M2 - Courbes elliptiques et cryptographie

Partiel du 26 novembre 2009 - Durée 2 heures

La calculatrice est autorisée. L'usage de tout document est interdit. La rigueur du raisonnement et la clarté de la rédaction seront prises en compte dans la notation.

Exercice 1 : Soit p un nombre premier impair $\neq 5$. On considère $\zeta \in \overline{\mathbb{F}_p}$ une racine primitive 5-ème de l'unité (i.e. $\zeta^5 = 1$ et $\zeta^\ell \neq 1$ pour tout $1 \leq \ell \leq 4$).

1- Montrer que $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$.

2- On pose $\theta = \zeta - \zeta^2 - \zeta^3 + \zeta^4$. Montrer que $\theta^2 = 5$.

3- Établir que $\theta = (\zeta + \zeta^{-1}) - (\zeta^2 + \zeta^{-2})$.

4- On suppose que $p \equiv \pm 1 \pmod 5$, montrer que $\theta^p = \theta$.

5- On suppose que $p \equiv \pm 2 \pmod 5$, montrer que $\theta^p = -\theta$.

6- En déduire que 5 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \pmod 5$.

7- Retrouver le résultat précédent en utilisant la loi de réciprocité quadratique.

Exercice 2 On admet que le polynôme $P(X) = X^4 + X^3 - 1$ est irréductible sur $\mathbb{F}_3[X]$. On a donc $\mathbb{F}_{81} = \mathbb{F}_3[\theta]$ où θ est une racine de $P(X)$ dans $\overline{\mathbb{F}_3}$.

1- Factoriser 80.

2- On admet que $\theta^{40} = -1$; en déduire que θ est un générateur du groupe $(\mathbb{F}_{81})^\times$.

3- Résoudre l'équation $\theta^\ell = 1 - \theta$.

4- Montrer que l'on a $\theta^3(1 + \theta) = 1$ et trouver $\ell \in \mathbb{N}$ tel que $\theta^\ell = 1 + \theta$.

5- Montrer que le polynôme $X^2 - \theta$ est irréductible dans $\mathbb{F}_{81}[X]$.

6- On pose $g = \theta^9 + \theta$. Montrer que $g \in \mathbb{F}_9$.

7- On admet que le l'on a $g = \theta^3 - \theta^2$. Calculer g^2.

8- Donner un polynôme, $P(X) \in \mathbb{F}_3[X]$, de degré 2 tel que $P(g) = 0$.

Exercice 3 On considère la courbe elliptique suivante définie sur $\mathbb{F}_{11}$:

$$E \ : \ y^2 = x^3 + x + 4$$

1) Quels sont les carrés modulo 11 ?

2) Énumérer tous les points de $E(\mathbb{F}_{11})$.