

The Principal Ideal Problem for endomorphism rings of superspecial abelian varieties

AM-PQC - Ohrid

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

COSIC - KU Leuven

12 aug 2026



Outline

1. The Principal Ideal Problem
2. Problem formulation in $B_{p,\infty}$
3. Results

Outline

1. The Principal Ideal Problem

2. Problem formulation in $B_{p,\infty}$

3. Results

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 $(\alpha, n(I))$
- ▶ 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 $p \equiv 3 \pmod{4}$)
- ▶ 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 $\mathcal{O} \longleftrightarrow \text{End}(E)$, E supersingular elliptic curve
- ▶ ideal between orders $\longleftrightarrow$ *isogeny* between curves
- ▶ $n(I) \longleftrightarrow \deg(\varphi_I)$
- ▶ $I = \langle \alpha, N \rangle = \mathcal{O}\alpha + \mathcal{O}N \longleftrightarrow \varphi_I$ 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 $n(\gamma) = \bar{\gamma}\gamma = n(I) \rightsquigarrow I = \langle \gamma, n(I) \rangle$ is principal

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

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

Outline

1. The Principal Ideal Problem
2. Problem formulation in $B_{p,\infty}$
3. Results

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 $\text{End}(E)$. 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 *Kernel to Ideal*
- ▶ Kernel to Ideal conceptually easier

Reductions

- ▶ assume $|H|$ is prime $\longleftarrow$ *factor* $|H|$
- ▶ assume $H = \langle (P, 0, \dots, 0) \rangle \longleftarrow$ *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:

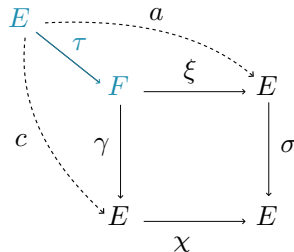
$$\mathbf{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O})$$

► $\ker(\mathbf{M}) = H = \langle (P, 0) \rangle$

- $n(\mathbf{M}) = |H|$
- $a(P) = c(P) = 0$

Constructing the square

- ▶ noncommutative determinant
- ▶ $\rightsquigarrow$ norm equation over the quaternions
- ▶ $\rightsquigarrow$ *isogeny square*



Outline

1. The Principal Ideal Problem
2. Problem formulation in $B_{p,\infty}$
3. Results

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 $\text{End}(E)$. 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: $\log |H|, \log p, g, F_H, D_H, \log n(I_c)$
- ▶ $n(I_c)$: 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: $\log p, \log n(I), g, \log n(I_c)$
- ▶ 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?