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

Devoir Surveillé, Jeudi 02 Avril 2009 (16:15 – 18:15)
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 `login1.gp`, `login2.gp`. Par exemple, `gricotta1.gp`.
- Pour rendre votre copie, taper `~gricotta/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 – Une **représentation binaire signée** d'un entier relatif n est la donnée d'un vecteur $S = [s_0, \ldots, s_q]$ satisfaisant

$$n = \sum_{j=0}^{q} s_j 2^j$$

où $s_j \in \{-1, 0, +1\}$ pour $0 \leqslant j \leqslant q$. Une telle représentation binaire signée est dite **creuse** si

$$\forall j \in \{0, \ldots, q-1\}, \quad s_j s_{j+1} = 0.$$

Vous **admettrez** que tout entier relatif admet une unique représentation binaire signée creuse.

1) Ecrire une procédure *basesignee(n)* qui, étant donné l'entier naturel n, renvoie la représentation binaire signée creuse de n sous la forme d'un vecteur $S = [s_0, \ldots, s_q]$.
Indication :

- vous connaissez la représentation binaire de n ;
- une procédure récursive devrait permettre de décaler vers la droite les bits consécutifs de 1 dans cette représentation binaire de n c'est-à-dire remplacer les séquences $[1, 1]$ par $[-1, 0, 1]$.

2) Ecrire une procédure *powsignee(n,E,P)* qui, étant donnés un entier naturel n, une courbe elliptique E sur un corps fini et un point P sur E, renvoie le point $[n]P$ et le nombre total d'additions et de soustractions réalisées sur la courbe elliptique. Cette procédure doit **obligatoirement** utiliser la représentation binaire signée creuse de n.

3) Tester sur de nombreux exemples. Limite de la méthode ?

Exercice 2 – Soit E la courbe elliptique sur $\mathbb{F}_q$ où $q = 10^{17}+19$ est un nombre **premier** d'équation

$$y^2 = x^3 + 1$$

et

$$\begin{aligned} P &= [72099116723710135, 13462105356828521], \\ Q &= [35311982324987694, 4803038159023948]. \end{aligned}$$

Résoudre le problème du logarithme discret

$$Q = [m]P.$$

Indication :

- vous pourriez vérifier que P et Q sont deux points de E ;
- vous pourriez vous souvenir qu'il suffit de connaître m modulo $n(P)$ où $n(P)$ est l'**ordre** de P ;
- vous pourriez calculer $n(P)$ en utilisant la méthode Pas de bébés-Pas de géants ;
- vous pourriez finalement résoudre ce problème du logarithme discret sachant que si p est un diviseur premier de $n(P)$ alors

  $$Q_p = [m_p]P_p$$

  où

  $$\begin{aligned} P_p &= \left[\frac{n(P)}{p}\right] P, \\ Q_p &= \left[\frac{n(P)}{p}\right] Q. \end{aligned}$$