Leçon 120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

1. Structure de $\mathbb{Z}/n\mathbb{Z}$. —

1. Structure de groupe. —

- Def : Relation de congruence d'entiers modulo n.
- Pro : C'est une relation d'équivalence.
- Def : $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence.
- Pro : $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien cyclique d'ordre n.
  L'application $x\mathbb{Z} \mapsto \overline{x} \in \mathbb{Z}/n\mathbb{Z}$ est un morphismes de groupes additifs.
- Pro : Les groupes monogènes sont isomorphes soit à $\mathbb{Z}$, soit à un $\mathbb{Z}/n\mathbb{Z}$.
- Ex : Le groupe U_n des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Pro : Pour tout $d|n$, $\mathbb{Z}/n\mathbb{Z}$ possède un unique groupe d'ordre d, dont des représentants des classes sont les $k.\frac{n}{d}$ pour $0 \leq k \leq d-1$.
- Def : On définit l'indicatrice d'Euler de n, $\phi(n)$ comme le nombre de $1 \leq k \leq n$ qui sont premiers avec n.
- Ex : $\phi(6) = 2$, $\phi(10) = 5$.
- Pro : Si k est premier avec n, alors $\overline{k}$ est d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$.
- Pro : On a ainsi : $\phi(n)$ est le cardinal de l'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$.
- Pro : Pour tout $d|n$, $\mathbb{Z}/n\mathbb{Z}$ possède $\phi(d)$ éléments d'ordre d.
- Pro : Pour p premier, $\phi(p^s) = p^s - p^{s-1}$.
- Pro : $n = \sum_{d|n} \phi(d)$.
- Pro : Les automorphismes de groupe de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{x} \mapsto k.\overline{x}$ pour $1 \leq k \leq n$ et $k \wedge n = 1$.
- Théorème de structure des groupes abéliens finis : Soit G un groupe abélien fini. Il existe des entiers $d_1, ..d_r$ tels que $d_1|..|d_r$ et tq $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times .. \times \mathbb{Z}/d_r\mathbb{Z}$.
  Cette écriture est de plus unique.
- Ex : Les groupes abéliens d'ordre 24 sont isomorphes à $\mathbb{Z}/24\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

2. Structure d'anneau. —

- Pro : $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif pour $\overline{x}.\overline{y} = \overline{x.y}$.
  On a ainsi un morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ surjectif dont le noyau est $n\mathbb{Z}$.
- Pro : Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ pour $k \wedge n = 1$. Il y en a $\phi(n)$.
- Pro : $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier.
- Rem : Pour $s \geq 2$, $\mathbb{Z}/p^s\mathbb{Z}$ n'est pas un corps, bien qu'il existe des corps à p^s éléments.
- Def+Pro : Pour p premier, on note $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Le groupe multiplicatif de $\mathbb{F}_p$ est cyclique de cardinal $p-1$.
- Pro : Les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{k}$ tels que $n|k^r$ pour un $r \geq 1$.
  $\mathbb{Z}/n\mathbb{Z}$ possède des éléments nilpotents non-nuls ssi il existe p premier tel que $p^2|n$.
- Théorème chinois : Soit $n = p_1^{a_1}..p_r^{a_r}$ avec p_i premiers entre eux deux à deux.
  Alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/(p_1^{a_1})\mathbb{Z} \times .. \times \mathbb{Z}/(p_r^{a_r})\mathbb{Z}$.
- Ex : $\mathbb{Z}/4\mathbb{Z}$ n'est pas isomorphe comme anneau à $(\mathbb{Z}/2\mathbb{Z})^2$.
- App : Pour p premier , $p \neq 2$ et $r \geq 2$, $(\mathbb{Z}/(p^r)\mathbb{Z}) \simeq (\mathbb{Z}/p^{r-1}\mathbb{Z}) \times (\mathbb{Z}/(p-1)\mathbb{Z})$.
- App : Pour $r \geq 2$, $\mathbb{Z}/(2^r)\mathbb{Z} \simeq \mathbb{Z}/(2^{r-1})\mathbb{Z}$.
- Pro : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = p$ ou $n = 2p$ pour un p premier.
- Résolution d'un système de congruences : Pour $q_1, .., q_r$ premiers entre eux deux à deux, et $a_1, .., a_r \in \mathbb{Z}$, il existe un unique $0 \leq x_0 \leq q_1..q_r$ tel que $x_0 \equiv a_i \ mod(q_i)\ \forall i$.
  Les solutions du système de congruences $x \equiv a_i \ mod(q_i)\ \forall i$ sont donc de la forme $x_0 + k.q_1..q_r$, pour $k \in \mathbb{Z}$.

2. Arithmétique dans $\mathbb{Z}/n\mathbb{Z}$. —

1. Nombres premiers. —

- Test de primalité d'Euler-Fermat : Un nombre impair n est dit pseudo-premier d'Euler en base a ssi $a^{\frac{n-1}{2}} \equiv \pm 1 \ mod(n)$.
- Rem : Ce test de primalité effectif (la multiplication et l'élévation au carré étant peu coûteuses dans $\mathbb{Z}/n\mathbb{Z}$) peut être utilisé de façon probabiliste en tirant au hasard un certain nombre de $1 \leq a \leq n$ et en vérifiant si n est pseudo-premier en base a.
  Ce test probabiliste de non-primalité est de type Monte-Carlo (on a une réponse en temps fini qui est vraie si elle est positive, et qui peut être fausse si elle est négative).

- Pro : Il existe des nombres entiers n non-premiers qui sont pseudo-premiers d'Euler en toute base a première à n. On appelle de tels nombres les nombres de Carmichael.
- Pro : Un nombre n est de Carmichael ssi il est sans facteurs carrés et que pour tout facteur premier p de n on a $p-1|n-1$.
- Ex : 561=3.11.17, et 1105=5.13.17 sont des nombres de Carmichael.
- Thm : Soient p,q premiers et $e, d \in \mathbb{N}$.
  Si $ed \equiv 1 \ mod((p-1)(q-1))$, alors $\forall x \in \mathbb{N}$, $x^{ed} \equiv x \ mod(pq)$.
- Procédé : Un organisme choisit deux grands nombres premiers p et q au hasard, et calcule n=pq. Il choisit d premier avec $(p-1)(q-1)$ et calcule e l'inverse de d dans $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$.
  Il émet alors une clé publique constituée de n et d.
  Un utilisateur va choisir son message $x \in \mathbb{Z}/n\mathbb{Z}$, puis le chiffrer en calculant $m = x^d$ dans $\mathbb{Z}/n\mathbb{Z}$ avant d'envoyer son message chiffré m.
  L'organisme peut alors déchiffrer le message chiffré en calculant $m^e = x^{ed} = x$.
  Les calculs de chiffrement et de déchiffrement sont rapides grâce à de l'exponentiation binaire.
  Trouver e revient exactement à trouver p et q, càd à factoriser n. La sécurité du cryptage repose sur le fait que les algorithmes de factorisation d'entiers de grande taille sont très coûteux en espace mémoire et en calculs. (les entiers étant de l'ordre de 2^{1024} actuellement)
- Théorème de Sophie-Germain : Soit p un nombre premier impair tel que $q = 2p+1$ soit premier.
  Alors l'équation $x^p + y^p + z^p = 0$ n'admet aucune solution entière telle que $xyz = 0$.
- **Dev** : Théorème de Chevalley-Waring : Soit p premier, $n \geq 1$.
  Soient $P_1, ⁝ P_r \in \mathbb{F}_p[X_1, ⁝ X_n]$ tels que $\sum_{i \leq r} \deg_{tot}(P_i) < n$, et soit $V := \cup_i P_i^{-1}(\{0\})$.
  Alors $Card(V) \equiv 0 \ \mathrm{mod}(p)$.

- Théorème de Ginszbourg-Erdös-Sziv : Soit $n \geq 1$ et soient $a_1, \dots, a_{2n-1} \in \mathbb{Z}$. Alors il existe $1 \leq i_1 < i_2 < \dot{<} i_n \leq 2n-1$ tels que $a_{i_1} + \dot{+} a_{i_n} \equiv 0$ mod(n).

2. Carrés et sommes de carrés. —

- Def : On définit $\mathbb{F}_p^2$ l'image de $x \mapsto x^2$ sur $\mathbb{F}_p$.
  On définit de même $(\mathbb{F}_p^*)^2$ l'ensemble des carrés de $\mathbb{F}_p^*$.
- Pro : Si $p = 2$, alors tous les éléments de $\mathbb{F}_p$ sont des carrés.
  Si $p \neq 2$, $Card(\mathbb{F}_p^*) = \frac{p-1}{2}$.
- Pro : Si $p \neq 2$, $x \in \mathbb{F}_p^*$ est un carré ssi $x^{\frac{p-1}{2}} = 1$.
- App : -1 est un carré dans $\mathbb{F}_{p^n}$ ssi $p \equiv 1\ mod(4)$.
- App : Il existe une infinité de nombres premiers de la forme $4k+1$.
- Def : Pour tout $x \in \mathbb{F}_p$, on définit $(\frac{x}{p}) = \begin{cases} 1 \text{ si x} \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$ le symbole de Legendre.
- Pro : Le symbole de Legendre définit un morphisme de groupes de $\mathbb{F}_p^*$ vers $\{-1, 1\}$
- Pro : $(\frac{x}{p}) = x^{\frac{p^n-1}{2}}$.
- Ex : $(\frac{-1}{p}) = (-1)^{\frac{p-1}{4}}$.
- Pro : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.
- Loi de réciprocité quadratique : Soient p,m des nombres premiers impairs distincts. Alors $(\frac{p}{m}) = (\frac{m}{p}).(-1)^{\frac{p-1}{2}.\frac{m-1}{2}}$.
- Ex : $(\frac{23}{59}) = -1$
- Thm : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ La loi de réciprocité quadratique, les formules pour -1 et 2, et la division euclidienne permettent de toujours calculer le symbole de Legendre $(\frac{q}{p})$.
- Ex : $(\frac{23}{59}) = -1$. L'équation $x^2 + 59y = 23$ n'a pas de solutions.

3. Polynômes irréductibles. —

1. Polynômes irréductibles sur $\mathbb{F}_p$. —

- Pro : Soit $P \in \mathbb{F}_p[X]$ irréductible, de degré n. Alors $\mathbb{F}_p[X]/(P)$ est un corps et une $\mathbb{F}_p$-algèbre de dimension n. Ce corps est donc de cardinal p^n, et est appelé corps de rupture de P sur $\mathbb{F}_p$.
- Thm : Pour tout p premier, pour tout $n \geq 1$, il existe un corps de cardinal p^n.
  De plus, un tel corps est unique à isomorphisme de $\mathbb{F}_p$ algèbre près. On le note $\mathbb{F}_{p^n}$.
- Thm : $\mathbb{F}_{p^n}^*$ est cyclique. Il existe ainsi $x \in \mathbb{F}_{p^n}$ tel que $\mathbb{F}_{p^n} = \mathbb{F}_p[x]$.
- App : Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$.
- Def : On note $I(n,p)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_p$.
- Pro : On a : $X^{p^n} - X = \Pi_{d|n}(\Pi_{P \in I(d,p)} P)$.
  Ainsi, $p^n = \sum_{d|n} d.Card(I(d,p))$.
- Exemple de factorisation de $X^8 - X$ dans $\mathbb{F}_2[X]$.
- Pro : Soit $P \in \mathbb{K}[X]$ de degré $n \geq 2$. P est irréductible sur $\mathbb{K}$ ssi P n'admet aucune racine dans toute extension de corps finie de degré $\leq \lceil \frac{n}{2} \rceil$.
- App : $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$ mais est pourtant réductible dans tous les $\mathbb{F}_p[X]$.

2. Irréductibilité sur $\mathbb{Z}$ et $\mathbb{Q}$. —

- Def : Un polynôme $P \in \mathbb{Z}[X]$ est dit primitif si les seuls diviseurs communs à tous les coefficients de P sont ± 1.
- Thm : Les polynômes irréductibles sur $\mathbb{Z}[X]$ sont les polynômes primitifs qui sont irréductibles sur $\mathbb{Q}[X]$.
- Pro : Critère d'Eisenstein : Soit $P(X) = a_n X^n + .. + a_0 \in \mathbb{Z}[X]$. Si il existe un nombre premier p tel que $p | a_i\ \forall 0 \leq i \leq n-1$, $p \nmid a_n$, $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Z}[X]$.
- Ex : $X^4 + 15X + 10$ est irréductible sur $\mathbb{Z}$.
  Pour p premier, $P(X) = X^{p-1} + .. + X + 1$, le polynôme $Q(X) = P(X+1)$ vérifie le critère d'Eisenstein car son terme constant vaut p et cas $Q(X) \equiv X^{p-1}$ mod(p).
  Il en est de même pour $P(X) = X^{p(p-1)} + .. + X + 1$.
- Thm : Critère d'irréductibilité par réduction modulo p : Soit $P(X) = a_n X^n + .. + a_0 \in \mathbb{Z}[X]$ et p premier tq $p \nmid a_n$. Si la projection de P dans $\mathbb{F}_p[X]$ est irréductible, alors P est irréductible dan $\mathbb{Z}[X]$.
- Ex : Pour p premier, $X^p + X + 1$ est irréductible dans $\mathbb{F}_p$, donc ce polynôme est irréductible dans $\mathbb{Z}[X]$.
- Rem : $X^4 + 1$ est un contre-exemple montrant que ce critère n'est pas une CNS.

3. Polynômes cyclotomiques. —

- Def : Pour tout $n \geq 1$, on définit $\Phi_n(X) := \Pi_{k \wedge n = 1,\ k \leq n}(X - e^{2i\pi\frac{k}{n}}) \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique.
- Pro : On a $\Pi_{d|n}\Phi_d = X^n - 1$.
- **Dev** : Φ_n est un polynôme unitaire à coefficients entiers, irréductible dans $\mathbb{Z}[X]$, de degré $\phi(n) = Card(\mathbb{Z}/n\mathbb{Z}^*)$.
- Pro : Pour p premier et n premier avec p, les facteurs irréductibles de $\overline{\Phi_n}$ dans $\mathbb{F}_p[X]$ sont de degré égal à l'ordre de p dans $\mathbb{Z}/n\mathbb{Z}$.
- Rem : Comme $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est cyclique que si $n = \widetilde{p}$ ou $n = 2\widetilde{p}$ avec $\widetilde{p}$ premier, une grande partie des polynômes cyclotomiques n'est automatiquement pas irréductible sur les $\mathbb{F}_q$.

Références

Risler : Structure de groupe, d'anneau. Th d'Euler, Th de Wilson.
Gozard : Construction des corps finis, propriétés.
Caldero,Germoni : Symbole de Legendre, propriétés, exemples, Loi de réciprocité quadratique.
Perrin : Automorphismes $\mathbb{Z}/n\mathbb{Z}$. Lemme chinois, corollaires, exemples. Carrés dans $\mathbb{F}_p$, -1 carré. Liens entre irréductibilité et recherche de racines. Irréductibilité sur $\mathbb{Z}$ ou $\mathbb{Q}$,critère d'Eisenstein, réduction modulo p, exemples, contre-ex. polynômes cyclotomiques.(Dev)

Gourdon : Test de Fermat, pseudo-premiers, nombres de Carmichael. Chiffrement RSA.
FGN : Test d'Euler-Fermat.
Zavidovique : Th de Chevalley-Wargning et Ginszbourg-Erdös-Sziv.(Dev)
Combes : Th de structure des groupes abéliens finis.

June 7, 2017

Vidal Agniel, École normale supérieure de Rennes