Exercice 1 – Soit $p \geqslant 5$ un nombre premier et soit q une puissance de p. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soit m un entier strictement positif. On note $E[m]$ l'ensemble des points P de la courbe E qui vérifient $[m]P = 0$.

1) Donner un exemple de courbe sur $\mathbb{F}_7$ telle que $E[2]$ contient au moins deux points.

2) On s'intéresse à présent au cas particulier $m = p$. Regardons la courbe E définie sur $\mathbb{F}_{19}$ par l'équation affine $y^2 = x^3 + x$. Calculer $\mathrm{Card}(E(\mathbb{F}_{19}))$. Calculer $\mathrm{Card}(E[19])$.

Lorsqu'une courbe E définie sur $\mathbb{F}_p$ vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p + 1$, on dit que c'est une courbe **supersingulière** en p.

Exercice 2 – On étudie dans cet exercice la notion de **courbe anormale**. Soit p un nombre premier. Une courbe elliptique E définie sur $\mathbb{F}_p$ est dite **anormale en** p si elle vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p$.

1) Quelle est la structure d'un groupe de cardinal p ? Que peut-on en déduire pour $E(\mathbb{F}_p)$?

2) Donner un exemple de courbe anormale pour $p = 23$.

Exercice 3 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Réviser les fonctions znlog, fflog. Terminer l'implémentation d'un calcul de log-discret sur une courbe elliptique (méthode de Pollard par exemple) et le tester sur des exemples sur $E(\mathbb{F}_{11^5})$.