UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2001–2002

DESS CCSI

Méthodes mathématiques de la cryptologie

Novembre 2001

Durée 2 heures

Documents manuscrits autorisés.

Exercice I

On considère l'équation

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

1) a) Montrer que pour tout $p \neq 2$ cette équation définit une courbe elliptique E sur $\mathbb{F}_p$.

b) Montrer que si $p \equiv 3 \pmod 4$ et si x est différent de 0 et ± 1, alors soit $x^3 - x$, soit $(-x)^3 - (-x)$ 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 $p \equiv 3 \pmod 4$.

2) On suppose maintenant que $p \equiv 1 \pmod 4$, ce qui équivaut d'après un théorème de Fermat au fait qu'il existe deux entiers a et b (évidemment avec a impair) tels que $p = a^2 + 4b^2$. On choisit le signe de a de telle façon que $a \equiv (p+1)/2 \pmod 4$.

Un beau résultat de la théorie de la multiplication complexe, qui n'est pas très difficile mais qu'on admettra, nous dit alors que le cardinal de $E(\mathbb{F}_p)$ est égal à $p + 1 - 2a$.

a) Ce résultat implique en particulier que $|E(\mathbb{F}_p)|$ est divisible par 8. Montrer directement qu'il est au moins divisible par 4.

b) En utilisant le résultat de multiplication complexe, calculer $|E(\mathbb{F}_p)|$ pour $p = 5$, $p = 13$, $p = 17$, puis pour $p = 661$.

c) Retrouver ce cardinal pour $p = 17$ en donnant explicitement la liste complète des points de $E(\mathbb{F}_p)$ (y compris le point à l'infini).

Exercice II

On rappelle l'important résultat suivant : si p est un nombre premier *différent de* 2 et $k \geq 1$, le groupe multiplicatif $(\mathbb{Z}/p^k\mathbb{Z})^*$ est un groupe cyclique de cardinal $p^k - p^{k-1}$. Un entier a dont la classe modulo p^k est un générateur de $(\mathbb{Z}/p^k\mathbb{Z})^*$ s'appelle une *racine primitive modulo* p^k

D'autre part on rappelle qu'un *nombre de Carmichael* est un entier $N \geq 2$ qui n'est pas un nombre premier, et tel que $a^{N-1} \equiv 1 \pmod N$ pour tout entier a tel que $(a, N) = 1$.

Soit donc N un nombre de Carmichael.

1) Soit p un diviseur premier de N différent de 2 et $k = v_p(N)$ l'exposant de p dans la factorisation de N.

a) En utilisant le théorème Chinois, montrer qu'on peut trouver a qui soit une racine primitive modulo p^k et qui vérifie de plus $(a, N) = 1$.

b) En déduire que $p^k - p^{k-1}$ divise $N - 1$.

c) En déduire que $k = 1$ et que $p - 1$ divise $N - 1$.

2) On se propose de montrer qu'en fait N est impair, c'est à dire que la restriction $p \neq 2$ de la première question n'est pas nécessaire. On suppose donc par l'absurde que N est impair.

a) En utilisant 1c), montrer que N doit être une puissance de 2, c'est à dire $N = 2^k$, et que $k \geq 2$.

b) En utilisant le groupe $(\mathbb{Z}/2^k\mathbb{Z})^*$ (qui n'est toutefois *pas* cyclique pour $k \geq 3$), en déduire une contradiction.

3) Nous avons donc démontré qu'un nombre de Carmichael est un nombre impair N sans facteur carré plus grand que 1, et tel que pour tout diviseur premier p de N on a $(p - 1) \mid (N - 1)$.

Réciproquement, on suppose ces propriétés vérifiées.

a) Montrer que pour tout diviseur premier p de N et pour tout entier a on a $a^N \equiv a \pmod p$.

b) En déduire que N est un nombre de Carmichael.

c) En déduire que si N est un nombre de Carmichael alors pour tout entier a (premier ou non avec N) on a $a^N \equiv a \pmod N$.

4) a) Montrer que tout nombre de Carmichael N possède au moins trois diviseurs premiers (par l'absurde, on écrira $N = pq$ avec $p < q$ et on utilisera la caractérisation obtenue à la question 2)).

b) Montrer que $N = 29341$ est un nombre de Carmichael (indication pour la factorisation : tous ses diviseurs sont congrus à 1 modulo 12).

Exercice III

Cet exercice est très semblable au précédent, et utilise des techniques très voisines.

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 de la forme pb avec p ne divisant pas b, 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, comme pour les nombres de Carmichael, N est égal à un produit de nombres premiers distincts.

2) a) En utilisant la question 1a) de l'exercice précédent, montrer que pour tout nombre premier p divisant N on a $(p-1) \mid N$.

b) 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 $(p-1) \mid N$.

c) 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 $j < k$.

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.