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

Partiel, 09 novembre 2007 (10:15 – 12:15)
Durée 2 heures. Notes de cours et programmes GP autorisés.

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

- Pour répondre aux questions, créer *un* fichier par exercice, intitulés *login*`1.gp`, *login*`2.gp`, etc. Par exemple, `kbelabas1.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.)

Exercice 1 – Soit $E : y^2 = x^3 + x + 5$ définie sur $\mathbb{F}_p$, où $p = 2^{200} + 235$. Utilisant `ellsea`, le cardinal[1] de la courbe

$$\#E(\mathbb{F}_p) = 1606938044258990275541962092339608375719161870554903347117269$$

est de la forme $3 \times p_9 \times p_{51}$, où p_i désigne un nombre premier de i chiffres décimaux.

1) Trouver 3 points d'ordres respectifs 3, p_9 et p_{51} dans $E(\mathbb{F}_p)$.

2) On désire construire un cryptosystème de type ElGamal à l'aide de la courbe. Quelles données utiliser ? [*décrire rapidement ; ne pas programmer le chiffrage/déchiffrage*] Évaluer sa sécurité.

3) En admettant que 3, p_9, p_{51} et p sont effectivement premiers, démontrer directement que le résultat de `ellsea` est effectivement correct [*Utiliser 1) et la borne de Hasse.*]

Exercice 2 –

1) Un crible d'Ératosthène naïf calcule les premiers $\leqslant B$, sous la forme d'un tableau T de longueur B tel que $T[i] = 1$ ssi i est premier. Pour chaque premier p consécutif le crible met $T[i]$ à 0 grâce à une boucle de type `forstep(i = p^2, B, p, T[i] = 0)`. Programmer un tel crible.

2) À condition de ne pas oublier de rajouter 2, il n'est pas utile de considérer les nombres pairs. Écrire un nouveau programme fournissant un tableau T de taille $\approx B/2$ tel que $T[i] = 1$ ssi $2i + 1$ est premier. Noter que si $p \geqslant 3$ est premier, p^2 est impair et les $i = p^2 + p$, $p^2 + 3p$, $p^2 + 5p$ ... sont pairs, donc sans intérêt. Quel gain espérer par rapport au 1) ?

3) Poursuivons : on fixe δ inversible mod $30 = 2 \times 3 \times 5$. Obtenir la liste des premiers de la forme $30i + \delta$, par un tableau T (de taille $\approx B/30$) tel que $T[i] = 1$ ssi $30i + \delta$ est premier. Quel gain espérer ?

★ **4)** Peut-on généraliser et continuer à gagner ?

[1] disponible dans `~kbelabas/ordre` si vous n'arrivez pas à le reproduire