Université Bordeaux 1 — **MHT814 – Courbes Elliptiques**
Mathématiques — Année 2012–2013

Examen, Jeudi 23 Avril 2009 (14:00 – 17:00)
Durée 3 heures. Notes de cours et programmes GP autorisés.

Clarté des programmes et pertinence des commentaires sont des éléments importants d'appréciation.

- Pour répondre aux questions, créer *un* fichier par exercice, intitulés `login1.gp` et `login2.gp`. Par exemple, `kbelabas1.gp`. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans les fichiers `login1.gp` et `login2.gp`.
- Pour rendre votre copie, taper `~kbelabas/copie` dans un terminal, depuis le répertoire où se trouvent vos fichiers. (Vous pouvez rendre plusieurs fois votre copie : seule la dernière fait foi, les précédentes sont détruites.)

Vous pouvez utiliser les deux techniques suivantes :

- utiliser `allocatemem` pour augmenter la mémoire allouée à gp.
- Vous pouvez compiler le fichier `nom.gp` et imprimer les résultats dans le fichier `result` en exécutant la commande `gp < nom.gp > result 2>&1`.

Exercice 1 –

1) Écrire un programme prenant en entrée un entier $k > 0$ et donnant en sortie un nombre premier p de k bits (soit $2^{k-1} \leqslant p < 2^k$).

2) Écrire un programme prenant en entrée un nombre premier p et donnant en sortie une courbe elliptique E sur $\mathbb{F}_p$ telle que $E(\mathbb{F}_p)$ soit *cyclique*, ainsi qu'un générateur de ce groupe.

3) Écrire un ensemble de fonctions implantant un cryptosystème d'ElGamal sur les points d'une courbe elliptique $E/\mathbb{F}_p$ (chiffrement, déchiffrement, signature).
[*On supposera que le message à transmettre est un point de $E(\mathbb{F}_p)$, et on omettra le hachage destiné à assurer l'intégrité du message. Commenter le choix des paramètres.*]

Exercice 2 – Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ où q est un nombre *premier*. Soient $P, Q \in E(\mathbb{F}_q)$, où P est d'ordre n et Q est dans le sous-groupe engendré par P ; on cherche à résoudre le problème du logarithme discret :

$$Q = [m]P,$$

où on désire déterminer $m \in \mathbb{Z}/n\mathbb{Z}$. On appelle *ordre* du logarithme discret l'ordre n du point P.

1) Soit p un diviseur premier de n. La valeur de m modulo p, notée m_1, est donnée par la résolution du problème du logarithme discret

$$Q_1 = [m_1]P_1, \qquad \text{où} \quad P_1 = \left[\frac{n}{p}\right] P, \quad Q_1 = \left[\frac{n}{p}\right] Q,$$

et P_1 est d'ordre p.

a) On écrit la division euclidienne $m = pm_0 + m_1$ (où m_1 est maintenant connu), montrer que m_0 est solution d'un problème de logarithme discret d'ordre n/p.

b) Implanter l'algorithme correspondant, en utilisant une fonction « boite noire » capable de résoudre les logarithmes discrets d'ordre un nombre premier.

2) Soient $p = 10^{18} + 3$ et E la courbe elliptique sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + 2$.

a) Calculer $\#E(\mathbb{F}_p)$.

b) Trouver un point $P_d \in E$ pour chacun des ordres possibles $d \mid \#E(\mathbb{F}_p)$.

3) Montrer qu'il existe deux points d'abscisse 2 dans $E(\mathbb{F}_p)$. Quel sont leurs ordres ? Choisissez l'un d'entre eux, noté P dans la suite.

4) Montrer que $Q = (6, 181579992970505432)$ est sur E.

5) Résoudre le problème du logarithme discret sur E

$$Q = [m]P.$$

6) Trouver des valeurs de p, E, P, Q pour lesquelles les programmes écrits ci-dessus ont des difficultés. Expliquez-les.