Université Bordeaux 1 — **MHT911 – Algorithmique**
Mathématiques — Année 2012–2013

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

La clarté des programmes et la pertinence des commentaires est un élément important d'appréciation.

- Créer un fichier par exercice, intitulés `login1.gp`, `login2.gp`, etc.
- 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.)

Exercice 1 – Donner une preuve de primalité ($p-1$ ou méthode des courbes elliptiques) des entiers N suivants :

$$10^{51} - 323, \quad 10^{101} - 203, \quad 10^{199} - 9.$$

Exercice 2 – On fixe un entier m, dont on désire qu'il soit le cardinal d'une courbe elliptique E sur un corps fini $\mathbb{F}_p$.

1) a) Écrire un programme trouvant le nombre premier p le plus proche de $m-1$.
b) Lui faire vérifier que la borne de Hasse n'exclut pas qu'il existe $E/\mathbb{F}_p$ de cardinal m.

2) Écrire un programme naïf, tirant E au hasard jusqu'à ce que $\#E(\mathbb{F}_p) = m$.

3) Trouver une courbe E explicite de cardinal $m = 2009$. Quelle est la structure de $E(\mathbb{F}_p)$?

4) a) Même question pour $m = 17122009$. On étudie maintenant cette courbe E.
b) Trouver un point P d'ordre maximal o dans $E(\mathbb{F}_p)$.
c) Ecrire un programme de calcul de log discret de base P, i.e. qui pour $Q \in \langle P \rangle$ retourne l'unique $x \in \mathbb{Z}/o\mathbb{Z}$ tel que $Q = [o]P$.

Exercice 3 – On *admet* que pour toute courbe elliptique $E/\mathbb{F}_p$ on a

$$\#E(\mathbb{F}_{p^k}) = p^k + 1 - \alpha^k - \beta^k, \quad k \geqslant 1,$$

où α, β sont les deux racines complexes d'un polynôme quadratique $X^2 - sX + p$, $s \in \mathbb{Z}$.

1) D'après le cours, quelle inégalité vérifie s ?

2) Soit E la courbe elliptique d'équation $y^2 = x^3 + 1$ sur $\mathbb{F}_5$. Compter naïvement les points de E dans $\mathbb{F}_{5^k}$ pour $k = 1, 2, \ldots, 10$.

3) Écrire la formule générale pour $\#E(\mathbb{F}_{5^k})$ et la simplifier.

4) Donner la structure de $E(\mathbb{F}_{5^k})$ pour $k \leqslant 10$.