PCMI 2021: Supersingular isogeny graphs in cryptography

Exercises Lecture 3: Quaternion algebras, Endomorphism rings

TA: Jana Sotáková **version July 29, 2021**

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

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) Compute the norm of all these ideals;

   (d) 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;

      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 $N = [\mathcal{O}_1 : \mathcal{O}_1 \cap O_2]$. 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 (3d) to narrow down the orders for elliptic curves defined 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) coming soon!