Feuille de TD n°10

Exercice 1 (Calcul de racines carrées dans $\mathbb{F}_p$)**.** Soit p un nombre premier impair. Soit $a \in \mathbb{F}_p$ non nul.

1. Montrer que $a^{\frac{p-1}{2}} = 1$ si et seulement si il existe $b \in \mathbb{F}_p$ tel que $a = b^2$. Dans la suite de l'énoncé, on se donne un tel b vérifiant $a = b^2$.

2. En utilisant le lemme chinois, montrer que

$$\begin{aligned} \mathbb{F}_p[X]/(X^2 - a) &\longrightarrow \mathbb{F}_p^2 \\ P &\longmapsto (P(b), P(-b)) \end{aligned}$$

est bien défini, et est un isomorphisme.

3. Soit $P \in \mathbb{F}_p[X]/(X^2-a)$. Quelles valeurs peut prendre le couple $(P(b)^{\frac{p-1}{2}}, P(-b)^{\frac{p-1}{2}})$? Pour combien de $P \in \mathbb{F}_p[X]/(X^2 - a)$ obtient-on chacune de ces valeurs ?

4. Supposons que $P(b)^{\frac{p-1}{2}} = 1$ et $P(-b)^{\frac{p-1}{2}} \neq 1$. Montrer que $\textsc{Pgcd}(P^{\frac{p-1}{2}} - 1, X^2 - a)$ a un sens, et le calculer.

5. En déduire un algorithme probabiliste permettant de calculer une racine carrée de a.

6. Estimer sa complexité en moyenne, en termes d'opérations dans $\mathbb{F}_p$.