UFR de Mathématiques et Informatique
Université Bordeaux I Année 2002–2003

DESS CCSI

Méthodes mathématiques de la cryptologie

Epreuve de TP du mardi 10 Décembre 2001

Durée 2 heures

On rédigera tous les programmes demandés en GP, et on enverra aussi bien les programmes, les commentaires et démonstrations éventuelles et les résultats par mail à
`cohen@math.u-bordeaux.fr`

Exercice I

Le but de cet exercice est de répondre au défi de Fermat de trouver deux nombres **rationnels positifs** autres que $(2,1)$ et $(1,2)$ vérifiant $x^3+y^3=9$. Comme celà ne coûte pas plus cher, nous choisirons un entier $d>0$ et nous travaillerons plus généralement sur la courbe E_d d'équation $x^3+y^3=d$.

1) a) Ecrire une fonction `rac(t)` qui étant donné $t\in\mathbb{R}$ renvoie son unique racine cubique réelle. Attention, quand $t<0$, la fonction `t^(1/3)` de GP renvoie un nombre complexe, donc on ne doit l'utiliser que pour un $t\geq 0$.

b) Tracer le graphe de E_d et de son asymptote en utilisant la commande suivante (pour $d=1729$) :

```
ploth(x=-30,30,[rac(1729-x^3),-x])
```

Observer (ne rien démontrer bien sûr) où se trouvent les points d'inflexion, les points à tangente horizontale, verticale, et parallèle à l'asymptote, et noter les résultats de vos observations sur votre fichier.

2) a) Remarquer que les points $(x_1,y_1)=(10,9)$ et $(x_2,y_2)=(12,1)$ se trouvent sur la courbe E_{1729} ci-dessus. Calculer (à la main!) l'équation $y=mx+b$ de la droite qui joint ces deux points.

b) En remplaçant dans l'équation de E_{1729}, en déduire les coordonnées du troisème point d'intersection de la droite avec E_{1729}. Pour celà, on écrira explicitement l'équation du troisème degré satisfaite par les abcisses, et on la résoudra en utilisant la commande `factor` de GP, qui s'applique aussi à des polynômes.

3) On va maintenant systématiser la construction ci-dessus. On appelle O_E le point à l'infini de la courbe, qu'on représentera comme d'habitude en machine par le vecteur à

une composante `[0]`. La méthode de la sécante et tangente de Fermat sur la courbe E_d donne la loi de composition suivante, exprimée sous forme d'algorithme.

• Si $P_1 = O_E$, on retourne $P_1 + P_2 = P_2$. Si $P_2 = O_E$, on retourne $P_1 + P_2 = P_1$. Sinon, on pose $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$.

• Si $x_2 = x_1$ on pose $m = -x_1^2$ et $n = y_1^2$, sinon on pose $m = y_2 - y_1$ et $n = x_2 - x_1$.

• Si $m = -n$, on retourne $P_1 + P_2 = O_E$. Si $n = 0$, on retourne $P_1 + P_2 = (0, x_1)$. Dans les autres cas, on pose

$$\begin{cases} y_3 & = -x_1 - x_2 + \dfrac{3m^2(mx_1 - ny_1)}{m^3 + n^3} \\ x_3 & = \dfrac{m}{n}(y_3 - x_1) + y_1 \end{cases}$$

et on retourne $P_1 + P_2 = (x_3, y_3)$.

a) Programmer cet algorithme en GP. Puisqu'il ne dépend pas explicitement de la constante d, inclure une vérification que les points P_1 et P_2 (quand ils sont différents de O_E) sont bien sur la même courbe E_d. Vérifier votre implantation sur l'exemple de la question 2) (le point trouvé aura ses coordonnées échangées, c'est normal).

b) Indiquer sur votre fichier votre jour J et mois M de naissance, prendre $d = J^3 + M^3$ et le point $P_1 = (J, M)$ sur la courbe E_d. Grâce à l'implantation ci-dessus, calculer successivement $2P_1$, $3P_1$, $4P_1$. Que constatez vous ?

4) On va résoudre problème de Fermat $x^3 + y^3 = 9$, étant donné le point $P_1 = (2, 1)$ sur la courbe E_9. Calculer les multiples successifs de $2P_1$, $3P_1$, etc... jusqu'à en obtenir un dont les **deux** coordonnées soient positives. Compter le nombre de chiffres des numérateurs et dénominateurs du résultat (on peut montrer que ce sont les plus petits possibles).

5) (Cette question est complètement indépendante des autres.) Le nombre $n = 9$, ainsi que le nombre $n = 1729$ sont somme de deux cubes de nombres rationnels (en fait entiers) positifs ou nuls. Il est clair que si n possède cette propriété, tous les nombres de la forme nk^3 aussi. On peut donc supposer n sans facteur cubique plus grand que 1. Ecrire (ici sans être guidé) un programme GP qui trouve une liste de tels nombres entiers inférieurs ou égaux à 100. Pour chacun des nombres n obtenus, on écrira une décomposition $n = u^3 + v^3$ avec u et v nombres rationnels (non nécéssairement entiers) **positifs**. Le nombre de tels n n'est pas le plus important, mais plutôt la correction (bien entendu) et l'élégance du programme.

Question facultative : si votre programme est suffisamment efficace, trouver deux nombres rationnels positifs u et v tels que $u^3 + v^3 = 30$, puis tels que $u^3 + v^3 = 33$ (ce n'est pas si facile, donc ne perdez pas trop de temps, ni CPU ni le votre).

Exercice II

Soient toujours J votre jour de naissance et M votre mois de naissance. On considère la courbe elliptique E d'équation

$$y^2 = x^3 + Jx + M$$

et un corps fini $\mathbb{F}_q$ avec q de la forme p^k avec $p \geq 5$.

1) On rappelle que si $A = 0$ l'équation $y^2 = A$ a 1 solution dans $\mathbb{F}_q$, et sinon elle a 2 ou 0 solutions selon que $A^{(q-1)/2} = 1$ ou non. Ecrire un programme calculant ce nombre de solutions, en supposant que A est bien donné comme élément de $\mathbb{F}_q$.

2) On considère le cas particulier $q = p^2$. Les ééments de $\mathbb{F}_q$ seront alors représentés en GP par des expressions du type

```
Mod(Mod(a,p)*x+Mod(b,p),x^2-Mod(d,p))
```

où d est un entier ordinaire vérifiant `kronecker(d,p)==-1`.

Ecrire un programme GP qui calcule le nombre de points de E (y compris le point à l'infini) sur un corps $\mathbb{F}_{p^2}$. Ce programme devra bien entendu commencer par calculer un d convenable, que l'on garde ensuite une fois pour toutes.

3) Applications numériques :

a) Pour $p = 101$, 103, 107 et 109, calculer le nombre de points de E à coefficients dans $\mathbb{F}_{p^2}$.

b) Pour les mêmes valeurs de p, calculer le nombre de points de E à coefficients dans le corps plus simple $\mathbb{F}_p$ en utilisant la formule démontrée en cours

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