Université de Bordeaux
Mathématiques

MHT814 – Courbes Elliptiques
2022–2023

Devoir Surveillé, Jeudi 20 Mars 2008 (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` et `login2.gp`. Par exemple, `gricotta1.gp`. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans les fichiers `login1.gp` et `login2.gp`.

Vous pouvez utiliser les deux astuces 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 – Une *représentation binaire signée* d'un entier relatif n est la donnée d'un vecteur $S = [s_0, \ldots, s_q]$ satisfaisant

$$n = \sum_{j=0}^{q} s_j 2^j, \qquad \text{où } s_j \in \{-1, 0, +1\} \text{ pour } 0 \leqslant j \leqslant q.$$

Une telle représentation est dite *creuse* si

$$s_j s_{j+1} = 0 \qquad \text{pour tout } j \in \{0, \ldots, q-1\}.$$

Tout entier relatif admet une unique représentation binaire signée creuse [*admis*].

1) Lors du TD1, vous avez écrit une procédure `base(n,2)` renvoyant l'écriture binaire d'un entier naturel $n > 0$ sous la forme d'un vecteur $B = [n_0, \ldots, n_q]$ i.e.

$$n = \sum_{j=0}^{q} n_j 2^j, \qquad \text{où } n_j \in \{0, +1\} \text{ pour } 0 \leqslant j < q, \text{ et } n_q = 1.$$

Faites très attention à l'ordre des bits, au cas où votre procédure `base(n,2)` renvoie le vecteur $[n_q, \ldots, n_0]$. Ecrire une procédure `basesignee(n)` qui, étant donné le vecteur $B = [n_0, \ldots, n_q]$, renvoie la représentation binaire signée creuse de n ie le vecteur $S = [s_0, \ldots, s_{q+1}]$ de longueur $q + 1$. [*Il s'agit d'éliminer les bits consécutifs de* 1 *dans l'écriture binaire de* n *en les décalant vers la droite via*

$$2^i + 2^{i+1} = -2^i + 2^{i+2}.$$

On applique cette formule pour le premier indice j noté j_0 satisfaisant $n_j n_{j+1} = 1$ puis on applique de facon récursive la même procédure à

$$\frac{1}{2^{j_0+2}}\left(n - \sum_{j=0}^{n_{j_0}-2} n_j 2^j + 2^{j_0}\right).$$

Traiter des exemples à la main pour comprendre ce qui se passe !]

2) Ecrire une procédure `pow(E,P,n)` 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 d'additions réalisées sur la courbe elliptique. Cette procédure doit obligatoirement utiliser la représentation binaire de n.

3) Ecrire une procédure `powsignee(E,P,n)` 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.

4) Soient E_1 la courbe elliptique d'équation $y^2 = x^3 + 146x + 33$ sur $\mathbb{F}_{173}$ et $P_1 = (168, 133)$. Comparer les différentes méthodes de calcul de $[n]P_1$ vues dans cet exercice. Quelle est la limite de chacune de ces méthodes ?

5) Soient E_2 la courbe elliptique d'équation $y^2 = x^3 + x + T^4$ sur $\mathbb{F}_{2^7} \simeq \mathbb{F}_2[T]/(Q(T))$ et $P_2 = (0, T^2)$. Comparer les différentes méthodes de calcul de $[n]P_2$ vues dans cet exercice. Quelle est la limite de chacune de ces méthodes ?

Exercice 2 – Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ où q est un nombre *premier*, sur laquelle on cherche à résoudre le problème du logarithme discret

$$Q = [m]P.$$

1) Justifier qu'il suffit de trouver la valeur de m modulo l'ordre de P noté n. Dans la suite, l'ordre du problème du logarithme discret est par définition l'ordre du point P.

2) Soit p un diviseur premier de n. Montrer que la valeur de m modulo p notée m_1 est donnée par la résolution du problème du logarithme discret

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

Montrer également que P_1 est d'ordre le nombre premier p.

3) Justifier l'assertion suivante : «*Pour résoudre un problème de logarithme discret d'ordre un entier $n > 1$, il suffit de savoir résoudre un nombre fini de problèmes de logarithme discret d'ordres des nombres premiers*».

4) Ecrire une procédure `babygiant(E,P,Q)` qui, étant donnés une courbe elliptique E sur un corps fini et deux points P et Q sur E, résoud le problème du logarithme discret

$$Q = [m]P.$$

Cette procédure doit reposer sur la méthode Pas de bébés-Pas de géants. [*Les bornes de Hasse vous permettent de déterminer un encadrement pour m modulo l'ordre de P.*]

5) Ecrire une procédure `ordrepoint(E,P,m)` qui, étant donnés une courbe elliptique E sur un corps fini et un point P sur E et un multiple m de l'ordre de P, renvoie l'ordre de P. [*Penser au théorème de Lagrange.*]

6) Ecrire une procédure `pollard(E,P,Q)` qui, étant donnés une courbe elliptique E sur un corps fini et deux points P et Q sur E, résoud le problème du logarithme discret

$$Q = [m]P.$$

Cette procédure doit reposer sur la méthode ρ de Pollard.

7) Soient $p = 10^{17} + 19$ et E_3 la courbe elliptique sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + 1$.

8) Montrer que $P = (9, 8813406397027940)$ est sur E_3 et trouver son ordre.

9) Montrer que $Q = (53068001696790685, 87339153641111313)$ est sur E_3.

10) Résoudre le problème du logarithme discret sur E_3

$$Q = [m]P.$$

[*Penser à la question 3.*]