

# PCMI 2021: Supersingular isogeny graphs in cryptography

## Exercises Lecture 2: Quaternion algebras, Endomorphism rings

TA: Jana Sotáková

version July 27, 2021

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  $p \equiv 3 \pmod{4}$ , use  $-r = -1$ ;
- (c) For  $p \equiv 5 \pmod{8}$ , use  $-r = -2$ ;
- (d) Otherwise, find  $r$  as a prime  $r \equiv 3 \pmod{4}$  such that  $\left(\frac{r}{p}\right) = -1$ .

Verify that  $B$  is only ramified at  $p$  and infinity. 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.

- (a) Using the Magma command `MaximalOrder`;
- (b) Using a basis and `QuaternionOrder`;

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

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

- (a) Enumerate all the left-ideal classes in  $\mathcal{O}$ ;
- (b) For every ideal class, pick a representative and find the right order of the ideal;
- (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. (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) List all the supersingular  $j$ -invariants;
- (c) Start from an elliptic curve with ‘known’ endomorphism ring, e.g.  $E : y^2 = x^3 - x$ ;
- (d) For small  $\ell$ , compare the  $\ell$ -isogenies between the elliptic curves and ideals of norm  $\ell$ . Use (3d) to narrow down the orders for elliptic curves defined over  $\mathbb{F}_p$ .

5. (Quaternion algebras and Matrix rings) To add