}_k(\mathbb{k}_3) &= \{(x,y) \in E_k \mid x^3 \in \mathbb{k}\} \cup \{\mathcal{O}\}.
\end{aligned}$$

THEOREM (–, P., T.)

The following diagram is commutative.

$$\begin{array}{ccccc}
(x,y) & & \mathcal{S}_{108}(\mathbb{k}) & \xrightarrow{\psi_{108}} & \mathcal{S}_{108}(\mathbb{k}) \\
\big\downarrow & & \pi \big\downarrow & & \big\downarrow \pi \\
[x:1] & & \mathbb{P}^1(\mathbb{k}) & \xrightarrow{\Lambda \text{ (Hesse pencil)}} & \mathbb{P}^1(\mathbb{k})
\end{array}$$

$$[\lambda : \mu] \longmapsto [108\mu^3 + \lambda^3 : -3\mu\lambda^2]$$

Hessian graph on $\Bbbk$

Some ingredients

$$
\begin{aligned}
\mathcal{S}_k(\Bbbk) &= \{(x,y) \in E_k \mid x \in \Bbbk\} \cup \{\mathcal{O}\},\\
\Bbbk_3 &= \Bbbk(\sqrt[3]{x})_{x \in \Bbbk},\\
\mathcal{S}_k(\Bbbk_3) &= \{(x,y) \in E_k \mid x^3 \in \Bbbk\} \cup \{\mathcal{O}\}.
\end{aligned}
$$

Theorem (–, P., T.)

The following diagram is commutative too.

$$
\begin{array}{ccccc}
(x,y) & \mathcal{S}_k(\Bbbk_3) & \xrightarrow{\psi_k} & \mathcal{S}_k(\Bbbk_3) \\
\big\downarrow & \pi \big\downarrow & & \big\downarrow \pi \\
[x^3 : 1] & \mathbb{P}^1(\Bbbk) & \xrightarrow{\phi_k} & \mathbb{P}^1(\Bbbk)
\end{array}
$$

$$[j : w] \longmapsto [(j + kw)^3 : -27j^2w]$$

Some ingredients

$$\mathcal{S}_k(\Bbbk) = \{(x,y) \in E_k \mid x \in \Bbbk\} \cup \{\mathcal{O}\},$$
$$\Bbbk_3 = \Bbbk(\sqrt[3]{x})_{x \in \Bbbk},$$
$$\mathcal{S}_k(\Bbbk_3) = \{(x,y) \in E_k \mid x^3 \in \Bbbk\} \cup \{\mathcal{O}\}.$$

THEOREM (–, P., T.)

The following diagram is commutative too.

$$\begin{array}{ccccc}
(x,y) & \mathcal{S}_{-6912}(\Bbbk_3) & \xrightarrow{\psi_{-6912}} & \mathcal{S}_{-6912}(\Bbbk_3) \\
\big\downarrow & \pi \big\downarrow & & \big\downarrow \pi \\
[x^3 : 1] & \mathbb{P}^1(\Bbbk) & \xrightarrow{\text{H } (j\text{-invariants})} & \mathbb{P}^1(\Bbbk)
\end{array}$$

$$[j : w] \longmapsto [(j - 6912w)^3 : -27j^2w]$$

$\mathcal{S}_k(\mathbb{k})$ AND $\mathcal{S}_k(\mathbb{k}_3)$

For every $k, u \in \mathbb{k}^*$, consider the isomorphism

$$\phi_u : E_k \to E_{u^6 k}, \quad (x, y) \to (u^2 x, u^3 y),$$

whose inverse is $\phi_{u^{-1}}$.

$\mathcal{S}_k(\Bbbk)$ AND $\mathcal{S}_k(\Bbbk_3)$

For every $k, u \in \Bbbk^*$, consider the isomorphism

$$\phi_u : E_k \to E_{u^6 k}, \quad (x, y) \to (u^2 x, u^3 y),$$

whose inverse is $\phi_{u^{-1}}$.

PROPOSITION (–, P., T.)

preimages of the quadratic twists

$$\mathcal{S}_k(\Bbbk) = \bigcup_{u \in \Bbbk^*/(\Bbbk^*)^2} \phi_{u^{-\frac{1}{2}}}\left(E_{u^3 k}(\Bbbk)\right)$$

$\mathcal{S}_k(\mathbb{k})$ AND $\mathcal{S}_k(\mathbb{k}_3)$

For every $k, u \in \mathbb{k}^*$, consider the isomorphism

$$\phi_u : E_k \to E_{u^6 k}, \quad (x, y) \to (u^2 x, u^3 y),$$

whose inverse is $\phi_{u^{-1}}$.

PROPOSITION (–, P., T.)

preimages of the quadratic twists

$$\mathcal{S}_k(\mathbb{k}) = \bigcup_{u \in \mathbb{k}^*/(\mathbb{k}^*)^2} \phi_{u^{-\frac{1}{2}}}\left(E_{u^3 k}(\mathbb{k})\right)$$

and

$$\mathcal{S}_k(\mathbb{k}_3) = \bigcup_{u \in \mathbb{k}^*/(\mathbb{k}^*)^6} \phi_{u^{-\frac{1}{6}}}\left(E_{uk}(\mathbb{k})\right).$$

preimages of the sextic twists

Hessian graph over $\mathbb{F}_q$

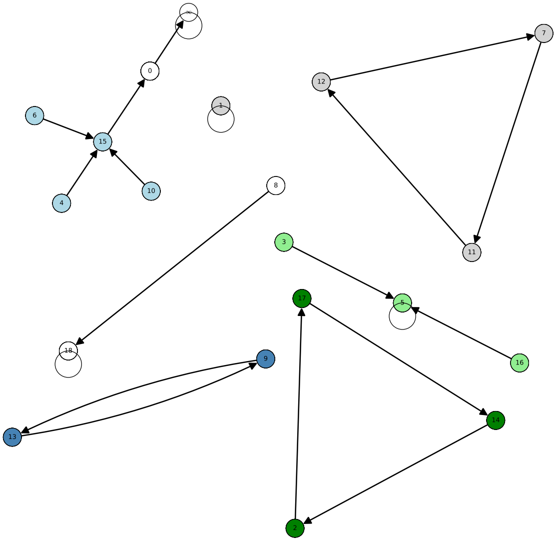
Benefits of finite fields

From now on we focus on H
(Hessian of j-invariants)

$$E: \quad y^2 = x^3 - 1728$$

$$\mathcal{S} = \mathcal{S}_k(\mathbb{k}_3)$$

Example: Hessian graph over $\mathbb{F}_{19}$



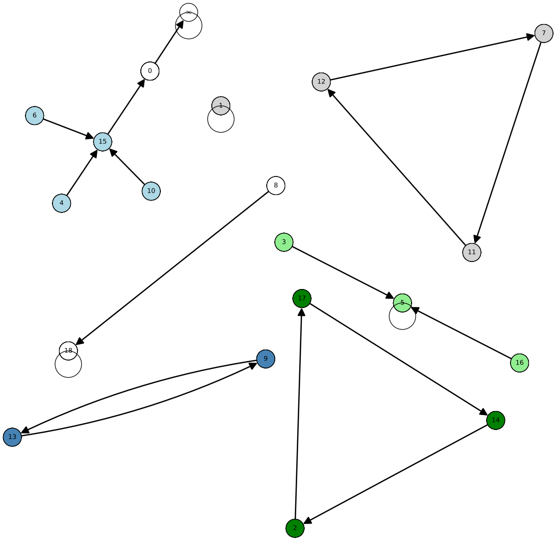
From now on we focus on H
(Hessian of j-invariants)

$$E: \quad y^2 = x^3 - 1728$$
$$\mathcal{S} = \mathcal{S}_k(\mathbb{k}_3)$$

- $\mathcal{S}$ is union of 2 or 6 subgroups.

Benefits of finite fields

Example: Hessian graph over $\mathbb{F}_{19}$

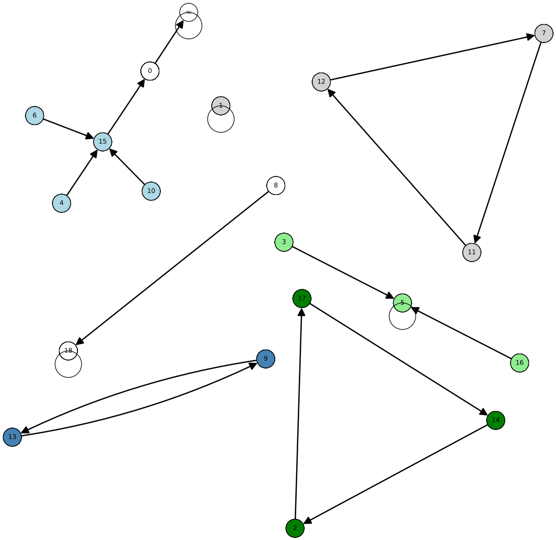


From now on we focus on H
(Hessian of j-invariants)

$$E: \quad y^2 = x^3 - 1728$$
$$\mathcal{S} = \mathcal{S}_k(\Bbbk_3)$$

- $\mathcal{S}$ is union of 2 or 6 subgroups.
- The structure of $E(\mathbb{F}_q)$ and its twists can be explicitly computed.

Example: Hessian graph over $\mathbb{F}_{19}$



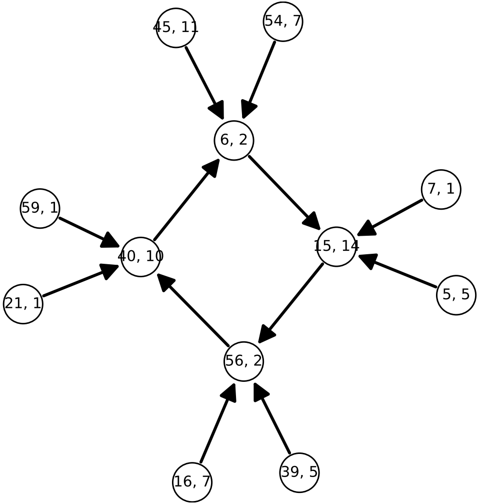
From now on we focus on H
(Hessian of j-invariants)

$$E: \quad y^2 = x^3 - 1728$$
$$\mathcal{S} = \mathcal{S}_k(\mathbb{k}_3)$$

- $\mathcal{S}$ is union of 2 or 6 subgroups.
- The structure of $E(\mathbb{F}_q)$ and its twists can be explicitly computed.
- Even more information when E is supersingular ($\mathrm{char}(\mathbb{F}_q) \equiv 2 \mod 3$).

Leaves and traces

Example: Connected component of Hessian graph over $\mathbb{F}_{61}$, vertices labelled as $(j, |\mathrm{tr}(E(j))|)$.



Proposition (–, P., T.)

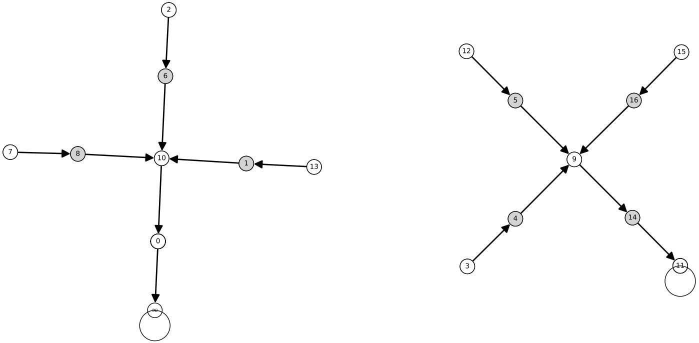
The leaves of the Hessian graph are exactly those corresponding to curves with odd trace.

$q \equiv 2 \mod 3$

Theorem (–, P., T.)

Let $q + 1 = 3^d N$, with $\gcd(3, N) = 1$. In the Hessian graph over $\mathbb{F}_q$:

1. *There are N periodic elements: $j = 1728, \infty$ are self-loops with indegree 2, while the others alternate between indegree 1 and 3.*



Example: Hessian graph over $\mathbb{F}_{17}$.
White vertices are those in $\pi(E(\mathbb{F}_{17}))$.

$q \equiv 2 \mod 3$

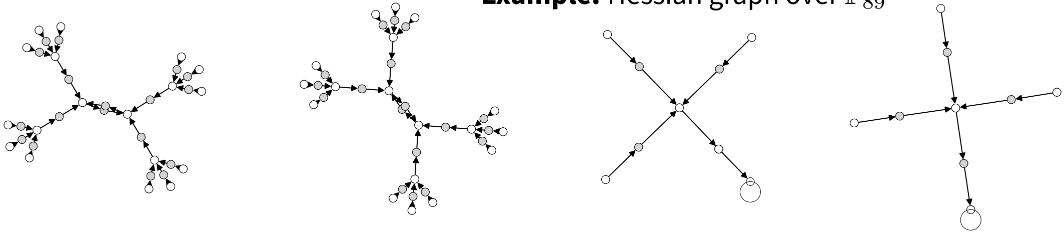
Theorem (–, P., T.)

Let $q+1 = 3^d N$, with $\gcd(3, N) = 1$. In the Hessian graph over $\mathbb{F}_q$:

2. *Every periodic element is the root of [indegree -1] isomorphic arborescences. The leaves have all depth $2d$, and the indegree of non-periodic elements is*

$$\begin{cases} 1 & \text{if odd depth,} \\ 3\ (\text{resp. } 0) & \text{if even depth and are not (resp. are) leaves.} \end{cases}$$

Example: Hessian graph over $\mathbb{F}_{89}$



$q \equiv 2 \mod 3$

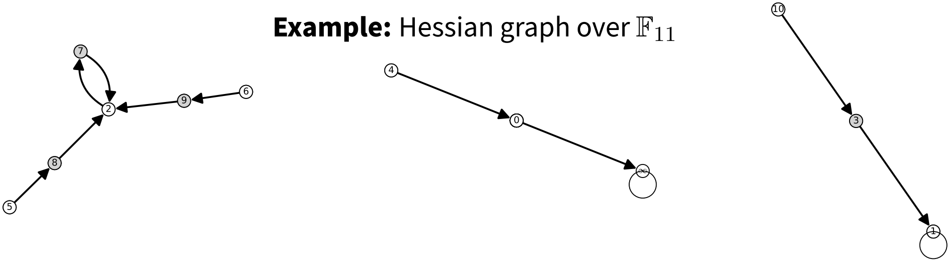
Theorem (–, P., T.)

Let $q + 1 = 3^d N$, *with* $\gcd(3, N) = 1$. *In the Hessian graph over* $\mathbb{F}_q$*:*

3. *The length of every cycle divides the length of a maximal cycle, which is*

$$\begin{cases} \mathrm{ord}_N(-3) & \text{if } \exists\, n \in \mathbb{N} \text{ s.t. } (-3)^n \equiv -1 \bmod N, \\ 2\,\mathrm{ord}_N(-3) & \text{otherwise.} \end{cases}$$

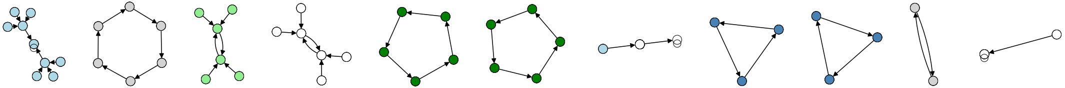
Example: Hessian graph over $\mathbb{F}_{11}$



$q \equiv 1 \mod 3$

Theorem (–, P., T.)

Let $q \equiv 1 \mod 3$. The Hessian graph over $\mathbb{F}_q$ is the union of six subgraphs, which can intersect only in $0, 1728, \infty \in \mathbb{P}^1(\mathbb{F}_q)$.

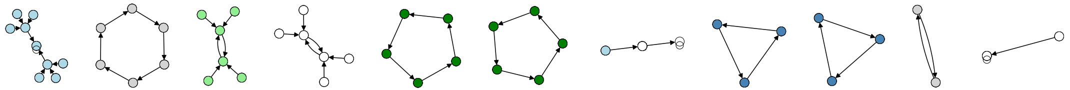


Example: Hessian graph over $\mathbb{F}_{7^2}$

$q \equiv 1 \mod 3$

Theorem (–, P., T.)

Let $q \equiv 1 \mod 3$. The Hessian graph over $\mathbb{F}_q$ is the union of six subgraphs, which can intersect only in $0, 1728, \infty \in \mathbb{P}^1(\mathbb{F}_q)$.
For each such subgraph, there is $m \in \mathbb{N}$ such that its connected components consist of cycles, whose vertices are the roots of arborescences T_3^m,



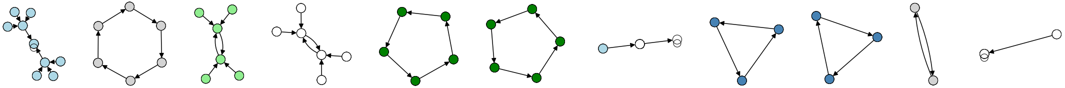
Example: Hessian graph over $\mathbb{F}_{7^2}$

$q \equiv 1 \mod 3$

THEOREM (–, P., T.)

Let $q \equiv 1 \mod 3$. The Hessian graph over $\mathbb{F}_q$ is the union of six subgraphs, which can intersect only in $0, 1728, \infty \in \mathbb{P}^1(\mathbb{F}_q)$.
For each such subgraph, there is $m \in \mathbb{N}$ such that its connected components consist of cycles, whose vertices are the roots of arborescences T_3^m, with the following modifications:

- *The arborescences rooted in ∞ are pruned of one node at depth 1 if $m \geq 1$, and of two additional nodes at depth 2 if $m \geq 2$.*
- *If the arborescences are rooted in 1728, then they are pruned of one node at depth 1 if $m \geq 1$.*



Example: Hessian graph over $\mathbb{F}_{7^2}$

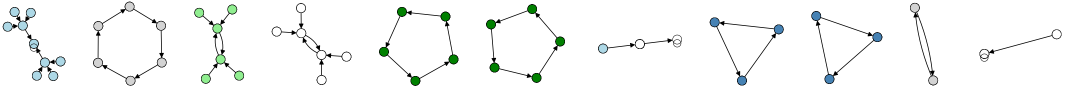
$q \equiv 1 \mod 3$

THEOREM (–, P., T.)

Let $q \equiv 1 \bmod 3$. The Hessian graph over $\mathbb{F}_q$ is the union of six subgraphs, which can intersect only in $0, 1728, \infty \in \mathbb{P}^1(\mathbb{F}_q)$.
For each such subgraph, there is $m \in \mathbb{N}$ such that its connected components consist of cycles, whose vertices are the roots of arborescences T_3^m, with the following modifications:

- *The arborescences rooted in ∞ are pruned of one node at depth 1 if $m \geq 1$, and of two additional nodes at depth 2 if $m \geq 2$.*
- *If the arborescences are rooted in 1728, then they are pruned of one node at depth 1 if $m \geq 1$.*

Moreover, three of such subgraphs have $m = 0$, two of them have $m = 1$, and the last one has $m > 1$.



Example: Hessian graph over $\mathbb{F}_{7^2}$

Wishful thinking on supersingular ECs

SECUERS: AN OPEN PROBLEM

Some cryptosystems require Supersingular Elliptic Curves of Unknown Endomorphism Ring (SECUERS).

Problem: The only known way to get a SECUER is by means of a trusted setup.

SECUERS: AN OPEN PROBLEM

Some cryptosystems require Supersingular Elliptic Curves of Unknown Endomorphism Ring (SECUERS).
Problem: The only known way to get a SECUER is by means of a trusted setup.

Dream: exploiting Hessian graphs by...

- ...finding which connected components contain supersingular elliptic curves,

SECUERS: AN OPEN PROBLEM

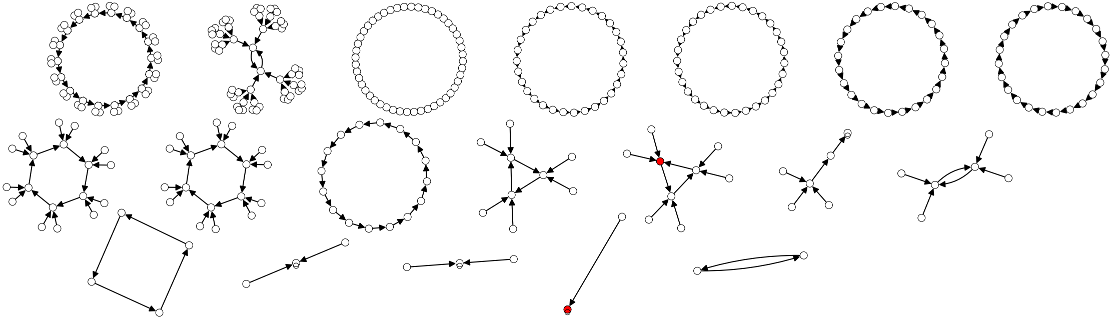
Some cryptosystems require Supersingular Elliptic Curves of Unknown Endomorphism Ring (SECUERS).
Problem: The only known way to get a SECUER is by means of a trusted setup.

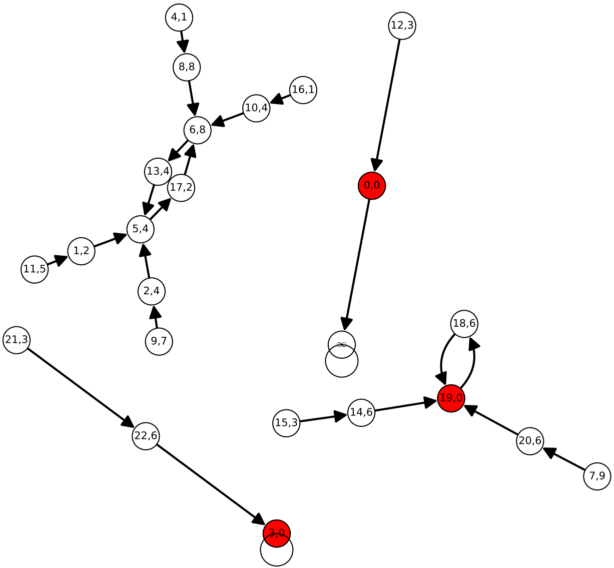
Dream: exploiting Hessian graphs by...

- ...finding which connected components contain supersingular elliptic curves,
- ...finding sufficient conditions on a (possibly ordinary) elliptic curve E to enforce that $\mathrm{Hess}^n(E)$ is supersingular for some $n \geq 1$.

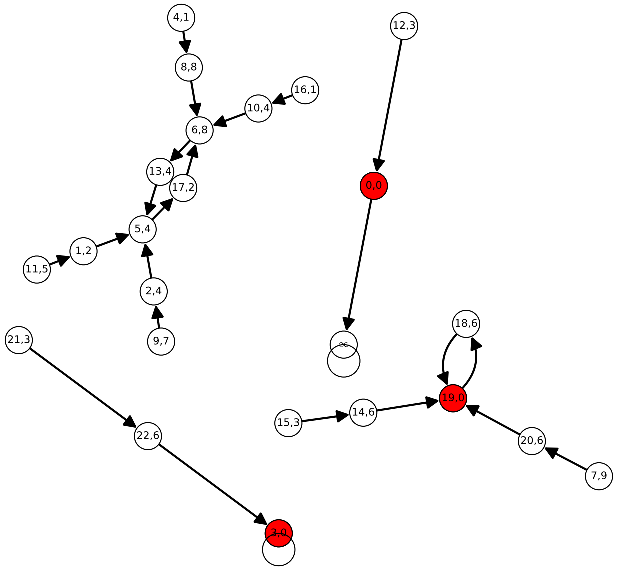
We say that a component of the Hessian graph is *supersingular* if it contains at least one supersingular vertex.

Example: Supersingular vertices on Hessian graph over $\mathbb{F}_{19^2}$.





Example: Hessian graph over $\mathbb{F}_{29}$, vertices labelled as $(j, |\mathrm{tr}(E(j))|)$.



Example: Hessian graph over $\mathbb{F}_{29}$, vertices labelled as $(j, |\mathrm{tr}(E(j))|)$.

PROPOSITION (–, P., T.)

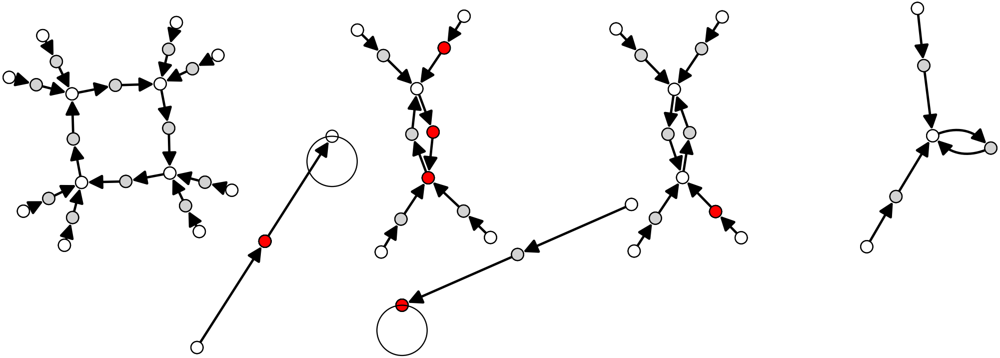
In the Hessian graph over $\mathbb{F}_p$, the trace of each elliptic curve (defined over $\mathbb{F}_p$) in a supersingular component is a multiple of 3.

Necessary conditions for supersingular components II

Proposition (–, P., T.)

In the Hessian graph over $\mathbb{F}_{p^2}$, each supersingular j-invariants lies in $\pi(E(\mathbb{F}_{p^2}))$.

Non-example: Hessian graph over $\mathbb{F}_{59}$.

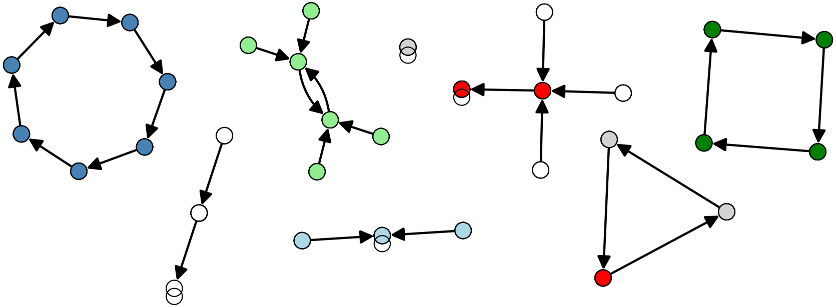


NECESSARY CONDITIONS FOR SUPERSINGULAR COMPONENTS II

PROPOSITION (–, P., T.)

In the Hessian graph over $\mathbb{F}_{p^2}$, each supersingular j-invariants lies in $\pi(E(\mathbb{F}_{p^2}))$.

Non-example: Hessian graph over $\mathbb{F}_{31}$.

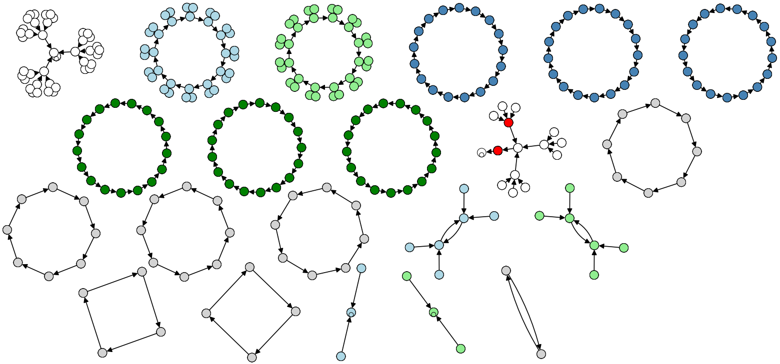


Necessary conditions for supersingular components II

Proposition (–, P., T.)

In the Hessian graph over $\mathbb{F}_{p^2}$, each supersingular j-invariants lies in $\pi(E(\mathbb{F}_{p^2}))$.

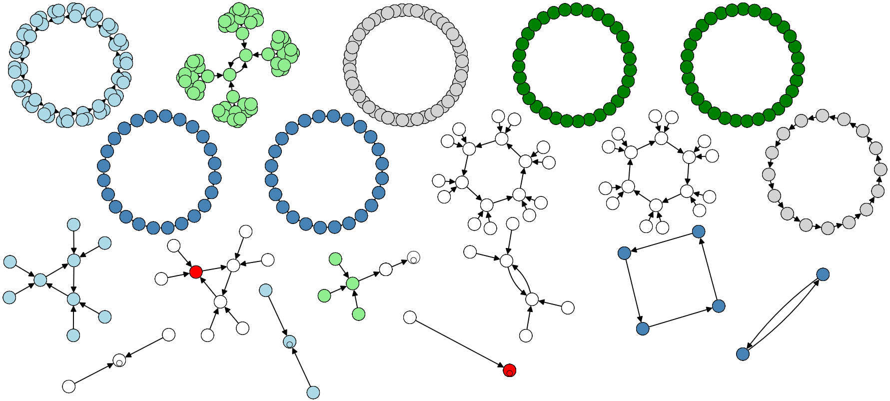
Example: Hessian graph over $\mathbb{F}_{17^2}$.



Proposition (–, P., T.)

In the Hessian graph over $\mathbb{F}_{p^2}$, each supersingular j-invariants lies in $\pi(E(\mathbb{F}_{p^2}))$.

Example: Hessian graph over $\mathbb{F}_{19^2}$.



Thank you for your attention!

M. Mula, F. Pintore, D. Taufer,
The Hessian of elliptic curves,
ArXiv: 2407.17042, 2024.

[AD09] M. Artebani and I. V. Dolgachev. "The Hesse pencil of plane cubic curves". In: *L'Enseignement Mathématique* 55.3 (2009), pp. 235–273.

[Mil06] J. W. Milnor. "On Lattès maps". In: *Dynamics on the Riemann sphere*. Eur. Math. Soc., 2006, pp. 9–43.

[PP08] P. Popescu-Pampu. "Iterating the hessian: a dynamical system on the moduli space of elliptic curves and dessins d'enfants". In: *Noncommutativity and Singularities, Adv. Stud. Pure Math* 55 (2008), pp. 83–98.

Hessian graphs (and their twins)

We call the *Hessian graph* the functional graph of the map

$$\mathrm{Hess}(j) = \frac{(6912 - j)^3}{27(j)^2}.$$

Hessian graphs (and their twins)

We call the *Hessian graph* the functional graph of the map

$$\mathrm{Hess}(j) = \frac{(6912 - j)^3}{27(j)^2}.$$

More generally, we can consider, for each $k, \ell \in \mathbb{F}_q^*$, the functional graphs of

$$g_{k,\ell}(x) = \frac{(x + k)^3}{\ell \cdot x^2},$$

so that $\mathrm{Hess} = g_{-4\cdot 1728, -27}$.

Proposition

The functional graphs corresponding to $g_{1,\ell}, g_{2,\ell}, \ldots$ are isomorphic.