Contrôle du 3 mars

La notation accordera la plus grande importance à la qualité de la rédaction.

Partie J.-M. Couveignes

Exercice 1 :

Soit C la courbe plane projective d'équation

$$Y^2Z = X^3 + 2XZ^2 + Z^3$$

sur le corps à 7 éléments $\mathbb{F}_7$.

Montrez que C est une courbe lisse.

Donnez la liste de tous les points dans $C(\mathbb{F}_7)$.

Soit P le point de coordonnées projectives $(0 : 6 : 1)$.

Calculez $2P$.

Soit Q le point de coordonnées projectives $(1 : 5 : 1)$.

Calculez $P + Q$.

Quelle est la structure du groupe $C(\mathbb{F}_7)$?

Exercice 2 :

Soit $f(x)$ le polynôme $x^2 + x + 1$ dans $\mathbb{F}_5[x]$.

Montrez que $f(x)$ est un polynôme irréductible.

On pose $\mathbf{K} = \mathbb{F}_5[x]/f(x)$.

On note $\alpha = x \bmod f(x) \in \mathbf{K}$.

Montrez que $\mathbf{K}$ est un corps. Quel est son cardinal ?

Soit D la courbe projective d'équation

$$Y^2Z = X^3 + XZ^2 + Z^3$$

sur $\mathbf{K}$.

Montrez que D est une courbe lisse.

Vérifiez que $P = (4 : 3 : 1)$ est un point de la courbe.

Calculez $2P$.

Vérifiez que $Q = (3\alpha + 1 : 4\alpha + 2 : 1)$ est un point de la courbe.

Calculez $P + Q$.

Partie G. Castagnos

Exercice 3 :

Soit P et Q deux points d'une courbe elliptique E sur un corps fini et u et v deux entiers strictement positifs. On suppose que u et v peuvent s'écrire sur $m + 1$ bits et on note $u = \sum_{i=0}^{m} u_i 2^{m-i}$ et $v = \sum_{i=0}^{m} v_i 2^{m-i}$ les décompositions binaires de u et de v. On pose $U_0 = u_0, V_0 = v_0$, puis pour tout k tel que $0 \leqslant k < m, U_{k+1} = 2U_k + u_{k+1}$ et $V_{k+1} = 2V_k + v_{k+1}$.

(a) Rappeler le fonctionnement de l'algorithme *double and add* permettant de calculer uP. Combien fait on de doublement de points et d'additions en moyenne ?

(b) On souhaite calculer $uP + vQ$. Dans quel protocole cryptographique un tel type de calcul est effectué ?

(c) Soit $0 \leqslant k < m$, on suppose avoir calculé $U_k P + V_k Q$. Montrer comment en déduire $U_{k+1}P + V_{k+1}Q$.

(d) En déduire un algorithme pour calculer $uP + vQ$. Est-il plus efficace que deux applications de l'algorithme *double and add* ?

Exercice 4 :

On considère une courbe elliptique E d'équation $y^2 = x^3 + ax + b$ sur le corps fini $\mathbb{F}_p$ avec p un grand nombre premier. Soit P un point de la courbe E d'ordre n avec n un grand nombre premier.

(a) Rappeler le fonctionnement du protocole d'échange de clef Diffie-Hellman utilisant cette courbe E.

(b) Lors d'une exécution de ce protocole, Alice envoie à Bob un point Q d'une courbe elliptique E' sur $\mathbb{F}_p$ d'équation $y^2 = x^3 + ax + c$ avec c différent de b au lieu de lui envoyer un point de la courbe E. Montrer qu'Alice peut ainsi obtenir de l'information sur l'exposant secret de Bob.

(c) Que peut faire Bob pour éviter cette attaque ?

Université Bordeaux I – 2012/2013 Courbes elliptiques
Master 1 Cryptologie et Sécurité Informatique Yu. Bilu / J. Gillibert

DS du 19 mars 2013, 14h – 16h

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 $\mathbb{F}_{61}$ par les coefficients

$$E = [0, 1, 1, -3, 1]$$

1. Quelle est la structure de $E(\mathbb{F}_{61})$ en tant que groupe abélien fini ?
2. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
3. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$?
4. $E(\mathbb{F}_{61})$ contient-il un sous-groupe isomorphe à $(\mathbb{Z}/27\mathbb{Z})$?
5. Existe-t-il un entier n tel que $E(\mathbb{F}_{61^n})$ soit un groupe cyclique ?

Exercice 2
Soit H la courbe elliptique définie sur $\mathbb{F}_{2423}$ par les coefficients

$$H = [0, 1, 0, -3, -2]$$

Soit $R(X)$ le polynôme donné par la commande `ffinit`$(2423, 2)$, et soit t la classe de X modulo $R(X)$. On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{2423^2}$

$$P = (1205 * t + 168, 1033 * t + 1637)$$

$$Q = (1073 * t + 770, 519 * t + 2276)$$

1. En utilisant le théorème de Hasse, donner un majorant de l'ordre du groupe $H(\mathbb{F}_{2423^2})$.
2. On admet que Q appartient au groupe cyclique engendré par P. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.
3. Déterminer l'ordre de P.
4. Les points P et Q engendrent-ils le même sous-groupe de $H(\mathbb{F}_{2423^2})$?

Exercice 3

Soit $A(X) \in \mathbb{F}_{5003}[X]$ le polynôme défini par

$$A(X) = X^3 + X^2 + X + 2$$

1. Expliquez brièvement pourquoi $\mathbb{F}_{5003}[X]/A(X)$ est isomorphe à $\mathbb{F}_{5003^3}$.
2. Soit x la classe de X modulo $A(X)$. A l'aide de la fonction `fforder`, dites si x est un générateur du groupe $(\mathbb{F}_{5003^3})^\times$.
3. On admet que $x^3 + 1$ est un générateur de $(\mathbb{F}_{5003^3})^\times$. A l'aide de la fonction `fflog`, déterminer un entier m tel que
$$(x^3 + 1)^m = x$$

Université Bordeaux 1
Mathématiques

MHT814 – Courbes Elliptiques
Année 2010–2011

Devoir Surveillé, 30 Mars 2011 (10:00 – 12:00)

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 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

$$fabien.pazuki@math.u-bordeaux1.fr.$$

Exercice 1 – Soit $p \geqslant 5$ un nombre premier et soit q une puissance de p. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soit m un entier strictement positif. On note $E[m]$ l'ensemble des points P de la courbe E qui vérifient $[m]P = 0$.

1) Montrer que $E[m]$ est non vide.

2) Donner un exemple de courbe sur $\mathbb{F}_5$ telle que $E[2]$ contient au moins deux points.

3) Donner un exemple de courbe sur $\mathbb{F}_{49}$ telle que $E[4]$ contient au moins deux points.

4) On s'intéresse à présent au cas particulier $m = p$. Regardons la courbe E définie sur $\mathbb{F}_7$ par l'équation affine $y^2 = x^3 + x$. Calculer $\mathrm{Card}(E(\mathbb{F}_7))$. Calculer $\mathrm{Card}(E[7])$.

Lorsqu'une courbe E définie sur $\mathbb{F}_p$ vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p+1$, on dit que c'est une courbe **supersingulière** en p.

5) Montrer que la courbe E définie sur $\mathbb{F}_{23}$ par l'équation $y^2 = x(x-1)(x+2)$ est supersingulière en 23. Calculer $\mathrm{Card}(E[23])$.

6) Considérons la courbe E définie sur $\mathbb{Z}$ par l'équation affine $y^2+y = x^3-x^2-10x-20$. Donner le discriminant de E. Si on réduit l'équation de E modulo un nombre premier p qui ne divise pas le discriminant, on obtient donc une courbe elliptique sur $\mathbb{F}_p$. Trouver tous les nombres premiers p compris entre 5 et 100 tels que E est supersingulière en p.

7) Reprenons la courbe E définie sur $\mathbb{Z}$ par l'équation affine $y^2+y = x^3-x^2-10x-20$. Calculer $\mathrm{Card}(E[p])$ pour tous les nombres premiers p inférieurs à 100. Que remarque-t-on ?

Exercice 2 – On étudie dans cet exercice la notion de **courbe anormale**. Soit p un nombre premier. Une courbe elliptique E définie sur $\mathbb{F}_p$ est dite **anormale en** p si elle vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p$.

1) Montrer que la courbe E définie sur $\mathbb{F}_{11}$ par l'équation $y^2 = x^3 + x + 5$ est anormale.

2) Quelle est la structure d'un groupe de cardinal p ? Que peut-on en déduire pour $E(\mathbb{F}_p)$?

3) Donner un exemple de courbe anormale pour $p = 19$.

Exercice 3 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Trouver un entier n tel que l'égalité $933 = 59^n$ soit vraie dans $\mathbb{F}_{2011}$.

2) Soit t la classe de X dans $\mathbb{F}_{13}[X]/(F(X)) \simeq \mathbb{F}_{13^3}$, où F est donné par la commande $ffinit$. Trouver un entier n tel que $3t^2 + 10t + 4 = t^n$.

3) Considérons la courbe E définie par $y^2 = x^3 + 3x + 4$. Soit $P = (17, 1238)$ et $Q = (3317, 13320)$ deux points de $E(\mathbb{F}_{20101})$. Trouver un entier n tel que $Q = [n]P$.

4) Considérons la courbe E définie par $y^2 = x^3 + x$. Soit $P = (t^4 + 9, 5t^3 + t^2 + 3t + 6)$ et $Q = (6t^4 + t^3 + 8, 8t^4 + 4t^3 + 2t + 5)$ deux points de $E(\mathbb{F}_{11^5})$, où t est la classe de X dans $\mathbb{F}_{11}[X]/(F(X)) \simeq \mathbb{F}_{11^5}$. Trouver un entier n tel que $Q = [n]P$.

Université Bordeaux 1 **MHT814 – Courbes Elliptiques**
Mathématiques Année 2009–2010

Devoir Surveillé, 22 Mars 2010 (8:00 – 10:00)

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 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

$$fabien.pazuki@math.u-bordeaux1.fr.$$

Exercice 1 – Soit $y^2 = x^3 + Ax + B$ une équation affine d'une courbe E avec A et B des éléments d'un corps K vérifiant $-16(4A^3 + 27B^2) \neq 0$. Soit m un entier strictement positif. On s'intéresse dans cet exercice aux polynômes de m-division sur la courbe elliptique E.

1) On définit par récurrence sur m les quantités suivantes :

$$\begin{cases} \psi_0 = 0, \ \ \psi_1 = 1, \ \ \psi_2 = 2y \\ \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geqslant 2) \\ 2y\,\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geqslant 3) \end{cases}$$

Justifier que ce sont bien des polynômes en x, y, A, B.

2) On définit pour tout $m \geqslant 2$ les quantités :

$$\begin{cases} \varphi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\ 4y\,\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \end{cases}$$

Vérifier pour quelques valeurs entières de k que les quantités ψ_{2k+1}, φ_{2k+1}, $y^{-1}\omega_{2k+1}$, $(2y)^{-1}\psi_{2k}$, φ_{2k} et ω_{2k} sont des polynômes en x, y^2, A, B. Pour A, B fixés, ces quantités ne dépendent donc que de x en vertu de l'équation de la courbe E. Vérifier alors sur une liste d'exemples que $\varphi_m(x)$ et $\psi_m(x)^2$ sont premiers entre eux dans $K[x]$.

$\varphi_2 = x\psi_2^2 - \psi_3\psi_1$

$\varphi_2 =$

$n-1+2$

3) Vérifier par récurrence que si $P = (x, y) \in E(K)$ alors pour tout $m \geqslant 2$, si $[m]P \neq 0$ on a

$$[m]P = \left(\frac{\varphi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

4) Exemple : Considérons la courbe définie par l'équation $y^2 = x^3 + x$. Posons $m = 2$ et $P = (0, 0)$.

(1) Calculer $P + P$.

(2) Calculer $\psi_2(P)$.

(3) Conclure sur l'utilité des racines de ψ_2 et de ψ_m plus généralement.

5) Lister tous les points de 5-torsion à coordonnées dans $\mathbb{F}_{25}$ sur la courbe donnée par $y^2 = x^3 + 1$.

6) Compter le nombre de points de 13-torsion à coordonnées dans $\mathbb{F}_{49}$ sur la courbe donnée par $y^2 = x^3 + x + 1$.

Exercice 2 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Trouver un entier n tel que l'égalité $87 = 23^n$ soit vraie dans $\mathbb{F}_{101}$.

2) Soit t la classe de X dans $\mathbb{F}_7[X]/(F(X)) \simeq \mathbb{F}_{7^5}$, où F est donné par la commande *ffinit*. Trouver un entier n tel que $3t^3 + 6t^2 + 5 = t^n$.

3) Considérons la courbe E définie par $y^2 = x^3 + 2x + 6$. Soit $P = (1, 3)$ et $Q = (15967, 13808)$ deux points de $E(\mathbb{F}_{20101})$. Trouver un entier n tel que $Q = [n]P$.

4) Considérons la courbe E définie par $y^2 = x^3 + 1$. Soit $P = (t^2 + 5, 5t^3 + 5t^2 + 8t + 5)$ et $Q = (8t^4 + t^3 + 6t^2 + 3t, 5t^3 + t^2 + 3t)$ deux points de $E(\mathbb{F}_{11^5})$, où t est la classe de X dans $\mathbb{F}_{11}[X]/(F(X)) \simeq \mathbb{F}_{11^5}$. Trouver un entier n tel que $Q = [n]P$.

$$P = \left(\frac{\varphi_2(P)}{\psi_2(P)^2}, \frac{\omega_2(P)}{\psi_2(P)^3}\right) = \frac{-3x^4 - 6x^2 + (4y^2 \cdot 1)x + 1}{(4y^2)}$$

$t, 3t^3 + 6t^2 + 5$

$(n-1)P + (2)P$

$$P = \frac{x\,\psi_2^{\,4}(P) + \psi_3\psi_1}{\psi_2^{\,2}(P)}\quad \frac{\varphi_{m-1}(P)}{\psi_{m-1}(P)^2},\ \frac{\text{omega}_m(P)}{\psi_{m-1}(P)^3}$$

$\boxed{3t^3 + 6t^2 + 5 = (n)t}$

$3Q^3 + 6Q + 5 = (n)P$