17 octobre 2014

AI 2014/2015

Dans tout le problème, p dsigne un nombre premier strictement supérieur à 3, $\mathbb{Z}/p\mathbb{Z}$ l'anneau quotient de $\mathbb{Z}$ formé des classes résiduelles modulo p, et $\overline{n}$ la classe modulo p de l'entier n.
Si A est un anneau fini, d'unité e, on appelle ordre d'un élément inversible a de A le plus petit entier strictement positif n tel que $a^n = e$.
Pour toute matrice carrée M à coefficients dans un corps, on note $\Delta(M)$ son déterminant et $T(M)$ sa trace.

Préliminaires

1. Soit $k \in \mathbb{N}$, calculer $\displaystyle\sum_{j=0}^{k-1} 4^j$.

2. Montrer que $\forall p \in \mathbb{N}^*, p$ premier, $\forall j \in [\![1, p-1]\!]$, $p | C_p^j$.

Partie I

1. Soit A_p l'ensemble des matrices à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, de la forme $R = \lambda M + \mu I$, où $M = \begin{pmatrix} \overline{4} & \overline{1} \\ -\overline{1} & \overline{0} \end{pmatrix}$ et $I = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$, λ et μ dans $\mathbb{Z}/p\mathbb{Z}$.

   Montrer que A_p est un anneau commutatif pour les opérations usuelles. Donner le nombre des éléments de A_p.

2. Calculer $T(R)$ et $\Delta(R)$ pour R dans A_p; puis exprimer $T(R^2)$ et $\Delta(R^2)$ en fonction de $T(R)$ et $\Delta(R)$.

3. Montrer que deux quelconques des situations suivantes impliquent la troisième :

   (a) $T(R) = \overline{0}$,

   (b) $\Delta(R) = \overline{1}$,

   (c) l'ordre de R est 4.

4. On considére la suite des entiers Y_k, $k \in \mathbb{N}$, définie par $Y_0 = 2$, et $Y_{k+1} = 2Y_k^2 - 1$, $k \in \mathbb{N}$.

   Comparer Y_k et $T(M^{2^k})$.

5. Montrer que M est d'ordre 2^k si et seulement si p divise Y_{k-2}.

Partie II

1. (a) Montrer que R est inversible dans A_p si et seulement si $\Delta(R) \neq \overline{0}$.
   (b) Montrer que A_p est un corps si et seulement si $\overline{3}$ n'est pas le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

2. Dans cette question, on suppose que $\overline{3}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ (avec $\overline{3} = a^2, a \in \mathbb{Z}/p\mathbb{Z}$).
   (a) Montrer que M est diagonalisable. On notera P la matrice de passage.
   (b) On introduit $U = P^{-1}E_{11}P$, et $V = P^{-1}E_{22}P$. Montrer que $A_p = Vect(U, V)$.
   (c) A l'aide de la question précèdente, introduire un isomorphisme d'espace vectoriel entre A_p et $(\mathbb{Z}/p\mathbb{Z})^2$, et montrer que c'est un isomorphisme d'algèbre.
   (d) Donner le nombre d'éléments de A_p de déterminant $\overline{1}$, ainsi que celui de ses éléments inversibles.

3. Dans cette question, on suppose que $\overline{3}$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.
   (a) Montrer que Δ donne un homomorphisme du groupe multiplicatif des éléments non nuls de A_p dans celui des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$.
   En déduire que le nombre des éléments de l'image de Δ est un diviseur de $p-1$ et que celui des éléments du noyau de Δ est un multiple de $p+1$.
   (b) Vérifier que pour tout $\lambda \in \mathbb{Z}/p\mathbb{Z}$, il y a au plus deux éléments μ de $\mathbb{Z}/p\mathbb{Z}$ tels que $\Delta(\lambda M + \mu I) = \overline{1}$. Donner alors le nombre des éléments de A_p de déterminant $\overline{1}$.

4. Montrer que l'ordre de M divise le nombre des éléments de A_p de déterminant $\overline{1}$.
   En déduire que, si p divise Y_{k-2}, alors 2^k divise $p-1$ ou $p+1$.

Partie III

On suppose dans cette partie que p est de la forme $2^m - 1$.

1. Montrer que m est impair, et que 3 divise $p-1$. Etablir aussi que $\overline{2}$ est un carré de $\mathbb{Z}/p\mathbb{Z}$ et que $-\overline{1}$ n'en est pas un.

2. Montrer que les ordres des éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ divisent $p-1$. A l'aide de $P(X) = X^{\frac{p-1}{3}} - \overline{1}$, montrer que les ordres de ces éléments ne divisent pas tous $\frac{p-1}{3}$.
   En déduire l'existence d'un élément b de $\mathbb{Z}/p\mathbb{Z}$ d'ordre 3. Calculer $(2b + \overline{1})^2$.

3. Montrer que ni $\overline{3}$, ni $\overline{6}$ ne sont des carrés dans $\mathbb{Z}/p\mathbb{Z}$. Prouver que les ordres des éléments de A_p de déterminant $\overline{1}$ divisent 2^m mais ne divisent pas 2^{m-1}.

4. Résoudre l'équation $X^2 = M, X \in A_p$.
   On notera X_1 une des deux racines.

5. (a) Calculer M^p à l'aide de X_1 et I.
   En déduire X_1^{p+1}.
   (b) Calculer l'ordre de M.

Partie IV

Etablir le critère suivant :
Soit q un entier supérieur ou égal à 3 ; alors $2^q - 1$ est premier si et seulement si $2^q - 1$ divise Y_{q-2}.
Décomposer Y_3 en facteur premier.

Les questions III.1 et III.2 sont indépendantes des parties I et II.
Les nombres de la forme $M(p) = 2^p - 1$ sont appelés nombres de Mersenne. (Marin Mersenne : 1644).

Valeur de p pour laquelle $M(p)$ premier:	$M(p)$	nombre de chiffres en base 10	date de la preuve	auteur(s) de la preuve:
2	3	1	antiquité	
3	7	1	antiquité	mentionnés dans les
5	31	2	antiquité	"éléments" d'Euclide
7	127	3	antiquité	
13	8191	4	1461	
17	131071	6	1588	Cataldi
19	524287	6	1588	Cataldi
31	2147483647	10	1772	Euler
61		19	1883	Pervushin
89		27	1911	Powers
107		33	1914	Powers
127		39	1876	Lucas
521		157	1952	Robinson
607		183	1952	Robinson
1279		386	1954	Robinson
2203		664	1954	Robinson
2281		687	1954	Robinson
3217		969	1957	Riesel
4253		1281	1961	Hurwitz
4423		1332	1961	Hurwitz
9689		2917	1963	Gillies
9941		2993	1963	Gillies
11213		3376	1963	Gillies
19937		6002	1971	Tuckerman
21701		6533	1978	Noll

A partir de Robinson, les calculs ont été fait par ordinateur. Le test utilisé a été énoncé en 1876 par Edouard Lucas et amélioré en 1930 par D.H. Lehmer : c'est le test de Lucas-Lehmer.