UFR de Mathématiques et Informatique
Université Bordeaux I Année 2003–2004

DESS CCSI

Méthodes mathématiques de la cryptologie

Epreuve de TP du mardi 13 Janvier 2004

Durée 2 heures

On rédigera tous les programmes demandés en `GP`, et on enverra aussi bien les démonstrations, les programmes, les commentaires et les résultats par mail à

`cohen@math.u-bordeaux.fr`

La question 1) est entièrement théorique et pourra être rédigée soit dans un fichier séparé, soit à la main. Le reste est entièrement sur machine.

Exercice I

Soit $q = 2^k$ avec $k \geq 1$ et $\mathbb{F}_q = \mathbb{F}_{2^k}$ le corps de caractéristique 2 ayant 2^k éléments.

1) a) On pose $f(x) = x^2 + x$. Montrer que f est un homomorphisme de groupes additifs de $\mathbb{F}_q$ dans lui-même et calculer le cardinal du noyau de f, ensemble des x tels que $f(x) = 0$. En déduire le cardinal de l'image I de f (on utilisera le théorème noyau-image).

b) Pour tout $a \in I$, montrer que

$$\sum_{0 \leq j \leq k-1} a^{2^j} = a + a^2 + a^4 + a^8 + \cdots + a^{2^{k-1}} = 0\ .$$

c) En utilisant le fait que dans un corps commutatif une équation de degré n possède au plus n solutions, en déduire que $a \in I$ si et seulement si $\sum_{0 \leq j \leq k-1} a^{2^j} = 0$.

2) Dans `GP` on représentera le corps $\mathbb{F}_q$ comme $\mathbb{F}_q = (\mathbb{Z}/2\mathbb{Z})[X]/P(X)(\mathbb{Z}/2\mathbb{Z})[X]$, où $P(X)$ est un polynôme irréductible de degré k appartenant à $(\mathbb{Z}/2\mathbb{Z})[X]$. Un tel polynôme est fourni par `GP` grâce à la commande `P=ffinit(2,k)`, et un élément de $\mathbb{F}_q$ est de la forme `Mod(A,P)`, où A est un polynôme de $(\mathbb{Z}/2\mathbb{Z})[X]$ de degré strictement inférieur à k.

a) Grâce à la question 1), écrire un programme `art(k,a)` qui calcule le nombre de solutions $x \in \mathbb{F}_{2^k}$ de l'équation $a = x^2 + x$ (en d'autres termes 2 si $a \in I$ et 0 sinon).

b) Dans $\mathbb{F}_q$ on considère l'équation $y^2 + by + c = 0$. On rappelle (ne pas le redémontrer) que cette équation possède 1 solution dans $\mathbb{F}_q$ si $b = 0$, et sinon possède

2 ou 0 solutions selon que c/b^2 appartient à I ou non. Ecrire un programme `sol(k,b,c)` qui calcule ce nombre de solutions en utilisant le programme `art(k,a)`.

3) On considère une courbe elliptique d'équation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ représenté en `GP` par le vecteur à 5 composantes $e=[a_1,a_2,a_3,a_4,a_6]$.

a) Etant donné $x\in\mathbb{F}_q$, écrire un programme `soly(e,k,x)` prenant comme paramètres la courbe (le vecteur) e, l'entier k tel que $q=2^k$ et l'abcisse (le polynôme modulo) x, et qui calcule le nombre de $y\in\mathbb{F}_q$ tels que le point (x,y) appartienne à la courbe e.

b) Ecrire un programme `comp(e,k)` qui calcule le nombre total de points de la courbe e à coefficients dans $\mathbb{F}_q$, y compris le point à l'infini. Il faudra bien sûr commencer par initialiser le polynôme P grâce à la fonction `ffinit`. La seule difficulté de cette question est d'écrire une boucle qui énumère les éléments de $\mathbb{F}_q$. Pour cela on pourra, soit procéder directement, soit utiliser la commande `forvec`.

4) Application numérique : soit e la courbe elliptique d'équation $y^2+y=x^3$. Ecrire un programme `apnum(k)` qui calcule le nombre de points de e dans $\mathbb{F}_{2^k}$, et calculer ce nombre de points pour $k=8$, $k=9$ et $k=10$.

Exercice II

Soit E une courbe elliptique d'équation $y^2=x^3+ax+b$ sur un corps fini $\mathbb{F}_p$ avec p premier tel que $p\geq 5$. On peut démontrer que le groupe $E(\mathbb{F}_p)$ est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z})\times(\mathbb{Z}/d_2\mathbb{Z})$, où d_1 divise d_2 et $p-1$, et où $\mathbb{Z}/\mathbb{Z}$ est le groupe trivial. En particulier le cardinal $|E(\mathbb{F}_p)|$ est égal à d_1d_2, et le PPCM des ordres des points de $E(\mathbb{F}_p)$ est égal à d_2.

1) Le but de cette question est de calculer l'ordre d'un point dans $E(\mathbb{F}_p)$ de manière pas trop bête. La courbe E sera représentée comme d'habitude par le vecteur $e=[0,0,0,a,b]$, où a et b sont des entiers modulo p.

a) En utilisant la formule

$$|E(\mathbb{F}_p)|=p+1+\sum_{0\leq x\leq p-1}\left(\frac{x^3+ax+b}{p}\right),$$

écrire un programme `card(e,p)` d'une ligne qui calcule $n=|E(\mathbb{F}_p)|$. Attention, la fonction `kronecker(m,p)` de `GP` a besoin d'un `m` qui soit entier, et pas entier modulo.

En particulier, pour tout point $P\in E(\mathbb{F}_p)$, on aura $n\cdot P=O_E$.

b) Soit $P\in E(\mathbb{F}_p)$, et n un entier (pas nécéssairement égal à $|E(\mathbb{F}_p)|$) tel que $n\cdot P=O_E$. Ecrire un programme `ordpart(e,p,P,n)` qui calcule un diviseur premier q de n tel que $(n/q)\cdot P=O_E$ s'il en existe, et qui rend 0 sinon. On rappelle que la liste des diviseurs premiers d'un entier n s'obtient par la commande `factor(n)[,1]`.

c) Ecrire un programme `ord(e,p,P,n)` qui calcule l'ordre d'un point $P\in E(\mathbb{F}_p)$, étant donné le cardinal $n=|E(\mathbb{F}_p)|$ calculé au préalable, par exemple par le programme `card` ci-dessus.

Remarque. Bien sûr on obtient un programme plus efficace en factorisant $|E(\mathbb{F}_p)|$ une seule fois, mais ce n'est pas demandé.

2) a) Ecrire un programme `allord(e,p)` qui calcule le vecteur $[d_1, d_2]$, où d_2 est le PPCM des ordres de tous les points de E et $d_1 = |E(\mathbb{F}_p)|/d_2$ comme ci-dessus. On utilisera les fonctions `GP` suivantes : la fonction `lcm(a,b)` qui calcule le PPCM de a et b, et la fonction `ellordinate(e,x)` qui calcule le vecteur des ordonnées y telles que $(x, y) \in P$ (ce vecteur étant donc de longueur 0, 1 ou 2). Les points correspondants sont donc `[x,ellordinate(e,x)[j]]` pour j allant de 1 à la longueur de `ellordinate(e,x)`.

b) Application numérique : Soit E la courbe d'équation $y^2 = x^3+1$. Calculer $[d_1, d_2]$ pour $p = 1201$, 1453 et 1723.