UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2003–2004

DESS CCSI

Méthodes mathématiques de la cryptologie

Examen de janvier 2004

Durée 3 heures. Documents manuscrits autorisés

Exercice I

On considère l'équation

$$y^2 = x^3 - 36x \ .$$

1) a) Montrer que pour tout $p \geq 5$ cette équation définit une courbe elliptique E sur $\mathbb{F}_p$. On suppose donc désormais que $p \geq 5$.

b) Montrer que si $p \equiv 3 \pmod 4$ et si x est différent de 0 et ± 6, alors soit $x^3 - 36x$, soit $(-x)^3 - 36(-x)$ mais pas les deux est un résidu quadratique modulo p.

c) En déduire le cardinal de $E(\mathbb{F}_p)$ (y compris le point à l'infini) quand $p \equiv 3 \pmod 4$.

d) Montrer à l'inverse que si $p \equiv 1 \pmod 4$ et si x est différent de 0 et ± 6, alors $x^3 - 36x$ et $(-x)^3 - 36(-x)$ sont soit tous les deux résidus quadratiques modulo p, soit non.

e) Calculer le cardinal de $E(\mathbb{F}_p)$ (y compris le point à l'infini) pour $p = 5$ et $p = 13$, soit directement, soit en utilisant la formule du cours et la question d).

2) a) Rappeler pourquoi $(x, y) \in E(\mathbb{F}_p)$ est d'ordre 2 si et seulement si $y = 0$. En déduire les coordonnées des trois points d'ordre 2 sur $E(\mathbb{F}_p)$ autres que le point à l'infini. On appellera T_1, T_2 et T_3 ces trois points (dans n'importe quel ordre).

b) Montrer qu'il existe un entier positif y tel que le point $P_0 = (-2, y)$ appartienne à E. En utilisant la formule d'addition sur E, calculer $P_i = P + T_i$ pour $i = 1$, 2 et 3, et constater que ce sont des points à coordonnées entières. On possède donc (en dehors du point à l'infini) 11 points à coordonnées entières sur E, à savoir T_i pour $1 \leq i \leq 3$ et $\pm P_i$ pour $0 \leq i \leq 3$. Il pourra être utile (mais ce n'est pas demandé) d'écrire explicitement les coordonnées de ces 11 points.

c) En réduisant modulo p ces 11 points, on obtient ainsi des points dans $E(\mathbb{F}_p)$. Donner le nombre de points **distincts** ainsi obtenus, en distinguant les cas $p = 5$, $p = 7$ et $p \geq 11$.

3) La question 3a) est calculatoire, et les calculs doivent être faits en nombres rationnels, pas dans $\mathbb{F}_p$.

a) En utilisant les formules d'addition et de doublement, pour $0 \leq i \leq 3$ calculer $3P_i = P_i + P_i + P_i$. On pourra exprimer les quatre résultats sous la forme $3P_i = (m_i/d_i^2, n_i/d_i^3)$.

b) Si $p \mid d_i$, $p \geq 5$, qu'en déduit-on sur le cardinal de $E(\mathbb{F}_p)$? Donner la liste des p pour lesquels ceci s'applique.

Exercice II

Dans cet exercice on va travailler dans $\mathbb{Z}/43\mathbb{Z}$, dont on représentera les éléments par des classes d'entiers entre -21 et 21. Pour simplifier les notations on identifie ces entiers avec leurs classes, c'est à dire qu'on écrira simplement a à la place de $\overline{a}$.

Dans $\mathbb{Z}/43\mathbb{Z}$ on considère les trois suites u_n, v_n et w_n définies par $u_n = 7^n$, $v_n = (-6)^n$ et $w_n = u_n + v_n$.

1) Montrer que ces trois suites satisfont à la même relation de récurrence $x_{n+2} = x_{n+1} - x_n$.

2) a) Calculer w_n pour $0 \leq n \leq 7$.

b) En déduire que w_n est périodique de période 6.

c) En déduire les valeurs de $n \geq 1$ pour lesquelles $w_n \equiv 1 \pmod{43}$.

3) Soit p un nombre premier tel que $p \geq 5$.

a) Montrer que $7^p - 6^p - 1$ est divisible par 43.

b) En déduire le résultat suivant : si p est un nombre premier tel que $p \geq 5$, alors $7^p - 6^p - 1$ est divisible par $1806 \cdot p$.

4) a) Calculer a et b tels que $7^6 \equiv 1 + 43a \pmod{43^2}$ et $6^6 = 1 + 43b \pmod{43^2}$ avec $-21 \leq a, b \leq 21$ (commencer par faire le calcul pour 7^3 et 6^3 ; il est inutile d'utiliser une calculette).

b) En déduire que si $p \equiv 1 \pmod 6$ alors $7^p - 6^p - 1$ est divisible par 43^2.

Exercice III

On dira qu'un entier positif N est un nombre de Lenstra si pour tout a (premier ou non avec N) on a

$$a^{N+1} \equiv a \pmod{N}\ .$$

Soit donc N un nombre de Lenstra.

1) En choisissant $a = p$ montrer que N est sans facteur carré plus grand que 1, c'est à dire que si $p \mid N$ alors p^2 ne divise pas N.

Il en résulte que N est égal à un produit de nombres premiers distincts.

2) a) Si $p \mid N$, montrer qu'il existe une racine primitive a modulo p telle que $(a, N) = 1$. Pour cela on appliquera le théorème Chinois à p et N/p, en expliquant pourquoi il est applicable.

b) En déduire que pour tout nombre premier p divisant N on a $(p-1) \mid N$.

c) Montrer la réciproque, c'est à dire qu'un nombre N est un nombre de Lenstra si et seulement si N est sans facteur carré plus grand que 1 et si pour tout nombre premier p divisant N on a $(p-1) \mid N$.

d) Donner la liste de tous les nombres de Lenstra N tels que $1 \leq N \leq 6$.

3) Supposons $N > 1$, et écrivons $N = p_1 p_2 \cdots p_n$ avec p_i premiers ordonnés par ordre croissant $p_1 < p_2 < \cdots < p_n$.

a) Pour tout k tel que $1 \leq k \leq n$, expliquer pourquoi p_k est de la forme $p_k = 1 + s$, où s est un produit (éventuellement vide) de certains nombres premiers p_j avec $j < k$ (on rappelle qu'un produit vide est par convention égal à 1).

b) En déduire que, si les indices donnés sont inférieurs ou égaux à n, on a $p_1 = 2$, $p_2 = 3$, $p_3 = 7$ et $p_4 = 43$.

c) Montrer que p_5 ne peut pas exister (on remarquera que $7 \mid 259$ et $13 \mid 1807$).

d) En déduire la liste complète (finie) des nombres de Lenstra.