UFR de Mathématiques et Informatique
Université Bordeaux I Année 2005–2006

Mastère CCSI 2

Méthodes mathématiques de la cryptologie

Epreuve de TP du jeudi 8 décembre 2005

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.

On prendra particulièrement soin de distinguer dans le programme les éléments de $\mathbb{Z}$, de $\mathbb{Z}/p\mathbb{Z}$ (représentés comme `Mod(a,p)`) et de $\mathbb{F}_q$ (représentés comme ci-dessus).

Exercice I

Soit p un nombre premier supérieur ou égal à 5, et soit E une courbe elliptique définie sur $\mathbb{Q}$ d'équation $y^2 = x^3 + ax + b$ avec a et b dans $\mathbb{Z}$. On supposera que $p \nmid (4a^3 + 27b^2)$, et on peut considérer E comme une courbe elliptique sur $\mathbb{F}_p$. Toutefois attention, dans ce cas dans le programme ne pas oublier de multiplier a et b par `Mod(1,p)`.

1) Soit p un nombre premier, $k \geq 1$, et `z=Mod(A,P)` un élément de $\mathbb{F}_{p^k}$ représenté comme ci-dessus. On rappelle que le nombre de solutions de l'équation $y^2 = z$ dans $\mathbb{F}_{p^k}$ est égal à 1 si $y = 0$, à 2 si $z^{(p^k-1)/2} = 1$, et à 0 si $z^{(p^k-1)/2} = -1$ dans $\mathbb{F}_{p^k}$. Attention, il y a un piège, il ne faudra pas écrire `==-1` car -1 n'est pas représenté comme tel dans $\mathbb{F}_{p^k}$.

a) Ecrire un programme `kropk(z,p,k)` qui détermine le nombre ci-dessus. On fera attention au piège indiqué, et on vérifiera que $z^{(p^k-1)/2}$ est bien égal à 0, 1 ou -1 dans $\mathbb{F}_{p^k}$, sinon on renvoie une erreur avec la fonction `error` (important dans la phase de debogage, pas après).

b) Ecrire un programme `compte(E,p,k)` qui calcule naivement le nombre de points de la courbe elliptique E sur le corps fini $\mathbb{F}_{p^k}$ (y compris le point à l'infini). Pour celà, on rappelle qu'il faut utiliser la commande `forvec` pour balayer les éléments de $\mathbb{F}_{p^k}$, et que les coefficients des polynômes vont de 0 à $p-1$ modulo p. Il faudra que ce programme comprenne la commande `ffinit` pour initialiser le corps $\mathbb{F}_{p^k}$. La courbe E sera simplement représentée par un vecteur `[a,b]`.

2) Application numérique: choisissez comme valeur de a votre mois M de naissance (de 1 à 12), et comme valeur de b votre jour de naissance (de 1 à 31) que vous indiquerez bien sûr. Enfin, soit p le plus petit nombre premier supérieur ou égal à 5 qui ne divise pas $4a^3+27b^2$ (calculez le et indiquez le).

On définit la fonction `ap(E,p,k)=p^k+1-compte(E,p,k)`.

a) Calculer $a(k) =$ `ap(E,p,k)` pour la courbe `E` et le nombre premier `p` ci-dessus, pour `k` prenant les valeurs 1, 2, 3, etc..., jusqu'à ce que le temps d'execution du programme soit supérieur à une vingtaine de secondes. Indiquez les résultats, et le temps approximatif en secondes.

b) Calculer $(a(k+1)-a(1)a(k))/a(k-1)$ pour les valeurs de $k \geq 2$ que vous avez pu calculer. Que constate-t-on ?

c) Recommencer les calculs ci-dessus avec la même courbe E mais le nombre premier qui suit celui que vous venez de choisir, toujours ne divisant pas $4a^3+27b^2$. Essayez d'autres nombres premiers si vous avez le temps.

Exercice II

On se propose d'établir une liste aussi grande que possible d'entiers n tels que $1 \leq n \leq 100$ qui sont somme de deux cubes de nombres rationnels c'est-à-dire pour lesquels il existe des *entiers* u, v et d tels que $d \geq 1$ et $n = (u/d)^3 + (v/d)^3$, soit encore $u^3+v^3 = nd^3$. Quitte à diviser u et v par un facteur commun, on peut supposer que n n'est pas divisible par un cube autre que 1.

1) En utilisant la fonction `factor` de `GP`, écrire un programme `enlevercub(n)` qui étant donné un entier strictement positif m renvoie l'unique entier positif n qui n'est pas divisible par un cube autre que 1 et tel que $m = nd^3$ pour un entier d convenable (ceci consiste à réduire les exposants modulo 3).

2) a) Ecrire un programme `sum2cub(L)` qui trouve tous les entiers $n \in [1, 100]$ non divisible par un cube autre que 1 de la forme $(u^3+v^3)/d^3$, avec $1 \leq u \leq L$ et $1-u \leq v \leq u-1$ (il est facile de voir qu'il suffit de se limiter à ces inégalités). Pour celà, on calculera n par la formule `n=enlevercub(u^3+v^3)`. On pourra aussi si on le désire accélerer les calculs en ne considérant que les couples u et v premiers entre eux.

b) Ecrire une légère modification `sum2cubplus(L)` du programme ci-dessus (tout en le gardant), où on se restreint à des cubes de nombres rationnels positifs, donc où la seule différence avec le programme précédent est que v varie de 0 à $u-1$.

3) Applications numériques.

a) Donner le nombre de n obtenus en choisissant `L=500` dans chacun des deux programmes ci-dessus.

b) Même question pour `L=1000`, et si vous le pouvez, pour `L=2000` (ce dernier peut prendre plusieurs minutes).

c) En utilisant ces résultats, exprimer 19 comme somme de deux nombres rationnels (de signe quelconque), 15 comme somme de deux nombres rationnels positifs, et enfin (si votre programme a pu aller jusqu'à 2000), 33 comme somme de deux nombres rationnels positifs.

Exercice III

Soit p un nombre premier supérieur à 10^6, et soit E la courbe elliptique déjà considérée à l'exercice I, d'équation $y^2 = x^3 + ax + b$, où a et b sont votre mois et jour de naissance.

1) En utilisant la formule

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

qui se programme en une ligne de `GP` (le symbole de Legendre étant appelé `kronecker`), calculer le nombre de points de $E(\mathbb{F}_p)$ pour $p = 1000003$ (`nextprime(10^6)`), ainsi que le temps nécéssaire (quelques secondes, mais pas immédiat).

2) On se propose de faire beaucoup mieux.

a) Initialisez votre courbe par la commande `e=ellinit(Mod(1,p)*[0,0,0,a,b],1)`. La fonction `ellordinate(e,x)` vous permet alors, si `x` est un entier modulo p, de trouver le vecteur (de longueur 0, 1 ou 2) des ordonnées possibles correspondant à l'abcisse x. Trouver ainsi au moins 3 points modulo p sur votre courbe personelle.

b) D'après le théorème de Hasse, $p + 1 - 2\sqrt{p} < |E(\mathbb{F}_p)| < p + 1 + 2\sqrt{p}$. D'autre part si $P \in E(\mathbb{F}_p)$ on doit avoir $n \cdot P = \mathcal{O}$, où $n = |E(\mathbb{F}_p)|$ et $\mathcal{O}$ est le point à l'infini, caractérisé je le rappelle comme étant le seul point de longueur 1. Soit P un des points modulo p que vous avez calculés. On commence par calculer $Q = p \cdot P$ (par la commande `ellpow(e,P,p)`), puis par addition et soustraction successive de P (mais sans puissances supplémentaires), calculer $Q + kP$ pour $k = 0, \pm 1$, etc... jusqu'à $k = \pm\lfloor 2\sqrt{p} \rfloor$. Si exactement l'un des ces points est le point à l'infini, on a gagné, on a $|E(\mathbb{F}_p)| = p + k$. Si aucun de ces points ne l'est, il y a une erreur dans le programme. Enfin, si plus d'un point est à l'infini on ne peut pas conclure, et il faut recommencer avec un autre point P.

Ecrire un programme `comp(e,p)` effectuant les opérations ci-dessus, et qui retourne soit $|E(\mathbb{F}_p)|$, soit un message d'erreur si on n'y est pas arrivé au bout de trois essais.

c) Executer ce programme, vérifier qu'on trouve bien le même résultat qu'en 1), et que le temps d'éxecution est complètement négligeable. Si vous avez le temps, essayez `p=nextprime(10^7)`, etc...