Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Perrine Jouteur

On construit rapidement $\mathbf{Z}/n\mathbf{Z}$, puis on en décrit 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.

Les applications sont très nombreuses. Les 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 $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}/m\mathbf{Z}$ ou le morphisme de Frobenius peuvent figurer dans la leçon.

S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le PGCD et le PPCM de ces éléments.

Enfin, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbf{Z}/n\mathbf{Z}$, au logarithme discret, ou à la transformée de Fourier rapide.

1 Plan

I- Introduction : constructions

- Prop : les idéaux de $\mathbb{Z}$
- Définition de $\mathbb{Z}/n\mathbb{Z}$, cardinal $= n$.
- Notation : quand deux entiers ont la même classe modolu n, on note $x \equiv y\ [n]$.
- Prop : ce sont des anneaux commutatifs, unitaires, euclidiens par transport de la structure de $\mathbb{Z}$.
- Exemple avec $\mathbb{Z}/12\mathbb{Z}$.

II - Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$

1) Inversibles dans $ZZ/n\mathbb{Z}$

- Prop : $[x]$ est inversible ssi x est premier avec n ssi $[x]$ n'est pas un diviseur de zéro.
- Définition de l'indicatrice d'Euler, c'est le cardinal des inversibles.
- Prop : si $n = p$ est premier, $\phi(p) = p - 1$ et tout le monde est inversible. Si $n = p^r$, avec p premier, alors $\phi(p^r) = p^{r-1}(p-1)$.
- Exemples
- Prop : les inversibles sont exactement les générateurs du groupe additif. (rem : c'est le cas dans n'importe quel anneau).
- Prop : lemme de Fermat (bien dire que c'est juste Lagrange en fait)
- Prop : lien avec les automorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$.

2) Cas où n est premier

- Rem : on vient de voir que si n est un nombre premier p, le groupe des inversibles est maximal. Ceci signifie que l'anneau est en fait un corps, noté $\mathbb{F}_p$.
- Prop : la réciproque est vraie, i.e. si $\mathbb{Z}/n\mathbb{Z}$ est un corps alors n est premier.
- Prop : $\mathbb{F}_p$ est l'unique corps de cardinal p (à isomorphisme près).
- Prop : le groupe des inversibles d'un corps fini est cyclique, donc $\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.
- Rem : d'après le lemme de Fermat, on a un critère de non primalité.
- Rem : l'application $x \mapsto x^p$ est un morphisme de corps de $\mathbb{F}_p$, qui est en fait l'identité.
- Rem : les corps $\mathbb{F}_p$ sont les sous-corps premiers de tous les corps de caractéristique non nulle.

III - Décompositions en produits d'anneaux modulaires

1) Théorème chinois
- recopier Mérindol
- Développement 1
- Exemple
- Application : RSA
- Rem : généralisation à plus de deux nombres premiers

2) Retour sur le groupe des inversibles
- Recopier Perrin page 25
- Coro : ϕ est multiplicative

3) Intérêt de la structure de groupe de $\mathbb{Z}/n\mathbb{Z}$
- Prop : pour tout d divisant n, il existe un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. C'est même caractéristique des groupes cycliques. (cf Delcourt)
- Prop : Théorème de structure des groupes abéliens de type fini

IV - Utilisation en algorithmique

1) Tests de primalité
- Développement 2 : Solovay-Strassen

2) Polynômes
- Algo de factorisation
- Borne de Mignotte, pour trouver des polynômes irréductibles de degré donné

3) Racines carrés

2 Développements

- Solovay-Strassen
- Théorème chinois généralisé