UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2002–2003

DESS CCSI

Méthodes mathématiques de la cryptologie

Epreuve du 17 décembre 2002

Durée 2 heures

Documents manuscrits autorisés.

Exercice I

On considère l'équation
$$y^2 = x^3 - 1\ .$$

1) On rappelle qu'une telle équation définit une courbe elliptique sur un corps K si et seulement si il n'existe pas de couples $(x, y) \in K^2$ vérifiant simultanément $f(x, y) = 0$, $\dfrac{\partial f}{\partial x}(x, y) = 0$ et $\dfrac{\partial f}{\partial y}(x, y) = 0$, où $f(x, y) = y^2 - (x^3 - 1)$.

a) Montrer que l'équation ci-dessus définit une courbe elliptique sur tout corps fini de caractéristique différente de 2 et 3.

b) Montrer qu'en revanche elle ne définit pas une courbe elliptique sur les corps de caractéristique 2 ou 3.

2) On se place désormais sur le corps fini $\mathbb{F}_p$, où p est un nombre premier tel que $p \geq 5$.

a) En utilisant la loi de réciprocité quadratique, calculer le symbole de Legendre $\left(\frac{-3}{p}\right)$ selon que $p \equiv 1 \pmod 3$ ou $p \equiv 2 \pmod 3$.

b) En déduire que si $p \equiv 2 \pmod 3$, l'équation $x^2 - xy + y^2 = 0$ n'a pas de solution dans $\mathbb{F}_p$ autre que $(0, 0)$ (on écrira $4(x^2 - xy + y^2) = (2x - y)^2 + 3y^2$).

c) En déduire que si $p \equiv 2 \pmod 3$ l'application $x \mapsto x^3$ de $\mathbb{F}_p$ dans lui-même est **bijective**.

d) En déduire finalement le cardinal de $E(\mathbb{F}_p)$ (y compris le point à l'infini) quand $p \equiv 2 \pmod 3$ (on comptera le nombre de valeurs de x correspondant à chaque valeur de y).

2) On suppose maintenant que $p \equiv 1 \pmod 3$. Calculer à la main, par la méthode que vous préférez, le cardinal de $E(\mathbb{F}_p)$ (y compris le point à l'infini) pour $p = 7$, $p = 13$ et $p = 19$. Pour chacune de ces valeurs de p, donner la liste complète des points de $E(\mathbb{F}_p)$.

Exercice II

1) Soit P un polynôme de degré exactement égal à n sur un corps commutatif K.

a) Montrer que quand $n = 2$ ou $n = 3$, P est irréductible dans $K[X]$ si et seulement si il n'a pas de racine dans K.

b) Montrer que quand $n = 4$, P est irréductible dans $K[X]$ si et seulement si il n'a pas de racine dans K et il n'est pas divisible par un polynôme de degré 2 de $K[X]$.

c) On considère le cas particulier où $K = \mathbb{F}_2$ est le corps fini à deux éléments, qu'on notera bien sûr 0 et 1 (avec $1 + 1 = 0$). En utilisant les questions ci-dessus, donner la liste complète des polynômes irréductibles de $K[X]$ de degré 1, 2, 3 et 4.

2) On considère le corps $\mathbb{F}_{16}$ défini comme $\mathbb{F}_2[X]/(X^4 + X + 1)\mathbb{F}_2[X]$, ou en d'autres termes comme l'ensemble des expressions de la forme $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$, où les a_i sont égaux à 0 ou 1 (dans $\mathbb{F}_2$) et où α vérifie $\alpha^4 + \alpha + 1 = 0$.

a) Enumérer les 16 éléments de $\mathbb{F}_{16}$ en fonction de α, puis faire un tableau comprenant dans la première colonne ces 16 éléments z, et dans la colonne suivante les éléments z^2, $z^2 - z$, $1/z$ $z + 1/z$ (quand $z \neq 0$). On rappelle que dans un corps de caractéristique 2 on a $1 + 1 = 0$ et $(a + b)^2 = a^2 + b^2$.

b) Rappeler la démonstration faite en cours du résultat suivant : dans un corps de caractéristique 2, l'équation $y^2 + by + c = 0$ a une seule solution si $b = 0$, et sinon possède 2 ou 0 solutions selon que $A = c/b^2$ est de la forme $z^2 - z$ ou non.

c) Soit E la courbe elliptique d'équation $y^2 + xy = x^3 + x$, considérée comme étant à coefficients dans $\mathbb{F}_{16}$. Calculer le nombre de points de $E(\mathbb{F}_{16})$ (y compris le point à l'infini). Facultatif : énumérer ces points.

d) Faire de même pour la courbe elliptique d'équation $y^2 + xy = x^3 + \alpha x$, où α est comme ci-dessus.

Exercice III

L'énoncé (et d'ailleurs la solution) de cet exercice est très court, mais on prendra bien soin de le résoudre correctement.

Soit p un nombre premier différent de 2. On rappelle que l'on peut définir le corps $\mathbb{F}_{p^2}$ à p^2 éléments comme $\mathbb{F}_p[X]/(X^2 - d)\mathbb{F}_p[X]$ (c'est-à-dire l'ensemble des $a + b\alpha$, où a et b sont dans $\mathbb{F}_p$ et $\alpha^2 = d$), où d est un élément quelconque de $\mathbb{F}_p$ **fixé** tel que $\left(\frac{d}{p}\right) = -1$.

Donner (en distinguant 3 cas) la solution générale dans $\mathbb{F}_{p^2}$ de l'équation du deuxième degré $ax^2 + bx + c = 0$, où on suppose que a, b et c sont dans $\mathbb{F}_p$ avec $a \neq 0$.

Application numérique : on choisit $p = 23$. Montrer que $d = -1$ convient pour définir $\mathbb{F}_{23^2}$. On choisit donc $d = -1$, et on note i une racine de $i^2 = -1$. Calculer les solutions dans $\mathbb{F}_{23^2}$ de l'équation $x^2 + x + 1 = 0$, qui doivent toutes s'exprimer sous la forme $u + iv$ avec u et v dans $\mathbb{F}_{23}$, sans dénominateur ni racine carrée.