Problems related to the computation of the endomorphism ring for principally polarised superspecial abelian surfaces

Mickaël Montessinos

Eötvös Loránd University

Okinawa Institute of Science and Technology,
Wednesday 21st January, 2026

Elevator pitch

In dimension 1, we have one problem to rule them all: computing the endomorphism ring.

Elevator pitch

In dimension 1, we have one problem to rule them all: computing the endomorphism ring.
Even if we come up with a different way to state the problem, it remains computationally equivalent.

Elevator pitch

In dimension 1, we have one problem to rule them all: computing the endomorphism ring.
Even if we come up with a different way to state the problem, it remains computationally equivalent.

Wish

Wouldn't it be nice if we had the same thing for principally polarised superspecial abelian surfaces?

For supersingular elliptic curves

"Compute the endomorphism rings of a supersingular variety" can have two meanings:

For supersingular elliptic curves

"Compute the endomorphism rings of a supersingular variety" can have two meanings:
The one for computing endomorphisms:

Problem: Endomorphism ring

Given a supersingular elliptic curve over $\mathbb{F}_{p^2}$, comute effective representations of endomorphisms of E that form a $\mathbb{Z}$-basis of $\mathrm{End}(E)$.

For supersingular elliptic curves

"Compute the endomorphism rings of a supersingular variety" can have two meanings:
The one for computing endomorphisms:

Problem: Endomorphism ring

Given a supersingular elliptic curve over $\mathbb{F}_{p^2}$, comute effective representations of endomorphisms of E that form a $\mathbb{Z}$-basis of $\mathrm{End}(E)$.

The one for computing isogenies:

Problem: Maximal order

Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, compute the basis of a maximal order $\mathcal{O}_E$ of $B_{p,\infty}$ that is isomorphic to $\mathrm{End}(E)$.

For supersingular elliptic curves

"Compute the endomorphism rings of a supersingular variety" can have two meanings:
The one for computing endomorphisms:

Problem: Endomorphism ring

Given a supersingular elliptic curve over $\mathbb{F}_{p^2}$, comute effective representations of endomorphisms of E that form a $\mathbb{Z}$-basis of $\mathrm{End}(E)$.

The one for computing isogenies:

Problem: Maximal order

Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, compute the basis of a maximal order $\mathcal{O}_E$ of $B_{p,\infty}$ that is isomorphic to $\mathrm{End}(E)$.

Theorem (Eisenträger, Hallgreen, Lauter, Morrison, Petit 2018, Wesolowski 2021)

Under GRH, these problems are equivalent.

Brief description of the reductions

Reduction of Maximal Order to Endomorphism Ring

1. Recover the symmetric bilinear form $(a, b) \mapsto \mathrm{Tr}(a\widehat{b})$.
2. Get an isomorphism to a quaternion order.

Brief description of the reductions

Reduction of Maximal Order to Endomorphism Ring

1. Recover the symmetric bilinear form $(a, b) \mapsto \mathrm{Tr}(a\widehat{b})$.
2. Get an isomorphism to a quaternion order.

Reduction of Endomorphism Ring to Maximal Order

1. Use KLPT to recover an isogeny from E_0 to E.
2. Transfer the endomorphism ring of E_0 to E.

Superspecial abelian surfaces

Definition (Superspecial abelian surface)

- An abelian surface is *superspecial* if it is isomorphic over $\overline{\mathbb{F}_p}$ to a product of supersingular elliptic curves.
- An abelian surface over $\mathbb{F}_{p^2}$ is *maximal* (resp. *minimal*) is it has $(p+1)^4$ (resp. $(p-1)^4$)) rational points.

Superspecial abelian surfaces

Definition (Superspecial abelian surface)

- An abelian surface is *superspecial* if it is isomorphic over $\overline{\mathbb{F}_p}$ to a product of supersingular elliptic curves.
- An abelian surface over $\mathbb{F}_{p^2}$ is *maximal* (resp. *minimal*) is it has $(p+1)^4$ (resp. $(p-1)^4$)) rational points.

Theorem

1. *An $\overline{\mathbb{F}_{p^2}}$-isogeny between maximal or minimal abelian variety is defined over $\mathbb{F}_{p^2}$.*
2. *A maximal abelian surface is superspecial, a superspecial abelian surface has a maximal and a minimal model.*
3. *All maximal (resp. minimal) abelian surfaces are isomorphic.*

Principally polarised abelian varieties

Definition (Dual abelian variety)

Let A be an abelian variety. The *dual variety* of A is the variety $\widehat{A}$ such that $\widehat{A}(k) = \mathrm{Pic}^0(A_k)$. If $\varphi\colon A \to B$ is a homomorphism, there is a dual homomorphism $\widehat{\varphi}\colon \widehat{B} \to \widehat{A}$.

Principally polarised abelian varieties

Definition (Dual abelian variety)

Let A be an abelian variety. The *dual variety* of A is the variety $\widehat{A}$ such that $\widehat{A}(k) = \mathrm{Pic}^0(A_k)$. If $\varphi\colon A \to B$ is a homomorphism, there is a dual homomorphism $\widehat{\varphi}\colon \widehat{B} \to \widehat{A}$.

Definition (Polarisation)

A *polarisation* is a self-dual isogeny $\lambda\colon A \to \widehat{A}$ such that the symmetric bilinear map $\mathrm{End}(A) \ni (f, g) \mapsto \mathrm{Tr}(f \circ \lambda^{-1} \circ \widehat{g} \circ \lambda)$ is definite positive. A polarisation is *principal* if it is an isomorphism. A homomorphism $f : (A, \lambda_A) \to (B, \lambda_B)$ is *polarised* if $f \circ \lambda_B \circ \widehat{f} = [N]\lambda_A$.

Principally polarised abelian varieties

Definition (Dual abelian variety)

Let A be an abelian variety. The *dual variety* of A is the variety $\widehat{A}$ such that $\widehat{A}(k) = \mathrm{Pic}^0(A_k)$. If $\varphi\colon A \to B$ is a homomorphism, there is a dual homomorphism $\widehat{\varphi}\colon \widehat{B} \to \widehat{A}$.

Definition (Polarisation)

A *polarisation* is a self-dual isogeny $\lambda\colon A \to \widehat{A}$ such that the symmetric bilinear map $\mathrm{End}(A) \ni (f, g) \mapsto \mathrm{Tr}(f \circ \lambda^{-1} \circ \widehat{g} \circ \lambda)$ is definite positive. A polarisation is *principal* if it is an isomorphism. A homomorphism $f : (A, \lambda_A) \to (B, \lambda_B)$ is *polarised* if $f \circ \lambda_B \circ \widehat{f} = [N]\lambda_A$.

- A product of elliptic curve is principally polarised by the *product* of the polarisations of its factors.
- A Jacobian $J(C)$ of a hyperelliptic curve of genus 2 admits a canonical principal polarisation.

Computational representation of a PPSAS

Theorem (Classification of PPAS)

A principally polarised abelian surface over $\overline{\mathbb{F}_p}$ is isomorphic to either a product of elliptic curves of a Jacobian. Two product of elliptic curves are isomorphic (as polarised abelian varieties) if their factors are isomorphic. Two jacobians $J(C)$ and $J(C')$ are isomorphic if C and C' are as well.

Computational representation of a PPSAS

Theorem (Classification of PPAS)

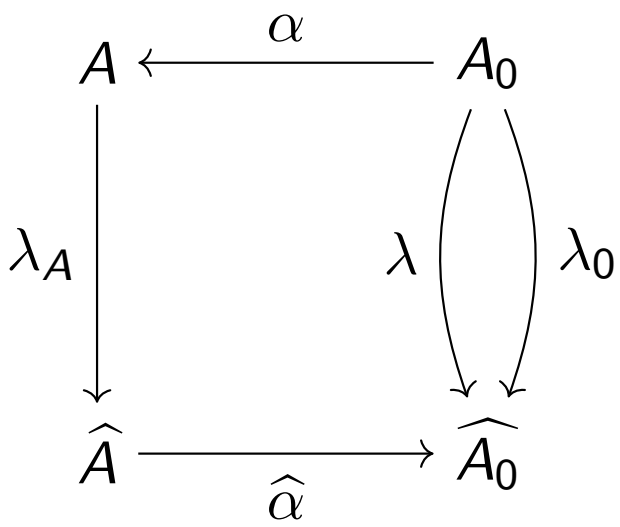
A principally polarised abelian surface over $\overline{\mathbb{F}_p}$ is isomorphic to either a product of elliptic curves of a Jacobian. Two product of elliptic curves are isomorphic (as polarised abelian varieties) if their factors are isomorphic. Two jacobians $J(C)$ and $J(C')$ are isomorphic if C and C' are as well.

A PPSAS is represented either as a product of supersingular elliptic curves by the data of a pair of j-invariants, or as the jacobian of a genus 2 hyperelliptic curve C by the data of the Igusa invariants of C.

This representation carries the information of the polarisation. So, any computation on such a surface may contain information about its relation to the polarisation.

The Ibukiyama-Katsura-Oort correspondence

Fix a supersingular elliptic curve E_0 with known endomorphism ring. Set $A_0 = E_0 \times E_0$.



$\lambda = \widehat{\alpha} \circ \lambda_A \circ \alpha$.
We set $\mu(A) = \mu(\lambda) = \lambda_0^{-1} \circ \lambda$.
$\mu(A)$ is well defined up to equivalence.
We call $\mu(A)$ the *Ibukiyama-Katsura-Oort matrix of A*.

Problem: Ibukiyama-Katsura-Oort matrix computation

Given a PPSAS A, compute $\mu(A)$.

The endomorphism ring and the Rosati involution

Problem : Effective endomorphism ring computation

Given a PPSAS A, compute effective representations of endomorphisms of A that form a $\mathbb{Z}$-basis of $\mathrm{End}(A)$.

The endomorphism ring and the Rosati involution

Problem : Effective endomorphism ring computation

Given a PPSAS A, compute effective representations of endomorphisms of A that form a $\mathbb{Z}$-basis of $\mathrm{End}(A)$.

Definition

Let (A, λ) be a principally polarised abelian variety. The *Rosati involution* of A with respect to λ is the map

$$\begin{array}{rccc} R_\lambda : & \mathrm{End}(A) & \to & \mathrm{End}(A) \\ & f & \mapsto & \lambda^{-1} \circ \widehat{f} \circ \lambda \end{array}$$

The endomorphism ring and the Rosati involution

Problem : Effective endomorphism ring computation

Given a PPSAS A, compute effective representations of endomorphisms of A that form a $\mathbb{Z}$-basis of $\mathrm{End}(A)$.

Definition

Let (A, λ) be a principally polarised abelian variety. The *Rosati involution* of A with respect to λ is the map

$$\begin{array}{rccc} R_\lambda : & \mathrm{End}(A) & \to & \mathrm{End}(A) \\ & f & \mapsto & \lambda^{-1} \circ \widehat{f} \circ \lambda \end{array}$$

Problem: Good endomorphism ring computation

Given a PPSAS A, solve the effective endomorphism ring problem, compute the matrix of the Rosati involution and the action of each endomorphism on the space $H^0(A, \Omega_0)$ of global differentials.

Wait, they are all isomorphic?

Theorem

Let A, B be maximal (resp. minimal) abelian surfaces over $\mathbb{F}_{p^2}$. Then there exists an $\mathbb{F}_{p^2}$-rational isomorphism from A to B.

Wait, they are all isomorphic?

Theorem

Let A, B be maximal (resp. minimal) abelian surfaces over $\mathbb{F}_{p^2}$. Then there exists an $\mathbb{F}_{p^2}$-rational isomorphism from A to B.

Theorem (Gaudry, Soumier, Spaenlehauer)

Let E_1, E_2, E_3, E_4 be maximal (resp. minimal) elliptic curves. We may compute an isomoprhism from $E_1 \times E_2$ to $E_3 \times E_4$ in polynomial time.

Wait, they are all isomorphic?

Theorem

Let A, B be maximal (resp. minimal) abelian surfaces over $\mathbb{F}_{p^2}$. Then there exists an $\mathbb{F}_{p^2}$-rational isomorphism from A to B.

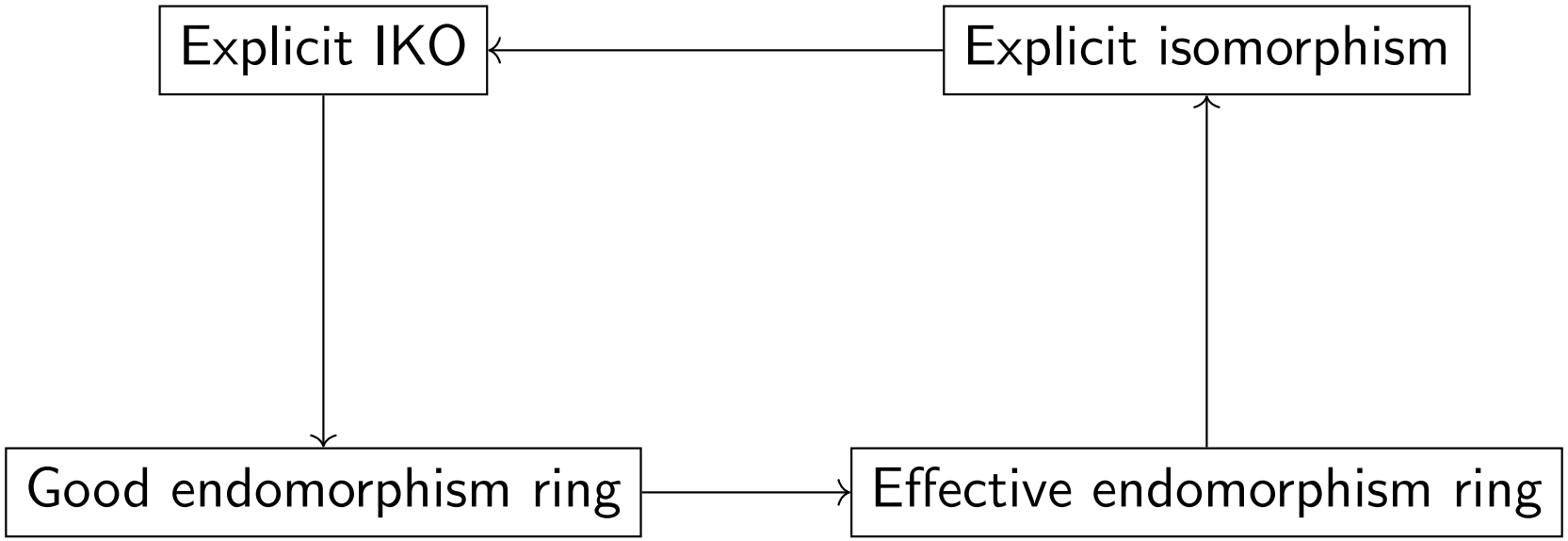
Theorem (Gaudry, Soumier, Spaenlehauer)

Let E_1, E_2, E_3, E_4 be maximal (resp. minimal) elliptic curves. We may compute an isomoprhism from $E_1 \times E_2$ to $E_3 \times E_4$ in polynomial time.

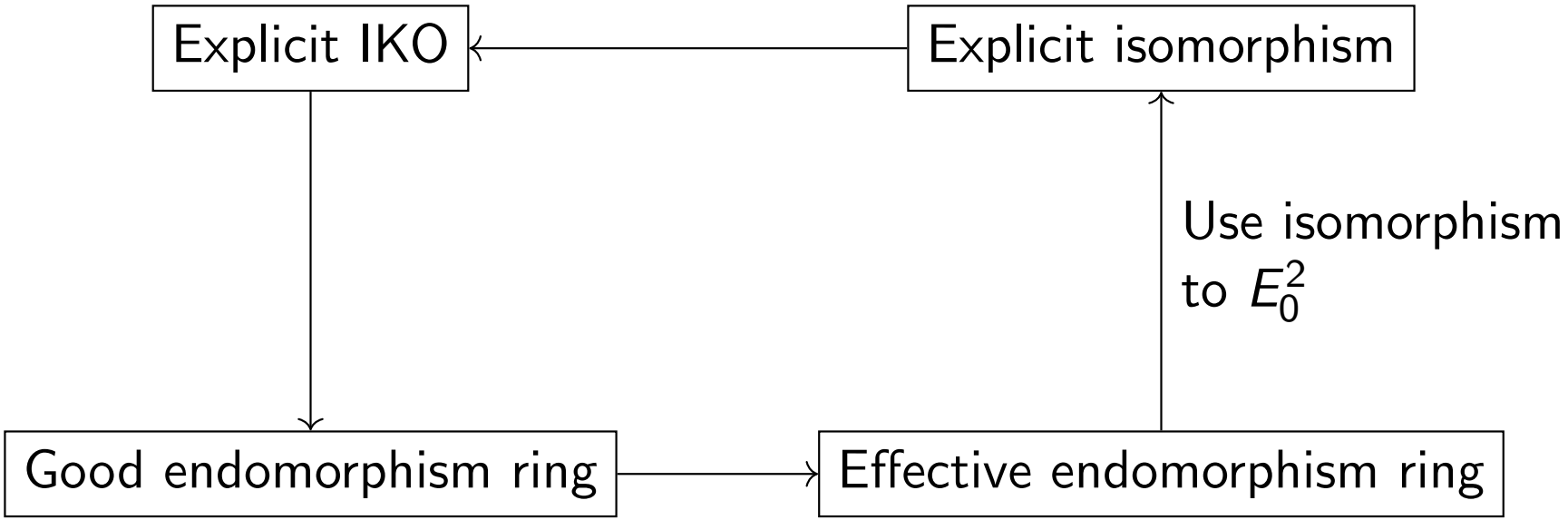
Intuition

The problem of computing isomorphisms between superspecial abelian surfaces should be equivalent to endomorphism ring computation, because an isomorphism $A \simeq E_0 \times E_0$ recovers the endomorphism ring of A.

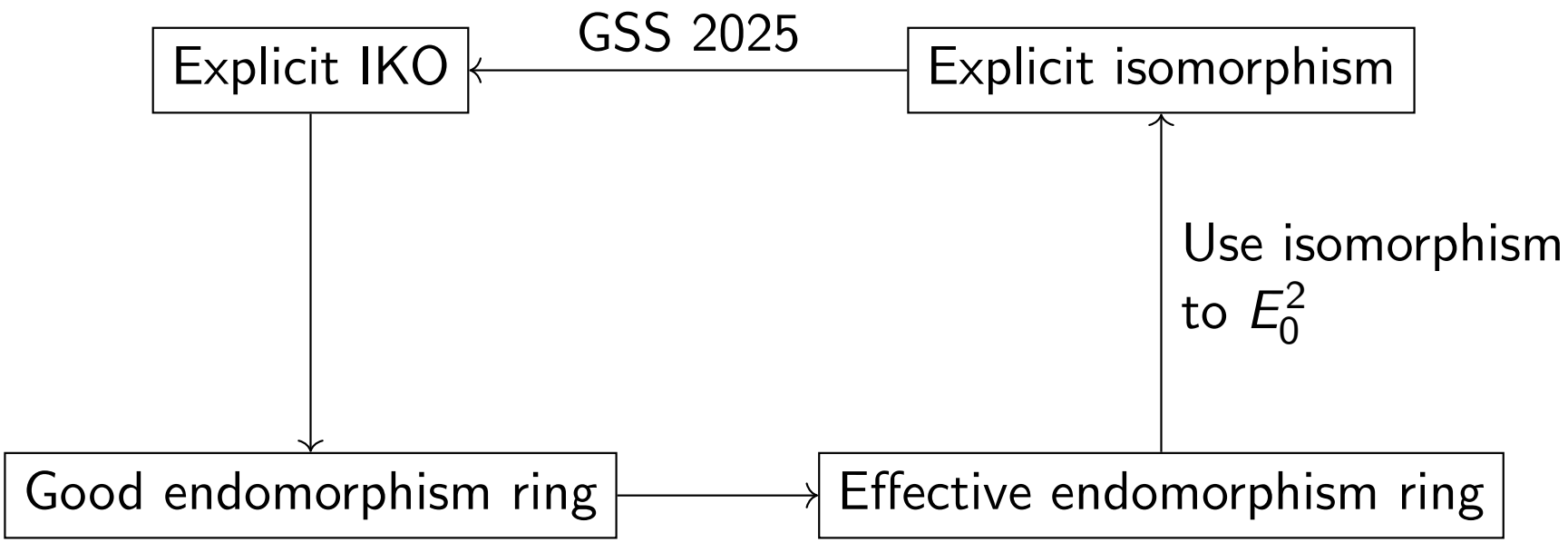
The reductions for products of superingular elliptic curves



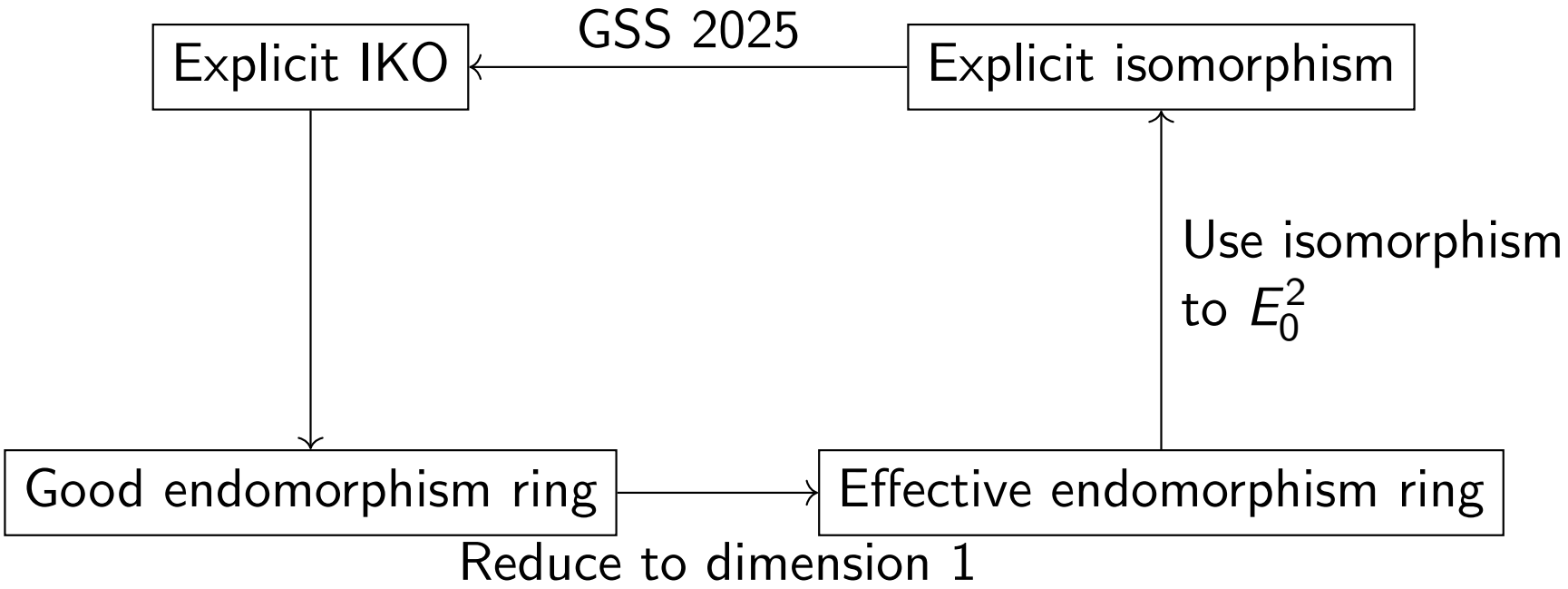
The reductions for products of superingular elliptic curves



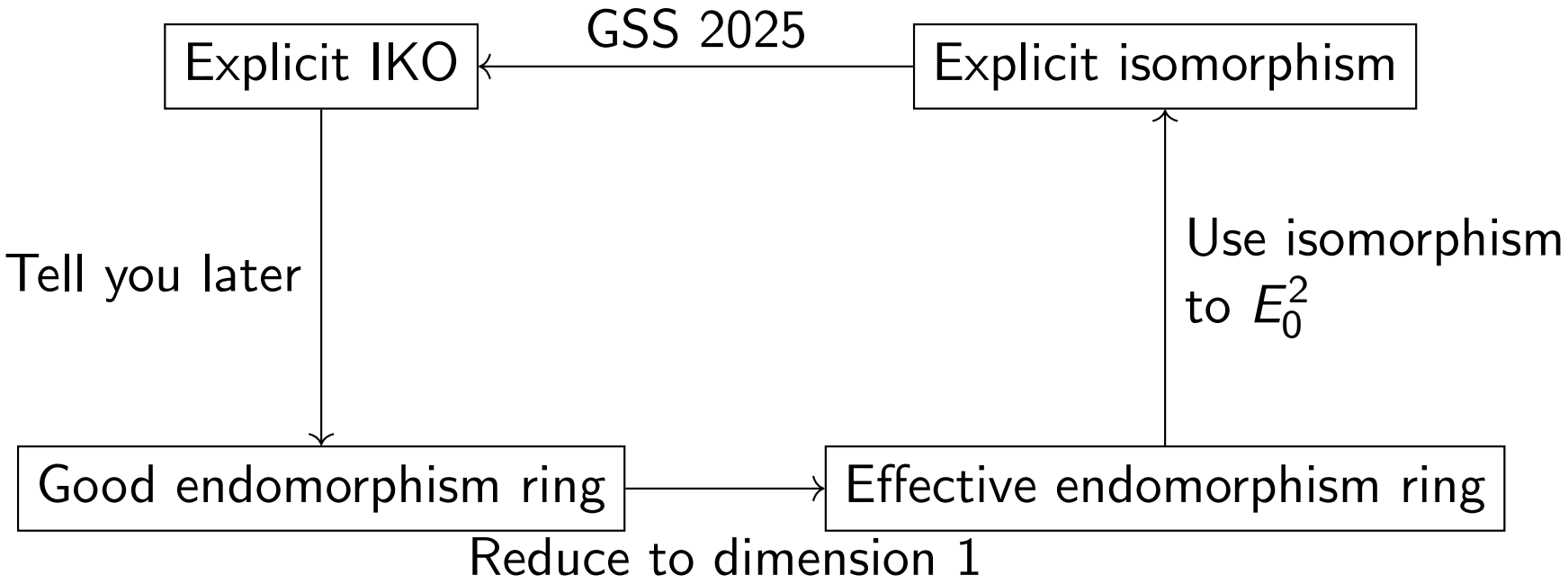
The reductions for products of superingular elliptic curves



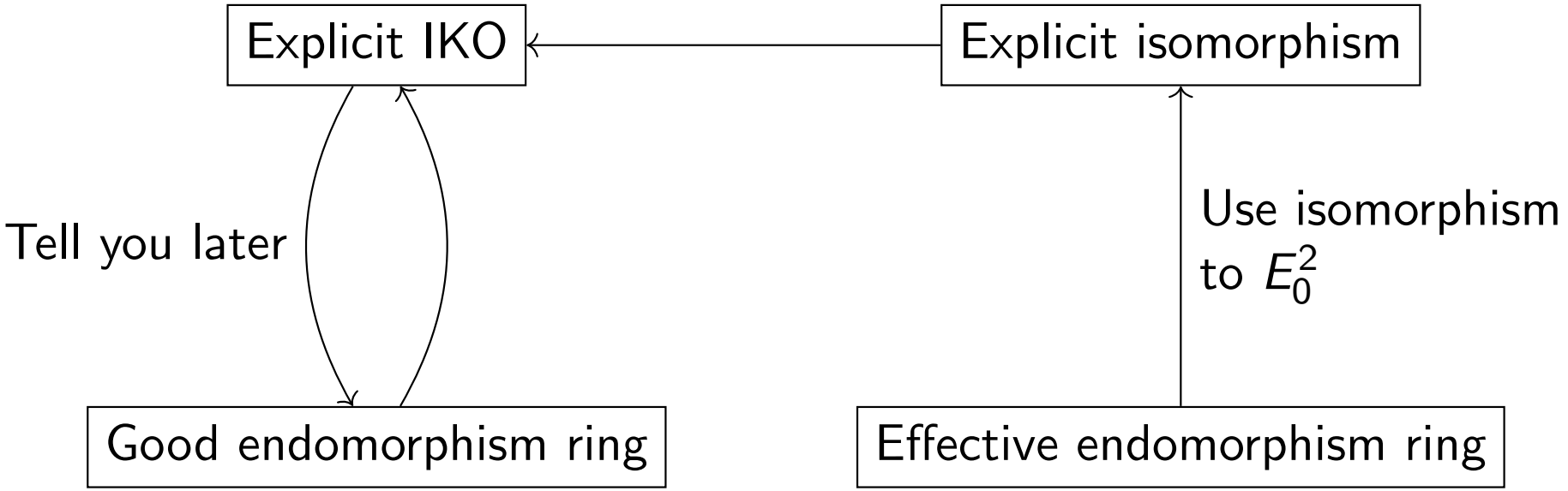
The reductions for products of superingular elliptic curves



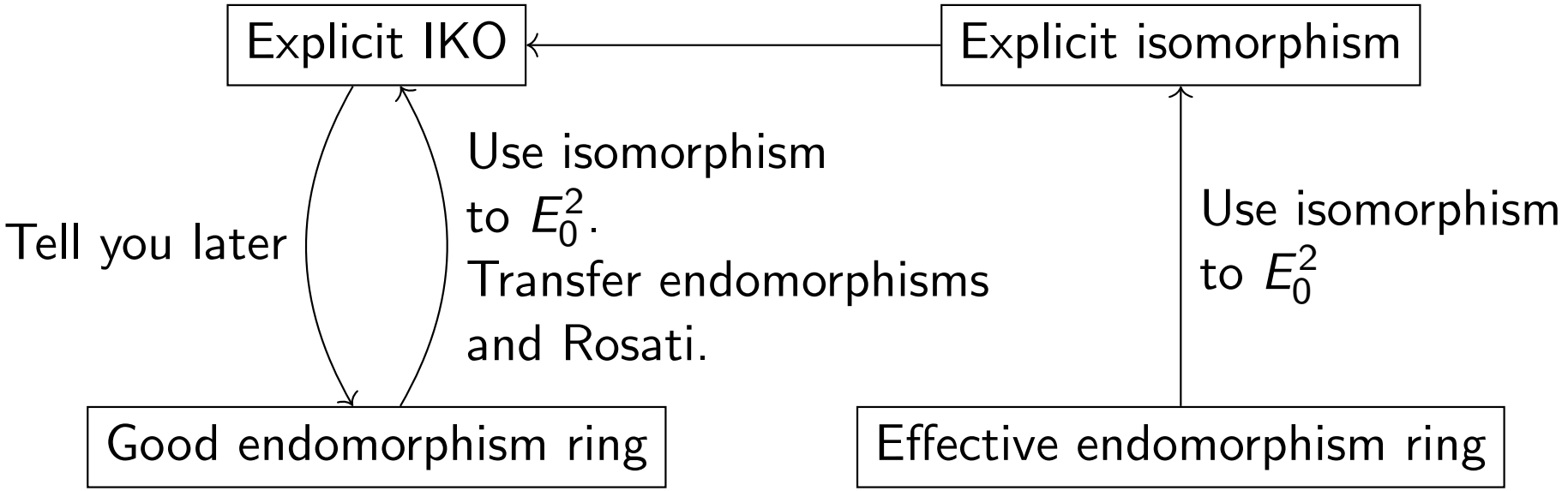
The reductions for products of superingular elliptic curves



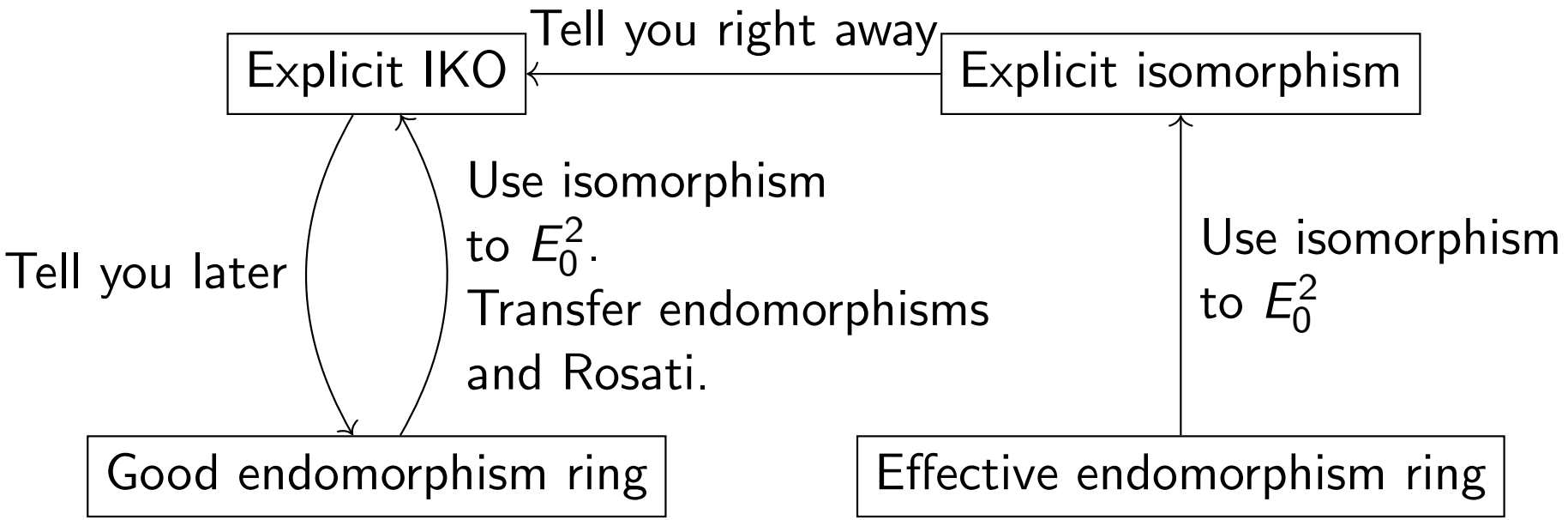
The general case



The general case



The general case



Computing an unpolarised isomorphism: the setting

Remark

We already know how to compute isomorphisms between products of elliptic curves, if we know their endomorphism rings.
It is enough to find an isomorphism from any product of elliptic curves to a given jacobian $J(C)$.

Computing an unpolarised isomorphism: the setting

Remark

We already know how to compute isomorphisms between products of elliptic curves, if we know their endomorphism rings.
It is enough to find an isomorphism from any product of elliptic curves to a given jacobian $J(C)$.

KLPT^2 and knowledge of $\mu(J(C))$ give us the following:

$$E_0 \times E_0 \xrightarrow{(2,2)} J(C_1) \xrightarrow{(2,2)} \dots \xrightarrow{(2,2)} J(C)$$

Computing an unpolarised isomorphism: the setting

Remark

We already know how to compute isomorphisms between products of elliptic curves, if we know their endomorphism rings.
It is enough to find an isomorphism from any product of elliptic curves to a given jacobian $J(C)$.

KLPT^2 and knowledge of $\mu(J(C))$ give us the following:

$$E_0 \times E_0 \xrightarrow{(2,2)} J(C_1) \xrightarrow{(2,2)} \dots \xrightarrow{(2,2)} J(C)$$

We want:

$$E_1 \times E_2 \xrightarrow{\sim} J(C)$$

with knowledge of $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$.

Computing an unpolarised isomorphism: the induction

We have

$$E_0 \times E_0 \xrightarrow{(2,2)} J(C_1) \xrightarrow{(2,2)} \dots \xrightarrow{(2,2)} J(C)$$

We do

$$\begin{array}{ccccccc} E_0 \times E_0 & \xrightarrow{\varphi} & J(C_1) & \xrightarrow{(2,2)} & \dots & \xrightarrow{(2,2)} & J(C) \\ \downarrow \theta & & \sim \uparrow & & & & \\ E_0 \times E_0 & \xrightarrow{(2,2)} & E_1 \times E_2 & & & & \end{array}$$

Where $\mathrm{Ker}(\varphi) = \langle (P_1, P_2), (Q_1, Q_2) \rangle$ and $\theta \in \mathrm{Aut}(E_0 \times E_0)$ satisfies

$$\theta((P_1, P_2)) = (P_1, 0)$$
$$\theta((Q_1, Q_2)) = (0, P_2)$$

Recovering the Ibukiyama-Katsura-Oort matrix

Input

A PPSAS A, with known endomorphism ring, over which we may compute the Rosati involution and the action on differentials

Recovering the Ibukiyama-Katsura-Oort matrix

Input

A PPSAS A, with known endomorphism ring, over which we may compute the Rosati involution and the action on differentials

Naive strategy

1. Recover the multiplication table of $\mathrm{End}(A)$.
2. Compute an isomorphism $\tau\colon \mathrm{End}(A) \otimes \mathbb{Q} \to M_2(B_{p,\infty})$.
3. Compute $\gamma \in \mathrm{GL}_n(B_{p,\infty})$ such that $\gamma^{-1}\tau(\mathrm{End}(A))\gamma = M_2(O_0)$.
4. Recover the following involution of $M_2(O_0)$:

$$\sigma\colon \alpha \mapsto \gamma^{-1}(\tau \circ r_A \circ \tau^{-1})(\gamma\alpha\gamma^{-1})\gamma$$

5. Deduce $\mu(A)$ from the following equation, for all $\alpha \in M_2(O_0)$,

$$\sigma(\alpha) = \mu(A)^{-1}\alpha^*\mu(A).$$

The problem of outer automorphisms

- An automorphism of $\mathrm{End}(A)$ is of the form φ_*, where $\varphi \in \mathrm{Aut}(A)$, if and only if it is inner.

The problem of outer automorphisms

- An automorphism of $\mathrm{End}(A)$ is of the form φ_*, where $\varphi \in \mathrm{Aut}(A)$, if and only if it is inner.
- The group $\mathrm{Out}(\mathrm{End}(A))$ is cyclic of order 2.

The problem of outer automorphisms

- An automorphism of $\mathrm{End}(A)$ is of the form φ_*, where $\varphi \in \mathrm{Aut}(A)$, if and only if it is inner.
- The group $\mathrm{Out}(\mathrm{End}(A))$ is cyclic of order 2.
- In $M_2(O)$, the non-trivial class of the group of outer automorphisms is induce by conjugation by $P = \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & \sqrt{-p} \end{pmatrix}$.
- An isomorphism $\theta\colon \mathrm{End}(A) \to M_2(O_0)$ does not respect the action of $\mathrm{End}(A)$ on the global differentials of A, it must be post composed by conjugation by P.

Once more with feelings

Write f^Ω for the action of an endomorphism of an abelian variety on its space of global differentials. f^Ω lives in $M_2(\mathbb{F}_{p^2})$.

Informed strategy

1. Recover the structure constants of $\mathrm{End}(A)$.
2. Compute an isomorphism $\tau\colon \mathrm{End}(A) \otimes \mathbb{Q} \to M_2(B_{p,\infty})$.
3. Compute $\gamma \in \mathrm{GL}_n(B_{p,\infty})$ such that $\gamma^{-1}\tau(\mathrm{End}(A))\gamma = M_2(O_0)$.
4. If for some $f \in \mathrm{End}(A)$, $\det f^\Omega \neq \det(\gamma^{-1}\tau(\mathrm{End}(A))\gamma)^\Omega$, set $\gamma = \gamma P$.
5. Recover the following involution of $M_2(O_0)$:

$$\sigma\colon \alpha \mapsto \gamma^{-1}(\tau \circ r_A \circ \tau^{-1})(\gamma\alpha\gamma^{-1})\gamma$$

6. Deduce $\mu(A)$ from the following equation, for all $\alpha \in M_2(O_0)$,

$$\sigma(\alpha) = \mu(A)^{-1}\alpha^*\mu(A).$$

Polynomial does not mean practical

- Computing the isomorphism $\tau\colon \mathrm{End}(A) \otimes \mathbb{Q} \to M_2(B_{p,\infty})$ may be done in polynomial time, but the constant is demonic. (Csahók, Kutas, M. and Zábrádi)

Polynomial does not mean practical

- Computing the isomorphism $\tau\colon \mathrm{End}(A) \otimes \mathbb{Q} \to M_2(B_{p,\infty})$ may be done in polynomial time, but the constant is demonic. (Csahók, Kutas, M. and Zábrádi)
- We also have a subexponential algorithm, whose subexponential part is the computation of the class group and group of S-units of a number field of degree 16. (Kutas, M.)

Polynomial does not mean practical

- Computing the isomorphism $\tau\colon \mathrm{End}(A) \otimes \mathbb{Q} \to M_2(B_{p,\infty})$ may be done in polynomial time, but the constant is demonic. (Csahók, Kutas, M. and Zábrádi)
- We also have a subexponential algorithm, whose subexponential part is the computation of the class group and group of S-units of a number field of degree 16. (Kutas, M.)
- The number field in question cannot a priori be known in advance (say, for precomputation). We need to know an embedding into $(\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} M_2(B_{p,\infty})$.
- The question of finding a practical algorithm for this problem is still open.

Thank you

Thank you for listening!
The manuscript will be on the eprint and on arXiv soon.
Please enjoy the cats while you wait for the preprint.