Université Bordeaux 1
Mathématiques

MHT814 – Courbes Elliptiques
Année 2010–2011

Examen, mercredi 23 Avril 2011 (14:00 – 17:00)

Durée 3 heures. Notes de cours et programmes GP autorisés.

Clarté des programmes et pertinence des commentaires sont des éléments importants d'appréciation.

Pour répondre aux questions, créer *un* fichier par exercice, intitulés *login*1.gp, *login*2.gp, etc. Par exemple, kbelabas1.gp. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans ces fichiers.

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.)

Les deux techniques suivantes peuvent être utiles :

- `allocatemem()` permet d'augmenter la mémoire allouée à la session gp.
- vous pouvez exécuter le programme contenu dans le fichier `nom.gp` et imprimer les résultats dans le fichier `result` (erreurs comprises) en exécutant la commande `gp < nom.gp > result 2>&1`.

Exercice 1 – Si $E/\mathbb{F}_q$ est une courbe elliptique, $c = \#E(\mathbb{F}_q)$ et $n \mid c$, la fonction GP

```
e(E, P,Q, n,c) = elltatepairing(E, P,Q, n)^(c/n)
```

renvoie le pairing de Tate modifié $e_n(P,Q)$ vu en cours, où P, Q sont 2 points de n-torsion.

1)a) Trouver une courbe elliptique $E/\mathbb{F}_{23}$ telle que $\#E(\mathbb{F}_{23}) = 22$.
b) Quelle est la structure de $E(\mathbb{F}_{23})$ comme groupe abélien ?

2)a) Trouver deux points P, Q distincts d'ordre 11 dans $E(\mathbb{F}_{23})$.
b) Illustrer sur un exemple la bilinéarite de e_{11}.

3) Résoudre directement le problème de logarithme discret $P = [x]Q$.

4) En utilisant le pairing e_{11}, transporter le problème de logarithme discret précédent dans (un sous groupe d'ordre 11 de) $\mathbb{F}_{23}^*$, et l'y résoudre de nouveau.

3

13 , 23
16 , 23

linéaire : $f(x+y) = f(x) + f(y)$
$f(\lambda x) = \lambda f(x)$

$e_n(P, Q)$

$e_n(P+P', Q+Q') = e_n(P,Q) \cdot e_n(P', Q')$

premier

Exercice 2 – Soit $E/\mathbb{F}_q$ une courbe elliptique, $n = \#E(\mathbb{F}_q)$ et $t = q + 1 - n$. On suppose que n est premier, et que $q = 12\ell^2 - 1$ et $t = -1 \pm 6\ell$, pour un $\ell \in \mathbb{Z}$.

1) Déterminer les valeurs de ℓ telles que t vérifie l'inégalité de Hasse.

2) On veut montrer que le degré de plongement de $E(\mathbb{F}_q)$ est 3, c'est-à-dire que le plus petit $k \geqslant 1$ tel que $n \mid q^k - 1$ est 3.
a) Quelle est l'interprétation de k en terme du groupe $(\mathbb{Z}/n\mathbb{Z})^*$?
b) Montrer par un calcul explicite avec des polynômes en ℓ que n divise $q^3 - 1$. [*Utiliser gp !*]
c) Montrer que n ne divise pas $q - 1$.
d) Conclure.

3) Construire une courbe explicite vérifiant les conditions de l'exercice. On pourra commencer par choisir un petit ℓ (non exclu par la question **1)**) tel que q et n soit deux nombres premiers. Il suffit ensuite de trouver une courbe du bon cardinal n.

4) On admet que le problème du log discret dans $\mathbb{F}_q^*$ est difficile si $\log_2 q \geqslant 1024$, et que le plus grand diviseur premier de q est $\geqslant 2^{160}$.
a) Quel ordre de grandeur pour n et q préconiseriez vous pour implanter un protocole cryptographique nécessitant une structure bilinéaire avec les courbes de cette famille ?
b) Fournir un ℓ explicite réalisant les conditions de la question précédente.
c) Quel problème rencontre t'on pour construire une courbe du cardinal voulu, pour ce ℓ ?

$\ell = 1$
$q = 12\ell^2 - 1$
$= 11$
$t = -1 + 6$
$= 5$
$t = q + 1 - n$
$5 = 11 + 1 - n$
$n = 7$.

★ **Exercice 3** – [*Facultatif*] Construire un nombre premier p et une courbe elliptique $E/\mathbb{F}_p$ de cardinal 230420111417.

$|n - (q+1)| \leq 2\sqrt{q}$
$|t| \leq 2\sqrt{q} \iff |-1 \pm 6\ell| \leq \sqrt{12\ell^2 - 1} \cdot 2$
$t = q + 1 - n$
$-t = n - (q+1)$
$-2\sqrt{12\ell^2 - 1} \leq -1 \pm 6\ell \leq 2\sqrt{12\ell^2 - 1}$
$-12\ell^2 - 1 \leq \frac{(-1 \pm 6\ell)^2}{4} \leq 12\ell^2 - 1$
$-12\ell^2 \leq \frac{(-1 \pm 6\ell)^2}{4} + 1 \leq 12\ell^2$
$-12 \leq \frac{(-1 \pm 6\ell)^2 + 4}{4\ell^2} \leq 12$

$n \mid q^3 - 1$
$n \mid$