UFR de Mathématiques et Informatique
Université Bordeaux I Année 2005–2006

Master CCSI 2

Méthodes mathématiques de la cryptologie

Examen du 15 décembre 2005

Durée 2 heures. Documents manuscrits autorisés

Les exercices ne sont **pas** indépendants, et il est conseillé de les résoudre dans l'ordre. Toutefois, si nécesaire, on pourra résoudre un exercice en admettant les résultats des autres.

Petit formulaire : la loi générique d'addition sur une courbe elliptique d'équation $y^2 = x^3 + ax + b$ est donnée par $x_3 = m^2 - x_1 - x_2$, $y_3 = m(x_1 - x_3) - y_1$, où $m = (y_2 - y_1)/(x_2 - x_1)$ si $x_2 \neq x_1$, et $m = (3x_1^2 + a)/(2y_1)$ sinon, avec des notations évidentes.

Exercice I

On rappelle qu'un point de n-torsion sur une courbe elliptique E est un point P (y compris le point à l'infini $\mathcal{O}$) tel que $P + P + \cdots + P = n \cdot P = \mathcal{O}$.

On considère une courbe elliptique E d'équation $y^2 = x^3 + ax + b$ définie sur un corps K.

1) Après avoir rappelé (sans démonstration) la caractérisation des points de 2-torsion autres que $\mathcal{O}$, donner le nombre maximal M_2 de tels points, en comptant cette fois $\mathcal{O}$. Expliquer très brièvement pourquoi ce nombre peut être atteint sur le corps $\mathbb{C}$ par exemple.

2) Soit $P = (x, y)$ un point de E autre que le point à l'infini.

a) Montrer que P est un point de 3-torsion si et seulement si l'abcisse de $P + P$ est égale à celle de P.

b) En déduire l'équation que doit satisfaire x (ce doit être une équation de degré 4). On devra bien sûr remplacer y^2 par $x^3 + ax + b$ pour obtenir cette équation.

c) En déduire le nombre maximal M_3 de points de 3-torsion sur E, y compris le point $\mathcal{O}$ (attention, regarder aussi les ordonnées). Montrer brièvement que ce maximum peut être atteint sur $\mathbb{C}$. Sachant que trivialement $M_1 = 1$, devinez-vous quelle pourrait être la valeur de M_n ? (on ne demande pas de le démontrer).

3) On considère plus spécifiquement le cas $a = 0$, donc les courbes E_b d'équation $y^2 = x^3 + b$, et on suppose que $b \in \mathbb{Z}$ et que $K = \mathbb{Q}$.

a) Montrer qu'il existe un point de 2-torsion T_2 autre que $\mathcal{O}$ si et seulement si b est un cube (positif ou négatif), et que dans ce cas il est unique.

b) Montrer qu'il existe un point de 3-torsion T_3 autre que $\mathcal{O}$ si et seulement si, soit b est un carré, soit b est de la forme $b = -432u^6$ pour $u \in \mathbb{Z}$, et que dans ce cas les seuls points de ce type sont T_3 et $-T_3 = 2T_3$. On demande un soin particulier pour cette question. Indication: pour les points avec $b < 0$, on écrira $b = -2^{v_2}3^{v_3}r$ avec r premier à 6, on trouvera les congruences modulo 2 et 3 que doivent satisfaire v_2 et v_3, et on montrera que r est une puissance sixième.

Exercice II

Soit $\mathbb{F}_q$ le corps fini a q éléments, soit g un générateur du groupe cyclique $\mathbb{F}_q^*$, soit $n \geq 1$ un entier, et notons f_n l'application $x \mapsto x^n$ de $\mathbb{F}_q^*$ dans lui-même.

1) a) Montrer que si a est donné, il existe b tel que $g^a = (g^b)^n$ si et seulement si $\mathrm{pgcd}(q-1, n) \mid a$ (il faut montrer que c'est bien une condition nécessaire et suffisante).

b) En déduire le cardinal de l'image de l'application f_n, puis le cardinal du noyau de f_n, c'est à dire le nombre de $x \in \mathbb{F}_q^*$ tel que $x^n = 1$.

c) En particulier, que peut-on dire de l'application $x \mapsto x^n$ de $\mathbb{F}_q$ dans lui-même quand $\mathrm{pgcd}(q-1, n) = 1$?

2) En remarquant que $4(x^3 - y^3) = (x-y)((2x+y)^2 + 3y^2)$, déduire de ce qui précède (appliqué à $n = 3$) une preuve du cas particulier suivant de la loi de réciprocité quadratique: si p est un nombre premier différent de 3 on a

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \pmod 3 , \\ -1 \text{ si } p \equiv 2 \pmod 3 . \end{cases}$$

Exercice III

On considère l'équation déjà considérée dans l'exercice I 3)

$$(E_b) : \qquad y^2 = x^3 + b ,$$

où b est un paramètre entier fixé.

1) Montrer brièvement que cette équation définit une courbe elliptique E sur tout corps fini de caractéristique différente de 2, de 3, et des diviseurs premiers de b. On se place désormais sur un corps fini $\mathbb{F}_p$, où p est un nombre premier autre que ceux qu'on vient de citer.

2) a) En utilisant le résultat de l'exercice II (ou la loi de réciprocité quadratique si vous n'avez pas fait l'exercice), montrer que si $p \equiv 2 \pmod 3$ l'application $x \mapsto x^3$ de $\mathbb{F}_p$ dans lui-même est *bijective*.

b) En déduire le cardinal de $E_b(\mathbb{F}_p)$ (y compris le point à l'infini) quand $p \equiv 2 \pmod 3$ (on comptera le nombre de valeurs de x correspondant à chaque valeur de y).

Pour la suite de cet exercice, on fixe $b = 64$.

3) a) En utilisant l'exercice I 3), montrer que le cardinal de $E_{64}(\mathbb{F}_p)$ est divisible par 6 pour tout $p \geq 5$ (noter que ceci est bien compatible avec le résultat de la question précédente).

b) On suppose que $p \equiv 1 \pmod 3$. Calculer à la main, par la méthode que vous préférez, le cardinal de $E_{64}(\mathbb{F}_p)$ (y compris le point à l'infini) pour $p = 7$, $p = 13$ et $p = 19$ (utiliser a) comme vérification de vos calculs). Pour chacune de ces valeurs de p, donner la liste complète des points de $E_{64}(\mathbb{F}_p)$.