Rapport du jury

> Il est attendu de construire rapidement Z/nZ, puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution des systèmes de congruences. Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème RSA. Si des applications en sont proposées, l'étude des morphismes de groupes de Z/nZ dans Z/mZ ou le morphisme de Frobenius peuvent figurer dans la leçon. Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans Z/nZ, au logarithme discret, ou à la transformée de Fourier rapide.

Références

- Elements d'analyse réelle - J-E. Rombaldi
- Cours d'algèbre - Damazure
- Théorie de Galois - Escofier
- Algèbre - le Grand combat - Berhuy

Développements

- Test de Solovey Strassen
- Cyclotomie (réductibilité dans $\mathbb{F}_q[X]$)

Méta-plan

1. Anneaux $\mathbb{Z}/n\mathbb{Z}$: une étude structurelle
    1. Construction des anneaux Z/nZ. Congruence
    2. Aspects arithmétiques
    3. Groupe des inversibles.

2. Occurences en algèbre abstraite
    1. Théorie des groupes
    2. Théorie des anneaux et des corps
3. Résidus quadratiques
    1. Symboles de Legendre et de Jacobi
    2. Test de Solovey-Strassen

Plan détaillé

I - Etude structurelle [Rombaldi]

On fixe n un entier naturel.

1 - Construction des anneaux Z/nZ. Congruence.

1. Proposition : $(\mathbb{Z}, +, \times)$ est un anneau euclidien, donc principal. En particulier, les seuls idéaux de $\mathbb{Z}$ sont les $(n\mathbb{Z})_{n\in\mathbb{N}}$.
2. Définition (anneau Z/nZ, congruence) : on appelle Z/nZ l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$, muni de sa structure d'anneau quotient. On dit alors que deux entiers a et b sont congrus modulo n si leurs projections dans le quotient Z/nZ sont égales.
3. Lemme : soient a et b deux entiers relatifs. Les assertions suivantes sont équivalentes :
    1. $a \equiv b[n]$
    2. Il existe $k \in \mathbb{Z}$ tel que $a = b + kn$
    3. a et b ont même reste dans la division euclidienne par n.
4. Exemples :
    1. La congruence modulo 0 est la relation d'égalité.
    2. Tous les entiers relatifs sont congrus modulo 1.
    3. 6 et 71 sont congrus modulo 7 mais pas modulo 2.
5. Remarque : les projections sur l'anneau quotient étant des morphismes de $\mathbb{Z}$-algèbres, la relation de congruence est compatible avec les opérations de $\mathbb{Z}$-algèbre.
6. Application : calcul du dernier chiffre de $7 \uparrow\uparrow 6$ en écriture décimale.
7. Application : un entier est divisible par 4 si, et seulement si, le nombre obtenu en ne gardant que ses deux derniers chiffres en écriture décimale est

divisible par 4.

8. Proposition : si $d|n$, alors la projection $\pi_d : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ passe au quotient dans $\mathbb{Z}/n\mathbb{Z}$.

2 - Théorème chinois

1. Théorème (chinois) : soit $(n_1, \dots, n_k)$ une famille d'entiers dont on note n le produit. On a équivalence :
    1. Ces entiers sont deux à deux premiers entre eux.
    2. On a l'isomorphisme de $\mathbb{Z}$-algèbres :

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$$

    Lorsque ces conditions sont satisfaites, l'isomorphisme de $\mathbb{Z}$-algèbres est donné explicitement par [formule habituelle].
2. Exemple : cas $n = \prod p_i^{\alpha_i}$
3. Corollaire : si $(n_1, \dots, n_k)$ sont deux à deux premiers entre eux de produit n, alors on a un isomorphisme de groupes :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{k} (Z/n_i\mathbb{Z})^\times$$

    obtenu par restriction de l'isomorphisme précédent.
4. Contre-exemple : $n = 4 = 2 \times 2$
5. Proposition : soient $(n_1, \dots, n_k)$ deux entiers deux à deux premiers entre eux. Soit $(u_1, \dots, u_k)$ des entiers tels que $\sum u_i n_i = 1$. L'isomorphisme du théorème précédent admet pour inverse :

$$(\pi_i(a_i))_{1 \leq i \leq k} \mapsto \pi_n \left(\sum_{i=1}^{k} u_i a_i \frac{n}{n_i} \right)$$

6. Application : on considère le système d'équations diophantiennes

$$k \equiv b_i [n_i],\ 1 \leq i \leq q$$

    om les n_i sont deux à deux premiers entre eux. Alors k est solution du système d'équation si, et seulement si, il est solution de l'équation unique

$k \equiv \sum_{i=1}^{k} u_i a_i \frac{n}{n_i}[n]$ avec n le produit des n_i est u_i des coefficients de Bézout associés à la famille n_i.

7. Exemple : L'ensemble des solutions de :

$$\begin{cases} k \equiv 2[4] \\ k \equiv 3[5] \\ k \equiv 1[9] \end{cases}$$

est donné par $118 + 180\mathbb{Z}$.

3 - Groupe des inversibles

On fixe a et n des entiers avec n strictement positif.

1. Lemme : a est inversible modulo n si, et seulement si, il est premier avec n. Dans ce cas, si u et v sont des entiers tels que $au + bv = 1$, u est l'inverse de a modulo n et peut être calculé à l'aide de l'algorithme d'Euclide étendu. Dans le cas contraire, a est nul ou un diviseur de 0 modulo n.
2. Corollaire : Les assertions suivantes sont équivalentes.
    1. $\mathbb{Z}/n\mathbb{Z}$ est intègre.
    2. $\mathbb{Z}/n\mathbb{Z}$ est un corps.
    3. n est premier.
3. Application : soi $1 \leq k \leq n$. Le nombre complexe $e^{(2k\pi)/n}$ est est une racine primitive n-ième de l'unité ssi k est premier avec n.
4. Définition (indicatrice d'Euler) : on note $\phi(n)$ l'ordre du groupe multiplicatif $(Z/nZ)^\times$.
5. Exemple : $\phi(4) = 2$. p est premier ssi $\phi(p) = p - 1$.
6. Proposition : si $n = \prod p_i^{\alpha_i}$, alors $\phi(n) = n \prod (1 - 1/p_i)$.
7. Lemme :

$$n = \sum_{d|n} \phi(d)$$

8. Application : soit K un corps et $G < K^\times$ un sous-groupe du groupe multiplicatif de K. Alors G est cyclique. En particulier, si p est premier, $(Z/pZ)^\times$ est cyclique.

II - Liens avec des structures algébriques abstraites

1 - Théorie des groupes [Rombaldi]

1. Proposition : Z/nZ est un groupe cyclique d'ordre n. L'ensemble de ses générateurs est donné par $(Z/nZ)^\times$.
2. Théorème : un groupe G est cyclique si, et seulement si, il est isomorphe à (Z/nZ).
3. Application : si G est un groupe cyclique et d un diviseur de son ordre, G admet un unique sous-groupe d'ordre d, et celui-ci est isomorphe à Z/dZ.
4. Théorème (structure des groupes abéliens de type fini) : soit G un groupe abélien de type fini. Il existe un unique entier r et une unique suite d'entiers $a_1|\dots|a_k$ tels que :

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{k} \mathbb{Z}/a_i\mathbb{Z}$$

5. Application : si G est un groupe abélien fini et si d divise l'ordre de n, G admet un sous-groupe d'ordre d.

2 - Théorie des anneaux et des corps [Escofier]

1. Proposition / définition (caractéristique d'un anneau) : soit A un anneau commutatif unitaire. Il existe un unique morphisme d'anneaux $\mathfrak{s} : \mathbb{Z} \to A$ dit morphisme structural de A. On appelle caractéristique de A l'unique entier positif n tel que $Ker(\mathfrak{s}) \cong n\mathbb{Z}$.
2. Remarque : si n est la caractéristique de A, alors Z/nZ s'identifie à un sous-anneau de A.
3. Application : si K est un corps fini, sa caractéristique est un nombre premier p, et il existe $\alpha > 0$ tel que $|K| = p^\alpha$.

> Dans la suite, on supposera connue la théorie élémentaire des corps finis.

4. Définition : polynôme cyclotomique à coefficients dans un corps quelconque.
5. Lemme : Dans un corps K quelconque, on a $X^n - 1 = \prod_{d|n} \Phi_d$ dès que n est premier avec la caractéristique du corps K.
6. Corollaire : si K est de caractéristique 0, $\Phi_n \in \mathbb{Z}[X]$.
7. Lemme : soit p un nombre premier, q une puissance non-nulle de p est $\mathbb{F}_q$ le corps fini à q éléments. Alors, si n est premier avec p, $\Phi_{n,\mathbb{F}_q}$ est le projeté

dans $\mathbb{Z}/p\mathbb{Z}[X]$ de $\Phi_{n,\mathbb{Q}}$. (DVT 1)

8. Théorème : on note $L/\mathbb{F}_q$ l'extension de décomposition de Φ_n et s son degré. Alors tous les facteurs irréductibles de Φ_n sont d'ordre s, et s est l'ordre de q dans $(Z/nZ)^\times$. (DVT 1)
9. Application : Φ_8 est un polynôme irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$ mais dont le projeté est réductible dans tout corps fini. (DVT 1)

III - Résidus quadratiques

1 - Symboles de Legendre et de Jacobi [Berhuy]

1. Définition : un entier a est dit résidus quadratique modulo n si son projeté dans Z/nZ est un carré non nul.

> On va commencer par traiter le cas où n est premier.

2. Définition (symbole de Legendre)
3. Lemme : $(a/p) \equiv (-1)^{(p-1)/2}[p]$
4. Définition (symbole de Jacobi)
5. Remarque : si a est un résidus quadratique modulo n, $(a/n) = 1$ mais la réciproque est fausse.
6. Théorème (lois de réciprocité quadratique, Legendre et Jacobi, admis)
7. Théorèmes (lois complémentaires)
8. Application : détermination d'un résidus quadratique

2 - Test de Solovey-Strassen [Demazure]

1. Définition (nombre de Carmichael)
2. Proposition : soit n un entier composé, $n = \prod p_i^{\alpha_i}$. Alors n est de Carmichael ssi tous les α_i valent 1 et si pour tout i, $p_i - 1 | n - 1$. (DVT 2)
3. Théorème (Solovey-Strassen) : soit n un entier impair. Alors n est premier ssi pour tout a premier avec n, $(a/n) \equiv (-1)^{\frac{n-1}{2}}[n]$. (DVT 2)
4. Remarque : si n est composé, l'ensemble des éléments a de $[[1, n-1]]$ premiers avec n tels que $(a/n) \not\equiv (-1)^{\frac{n-1}{2}}[n]$ est de cardinal au moins $\phi(n)/2$ (DVT 2)
5. Application (algorithme de Solovey-Strassen) :
   Entrée : n, k des entiers

Sortie : 0 ou 1
Répéter k fois :
choisir a aléatoirement dans $[[1, n-1]]$ et calculer $a \wedge n$
si $a \wedge n \neq 1$:
renvoyer 0
sinon calculer a^{n-1} modulo n.
si ça n'est pas 1 :
renvoyer 0
sinon calculer (a/n) et $a^{\frac{n-1}{2}}$ modulo n.
si ces quantités sont différentes :
renvoyer 0
renvoyer 1
Si cet algo renvoie 0, n est composé. Sinon, n est premier avec probabilité $> 1/2^k$.