Feuille d'exercices 5.

Exercice 1 1) Montrer que le symbole de Legendre $\left(\frac{n}{3}\right) = n \bmod 3$.
2) Calculer $\left(\frac{3}{23}\right)$ en utilisant la formule d'Euler.

Exercice 2 1) Calculer le symbole de jacobi $\left(\frac{22}{105}\right)$ en utilisant la définition.
2) Montrer que si a est un résidu quadratique modulo b alors $\left(\frac{a}{b}\right) = 1$. Est-ce que la réciproque est vraie?
3) Calculer le symbole de Legendre $\left(\frac{365}{1847}\right)$ à l'aide de la loi de réciprocité quadratique pour le symbole de Legendre.
4) Refaire le calcul en utilisant la loi de réciprocité pour le symbole de Jacobi.

Exercice 3 Soit p un nombre premier tel que $p = 3 \bmod 4$. Soit a un entier qui est un résidu quadratique modulo p. Montrer que $a^{(p+1)/4}$ est une racine carrée de $a \bmod p$.

Exercice 4 Soit E la courbe elliptique $y^2 = x^3 + x + 6$ sur $\mathbb{F}_{11}$.
1) En vous aidant de la formule d'Euler, donner les coordonnées des points de E. Combien E a-t-elle de points? Est-ce que cela est conforme au théorème de Hasse? Pourquoi E est-il un groupe cyclique?
2) Rappeler comment est définie l'addition sur E. Quel est l'élément neutre de E? Soient $P = (2, 7)$ et $Q = (3, 5)$ et $R = (2, 4)$, comme l'ont montré les calculs faits dans le 1), P, Q, R sont des points de E. Calculer $P + Q$ et $P + R$.
3) Calculer $i.P$, pour $i = 2, ..., 13$. Que peut-on dire de P? Est-ce conforme à ce que vous avez trouvé dans le 1)?
4) Alice et Bob veulent échanger un message en utilisant le chiffrement d'El Gamal sur la courbe elliptique E. Les données publiques sont E, $\mathbb{F}_{11}$, et $P = (2, 7)$ (générateur de E).
Alice choisit un exposant secret $a = 7$. Elle envoie $\beta = 7.P$ à Bob.
Bob choisit un exposant $b = 3 \in \{1, ..., 12\}$.
Bob veut envoyer à Alice le message $m = (10, 9)$.
Faire le calcul fait par Bob pour chiffrer m et ensuite celui fait par Alice pour déchiffrer.