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

Examen, 13 décembre 2007 (8:30 – 11:30)
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.)

Exercice 1 – Dans cet exercice, N désigne un nombre premier et D est un entier négatif, congru à 0 ou 1 modulo 4. On note $(*)$ l'équation $U^2 - DV^2 = 4N$, où U et V sont entiers. La fonction `qfbsolve(Q,N)` résoud l'équation $Q(U,V) = N$, où Q est une forme quadratique binaire, créée par `Qfb`.

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 $U^2 - DV^2 = 4N$ 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)`.

3) Donner une preuve de primalité ($p-1$ ou ECPP) des entiers N suivants :

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

Pour ECPP, 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.

4) Chronométrer les différentes parties de votre programme sur un exemple de taille raisonnable. Quelles pistes d'amélioration pourrait-on suivre ?

Exercice 2 – Soit E la courbe elliptique d'équation $y^2 = x^3 + 1$.

1) Soit $p = 10^{15} + 37$ (qui est premier) et on considère E sur $\mathbb{F}_p$

a) Trouver un point P de la forme $(11, y)$ d'ordre $p + 1$ dans $E(\mathbb{F}_p)$.

b) En déduire le cardinal $\#E(\mathbb{F}_p)$.

c) Soit $Q = [6, 92312033003029]$, trouver l'entier n (modulo $p+1$) tel que $Q = [n]P$.

[*Une méthode de Shanks directe sera coûteuse. Par contre, $p+1$ se factorise facilement.*]

2) Soit maintenant $p = 10^{29} + 319$.

a) Trouver un point P d'ordre $p + 1$ sur E.

b) Soit Q un point d'abscisse 14 (il y en a deux, choisissez-en un). Calculer le logarithme discret de Q en base P.