UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2004–2005

Mastère CCSI 2

Méthodes mathématiques de la cryptologie

Epreuve de TP du vendredi 21 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-bordeaux1.fr`

Indication préliminaire. Si $q = p^k$ est une puissance d'un nombre premier p on représentera dans `GP` le corps $\mathbb{F}_q$ comme $\mathbb{F}_q = (\mathbb{Z}/p\mathbb{Z})[X]/P(X)(\mathbb{Z}/p\mathbb{Z})[X]$, où $P(X)$ est un polynôme irréductible de degré k appartenant à $(\mathbb{Z}/p\mathbb{Z})[X]$. Un tel polynôme est fourni par `GP` grâce à la commande `P=ffinit(p,k)`, et un élément de $\mathbb{F}_q$ est de la forme `Mod(A,P)`, où A est un polynôme de $(\mathbb{Z}/p\mathbb{Z})[X]$ de degré strictement inférieur à k. Pour vous familiariser avec cette commande regardez par exemple le résultat de `ffinit(2,4)` et de `ffinit(5,3)`.

Exercice I

Le but de cet exercice est d'écrire un programme complètement général qui calcule (de manière naïve) le nombre de points d'une courbe elliptique sur un corps fini de caractéristique 2. Soit donc $q = 2^k$ avec $k \geq 1$ et $\mathbb{F}_q = \mathbb{F}_{2^k}$ le corps de caractéristique 2 ayant 2^k éléments.

On appellera G l'ensemble des $y^2 + y$ pour $y \in \mathbb{F}_q$, et on admettra le résultat suivant: $z \in G$ si et seulement si $\sum_{0 \leq j \leq k-1} z^{2^j} = 0$.

1) a) Grâce àu résultat admis, écrire un programme `art(k,z)` qui calcule le nombre de solutions $x \in \mathbb{F}_q$ de l'équation $z = x^2 + x$ (en d'autres termes 2 si $z \in G$ et 0 sinon). On représentera bien sûr $\mathbb{F}_q$ comme expliqué dans l'indication préliminaire.

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,z)`.

2) On considère une courbe elliptique d'équation $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ représentée 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 `soly2(e,k,x)` prenant comme paramètres la courbe (le vecteur) e, l'entier k tel que $q = 2^k$ et l'abcisse x (en tant que polynôme modulo), 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 `comp2(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`.

3) Application numérique : soit e la courbe elliptique d'équation $y^2 + xy = x^3 + x$ (qui est de discriminant $-63 \neq 0$ comme on l'a vu en devoir). Ecrire un programme `apnum2(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 $p \geq 5$, et soit $q = p^k$. Le but de cet exercice est identique au précédent, à savoir le calcul de $|E(\mathbb{F}_q)|$, mais le fait que $p \geq 5$ change les algorithmes.

1) a) On rappelle que l'équation $y^2 = z$ dans $\mathbb{F}_q$ possède 1 solution si $z = 0$, et sinon possède 2 ou 0 solutions selon que $z^{(q-1)/2} = 1$ ou non. Ecrire un programme `kum(p,k,z)` qui calcule ce nombre de solutions, en supposant bien sûr que z est représenté comme élément de $\mathbb{F}_q$ comme expliqué dans la question préliminaire.

b) Etant donné $x \in \mathbb{F}_q$, écrire un programme `solyp(e,p,k,x)` prenant comme paramètres la courbe e (c'est à dire le vecteur $[0, 0, 0, a, b]$), l'abcisse x (en tant que polynôme modulo), et qui calcule le nombre de $y \in \mathbb{F}_q$ tels que le point (x, y) appartienne à la courbe e.

c) Ecrire un programme `compp(e,p,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.

2) Applications numériques : soit e la courbe elliptique d'équation $y^2 = x^3 + x + 1$, qui est de discriminant $-496 = -2^4 \cdot 31$.

a) Calculer $|E(\mathbb{F}_p)|$ et $|E(\mathbb{F}_{p^2})|$ pour $p = 101$, 103, 107 et 109. Dans chacun de ces cas, calculer

$$u = \frac{|E(\mathbb{F}_p^2)| + |E(\mathbb{F}_p)|^2}{2|E(\mathbb{F}_p)|} .$$

Que constate-t-on ?

b) Calculer $|E(\mathbb{F}_{5^k})|$ pour $1 \leq k \leq 5$, puis $u_k = 5^k + 1 - |E(\mathbb{F}_{5^k})|$.

c) Calculer $(u_{k+1} - u_1u_k)/u_{k-1}$ pour $2 \leq k \leq 4$. Que constate-t-on ?