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

**Examen, 17 avril 2008 (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` 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.)

Dans tout le texte, $D$ est un entier négatif, congru à 0 ou 1 modulo 4 et $p > 3$ désigne un nombre premier. Une fois fixé $D, p$ comme ci-dessus, on note $(*)$ l'équation

$$(*) \qquad U^2 - DV^2 = 4p,$$

où $U, V \in \mathbb{Z}$ sont des inconnues.

**Exercice 1** – La fonction `qfbsolve(Q,p)` résoud l'équation $Q(U,V) = p$, où $Q(x,y) = ax^2 + bxy + cy^2$ est une forme quadratique binaire, créée par `Qfb(a,b,c)`.

**1)** Rédiger un programme de résolution de $(*)$ dans le cas $D \equiv 0 \pmod 4$. On pourra utiliser `qfbsolve` et `Qfb(1,0,-D/4)`.

**2)** En remarquant qu'une solution de $U^2 - DV^2 = 4p$ où $U$ et $V$ sont de même parité est de la forme $(U,V) = (2x + y, y)$, écrire un programme de résolution de $(*)$ pour $D \equiv 1 \pmod 4$. On pourra utiliser `qfbsolve` et `Qfb(1,1,(1-D)/4)`.

**Exercice 2** – Soit $m = p + 1 - U$, un cardinal possible pour le cardinal $\#E(\mathbb{F}_p)$ d'une courbe elliptique $E/\mathbb{F}_p$, c'est-à-dire que $|U| < 2\sqrt{p}$.

**1)** Rédiger un programme trouvant $D < 0$ de valeur absolue minimale, tel que l'équation $(*)$ admette une solution $(U,V)$, dont la première coordonnée est $U = p + 1 - m$. On pourra utiliser `coredisc`.

**2)** Pour un tel $D$, obtenir le polynôme à coefficient entiers $H_D \in \mathbb{Z}[X]$ dont les racines sont les $j((-b + \sqrt{D})/(2a))$, où $(a, b, *)$ décrit $C\ell(D)$.

**3)** On désire construire une courbe elliptique explicite sur $\mathbb{F}_p$ (donnée par une équation), de cardinal $m$. On pourra supposer que $D < -4$.

On rappelle que la courbe $E_j$ suivante a pour $j$-invariant $j$ :

(1) Si $j = 0$, poser $E_0 : y^2 = x^3 - 1$.
(2) Si $j = 1728$, poser $E_{1728} : y^2 = x^3 - x$.
(3) Si $j \neq 0, 1728$, poser $c := j/(1728 - j)$ puis $E_j : y^2 = x^3 + 3cx + 2c$.

Si $D < -4$, on appelle tordue quadratique de $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ une courbe $E' : y^2 = x^3 + ag^2x + bg^3$, où $g$ n'est pas un carré dans $\mathbb{F}_p$. (Le choix de $g$ n'a pas d'importance : les courbes associées aux différents $g$ sont isomorphes sur $\mathbb{F}_p$.)

a) Écrire un programme calculant une racine $\bar{j}$ de $H_D$ dans $\mathbb{F}_p[X]$. On pourra utiliser `polrootsmod`.

b) Écrire un programme donnant l'équation d'une courbe $E/\mathbb{F}_p$ de $j$-invariant $\bar{j}$ et de sa tordue quadratique $E'$.

c) Étant donnée une courbe $E/\mathbb{F}_p$, et un entier $n$, écrire un programme essayant de trouver un point d'ordre $n$ dans $E(\mathbb{F}_p)$. [*On pourra supposer le cardinal $\#E(\mathbb{F}_p)$ connu.*]

d) Expliquer sur un exemple comment on pourrait utiliser ce dernier programme pour démontrer directement que $E$ et $E'$ ont bien le cardinal prévu. [*Attention : $E(\mathbb{F}_p)$ n'a aucune raison d'être cyclique. Il faudra tatonner pour bien choisir son exemple !*]

**4)** Donner une preuve de primalité (ECPP) des entiers $N$ suivants :

$$10^{50} + 151, \quad 10^{200} + 357, \quad 10^{400} + 69$$

Tant mieux si on dispose d'une preuve complète, mais on pourra se contenter

- de la suite des cardinaux des courbes à construire,
- de la construction explicite d'une courbe de la liste,
- d'un point d'ordre suffisant sur cette courbe.