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

1. Rapport du jury. — *Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il serait bon de connaître les idéaux de Z/nZ et, plus généralement, les morphismes de groupes de Z/nZ dans Z/mZ. Il est nécessaire de bien maîtriser le théorème chinois et sa réciproque. 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. Il faut bien sûr savoir appliquer le théorème chinois à l'étude du groupe des inversibles et, ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du théorème chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents et les idempotents. Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux Z/nZ, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans Z/nZ.*

2. Généralités. —

1. *Définition et appropriation.* —

- Rappels sur $\mathbb{Z}$:
  - $(\mathbb{Z}, +, \cdot)$ est un anneau intègre euclidien. Il est donc aussi factoriel et principal.
  - Rem : son corps de fractions est $\mathbb{Q}$.
  - Ses seuls idéaux sont les $n\mathbb{Z}$. Ils sont principaux. Nous avons donc les notions de PGCD et de PPCM.
- $\mathbb{Z}/n\mathbb{Z}$. Puisque $n\mathbb{Z}$ est *un idéal* :
  - $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.
  - $\mathbb{Z}/n\mathbb{Z}$ est cyclique et $Card(\mathbb{Z}/n\mathbb{Z}) = n$.
  - La multiplication est ici la répétition de la somme : on a donc
$$\overline{nm} = (\overline{n})(\overline{m}) = n\overline{m} = nm\overline{1}$$
  - La relation d'équivalence induite par $n\mathbb{Z}$ par $(x\mathscr{R}x) \iff (x - y \in n\mathbb{Z})$ est compatible avec les deux opérations.
  - On note souvent $(a\mathscr{R}b)$ ainsi : $a \equiv b\ (mod.n)$
  - La projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, qui à $x \mapsto \dot{x}$ est un épimorphisme d'anneaux.
- Si $p \in \mathbb{P}$:
  - (p) est alors *un idéal premier* et ce sont les seuls.
  - Conséquence : $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre ssi p est premier.
  - (p) est *un idéal maximal* et ce sont les seuls.
  - Conséquence : $\mathbb{Z}/p\mathbb{Z}$ est un corps ssi p est premier.
  - Rem : il existe un résultat plus général : "tout anneau intègre fini est un corps". En effet, $\forall a \in A$, le caractère intègre assure l'injectivité du morphisme $x \mapsto ax$ et donc la bijectivité et l'existence d'un inverse.
- Rem : comme les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont, soit des corps, soit non intègres, on ne parlera pas de division euclidienne ni de PGCD/PPCM. En revanche, on pourra le faire pour les anneaux $\mathbb{Z}/p\mathbb{Z}[X]$.
- Pro : tout anneau cyclique (dans le sens monogène et fini) (A) d'ordre k est isomorphe à $\mathbb{Z}/k\mathbb{Z}$.
  - On considère le morphisme $\varphi : \mathbb{Z} \to (A)$ qui envoie $n \mapsto n \cdot x = \sum_{i=1}^{n} x$, où x est un générateur de A.
  - φ est donc surjective.
  - $Ker(\varphi) \neq \{0\}$ puisque A est infini et pas $\mathbb{Z}$.
  - $\exists n \in \mathbb{N}$, tel que $Ker(\varphi) = n\mathbb{Z}$.
  - Et donc $A \sim \mathbb{Z}/n\mathbb{Z}$
- Exe : $(\mathbb{U}_n(\mathbb{C}), \cdot)$, groupe des racines n-ièmes de l'unité, est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Pro : il existe un sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ ssi $d|n$ auquel cas ce groupe est unique et cyclique.
- CN : par Lagrange et car un sous-groupe cyclique est cyclique. Enfin, YYYY

2. *Éléments générateurs et groupe des unités de* $\mathbb{Z}/n\mathbb{Z}$. —

- *Éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$:
  - Pro : les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ sont les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$
  - En effet, $\dot{x}$ est générateur ssi $1 \in < x >$ et Bézout permet de conclure.
- *Éléments générateurs de* $\mathbb{Z}/n\mathbb{Z}$:
  - Pro : les générateurs sont donnés par les $k \leq n$ tels que $k \wedge n = 1$.
  - Ceci découle en fait de Bézout ($uk + vn = 1$ et donc $m \equiv (mu)k\ (mod.n)$).
  - Pro : il existe donc $\varphi(1)$ où φ désigne l'indicatrice d'Euler comme on le verra ci-après.
- *Lemme Chinois :*
  - $p \wedge q = 1 \iff [\mathbb{Z}/pq\mathbb{Z} \equiv (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})]$
  - On a en effet un homomorphisme donné par $h : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ tel que $n \mapsto (n_{modp}, n_{modq})$
  - $Ker(h) = pq\mathbb{Z}$ (car dans ce cas $PPCM(p, q) = pq$).
  - On a donc l'isomorphisme $\mathbb{Z}/pq\mathbb{Z} \equiv (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})$
- *Fonction indicatrice d'Euler :* nombre d'entiers inférieur à n et premiers avec lui.
  - $\varphi : \mathbb{N}^* \to \mathbb{N}$
  - Suite au lemme Chinois : $\varphi(ab) = \varphi(a)\varphi(b)$ si $a \wedge b = 1$. Il suffit en effet de comparer les cardinaux des inversibles des deux anneaux isomorphes que sont dans ce cas $\mathbb{Z}/pq\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})$.
  - Par définition : $\varphi(p) = p - 1 = p(1 - \frac{1}{p})$ ssi $p \in \mathbb{P}$.
  - On observe que : $\varphi(p^\alpha) = p^{\alpha-1}(p - 1)$ si $p \in \mathbb{P}$.
  - Au final, si $n = \Pi p_i^{\nu_i}$, $\varphi(n) = \Pi[p_i^{\nu_i - 1}(p_i - 1)]$

- Et aussi : $\varphi(n) = n\Pi[(1 - \frac{1}{p_i})]$

– Thé : *Théorème de structure des groupes multiplicatifs des* $(\mathbb{Z}/n\mathbb{Z})^*$:
- Si $p \in \mathbb{P}$, $((\mathbb{Z}/p\mathbb{Z})^*, \dot{})$ est un groupe cyclique d'ordre $p-1$ ayant $\varphi(p_1)$ générateurs.
- Pour $n = p^\alpha$ avec $p \geq 3 \in \mathbb{P}$, $((\mathbb{Z}/p^\alpha\mathbb{Z})^*, \dot{})$ est un groupe cyclique ayant $\varphi(p_1)$ générateurs. Il est donc isomorphe à $(\mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}, .) = (\mathbb{Z}/(p^{\alpha-1}(p-1)\mathbb{Z}, .)$
- Pour $n = 2^\alpha$, avec $\alpha \geq 3$, $((\mathbb{Z}/2^\alpha\mathbb{Z})^*, \dot{}) \sim (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}, \dot{})$. Le groupe $((\mathbb{Z}/2^\alpha\mathbb{Z})^*, \dot{})$ n'est donc pas cyclique.
- Grâce au lemme Chinois, on peut compléter pour $n = \Pi p_i^{\alpha_i}$, $((\mathbb{Z}/n\mathbb{Z})^*, \dot{}) \sim \Pi(\mathbb{Z}/{p_i}^{\alpha_i}\mathbb{Z})^*$

3. *Quelques propriétés.* —

– Pro : Les automorphismes de groupe de $\mathbb{Z}/n\mathbb{Z}$ sont les applications de la forme $\bar{x} \mapsto kx$ où $k \in \{1, \cdots, n\}$ et $k \wedge n = 1$.
– Pro : Tout corps fini a un sous-corps isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est sa caractéristique.
– Cor : Les corps finis $\mathbb{F}_q$ sont de cardinal $q = p^n$ et ne sont pas isomorphes à $\mathbb{Z}/q\mathbb{Z}$ dès lors que $n > 1$.
– Exe : YYYYY $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe à F_4
– Pro : les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ sont les k tels que $n|k^r$. $\mathbb{Z}/n\mathbb{Z}$ possède des éléments nilpotents non-nuls ssi il existe p premier tel que $p^2|n$.
– Quelques résultats de congruences :
- Thé : théorème de Wilson - p est premier ssi $(p-1)! \equiv -1\ (mod.p)$
- Pro : si p premier alors $C_p^k \equiv 0\ (mod.p)$ pour tout $k \in \{1, p-1\}$
- Pro : si p premier alors $(a+b)^{p^i} = a^{p^i} + b^{p^i}\ \forall a, b, i \in \mathbb{N}$ (par récurrence).
- Thé : théorème de Fermat-Euler - $\forall a \in (\mathbb{Z}/n\mathbb{Z})^*$ et $\forall n \geq 2$, $a^{\varphi(n)} \equiv 1\,(mod.n)$
- Cor : petit théorème de Fermat - $\forall p$ premier et $\forall a$ tels que $a \wedge p$ on a $a^(p-1) \equiv 1\ (mod.p)$.

4. *Applications : calculs.* — .
Équation du premier degré dans $\mathbb{Z}/n\mathbb{Z}$:$ax + by = c$

– Aucune solution si $a \wedge b$ ne divise pas c.
– Sinon, $\{(x_0 + \frac{bk}{a \wedge b}, y_0 - \frac{bk}{a \wedge b})\}$ où (x_0, y_0) solution particulière.

.

Équation du second degré dans $\mathbb{Z}/n\mathbb{Z}$:$x^2 + bx + cy = 0$ dans les cas où 2 ne divise pas n

– On se base sur la méthode connue de façon à obtenir : $[2(x + \frac{b}{2})]^2 = (b^2 - 4c) = \delta$.
– Sur ces anneaux, on peut trouver 0 ou plusieurs racines et obtenir autant de valeurs pour δ.

.

Résolution d'un système de congruences :

– Étant donnés $(a_i)_{i \leq r}$ et $(q_i)_{i \leq r}$
– tels que $q_i \wedge q_j = 1$ pour tout i et tout j
– $\exists! x_0$ vérifiant $x_0 \equiv a_i\ (mod.q_i)\ \forall i$ avec $x_0 < q_1 \cdot q_r$
– Les solutions du système de congruences $x \equiv a_i\ (mod.q_i)\ \forall i$ sont de la forme $x = x_0 + k \cdot (q_1 \cdots q_r)$
– Exe : le problème des pirates et du cuisinier Chinois : des pirates se partagent un butin mais ils s'entre-tuent. A chaque fois le cuisinier est destinataire du rompu. On déduit le butin à partir des chroniques de la part du cuistot. (17, 11, 6) pour (3, 4, 5).

.

Développement : Cryptographie RSA :

– Thé : Soient $p, q \in \mathbb{P}$ et c, d tels que $cd \equiv 1\ (mod.(p-1)(q-1)$, alors $\forall x \in \mathbb{Z}$, $x^{cd} \equiv 1\ (mod.pq)$
– Application de Chiffrement : $C : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ telle que $x \mapsto x^c$.
– Application de Déchiffrement : $D : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ telle que $x \mapsto x^d$.
– $D(C(x)) = x^{cd} \equiv x\ (mod.pq)$
– Secret : p, q, d
– Publics : n, c.
– Rem : déduire p, q nécessite de factoriser un nombre ce qui est ardu pour p et q grands.
– Exe : $p = 163$, $q = 359$, $n = 58517$, $\varphi(n) = (p-1)(q-1) = 2^2 3^4 179$
– On prend un c premier avec $\varphi(n)$, par exemple $c = 5 \cdot 17 \cdot 59 = 5015$.
– On construit d grâce à Bézout : $5015d_0 = 1 + 57996k$
– l'algorithme d'Euclide donne : $d_0 = 19093$ et $k = 1651$.
– $C(x) = x^{5015}(mod.58517)$
– $D(x) = x^{38903}(mod.58517)$

.

Développement : Théorème de Sophie Germain :

– *Énoncé* : p est un nombre premier impair dit de Sophie Germain, ie tel que $q = 2p + 1$ est également premier. Alors, il n'existe pas de solution sur $\mathbb{Z}$ à l'équation $x^p + y^p + z^p = 0$ telle que $xyz \not\equiv 0(p)$.

.

Développement : Théorème des deux carrés :

– *Énoncé* : Un nombre entier est la somme de deux carrés ssi la valuation p-adique pour les facteurs premiers congrus à 3 modulo 4 est paire.

5. *Développements :* —

– Sophie Germain
– RSA
– Th des deux carrés

6. *Sources : —*

- DJ Mercier : Fondamentaux
- Invitation à l'algèbre
- D. Perrin

January 6, 2018

Bruno Nitrosso, EPP et candidat libre