DM n°7

PREMIER EXERCICE

Il s'agit d'un résultat classique à connaitre

Cryptographie

Le but de se problème est l'étude du principe de criptage RSA, qui permet de communiquer de façon sure des données. Ce résultat est à connaitre

1. Chiffrement du message

   On étudie le cryptage d'un message par un expéditeur. Soient p et q des nombres premiers distincts et n leur produit : $n = pq$. On appelle n *module de chiffrement*

   (a) Donner sans démonstration, en fonction de p et q, la valeur de $\varphi(n)$.

   (b) Soit e un entier premier avec $\varphi(n)$. On appelle e *exposant de chiffrement*. Montrer qu'il existe un entier naturel d tel que $ed \equiv 1\,[\varphi(n)]$

   Le couple (n, e) est appelé clef publique (elle peut être transmise à l'expéditeur), le couple (n, d) est appelé clef privée, elle reste connue du seul destinataire du message.

   Dans la suite on considère un entier M (représentant le message) strictement inférieur à n. On note C l'élément de $\{0, 1, \ldots, n-1\}$ congru à M^e modulo n. Cet entier représente le message codé qui est transmis.

2. déchiffrement du message

   On se propose de montrer que C^d est congru à M *modulo* n, ce qui permet au destinataire de trouver M, grâce à sa clef (n, d).

   (a) Montrer que M^{ed} est congru à M *modulo* p. On distinguera les deux cas M premier avec p et M non premiers avec p.

   (b) En déduire que $C^d \equiv M[n]$.

   Remarque : pour trouver d à partir de e et n il faut savoir inverser e dans $\mathbf{Z}/\varphi(n)\mathbf{Z}$ ce qui nécessite de connaitre $\varphi(n)$ et donc le couple (p, q). La décomposition de n en facteurs premiers peut être très difficile si les nombres premiers p et q ont été choisis très grands.

SECOND EXERCICE (3/2 : 1.,2.,3.,4. et 5. ; 5/2 : tout)

Entiers de Gauss

Soient $\mathbf{Z}[i]$ l'ensemble des nombres complexes de la forme $u + iv$, avec $(u, v) \in \mathbf{Z}^2$ et l'application. $\varphi\,;\, \mathbf{Z}[i] \to \mathbf{N}\,;\, a \mapsto \bar{a}a$.

1. Montrer que $\mathbf{Z}[i]$ est un sous-anneau du corps $\mathbf{C}$.
2. Déterminer $\mathbf{Z}[i]^*$, ensemble des éléments inversibles de $\mathbf{Z}[i]$.
3. Montrer que pour tout élément a de $\mathbf{Z}[i]$ et tout élément b de $\mathbf{Z}[i]^*$, il existe un couple (q, r) d'éléments de $\mathbf{Z}[i]$ tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$. On dit que l'anneau $\mathbf{Z}[i]$ est euclidien pour φ.
4. Montrer que tout idéal de $\mathbf{Z}[i]$ est de la forme $a\mathbf{Z}[i]$, on dit que $\mathbf{Z}[i]$ est principal.
5. Soit a un élément de $\mathbf{Z}[i]$. Montrer que si $\varphi(a)$ est premier, alors a est un élément irréductible de $\mathbf{Z}[i]$. Rappelons qu'un élément a d'un anneau intègre est dit irréductible si par définition il n'est pas inversible et si il admet la décomposition $a = bc$, alors a ou b est inversible.
6. Soit p un nombre premier impair et y un élément de $(\mathbf{Z}/p\mathbf{Z})^*$, on dit que y est un carré s'il existe un élément z de $(\mathbf{Z}/p\mathbf{Z})^*$ tel que $z^2 = y$.

   (a) Montrer que $\displaystyle\prod_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x = \begin{cases} -y^{\frac{p-1}{2}}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}}, & \text{sinon .} \end{cases}$

   Indication : on pourra regrouper deux à deux dans le produit les termes x et yx^{-1}.

(b) En déduire

$$\begin{cases} y^{\frac{p-1}{2}} = \bar{1}, & \text{si } y \text{ est un carré,} \\ y^{\frac{p-1}{2}} = -\bar{1}, & \text{sinon .} \end{cases}$$

7. Soit p un nombre premier, impaire OU NON. Montrer l'équivalence entre les propriétés suivantes :
   i. p est irréductible dans $\mathbf{Z}[i]$;
   ii. $p \equiv 3\ [4]$;
   iii. Il n'existe pas d'élément a de $\mathbf{Z}[i]$ tel que $p = \phi(a)$.
8. En déduire les irréductibles de $\mathbf{Z}[i]$.

PROBLÈME

Première partie : Un exemple d'extension du corps $\mathbf{Q}$ (3/2)

1. Soit P le polynôme $X^3 - X - 1$.
   Montrer que P n'a pas de racines rationnelles. En déduire que P est irréductible dans $\mathbf{Q}[X]$.
   Montrer que P a une racine réelle que l'on notera ω.
2. Soit $\mathbf{K}$ le $\mathbf{Q}$-espace vectoriel engendré par $\left(\omega^i\right)_{i\in\mathbf{N}}$.
   Montrer que $\mathbf{K}$ est de dimension finie, et donner une base simple de K.
3. Montrer que $\mathbf{K}$ est une $\mathbf{Q}$-sous-algèbre de $\mathbf{R}$, muni de sa structure naturelle de $\mathbf{Q}$-algèbre.
4. Montrer que $\mathbf{K}$ est un sous-corps de $\mathbf{R}$.

Deuxième partie : Cas général d'extension de $\mathbf{Q}$ (5/2)
Soit a un réel.

1. Montrer que tout sous-corps de $\mathbf{R}$ contient $\mathbf{Q}$.
2. Montrer que l'ensemble des sous-corps de $\mathbf{R}$ qui contiennent a admet un plus petit élément pour l'inclusion. On le notera dans la suite $\mathbf{Q}(a)$.
3. Montrer que $\phi\ :\ \mathbf{Q}[X] \to \mathbf{R}\,;\ P \mapsto P(a)$ est un morphisme de la $\mathbf{Q}$-algèbres $\mathbf{Q}[X]$ dans la $\mathbf{Q}$ algèbre $\mathbf{R}$. On note $\mathbf{Q}[a]$ son image.
4. Soit $I := \{P \in \mathbf{Q}\,[X]\,, P\,(a) = 0\}$. Montrer que I est un idéal de $\mathbf{Q}[X]$.
5. Le réel a est dit algébrique (sur $\mathbf{Q}$), si, par définition, a est racine d'un polynôme non nul à coefficients entiers.
   Montrer que a est algèbrique si et seulement si I est non réduit à $\{0\}$.
   Dans cette partie on suppose dans la suite que que a est algèbrique, sauf à la dernière question.
6. Montrer qu'il existe un et un seul élément de $\mathbf{Q}[X]$ unitaire, μ_a, tel que $I = \mu_a\mathbf{Q}[X]$.
   Montrer que μ_a est irréductible dans $\mathbf{Q}[X]$. Montrer que si a est irrationnel, alors le degré de μ_a est supérieur ou égal à 2. Déterminer μ_a pour $a = \sqrt{2}$ et pour $a = \sqrt{\frac{1+\sqrt{5}}{2}}$.
7. Montrer que $\mathbf{Q}[a]$ est un corps. Montrer que $\mathbf{Q}(a) = \mathbf{Q}[a]$.
   Montrer que $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension n, où n est le degré de μ_a, dont on donnera une base simple.
8. Si a est non algébrique, montrer qu'alors $\mathbf{Q}(a)$ est un $\mathbf{Q}$-espace vectoriel de dimension infinie [1].

Troisième partie : Corps finis (5/2) (3/2)
Soit $(\mathbf{F}, +, \times)$ un corps. On note $1_\mathbf{F}$ l'unité de $\mathbf{F}$ et pour tout entier k et tout élément a de $\mathbf{F}$, $k \cdot a$, désigne l'élément $\underbrace{a + a + \cdots + a}_{k \text{ termes}}$ pour $k \geq 1$, l'élément $\underbrace{(-a) + (-a) + \cdots + (-a)}_{-k \text{ termes}}$ pour $k \leq -1$ et enfin $1_\mathbf{F}$ pour $k = 0$
On admet le résultat élémentaire suivant :
L'application

$$\varphi\ :\ \mathbf{Z} \to \mathbf{F}\,;\ k \mapsto k \cdot 1_\mathbf{F}$$

est un morphisme d'anneaux.
Son noyau est donc un sous groupe de $(\mathbf{Z}, +)$, donc de la forme pZ, où p désigne un élément de $\mathbf{N}$. L'entier naturel p s'appelle caractéristique de $\mathbf{F}$.

1. On pourrait montrer que $\mathbf{Q}(a)$ est isomorphe en tant que corps au corps $\mathbf{Q}(X)$.

1. Montrer que si p est nul alors $\mathbf{F}$ est infini.

   Dans toute la suite on supposera que F est fini, donc que p est non nul.

2. Montrer qu'il existe une et une seule application $\tilde{\varphi}$ de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathbf{F}$ tel que $\varphi = \tilde{\varphi} \circ \pi_p$, où π_p désigne la surjection (dite canonique) de $\mathbf{Z}$ sur $Z/p\mathbf{Z}$, qui à un entier x associe sa classe modulo p.
3. Montrer que $\tilde{\varphi}$ est un morphisme d'anneaux injectif.
4. On note $\mathbf{k} = \tilde{\varphi}(\mathbf{Z}/p\mathbf{Z})$. Montrer que $\mathbf{k}$ est un sous-anneau de $\mathbf{F}$ isomorphe à $\mathbf{Z}/p\mathbf{Z}$. En déduire que p est un nombre premier.
5. Montrer que $\mathbf{k}$ est le plus petit sous-corps de $\mathbf{F}$.

   Le sous-corps $\mathbf{k}$ est appelé sous corps premier de $\mathbf{F}$, on vient de voir qu'il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$
6. En munissant $\mathbf{F}$ d'une structure d'espace vectoriel sur $\mathbf{k}$, montrer que le cardinal de $\mathbf{F}$ est une puissance de p.

   L'étude de la réciproque est traitée dans le DM 1-ter.