The Principal Ideal Problem for endomorphism rings of superspecial abelian varieties

ANTS XVII - Groningen

W. Castryck, J. K. Eriksen, R. Invernizzi*, F. Vercauteren

COSIC - KU Leuven

6 jul 2026

Outline

fwo

KU LEUVEN

Outline

The Principal Ideal Problem

Principal Ideal Problem

Let R be a ring, and I a principal ideal of R. Find a generator of I.

- I is given as pair $(\alpha, \mathsf{n}(I))$
- different $R \rightsquigarrow$ different applications (NTRU, *HAWK*...)

Our setting

- quaternion algebras $B_{p,\infty} = \langle 1, i, j, k \rangle$ over $\mathbb{Q}$
- multiplication rules: $ij = -ji = k$, $j^2 = -p$
- $i^2 = -1$ (assume $p \equiv 3 \bmod 4$)
- subrings $\mathcal{O} \subset B_{p,\infty}$ that are rank 4 lattices are called *orders*
- work with (left) *$\mathcal{O}$-ideals*

Deuring Correspondence

- maximal order $\mathcal{O} \longleftrightarrow \mathrm{End}(E)$, E supersingular elliptic curve
- ideal between orders $\longleftrightarrow$ *isogeny* between curves
- $\mathsf{n}(I) \longleftrightarrow \deg(\varphi_I)$
- $I = \langle \alpha, N \rangle = \mathcal{O}\alpha + \mathcal{O}N \longleftrightarrow \varphi_I$ with kernel $E[N] \cap \ker(\alpha)$

PIP in $B_{p,\infty}$ (Kirschmer-Voight)

- principal ideals $I = \langle \gamma \rangle \longleftrightarrow$ *endomorphisms*
- I is a (rank 4) lattice with a *quadratic form*
- $\rightsquigarrow$ can find shortest vector γ
- if $\mathsf{n}(\gamma) = \overline{\gamma}\gamma = \mathsf{n}(I) \rightsquigarrow I = \langle \gamma, \mathsf{n}(I) \rangle$ is principal

PIP in $M_g(B_{p,\infty})$

- $M_g(\mathcal{O}) \longleftrightarrow \mathrm{End}(E^g)$
- *principal ideal ring*
- *no quadratic form*

Outline

Main problems

Problem 1 - PIP in $M_g(B_{p,\infty})$

Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order. Given a left ideal $I \subset M_g(\mathcal{O})$, with $g \geq 2$, compute a matrix $\mathbf{M} \in M_g(\mathcal{O})$ such that $I = M_g(\mathcal{O})\mathbf{M}$.

Main problems

Problem 2 - Kernel to Ideal

Let E be a supersingular elliptic curve, and $\mathcal{O} \subset B_{p,\infty}$ a maximal order isomorphic to $\mathrm{End}(E)$. Given a finite subgroup $H \subset E^g$, with $g \geq 2$, compute a matrix $\mathbf{M} \in M_g(\mathcal{O})$ such that $\ker(\mathbf{M}) = H$.

- geometric formulation
- 1-dimensional version useful in cryptography

Connection

- given $H \subset E^g$ look at

$$I_H = \{\mathbf{M} \in M_g(\mathcal{O}) \mid \mathbf{M}(H) = 0\}$$

- *PIP* solver on $I_H \rightsquigarrow$ solves *Ideal to Kernel*
- Ideal to Kernel conceptually easier

Reductions

- assume $|H|$ is prime $\longleftarrow$ *factor* $|H|$
- assume $H = \langle (P, 0, ..., 0) \rangle \longleftarrow$ *discrete logarithms over* $|H|$
- reduce to $H = \langle (P, 0) \rangle$ (i.e. $g = 2$) $\longleftarrow$ *free*
- $|H|$ generally *smooth* in practice
- factorization and logarithms can be avoided for PIP

Reformulating the problem

Requirements:

$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O})$$

- $\ker(\mathbf{M}) = H = \langle (P, 0) \rangle$
  - $\mathrm{n}(\mathbf{M}) = |H|$
  - $a(P) = c(P) = 0$

Reformulating the problem

- $\mathsf{n}(\mathbf{M}) = \det(\mathbf{M})$ in *non-commutative ring*
- in dimension 2:

$$\mathsf{n}(c)\,\mathsf{n}(\mathbf{M}) = \mathsf{n}(\mathsf{n}(c)b - a\bar{c}d)$$

- (...technical steps...)
- solutions correspond to *isogeny squares*

Reformulating the problem

$$
\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, bend left, dashed, "a"] \arrow[ddr, bend right, dashed, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}
$$

Outline

Constructing the square

- τ is the isogeny with kernel P

$$
\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, bend left, dashed, "a"] \arrow[ddr, bend right, dashed, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}
$$

Constructing the square

- ξ is *equivalent* to $\hat{\tau}$
- $I_\xi = \overline{I}_\tau \alpha / \mathsf{n}(I_\tau)$, $\alpha \in \overline{I}_\tau$
- sample $\alpha \in \overline{I}_\tau$
- must have $\deg(\chi) = \deg(\xi)$

$$\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, dashed, bend left, "a"] \arrow[ddr, dashed, bend right, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}$$

Constructing the square

- $\chi \in \mathrm{End}(E)$ of given degree
- assume $\mathbb{Z}[i] \subset \mathrm{End}(E)$
- sample $\deg(\xi)$ prime $1 \bmod 4$
- set $\chi = l_1 + il_2$

$$
\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, dashed, bend left, "a"] \arrow[ddr, dashed, bend right, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}
$$

Constructing the square

- σ maps $\ker(\hat{\xi})$ in $\ker(\hat{\chi})$
- computed by *linear algebra*
- $\gamma = [\xi]^*\sigma$ is fixed

$$
\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, dashed, bend left, "a"] \arrow[ddr, dashed, bend right, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}
$$

Reconstructing the matrix

- a and c given by the diagram
- solve a *one-dimensional PIP*
- b and d computed from $\overline{\sigma}$ and $\overline{\chi}$

$$
\begin{tikzcd}
E \arrow[dr, "\tau"] \arrow[drr, dashed, bend left, "a"] \arrow[ddr, dashed, bend right, "c"'] & & \\
& F \arrow[r, "\xi"] \arrow[d, "\gamma"'] & E \arrow[d, "\sigma"] \\
& E \arrow[r, "\chi"'] & E
\end{tikzcd}
$$

Outline

Results

Problem 2 - Kernel to Ideal

Let E be a supersingular elliptic curve, and $\mathcal{O} \subset B_{p,\infty}$ a maximal order isomorphic to $\mathrm{End}(E)$. Given a finite subgroup $H \subset E^g$, with $g \geq 2$, compute a matrix $\mathbf{M} \in M_g(\mathcal{O})$ such that $\ker(\mathbf{M}) = H$.

- complexity: $\log |H|$, $\log p$, g, F_H, D_H, $\log \mathsf{n}(I_c)$
- $\mathsf{n}(I_c)$: distance from E to a "nice" curve

Results

Problem 1 - PIP in $M_g(B_{p,\infty})$

Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order. Given a left ideal $I \subset M_g(\mathcal{O})$, with $g \geq 2$, compute a matrix $\mathbf{M} \in M_g(\mathcal{O})$ such that $I = M_g(\mathcal{O})\mathbf{M}$.

- complexity: $\log p$, $\log \mathsf{n}(I)$, g, $\log \mathsf{n}(I_c)$
- implemented and fast for cryptographic sizes

Results

Problem 1 - PIP in $M_g(B_{p,\infty})$

Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order. Given a left ideal $I \subset M_g(\mathcal{O})$, with $g \geq 2$, compute a matrix $\mathbf{M} \in M_g(\mathcal{O})$ such that $I = M_g(\mathcal{O})\mathbf{M}$.

- concurrent work by Page, Robert, Soumier using *KLPT*
- larger sizes but potentially only assumes GRH

Thank you for your attention.
Questions?