120 ANNEAUX $\mathbb{Z}/n\mathbb{Z}$. APPLICATIONS.

Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{P}$ l'ensemble des nombres premiers.

I. Structure de $\mathbb{Z}/n\mathbb{Z}$

I. A. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

[Rom17, §1.4-5/1.9/10.1, p13–19/27/277] [Per96, §1.1/1.7, p10/24]

Définition 1. Deux entiers x, y sont dis congrus modulo n si $x - y \in n\mathbb{Z}$. C'est une relation d'équivalence sur $\mathbb{Z}$. On note $\overline{x}$ la classe de x et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$.

Proposition 2. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique à n éléments engendré par $\overline{1}$.*

Application 3. Tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 4. $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$: considérer $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{U}_n, \overline{k} \longmapsto \mathrm{e}^{2ik\pi/n}$.

Proposition 5. *L'ordre de $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est $\frac{n}{k \wedge n}$.*

Corollaire 6. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est engendré par les $\overline{k}$ tels que $k \wedge n = 1$.*

Exemple 7. $\mathbb{Z}/8\mathbb{Z}$ est engendré par $\overline{1}, \overline{3}, \overline{5}$ et $\overline{7}$.

Définition 8. [Indicatrice d'Euler]
Pour $n \geq 2$, on définit $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exemple 9. Pour $p \in \mathcal{P}$, on a $\varphi(p^\alpha) = p^\alpha(p-1)$ pour $\alpha \in \mathbb{N}^*$.

Proposition 10. [Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$]
Pour $d \mid n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, engendré par $\frac{n}{d}$ et formé des éléments dont l'ordre divise d.

Proposition 11. *Si $d \mid n$, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d.*

Application 12. $n = \sum_{d \mid n} \varphi(d)$

Théorème 13. [Structure des groupes abéliens finis]
Soit G un groupe abélien fini. Alors il existe $r \geq 1$ et $2 \leq d_1 \mid \cdots \mid d_r$ uniques tels que $G \simeq \prod_{i=1}^r \mathbb{Z}/d_i\mathbb{Z}$.

Exemple 14. Les groupes abéliens d'ordre 24 sont isomorphes à $\mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

I. B. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

[Rom17, §10.1-3, p277–288] [Per96, §1.7, p24–28]

Proposition 15. *Les idéaux de $\mathbb{Z}$ sont les $(k\mathbb{Z})_{k \in \mathbb{N}}$.*

Définition 16. L'ensemble des classes modulo n est muni d'une structure d'anneau : on définit l'anneau commutatif $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Remarque 17. Les idéaux de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les sous-groupes du groupe $\mathbb{Z}/n\mathbb{Z}$.

Application 18. Soit A un anneau commutatif unitaire. Il existe un unique entier positif, appelé caractéristique de A, noté $\mathrm{car}(A)$, tel que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

Proposition 19. *Les inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les $\overline{k}$ tels que $k \wedge n = 1$. Ils forment un groupe à $\varphi(n)$ éléments.*

Application 20. On a l'isomorphisme $(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/n\mathbb{Z})^\times, \times)$.

Proposition 21. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si c'est un corps si et seulement si $n \in \mathcal{P}$. [Rom17, §11.5, p324–327]*

Théorème 22. [Théorème chinois]
Si $n, m \geq 1$, alors on a l'isomorphisme d'anneaux $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ si et seulement si $n \wedge m = 1$.

Corollaire 23. *Si $n = \prod_{i=1}^r p_i^{\alpha_i}$, alors $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ et on en déduit $\varphi(n) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1)$.*

Théorème 24. *Si $p \in \mathcal{P}$, $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est cyclique.*

II. Application à l'arithmétique dans $\mathbb{Z}$

II. A. Tests de primalité [Rom17, §10.2/11.5-6, p280–282/324–329] [Gou09, §1.4, p34–37]

Théorème 25. [Théorème d'Euler] *Soit $a \in \mathbb{Z}$ premier avec n. Alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Théorème 26. [Petit théorème de Fermat]
Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tels que $p \nmid a$. Alors $a^{p-1} \equiv 1 \mod p$.

Remarque 27. La réciproque est fausse ! Par exemple avec 561. En revanche, pour tout $a \in \mathbb{Z}$, on a $a^p \equiv 1 \mod p$.

Définition 28. [Nombre de Carmichaël]
Un entier $n > 1$ non premier est de Carmichaël si $\forall a \in \mathbb{Z}, a \wedge n = 1 \implies a^{n-1} \equiv 1 \mod n$.

Proposition 29. *Un nombre de Carmichaël est impair et sans facteur carré.*

Application 30. [Algorithme RSA]
Alice veut envoyer un message privé à Bob.
- Bob choisit deux entiers premiers distincts $p, q \in \mathcal{P}$ et pose $n = pq$, puis il choisit ensuite $d, e \in \mathbb{Z}$ tels que $de \equiv 1 \mod \varphi(n)$ (on a $\varphi(n) = (p-1)(q-1)$ et il suffit de trouver d premier à $\varphi(n)$ et son inverse).
- Bob diffuse la clé publique (n, d) à tout le monde et converse la clé secrète (n, e).
- Pour envoyer son message $m \mod n$, Alice envoie le message chiffré $M \equiv m^d \mod n$.
- Bob déchiffre le message $m = M^e \mod n$ d'après le théorème d'Euler.

Le succès de cet algorithme réside dans la difficulté de factorisation d'un entier.

Théorème 31. [Théorème de Wilson] *Si $n \geq 2$, on a $n \in \mathcal{P} \iff (n-1)! \equiv -1 \mod n$.*

II. B. Équations arithmétiques [Rom17, §10.3-4, p283–290]

Soient $n, m \geq 2$.

Théorème 32. *Soit $a \in \mathbb{N}^*, b \in \mathbb{Z}$. On note $\delta = a \wedge n$ et on écrit $a = \delta a'$ et $n = \delta n'$. L'équation $ax \equiv b \mod n$ a des solutions entières si et seulement si $\delta \mid b$ et dans ce cas, si $b = \delta b'$, les solutions sont les $b'x'_0 + kn'$ avec $k \in \mathbb{Z}$ et x'_0 est une solution particulière de $a'x \equiv 1 \mod n'$.*

Théorème 33. *Dans le Théorème 22, l'isomorphisme est donné par $\psi : a \mod nm \longmapsto (a \mod n, a \mod m)$ de réciproque $\psi^{-1} : (a \mod n, b \mod m) \longmapsto unb + vma \mod nm$ où l'on a choisit $u, v \in \mathbb{Z}$ tels que $un + vm = 1$.*

Application 34. Soit $a, b \in \mathbb{Z}$ et $(\mathscr{S})$ le système d'équations $\begin{cases} x \equiv a \mod n \\ x \equiv b \mod m \end{cases}$ d'inconnue $x \in \mathbb{Z}$. Si $n \wedge m = 1$, alors
- on cherche une relation de Bézout $un + vm = 1$ avec $u, v \in \mathbb{Z}$,
- on a alors une solution particulière de $\mathscr{S}$: $x_0 = unb + vma$,
- les solutions de $\mathscr{S}$ sont les $(x_0 + knm)_{k \in \mathbb{Z}}$.

Exemple 35. Les solutions de $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 4 \mod 5 \end{cases}$ sont les $(14 + 15k)_{k \in \mathbb{Z}}$.

II. C. Résidus quadratiques modulo p
[Rom17, §13.6-7, p429–436] [Per96, §3.2, p72–76]

Soit $p \in \mathcal{P}$. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$, puis $\mathbb{F}_p^2 = \left\{x^2 \mid x \in \mathbb{F}_p\right\}$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Proposition 36. *Si $p = 2$, alors $\mathbb{F}_p^2 = \mathbb{F}_p$. Sinon, on a $\left|\mathbb{F}_p^2\right| = \frac{p+1}{2}$.*

Application 37. Pour $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$, $ax^2 + by^2 = c$ admet des solutions dans $\mathbb{F}_p$.

On suppose dans la suite p impair.

Lemme 38. *On a $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.*

Exemple 39. Dans $\mathbb{Z}/7\mathbb{Z}$, 2 est un carré mais par 3.

On aimerait savoir rapidement si un entier a donné est un carré modulo p, donc savoir si $x^2 \equiv a \mod p$ admet ou non une solution entière.

Définition 40. [Symbole de Legendre]
Soit $a \in \mathbb{Z}$, on appelle symbole de Legendre (de a modulo p) l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ est résoluble et } p \nmid a \\ 0 & \text{si } p \mid a \\ -1 & \text{sinon} \end{cases}$$

Proposition 41. *On a $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ pour tout $a \in \mathbb{Z}$.*

Exemple 42. -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$.

Proposition 43. *$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$ pour tout $a, k \in \mathbb{Z}$. On peut donc définir $\overline{x} \in \mathbb{F}_p \longmapsto \left(\frac{x}{p}\right)$. C'est l'unique morphisme de groupes non trivial de $(\mathbb{F}_p^*, \times)$ vers $(\{\pm 1\}, \times)$.*

Remarque 44. Pour $a \in \mathbb{Z}$, le nombre de solutions de $x^2 = \overline{a}$ dans $\mathbb{F}_p$ est $1 + \left(\frac{a}{p}\right)$.

Théorème 45. [Loi de réciprocité quadratique]
Soient $p \neq q$ des nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Proposition 46. *Pour p premier impair, on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Ainsi 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$.*

On peut donc calculer $\left(\frac{n}{p}\right)$ pour tout entier n.

Exemple 47. $\left(\frac{26}{307}\right) = \left(\frac{2}{307}\right)\left(\frac{13}{307}\right) = -(-1)^{\frac{13-1}{2}\frac{307-1}{2}}\left(\frac{307}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)\left(\frac{4}{13}\right) = -1$
Ainsi 26 n'est pas un carré modulo 307.

III. Applications aux polynômes et à la théorie des corps

III. A. Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, réduction modulo p

[Rom17, §12.11.4, p381–383] [Per96, §3.3-3.4, p76–85] [FGN07, §5.16, p188–190]

Proposition 48. *Un polynôme de degré supérieur ou égal à 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement si il est de contenu 1 et irréductible dans $\mathbb{Q}[X]$.*

Proposition 49. [Critère d'Eisenstein]
Soit $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $p \in \mathcal{P}$. Si $p \nmid a_r$, $\forall i < r, p \mid a_i$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 50. Si $m \in \mathbb{Z}$ a un facteur premier sans carré alors $X^n - m$ est irréductible dans $\mathbb{Z}[X]$ pour tout $n \in \mathbb{N}$.

Proposition 51. *Soit $p \in \mathcal{P}$ et $P = \sum_{i=0}^{r} a_i X^i \in \mathbb{Z}[X]$. Soit $\overline{P}$ la réduction de P modulo p. Si $p \nmid a_n$ et si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.*

Exemple 52. $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$, tout comme $X^p - X - 1$ pour tout $p \in \mathcal{P}$.

Définition 53. [Polynômes cyclotomiques]
On définit le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ par $\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^\times} (X - \zeta)$.

Proposition 54. *$\Phi_n \in \mathbb{Z}[X]$.*

Théorème 55. *Φ_n est irréductible sur $\mathbb{Z}$ et donc sur $\mathbb{Q}$.*

Corollaire 56. *On a $[\mathbb{Q}[e^{2i\pi/n}] : \mathbb{Q}] = \varphi(n)$.*

III. B. Corps finis

[Per96, §3.2, p72–76] [Rom17, Ch13, p415]

Proposition 57. *Si $\mathbb{K}$ est un corps fini, sa caractéristique est un nombre premier $p \in \mathcal{P}$ et son sous-corps premier est isomorphe à $\mathbb{F}_p$.*

Corollaire 58. *Si $\mathbb{K}$ est un corps fini, alors $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectorieloù $p = \mathrm{car}(\mathbb{K})$, de cardinal p^n où $n = \dim_{\mathbb{F}_p}(\mathbb{K})$. De plus, tout sous-corps de $\mathbb{K}$ est de cardinal p^d pour un $d \mid n$ et réciproquement pour tout $d \mid n$ il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d.*

Théorème 59. *Il existe un corps fini à $q = p^n$ éléments pour tout $p \in \mathcal{P}, n \in \mathbb{N}^*$. Il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$ ou de tout autre polynôme irréductible de $\mathbb{F}_p$. Ce corps est unique à isomorphisme près.*

Exemple 60. $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 éléments de caractéristique 2.

Corollaire 61. *Tout corps de rupture d'un polynôme P irréductible sur $\mathbb{F}_p[X]$ est un corps de décomposition de P sur $\mathbb{F}_p$.*

SPEECH

Lorsque l'on fait de l'arithmétique dans $\mathbb{Z}$, on s'intéresse rapidement à l'arithmétique modulaire, c'est-à-dire le reste d'un nombre modulo n. La puissance de l'arithmétique modulaire provient surtout des différentes structures de $\mathbb{Z}/n\mathbb{Z}$, naturellement héritées de la structure de $\mathbb{Z}$.
Dans la première partie, on quotiente $\mathbb{Z}$ par $n\mathbb{Z}$. Tout groupe cyclique est de ce type, et on connaît précisément ses générateurs. En ajoutant la multiplication, on obtient une structure d'anneau. On peut alors déterminer les inversibles de $\mathbb{Z}/n\mathbb{Z}$, ce qui set par exemple pour les équations arithmétiques. Le cas particulier des corps (n premier) et le théorème chinois sont des résultats très utiles.
Ensuite, on s'intéresse à l'arithmétique dans $\mathbb{Z}$, avec le théorème de FERMAT, dont la réciproque est fausse et les contre-exemples sont les nombres de CARMICHAËL. Les applications en cryptographie sont importantes comme par exemple l'algorithme RSA, mais. De nombreux résultats sur les équations diophantiennes découlent également de notre étude. Enfin le cas particulier des corps mène à la loi de réciprocité quadratique afin de savoir rapidement si un nombre est un carré ou non dans $\mathbb{Z}/p\mathbb{Z}$.
Enfin, l'étude de $\mathbb{Z}/n\mathbb{Z}$ amène des avancées dans d'autres domaines de l'algèbre, notamment des résultats d'irréductibilité de polynômes et la construction de tous les corps finis à partir d'un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.

COMMENTAIRES

Pour les tests de primalité et les algorithmes de chiffrement, voir aussi [Zé17].
Il faut connaître :

- les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ s'identifient au groupe $\mathbb{Z}/(n \wedge m)\mathbb{Z}$. Si $m \mid n$ le seul morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est $\overline{k}_n \longmapsto \overline{k}_m$. Sinon, il n'y a aucun morphisme,
- les diviseurs de 0 de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont les $\overline{k}$ avec $k \wedge n = 1$. Les éléments nilpotents forment l'idéal de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{p_1 \dots p_r}$ où $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$,
- savoir ce que devient le théorème chinois si n et m ne sont plus premiers entre eux,
- savoir que la réciproque du théorème de réduction modulo p pour les polynômes de $\mathbb{Z}[X]$ est vraie : voir pour $X^4 + 1$ dans [Per96].

QUESTIONS

Q Démontrer la proposition 7.

Q Quel est l'ordre maximal d'un élément de $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$?

R $\mathrm{PPCM}(m, n)$.

Q Quelle est la caractéristique de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ pour $a, b \in \mathbb{N}$? Et de $\prod_{k \in \mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$?

R $\mathrm{PPCM}(a, b)$ puis 0, bien que $\prod_{k \in \mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$ « contienne » tous les $\mathbb{Z}/n\mathbb{Z}$.

Q Expliciter l'isomorphisme du théorème chinois.

Q Résoudre $x \iff 1 \mod 3, x \equiv 4 \mod 5$ et $x \equiv 0 \mod 7$.

R On trouve une relation de BÉZOUT ($3 + 5 - 7 = 1$) ou on résout deux systèmes puis on ajoute le troisième.

Q Quels sont les nilpotents de $\mathbb{Z}/n\mathbb{Z}$?

R Écrivons $n = \prod_{i=1}^r p_i^{\alpha_i}$. Si $m \in \prod_{i=1}^r p_i\mathbb{Z}$, alors m est nilpotent d'ordre au plus $\max_{1 \leq i \leq r} \alpha_i$. Réciproquement si m est nilpotent alors pour tout $1 \leq i \leq r$, on a $p_i \mid m$.
Attention : être nilpotent ne signifie pas être non inversible ! Par exemple 2 dans $\mathbb{Z}/6\mathbb{Z}$ n'est ni nilpotent, ni inversible.

Q Condition nécessaire pour que $P \in \mathbb{Z}/n\mathbb{Z}[X]$ soit inversible ?

Q Soit $n \geq 2$ et e premier avec $\varphi(n)$. Montrer que $\mathbb{Z}/n\mathbb{Z}^* \longrightarrow \mathbb{Z}/n\mathbb{Z}^*, x \longmapsto x^e$ est une bijection, et exhiber la réciproque (voir l'algorithme RSA).

Q Soient p, q premiers impairs, $\psi : (\mathbb{Z}/pq\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ et $E = \left\{x \in (\mathbb{Z}/pq\mathbb{Z})^* \mid 1 \leq x < \frac{pq}{2}\right\}$. Déterminer $\mathrm{Im}(E)$.

BIBLIOGRAPHIE

[FGN07] S. FRANCINOU, H. GIANELLA et S. NICOLAS : *Oraux X-ENS - Algèbre 1*. Cassini, 2007.

[Gou09] X. GOURDON : *Les maths en tête - Algèbre*. Ellipses, 2ème édition, 2009.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Rom17] J.-E. ROMBALDI : *Mathématiques pour l'agrégation : Algèbre et géométrie*. De Boeck, 2017.

[Zé17] G. ZÉMOR : *Cours de cryptographie*. Cassini, 2017.