Anneau $\mathbb{Z}/n\mathbb{Z}$ - Applications

I Généralités

1) Définitions et premières propriétés

Rappel : $(\mathbb{Z},+,\times)$ est l'anneau des entiers naturels relatifs

P/té : Soit $n\in\mathbb{N}$. Alors $n\mathbb{Z}=\{nx/x\in\mathbb{Z}\}$ est un idéal de $\mathbb{Z}$

Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ où $n\in\mathbb{N}^*$

Déf P/té : On note $x\equiv y\,[n]$ si $x-y\in n\mathbb{Z}$ pour x,y entiers relatifs

c'est une relation d'équivalence et elle permet de définir l'anneau quotient $(\mathbb{Z}/n\mathbb{Z},+,\times)$ où $+$ et $\times$ sont les mêmes lois que pour $\mathbb{Z}$

Deux éléments x et y qui ont même classe sont dits congrus modulo n

On notera ici $\bar{x}$ en omettant $^{-}$ pour la classe d'équivalence.

P/té : $\mathbb{Z}/n\mathbb{Z}=\{0,1,\dots,n-1\}=\{1,\dots,n\}$ et $|\mathbb{Z}/n\mathbb{Z}|=n$

Prop : Soit $n\in\mathbb{N}^*$. Alors

- $\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow$ $n\in\mathbb{P}$
- Pour $k\in\mathbb{N}$, $k\in(\mathbb{Z}/n\mathbb{Z})^*$ $\Leftrightarrow$ $k\wedge n=1$ $\Leftrightarrow$ $\langle k\rangle=((\mathbb{Z}/n\mathbb{Z})^*,\times)$

Rq : Conséquence du th. de Bezout

2) Le théorème chinois

Th : Soient $(m,n)\in(\mathbb{N}^*)^2$. Soit $\varphi\left(\begin{array}{l}\mathbb{Z}/mn\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\\ \bar{x}_{mn}\mapsto(\bar{x}_m,\bar{x}_n)\end{array}\right)$

Alors φ est un morphisme d'anneau $\Leftrightarrow$ m et n sont premiers entre eux

et dans ce cas, on a $\boxed{\mathbb{Z}/mn\mathbb{Z}\simeq\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}$ en tant qu'anneau

Rq : Il suffit de : lorsque $m\wedge n=1$ ~~...~~ par théorème de Bezout $\exists(u,v)\in\mathbb{Z}^2$ tq $um+nv=1$. Soit $\psi\left(\begin{array}{l}\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/mn\mathbb{Z}\\ x,y\mapsto \cancel{\dots}\ umy+nvx\end{array}\right)$

On vérifie que $\varphi^{-1}=\psi$!

Rq : ~~...~~ $= \mathrm{ppcm}(x,y)=x\mathbb{Z}\cap y\mathbb{Z}$, $\mathrm{pgcd}(x,y)=x\mathbb{Z}+y\mathbb{Z}$

Rq : Se généralise par récurrence à n entiers premiers entre eux.

Application pratique : Si $m\wedge n=1$, alors $\forall x,y\in\mathbb{Z}$ ($um+nv=1$)

$x\equiv y\,[mn]\Leftrightarrow\begin{cases}x\equiv y\,[m]\\x\equiv y\,[n]\end{cases}$

$\begin{cases}x\equiv y_1\,[m]\\x\equiv y_2\,[n]\end{cases}\Leftrightarrow x\equiv umy_2+vny_1\,[mn]$

Ex : Calcul des nilpotents et idempotents dans un $\mathbb{Z}/n\mathbb{Z}$.

- Si $n\in\mathbb{P}$, $x^2\equiv1\,[n]$ et $x^k\equiv0\,[n]$ ont resp 2 et k solutions dans $\mathbb{Z}/n\mathbb{Z}$
- Si $n\notin\mathbb{P}$, découper les $\mathbb{Z}/n\mathbb{Z}$ en produits $\mathbb{Z}/p\mathbb{Z}$, étudier chaque équation $\mathbb{Z}/p\mathbb{Z}$ et rassembler les solutions.

Ainsi, dans $\mathbb{Z}/6\mathbb{Z}$, $x^3\equiv0\,[6]$ a plus que 3 solutions : 0,2,3,4 !
$x^2\equiv1\,[6]$

Appli : Th de Wilson : $p\in\mathbb{P}\Leftrightarrow(p-1)!\equiv-1\,(p)$

3) Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$

On a remarqué que $|(\mathbb{Z}/n\mathbb{Z})^*|\neq n-1$ $\forall n\in\mathbb{N}$!
$=|\{\text{nombre}\leq n \text{ premier à } n\}|$

Déf : On appelle fonction indicatrice d'Euler notée φ la fonction de $\mathbb{N}$ dans $\mathbb{N}^*$ tel que $\varphi(n)=|(\mathbb{Z}/n\mathbb{Z})^*|$. $\varphi(p)=p-1$

P/té : On peut généraliser le petit théorème de Fermat : $\forall n\in\mathbb{N}^*$, k premier à n, $k^{\varphi(n)}\equiv1\,[n]$

Rq : P/té de l'ordre des groupes !

L'intérêt de cette fonction φ est qu'on peut la calculer : $\to$ calcul

Prop : - Si $p\in\mathbb{P}$ et $\alpha\in\mathbb{N}$, $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$
- Si p et q sont premiers entre eux, $\varphi(pq)=\varphi(p)\varphi(q)$ $\to$ th chinois

Coro /Conclusion : Si $n=\prod_{i=1}^{k}p_i^{\alpha_i}$, $\varphi(n)=\prod_{i=1}^{k}p_i^{\alpha_i-1}(p_i-1)$

P/té : $n=\sum_{d|n}\varphi(d)$ (partition des sous-groupes multiplicatifs de $\mathbb{Z}/n\mathbb{Z}$)

Th : Soit $n\in\mathbb{N}$. Alors $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})\simeq(\mathbb{Z}/n\mathbb{Z})^*$

En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est cyclique d'ordre $\varphi(n)$)

Rq : Pour $\varphi\in\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, il est caractérisé par $\varphi(1)$ qui doit vérifier $\varphi(1)\wedge n=1$

Intéressant si on connait la structure de $(\mathbb{Z}/n\mathbb{Z})^*$

Th : Structure de $(\mathbb{Z}/n\mathbb{Z})^*$.

Si $p\in\mathbb{P}\setminus\{2\}$ et $\alpha\in\mathbb{N}\setminus\{0,1\}$, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^*\simeq\mathbb{Z}/(p^{\alpha-1}(p-1))\mathbb{Z}$

Pour le cas $n=2$, on a $(\mathbb{Z}/2\mathbb{Z})^*=\{1\}$, $(\mathbb{Z}/4\mathbb{Z})^*\simeq\mathbb{Z}/2\mathbb{Z}$
$(\mathbb{Z}/2^\alpha\mathbb{Z})^*\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ pour $\alpha\geq3$

Rq : Le théorème chinois permet de connaitre $(\mathbb{Z}/n\mathbb{Z})^*$ $\forall n\in\mathbb{N}$.

La suite va donner une autre appli de ce théorème.

Prop : Soit G cyclique d'ordre n : Alors $G\simeq\mathbb{Z}/n\mathbb{Z}$

Rq : Permet de généraliser les résultats sur $\mathbb{Z}/n\mathbb{Z}$ aux groupes cycliques !

Rq : Si $G=\langle a\rangle$, alors l'iso via $\varphi\left(\begin{array}{l}\mathbb{Z}\to G\\ k\mapsto a^k\end{array}\right)$

Ex : Il y a $\varphi(n)$ générateurs à U_n.

II Applications à l'arithmétique

1) Etude des carrés de $\mathbb{Z}/p\mathbb{Z}$, $p \in \mathcal{P}\setminus\{2\}$

Def : Soit $p \in \mathcal{P}\setminus\{2\}$ et $n \in \mathbb{Z}$. On définit le symbole de Legendre de n sur p par : $\left(\frac{n}{p}\right) = \begin{cases} 1 & n \text{ est un carré de } \mathbb{Z}/p\mathbb{Z} \\ 0 & \text{si } p \mid n \\ -1 & \text{sinon} \end{cases}$

Ex : $\left(\frac{3}{7}\right) = -1$ car 3 pas un carré de $\mathbb{Z}/7\mathbb{Z}$

Prop : Pour $n \in \mathbb{N}^*$, on a $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} [p]$ $(p \neq 2)$

DEV 1 Loi de réciprocité quadratique :

Soit $p,q \in \mathcal{P}\setminus\{2\}$, $p \neq q$ et on pose $G = (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ et $U = \{(1,1),(-1,-1)\}$.
A partir des systèmes de représentants du groupe quotient G/U : $E_2 = \{(x,y) \in G \,/\, 1 \leq x \leq \frac{p-1}{2}, \dots\}$,
$E_1 = \{(i,j) \in G \,/\, 1 \leq i \leq \frac{p-1}{2},\ 1 \leq j \leq \frac{q-1}{2}\}$
on démontre l'égalité $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ via $P = \prod_{x \in G/U} x$

Ex :

2) Equations diophantiennes

Def : On appelle équation diophantienne une équation $P(x,y,z) = 0$ où les inconnues x, y et z sont des entiers et $P \in \mathbb{Z}[X,Y,Z]$

Ex 1 : L'identité de Bézout $ax + by = c$, a,b,c entiers donnés.
Elle admet une solution ssi $a \wedge b \mid c$ et sa solution peut être exprimée via des congruences

Ex 2 : L'équation de Pythagore $x^2 + y^2 = z^2$.
Les solutions sont du type $(d(u^2 - v^2), 2duv, d(u^2+v^2))$
où $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ tq $u \wedge v$.

DEV 2 Théorème des deux carrés

Soit $\Sigma = \{n \in \mathbb{N} \,/\, n = a^2 + b^2,\ a,b \in \mathbb{N}\}$
Alors $n \in \Sigma$ ssi $\forall p \equiv 3 [4]$, $v_p(n)$ est pair

Rappel (Admis) : $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme multiplicatif $N(a+ib) = a^2 + b^2$ et $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

Appli : Etude des irréductibles de $\mathbb{Z}[i]$

Ex 3 : L'équation de Fermat $x^4 + y^4 = z^4$ n'a pas de solution non triviale

Rq : Plus loin, le théorème de Sophie-Germain

III Autres applications

1) Etude des polynômes de $\mathbb{Z}[X]$

Soit $P \in \mathbb{Z}[X]$: il est bon de savoir si P est irréductible ou non

Prop (Réduction modulo p) : Soit $P \in \mathbb{Z}[X]$ de coefficient dominant non divisible par un nombre premier p.
Alors $\bar{P}$ irréductible sur $\mathbb{Z}/p\mathbb{Z}[X] \Rightarrow P$ irréductible sur $\mathbb{Q}[X]$ (sur $\mathbb{Z}[X]$ si P unitaire)

Ex : $X^3 + 2014X^2 + 1991 - 1$ est irréductible sur $\mathbb{Z}$ via la réduction modulo 2.

Prop (Critère d'irréductibilité d'Eisenstein) : Soit $P \in \mathbb{Z}[X]$
où $P(X) = a_n X^n + \dots + a_0$ et $p \in \mathbb{Z}$ vérifiant :
- $p \nmid a_n$ et $p^2 \nmid a_0$
- $\forall i \in \{0, \dots, n-1\}$, $p \mid a_i$

Alors P est irréductible sur $\mathbb{Q}[X]$

Rq : La réduction sur $\mathbb{Q}[X]$ peut donner la réduction sur $\mathbb{Z}[X]$: si P irréductible sur $\mathbb{Q}[X]$ et le pgcd des coefficients égal à 1, alors P irréductible sur $\mathbb{Z}[X]$. (Cf des contenus de Gauss)

Ex : Si $p \in \mathcal{P}$, $X^{p-1} + \dots + X + 1$ irréductible sur $\mathbb{Z}[X]$.

Appli : De $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ en passant par les polynômes
- Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Z}[X]$.

$\Rightarrow$ • Théorème de Dirichlet faible
Soit $n \in \mathbb{N}$: il existe une infinité de nombres premiers p tels que $p \equiv 1 [n]$

Rq : Th de Dirichlet fort pour la culture.

2) Cryptographie et recherche des nombres premiers

Méthode RSA : D'abord, un lemme dû à Euler

Lemme : Soit $n \in \mathbb{N}^*$ sans facteur multiple et $r \equiv 0\ [\varphi(n)]$
Alors $\forall a \wedge n = 1$, $a^r \equiv 1\ [n]$ et $a^{r+1} \equiv a\ [n]$

Méthode : Un entier définit un message, soit n sans facteur carré, r tq $r \wedge \varphi(n) = 1$
n et r sont public

Soit l'application de chiffrement public $C \begin{pmatrix} \mathbb{N} \to \mathbb{Z}/n\mathbb{Z} \\ m \mapsto m^r \end{pmatrix}$

Soit l'application de déchiffrement privé $D \begin{pmatrix} \mathbb{N} \to \mathbb{Z}/n\mathbb{Z} \\ m \mapsto m^s \end{pmatrix}$

Ainsi, s est pris tq $\forall m \in \mathbb{N}$, $m^{rs} \equiv m\ [n]$
ie tq $rs \equiv 1\ [\varphi(n)]$ d'après le lemme

s est privé.

Dans la pratique, on prend n comme produit de 2 très grands nombres premiers p et q. Si on publie le produit $n = pq$, il est impossible de connaître la décomposition de n, donc de connaître $\varphi(n)$ et de calculer s : s reste bien privé !
De notre côté, connaissant $n = pq$, on a $\varphi(n) = (p-1)(q-1)$ et l'algorithme d'Euclide permet de déterminer s tq $rs \equiv 1\ [\varphi(n)]$

Dès lors, il est intéressant de trouver des nombres premiers grands.

Critère de non primalité de Fermat : Soit $n \in \mathbb{N}$.
$n \notin \mathbb{P}$ si $\exists a$ tq $a^{n-1} \not\equiv 1\ [n]$ et $1 < a < n$ (def de $\mathbb{Z}/p\mathbb{Z}$!)

Rq : Condition suffisante mais nécessaire : $\exists n \notin \mathbb{P}$ tq $\forall a \in [\![1, n-1]\!]$
$a^{n-1} \equiv 1\ [n]$: ce sont les nombres de Carmichael (donc $\notin \mathbb{P}$)

Critère de non primalité de Miller-Rabin : Soit $n \in \mathbb{N}$.
et posons $n-1 = 2^s t$ où $2 \nmid t$.
Si $\exists a \in [\![2, n-1]\!]$ tq $a^t \not\equiv 1\ [n]$ et $a^{2^i t} \not\equiv -1\ [n]$ $\forall i \in [\![0, s-1]\!]$ alors $n \notin \mathbb{P}$

Rq : Améliore le critère précédent
$a = 2, 3$ ou 5 marche souvent donc facile à manipuler
(25 326 001, plus petit nombre où 2, 3 ou 5 pas témoin)

Critère de primalité de Lucas-Lehmer : Soit $n \in \mathbb{N}$ tq la déc de $n-1$ soit connue. Alors
si $\exists a \in \mathbb{N}$ tq $a^{n-1} \equiv 1\ [n]$ et $a^{\frac{n-1}{q}} \not\equiv 1\ [n]$ tq $q \mid n-1$, alors $n \in \mathbb{P}$

Rq : Test hasardeux, à faire si on suspecte n d'être premier.
Il faut connaître la déc de $n-1$ → pas évident.
Marche bien pour les nombres de Fermat ou de Mersenne.

Rq. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ et leurs propriétés à la base de ces critères !

Ex : F_5 ~~par~~ Solas !

3) Th de structure des groupes abéliens finis

Th

Appli : étude de $|G| = 200$, étude des ordres possibles ...

Références : GOURDON
COMBES
DEMAZURE
PERRIN