# EXERCISES FOR WEEK 5

AURORE GUILLEVIC

## Exercises

**Exercise 1.** Consider an elliptic curve $E$ defined over a prime field $\mathbb{F}_p$ of $j$-invariant 0, and $p = 1 \bmod 3$. The curve has an endomorphism $\psi\colon (x, y) \mapsto (\omega x, y)$ where $\omega$ (omega) in $\mathbb{F}_p$ satisfies $\omega^2 + \omega + 1 = 0$ ($\omega$ is a primitive 3rd root of unity). The characteristic polynomial of $\psi$ is $X^2 + X + 1$. The ring of integers of $\mathbb{Q}(\omega)$ is $\mathbb{Z}(\omega)$ (the Eisenstein integers), and $\omega = (-1 + \sqrt{-3})/2$. The Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ has characteristic polynomial $X^2 - tX + p$ of discriminant $t^2 - 4p = -3y^2$.

Find the short basis $\vec{b}_1, \vec{b}_2$ for the scalar decomposition. Warning: there is (are) a sign mistake in the paper [1].

## References

[1] Benjamin Smith. Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians. *Contemporary mathematics*, 637:15, May 2015. https://hal.inria.fr/hal-00874925.

*E-mail address*: aurore.guillevic@inria.fr

*Date*: Week 5.