PCMI 2021: Supersingular isogeny graphs in cryptography
Exercises Lecture 3: Quaternion algebras, Endomorphism rings

TA: Jana Sotáková **version July 30, 2021**

All the commands are in Magma. Similar commands also exist for Sage.

Solutions for the first 3 exercises are on the website if you want to focus on Exercise 4.

1. (Quaternion algebras and orders) For small primes p, define the quaternion algebra $B := B_{p,\infty} = \mathbb{Q}\langle 1, i, j, k\rangle$ with $i^2 = -r$ and $j^2 = -p$ and $ij = -ji = k$:

   (a) Use `QuaternionAlgebra< RationalField() | -r, -p >`;

   (b) For $p \equiv 3 \bmod 4$, use $-r = -1$;

   (c) For $p \equiv 5 \bmod 8$, use $-r = -2$;

   (d) Otherwise, find r as a prime $r \equiv 3 \bmod 4$ such that $\left(\frac{r}{p}\right) = -1$.

   Verify that B is only ramified at p and infinity (`RamifiedPrimes`). Find the discriminant of B. Note that again, ramified primes are those that divide the discriminant. In the last exercise 5, you will see what makes the ramified primes special.

   Verify that $i^2 = -r$ and $j^2 = -p$. Find the norm, trace and the minimal polynomial of the element $w = 2 + i - 3j + 4k$.

2. (Maximal orders) Write down a maximal order in each of the quaternion algebras. You can find examples for different congruence conditions on p in Lemmas 2-4 in Kohel-Lauter-Petit-Tignol.

   (a) Using the Magma command `MaximalOrder`;

   (b) Using a basis and `QuaternionOrder`;

   Find the discriminant and the norm form of the maximal order. `GramMatrix`

3. For $p = 67$, take any maximal order $\mathcal{O} \subset B_{p,\infty}$. Then:

   (a) Enumerate all the left-ideal classes in $\mathcal{O}$; `LeftIdealClasses`

   (b) For every ideal class, pick a representative and find the right order of the ideal; `RightOrder`;

   (c) Check how many isomorphism classes there are as right orders. Deduce the number of supersingular j-invariants in $\mathbb{F}_p$ and pairs of conjugate j-invariants in $\mathbb{F}_p^2$. Hint available.

   (d) Compute the norm of all these ideals;

   (e) Figure out which of these maximal orders correspond to elliptic curves defined over $\mathbb{F}_p$. Show that the following suffices:

      i. Compute the norm form of these maximal orders; Hint available.

      ii. Find out whether they represent p;

   Check the count by looking at how many supersingular j-invariants there are in $\mathbb{F}_p$.

4. ("Effective Deuring Correspondence") In this exercise, you will be matching endomorphism rings to supersingular elliptic curves. For $p = 67$, determine the endomorphism rings of all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$:

(a) List all the maximal orders in $B_{p,\infty}$;

(b) Find the connecting ideals for some of these orders;

Note that you can build them as follows: for maximal orders $\mathcal{O}_1, \mathcal{O}_2$:

- Let $N = [\mathcal{O}_1 : \mathcal{O}_1 \cap \mathcal{O}_2]$. Compute intersections using `O1 meet O2;`
- Then take $I := N\mathcal{O}_1 + N\mathcal{O}_1\mathcal{O}_2$.
  You can define such ideals using `LeftIdeal(Order ,Generators)` where Generators is any tuple.
- Verify that this ideal is integral.
- Verify that it is a left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal;
- Compute its norm.

(c) List all the supersingular j-invariants;

(d) Start from an elliptic curve with 'known' endomorphism ring, e.g. $E : y^2 = x^3 - x$;

(e) For small ℓ, compare the ℓ-isogenies between the elliptic curves and ideals of norm ℓ. Use (3e) to narrow down the orders for elliptic curves defined over $\mathbb{F}_p$.

(f) Note that for curves for which you do know the endomorphism ring, you can use the kernel ideals. Every isogeny φ corresponds to the kernel ideal $I_\varphi := \{\alpha \in \mathcal{O} : \alpha_{|\ker\varphi} = 0\}$. For instance, the ideal $(\ell, \pi - 1) \leftrightarrow (\ell, j - 1)$ corresponds to the subgroup of E on which Frobenius acts like identity. This approach can help you identify some of the edges (especially for curves over $\mathbb{F}_p$).

You can find more things that will help you distinguish the orders and match them to elliptic curves in Cervino and Lauter and McMurdy and in the WIN-4 collaboration.

5. (Quaternion algebras and Matrix rings) Let B be a quaternion algebra over $\mathbb{Q}$ with basis $1, i, j, k$ with $i^2 = a$ and $j^2 = b$ and $ij = -ji$. Check that B embeds into the matrix ring

$$B \to M_2(\mathbb{Q}(\sqrt{a})),$$
$$x + yi + zj + wk \mapsto \begin{pmatrix} x + y\sqrt{a} & b(z + t\sqrt{a}) \\ z - t\sqrt{a} & x - y\sqrt{a} \end{pmatrix}.$$

so quaternion algebras naturally live in matrix rings. Moreover, localizing we almost always get the matrix ring

$$B \otimes \mathbb{Q}_\ell = M_2(\mathbb{Q}_\ell);$$

this holds for all but finitely many primes, which we call the ramified primes - these are exactly the primes that divide the discriminant.

Hints, comments, commands

1. d) Compare with the notes 1b) from the second exercise sheet, the choice of r is the same. In exercise 2, you were looking for a supersingular reduction of an elliptic curve with CM by an order in $\mathbb{Q}(\sqrt{-r})$. Moreover, because $r \equiv 3 \bmod 4$ and the class number of such an order is odd, there will be a curve E with j-invariant already in $\mathbb{F}_p$.

   But the reduction of isogenies is injective, so you know that $\mathbb{Q}(\sqrt{-r}) \hookrightarrow B_{p,\infty} = \mathrm{End}(E) \otimes \mathbb{Q}$. Moreover, this imaginary quadratic field cannot commute with Frobenius, because these endomorphisms of E cannot be defined over $\mathbb{F}_p$: we know that $\mathrm{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p})$ with $\sqrt{-p} \leftrightarrow$ Frob. You still need to argue that then $\sqrt{-r}$ anticommutes with Frobenius.

   * Discriminants. There is a notion of discriminant for all orders in the quaterion algebra. Moreover, an order is maximal if and only if its discriminant is equal to the discriminant of the quaternion algebra. For orders in inclusion, you can read off the relative index from the discriminant, for Magma it is just the cofactor. Checking inclusion is the easiest by checking membership for each basis member.

3. c) Deuring's correspondence can be written in two ways:

   - j-invariants (up to conjugation in $\mathbb{F}_{p^2}$, that is, $j \mapsto j^p$) correspond to maximal orders up to isomorphism of maximal orders (that is, conjugation in the quaternion algebra B - Skolem Noether);
   - Starting from an elliptic curve E, the left ideal classes in $\mathcal{O} := \mathrm{End}(E)$ correspond to supersingular elliptic curves, such that if $E1 \leftrightarrow \mathcal{O}_1$ then the right order can be identified with $O_R(I) = \mathrm{End}(O_1)$.

   For j-invariants in $\mathbb{F}_p^2$, the endomorphism rings of supersingular elliptic curves with j-invariants j and j^p are isomorphic as orders in the quaternion algebra, even though the curves are not isomorphic. So if you find 6 left ideal classes and 4 non-isomorphic maximal orders, you see that exactly 2 supersingular j-invariants are in $\mathbb{F}_p$.

3. e) Curves over $\mathbb{F}_p$ have the Frobenius endomorphism in their endomorphism ring, which is an endomorphism of norm p and trace 0.

   You can use the `GramMatrix`, which is the Gram matrix for the inner product $\langle x, y\rangle$ on the maximal order satisfying
   $$\langle x, y\rangle = \mathrm{Norm}(x+y) - \mathrm{Norm}(x) - \mathrm{Norm}(y),$$
   So we have $\mathrm{Norm}(x) = \frac{1}{2}\langle x, x\rangle$.

   You can create a quadratic form for the order O : `QuadraticForm(GramMatrix(O));`.

   So you need to represent the element $2p$ in this quadratic form. Note that $\mathrm{Tr}(x) = 0$ means that the first coordinate can be set to 0 (if the order has 1 in its basis). But Magma doesn't naturally create orders with 1 in the basis, so you can't just set $a = 0$.