

N1MA8W04 – Courbes Elliptiques – Master CSI - année 2012/13

Examen: partie théorique - durée 1 heure

Aucun document ni l'ordinateur n'est autorisé

1. Le morphisme de Frobenius

- (a) Soit p un nombre premier. Montrer que pour $1 \leq k \leq p-1$ le coefficient binomial $\binom{p}{k}$ est divisible par p .
- (b) Soit K un corps de caractéristique p . Montrer que pour $x, y \in K$ on a $(x+y)^p = x^p + y^p$. Plus généralement, $(x+y)^{p^k} = x^{p^k} + y^{p^k}$ avec $k = 0, 1, 2, \dots$
- (c) Soit \mathbb{F}_q le corps de q éléments et $\bar{\mathbb{F}}_q$ sa clôture algébrique.
 - i. Montrer que l'application $\bar{\mathbb{F}}_q \rightarrow \bar{\mathbb{F}}_q$ définie par $x \mapsto x^q$ est un automorphisme du corps $\bar{\mathbb{F}}_q$ (le *morphisme de Frobenius*).
 - ii. Montrer que pour $x \in \bar{\mathbb{F}}_q$ on a $x^q = x$ si et seulement si $x \in \mathbb{F}_q$.

2. Frobenius sur les courbes elliptiques On fixe une courbe elliptique E sur \mathbb{F}_q .

- (a) Rappeler la définition du morphisme de Frobenius $\phi_q : E \rightarrow E$.
On admet (mais vous pouvez essayer de le démontrer) que l'application ϕ_q est un automorphisme du groupe abélien E .
- (b) Montrer que $\phi_q^k = \phi_{q^k}$ et que $\phi_q(P) = P$ si et seulement si $P \in E(\mathbb{F}_q)$.
- (c) Soit $m \in \mathbb{Z}$ un entier vérifiant $m\phi_q(P) = O$ pour tout $P \in E$. Montrer que $m = 0$. En déduire que l'égalité $m_1\phi_q = m_2\phi_q$ (avec $m_1, m_2 \in \mathbb{Z}$) implique $m_1 = m_2$.

3. Le théorème de Weil On fixe toujours une courbe elliptique E sur \mathbb{F}_q . On admet l'énoncé suivant.

- Posons $a_q = q + 1 - N_q$, où $N_q = |E(\mathbb{F}_q)|$. Alors le morphisme de Frobenius ϕ_q vérifie $\phi_q^2(P) - a_q\phi_q(P) + qP = O$ pour tout $P \in E$. Autrement dit, $\phi_q^2 - a_q\phi_q + q\text{Id} = 0$.

On note par α et β les racines du polynôme $X^2 - a_qX + q$. (Le théorème de Hasse affirme que $\beta = \bar{\alpha}$, mais ceci ne joue aucun rôle dans la suite.)

Notre objectif est de démontrer le *théorème de Weil*:

$$a_{q^k} = \alpha^k + \beta^k \quad (k = 1, 2, 3, \dots).$$

Dans la suite on note $a = a_q$, $b_k = \alpha^k + \beta^k$.

- (a) Montrer que $b_2 = a^2 - 2q$ et que $b_{k+1} = ab_k - qb_{k-1}$ pour $k \geq 2$. (Indication: vérifier que $\alpha^{k+1} = a\alpha^k - q\alpha^{k-1}$, et le même pour β .) En déduire que $b_k \in \mathbb{Z}$ pour tout $k \geq 1$.
- (b) Montrer que le polynôme $X^2 - aX + q$ divise le polynôme $X^{2k} - b_kX^k + q^k$. (Indication: montrer que $X^{2k} - b_kX^k + q^k = (X^k - \alpha^k)(X^k - \beta^k)$.)
- (c) Montrer que $\phi_{q^k}^2 - b_k\phi_{q^k} + q\text{Id} = 0$. En déduire que $b_k\phi_{q^k} = a_{q^k}\phi_{q^k}$. Conclure, en utilisant la question 2c.

4. Un exemple numérique Dans la suite $q = 5$ et E est la courbe elliptique $y^2 = x^3 + 2x$ sur \mathbb{F}_5 .

- (a) Sans utiliser l'ordinateur déterminer les nombres a_{5^k} et $N_{5^k} = |E(\mathbb{F}_{5^k})| = 5^k + 1 - a_{5^k}$ pour $k = 1, 2, 3, 4$.
- (b) Déterminer la structure des groupes $E(\mathbb{F}_5)$ et $E(\mathbb{F}_{5^3})$.
- (c) Montrer que le sous-groupe de 2-torsion $E[2]$ est contenu dans $E(\mathbb{F}_{5^2})$. (Indication: rappelons que les points de 2-torsion sont l'origine et les points avec $y = 0$.)
- (d) Déterminer la structure des groupes $E(\mathbb{F}_{5^2})$ et $E(\mathbb{F}_{5^4})$.

DS du 25 avril 2013
sujet sur machine 9h30 – 11h30

Durée : 2 heures. Les notes de cours et les programmes GP sont autorisés.

- Pour répondre aux questions, créer un seul fichier pour tout le sujet et séparer les exercices. Nommer le fichier `login.gp`, où login est votre identifiant informatique. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans le fichier `login.gp`.
- Pour rendre votre travail, envoyez le fichier par courriel à la fin de l'épreuve à l'adresse
`jean.gillibert@math.u-bordeaux1.fr`
- Rappelons que la clarté des programmes et la pertinence des commentaires sont des éléments importants d'appréciation.

Exercice 1

Soit E la courbe elliptique définie sur \mathbb{F}_{521} par les coefficients

$$E = [1, 1, 1, -3, 1]$$

1. Quelle est la structure de $E(\mathbb{F}_{521})$ en tant que groupe abélien fini ?
2. Le groupe $E(\mathbb{F}_{521})[5]$ est-il isomorphe à $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$?
3. On considère les points $P = (1, 0)$ et $Q = (21, 185)$ appartenant à $E(\mathbb{F}_{521})$. Vérifiez que P est d'ordre 5, et que Q est d'ordre 105.
4. Calculer le couplage de Weil $e_{105}(P, Q)$. En déduire que P n'appartient pas au sous-groupe cyclique engendré par Q .
5. Est-il vrai que le groupe $E(\mathbb{F}_{521})$ est engendré par P et Q ?

On considère à présent le point $R = (0, 99)$ qui est d'ordre 3. On souhaite construire un autre point S d'ordre 3 tel que R et S engendrent le groupe $E(\overline{\mathbb{F}_{521}})[3]$. D'après les propriétés du couplage de Weil on sait que, pour construire un tel S , il faut aller dans une extension de \mathbb{F}_{521} qui contient les racines 3-ièmes de l'unité.

6. Déterminer le plus petit entier k tel que \mathbb{F}_{521^k} contienne les racines 3-ièmes de l'unité.
7. En utilisant les fonctions `elldivpol` et `factorff`, montrer que tous les points de 3-torsion de E sont définis sur \mathbb{F}_{521^k} , où k est l'entier de la question précédente.
8. Déterminer un point S tel que $E(\overline{\mathbb{F}_{521}})[3] = \langle R, S \rangle$.

Exercice 2

Soit H la courbe elliptique définie sur $\mathbb{F}_{90000049}$ par les coefficients

$$H = [0, 0, 1, 1, 0]$$

On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{90000049}$

$$P = (36502070, 72583757)$$

$$Q = (74197837, 65666440)$$

On admet que Q appartient au groupe cyclique engendré par P .

1. Quel est l'ordre du groupe $H(\mathbb{F}_{90000049})$? Quel est l'ordre de P ? Que peut-on en déduire?
2. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.
3. Même question en utilisant la méthode rho de Pollard. Laquelle des deux méthodes est la plus rapide?
4. Le point Q engendre-t-il le groupe $H(\mathbb{F}_{90000049})$?

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 `login1.gp`, `login2.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.

- Trouver une courbe elliptique E/\mathbb{F}_{23} telle que $\#E(\mathbb{F}_{23}) = 22$.
- Quelle est la structure de $E(\mathbb{F}_{23})$ comme groupe abélien?
- Trouver deux points P, Q distincts d'ordre 11 dans $E(\mathbb{F}_{23})$.
- Illustrer sur un exemple la bilinéarité de e_{11} .
- Résoudre directement le problème de logarithme discret $P = [x]Q$.
- 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.

linéaire:

$$f(x+y) = f(x) + f(y)$$

$$f(\lambda x) = \lambda f(x)$$

$$e_n(P, Q)$$

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

$$\begin{matrix} 13 & 23 \\ 16 & 23 \end{matrix}$$

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 $\ell \in \mathbb{Z}$.

- Déterminer les valeurs de ℓ telles que t vérifie l'inégalité de Hasse.
- On veut montrer que le degré de plongement de $E(\mathbb{F}_q)$ est 3, c'est-à-dire que le plus petit $k \geq 1$ tel que $n \mid q^k - 1$ est 3.

- Quelle est l'interprétation de k en terme du groupe $(\mathbb{Z}/n\mathbb{Z})^*$?
- Montrer par un calcul explicite avec des polynômes en ℓ que n divise $q^3 - 1$.

[Utiliser gp !]

- Montrer que n ne divise pas $q - 1$.
- 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 $\log_2 q \geq 1024$, et que le plus grand diviseur premier de q est $\geq 2^{16}$.

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 ?

- Fournir un ℓ explicite réalisant les conditions de la question précédente.
- Quel problème rencontre-t-on pour construire une courbe du cardinal voulu, pour ce ℓ ?

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

$$\begin{aligned} |n - (q+1)| &\leq 2\sqrt{q} \\ |t| &\leq 2\sqrt{q} \Rightarrow |-1 \pm 6P| \leq \sqrt{12P^2 - 1} = 2 \\ t = q + 1 - n & \\ t = n - (q+1) & - 2\sqrt{12P^2 - 1} \leq -1 \pm 6P \leq 2\sqrt{12P^2 - 1} \end{aligned}$$

$$-12P^2 - 1 \leq \frac{(-1 \pm 6P)^2}{4} \leq 12P^2 - 1$$

$$-12 \leq \frac{(-1 \pm 6P)^2 + 4}{4P^2} \leq 12$$

$$-12 \leq \frac{(-1 \pm 6P)^2 + 4}{4P^2} \leq 12$$

Préparation à l'Examen du mercredi 21 Avril 2009 (8:30 – 11:30)

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 `login1.gp` et `login2.gp`. Par exemple, `kbelabas1.gp`. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans les fichiers `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.)

Les deux techniques suivantes peuvent être utiles :

- `allocatemem()` permet d'augmenter la mémoire allouée à la session 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 – On fixe un entier m , dont on désire qu'il soit le cardinal d'une courbe elliptique E sur un corps fini \mathbb{F}_p .

- a) Écrire un programme trouvant le nombre premier p le plus proche de $m - 1$.
b) Écrire un programme trouvant un nombre premier p satisfaisant la borne de Hasse, tel que $4p - u^2$ soit minimal, où $u := m - (p + 1)$. En quoi ce dernier p est-il intéressant ?
- 2) Écrire un programme naïf, tirant E au hasard jusqu'à ce que $\#E(\mathbb{F}_p) = m$.
- 3) a) Trouver une courbe E explicite de cardinal $m = 201021040811$.
b) Trouver une courbe E explicite de cardinal $m = 2010210408301130$.

Exercice 2 –

- a) Écrire un programme prenant en entrée un nombre premier p et donnant en sortie une courbe elliptique E sur \mathbb{F}_p telle que $E(\mathbb{F}_p)$ soit *non cyclique*, ainsi que deux générateurs de ce groupe.
b) Quelle est la complexité de votre programme ?
- 2) a) Pour (a, b) fixés, écrire un programme tentant de construire un premier p et une courbe elliptique E/\mathbb{F}_p telle que $E(\mathbb{F}_p) \simeq \mathbb{Z}/(ab)\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$, avec $p \equiv 1 \pmod{b}$.
b) Trouver p premier et une courbe E/\mathbb{F}_p explicite telle que $E(\mathbb{F}_p) \simeq \mathbb{Z}/(11a)\mathbb{Z} \oplus \mathbb{Z}/11\mathbb{Z}$, pour un certain a .

Exercice 3 – Produire un certificat de primalité pour $10^{199} + 153$.

Préparation à l'Examen du mercredi 21 Avril 2009 (8:30 – 11:30)**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 `login1.gp` et `login2.gp`. Par exemple, `kbelabas1.gp`. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans les fichiers `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.)

Les deux techniques suivantes peuvent être utiles :

- `allocatemem()` permet d'augmenter la mémoire allouée à la session 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 –

- 1) Écrire un programme prenant en entrée un entier $k > 0$ et donnant en sortie un nombre premier p de k bits (soit $2^{k-1} \leq p < 2^k$).
- 2) Écrire un programme prenant en entrée un nombre premier p et donnant en sortie une courbe elliptique E sur \mathbb{F}_p telle que $E(\mathbb{F}_p)$ soit non cyclique, ainsi que deux générateurs de ce groupe.
- 3) Quelle est la complexité de votre programme ?

Exercice 2 – On fixe un entier m , dont on désire qu'il soit le cardinal d'une courbe elliptique E sur un corps fini \mathbb{F}_p .

- 1)a) Écrire un programme trouvant le nombre premier p le plus proche de $m - 1$.
b) Lui faire vérifier que la borne de Hasse n'exclut pas qu'il existe E/\mathbb{F}_p de cardinal m .
- 2)a) Écrire un programme naïf, tirant E au hasard jusqu'à ce que $\#E(\mathbb{F}_p) = m$.
- 3) Trouver une courbe E explicite de cardinal $m = 201008041416$.

Exercice 3 – Démontrer que $10^{199} - 9$ est premier. (Produire un certificat de primalité.)