2.17 Quelques résultats de structure dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (120) [20] [23] [27]

Les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont centraux en algèbre pour plusieurs raisons. Une des raisons est historique : la division euclidienne est manipulée depuis l'Antiquité et joue des rôles centraux dans la vie de tous les jours (on vit dans un monde où 60 secondes font 1 minute, 60 minutes font 1 heure, 24 heures font 1 jour, 7 jours font 1 semaine, etc.). Une autre raison est structurelle : les groupes abéliens finis sont tous des produits de $\frac{\mathbb{Z}}{n\mathbb{Z}}$! Ainsi, il est intéressant d'étudier la structure de ces objets, sans négliger la partie "anneaux" ! En effet, en cryptographie, on travaille surtout dans le groupe des inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$, notamment pour les problèmes de logarithme discret, base de la procédure d'échange de clefs Diffie-Hellman. Je mets dans ce développement, plein de petits résultats, et vous pourrez choisir vos résultats préférés pour les mettre dans un développement !

Proposition 2.44 (Fonctions puissance dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$)**.** Soient $k \geqslant 2$ et $n \geqslant 2$. Alors l'application :

$$\begin{array}{rccc} e_k & : & \frac{\mathbb{Z}}{n\mathbb{Z}} & \longrightarrow & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & & x & \longmapsto & x^k \end{array}$$

est bijective si et seulement si n est sans facteur carré et si $p-1$ est premier avec k pour tout facteur premier p de n.

Démonstration. On va se ramener, grâce au théorème des restes chinois, au cas où $n = p^\alpha$ avec p un nombre premier et $\alpha \in \mathbb{N}^*$.

Étape 1 : Réduction au cas $n = p^\alpha$

Posons $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, et notons ψ l'isomorphisme des restes chinois :

$$\begin{array}{rccc} \psi & : & \frac{\mathbb{Z}}{n\mathbb{Z}} & \longrightarrow & \prod_{i=1}^{s} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}. \end{array}$$

On a donc que e_k est bijective si et seulement si $\psi \circ e_k \circ \psi^{-1}$ est bijective. Or :

$$\forall (x_1, \dots, x_s) \in \prod_{i=1}^{s} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}, \quad \psi \circ e_k \circ \psi^{-1}(x_1, \dots, x_s) = \left(x_1^k, \dots, x_s^k\right).$$

Ainsi, l'application e_k est bijective si et seulement si les applications e_k définies sur $\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$ sont bijectives pour tout $i \in [\![1, s]\!]$.

Étape 2 : e_k n'est pas bijective sur $\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}$ si $\alpha \geqslant 2$

Supposons donc $n = p^\alpha$ avec p premier et $\alpha \geqslant 2$. On va montrer que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ admet un élément nilpotent d'indice 2 (et donc non-nul). Posons $x = \overline{p}^{\alpha-1}$. On a bien que $x \neq 0$ et :

$$x^2 = \overline{p}^{2\alpha-2} = 0$$

car, étant donné que $\alpha \geqslant 2$, $2\alpha - 2 \geqslant \alpha$, et donc p^α divise $p^{2\alpha-2}$. Ainsi, e_k n'est pas injective (car $e_k(x) = x^k = x^2 x^{k-2} = 0 = e_k(0)$), donc n'est pas bijective.

Étape 3 : si e_k est bijective sur $\frac{\mathbb{Z}}{p\mathbb{Z}}$, alors $p-1$ est premier avec k.

Supposons maintenant $n = p$, nombre premier et e_k bijective. On a alors que e_k induit un automorphisme du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$. En particulier, e_k envoie un générateur g de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$ sur un autre générateur de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$, qui est donc g^k. En particulier, il existe $l \in \mathbb{N}^*$ tel que $g^{kl} = g$, et donc $g^{kl-1} = 1$. Ainsi, $\mathrm{o}(g) = p-1$ divise $kl-1$:

$$\exists u \in \mathbb{N}, \quad kl - 1 = u(p-1)$$

et donc, par le théorème de Bézout, k et $p-1$ sont premiers entre eux.

Étape 4 : Réciproque

Supposons donc $n = p$ et tel que $p-1$ soit premier avec k. Montrons que e_k est inijective (par cardinalité, e_k sera automatiquement bijective). Soient alors $x, y \in \frac{\mathbb{Z}}{p\mathbb{Z}}$ tels que $x^k = y^k$. Alors ou bien $x = y = 0$, ou bien x et y sont inversibles et donc :

$$\left(xy^{-1}\right)^k = 1.$$

Ainsi, $\mathrm{o}\left(xy^{-1}\right)$ divise k. Or, il divise également l'ordre du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$, qui est $p-1$. Ainsi, $\mathrm{o}\left(xy^{-1}\right)$ divise $k \wedge (p-1) = 1$. Ainsi, $xy^{-1} = 1$, i.e. $x = y$. L'application e_k est donc bijective ! □

Proposition 2.45 (Nilpotents et idempotents de $\frac{\mathbb{Z}}{n\mathbb{Z}}$)**.** Soit $n \in \mathbb{N}^*$ et écrivons-le $p_1^{\alpha_1} \dots p_s^{\alpha_s}$. Alors :

1. $a \in \mathbb{Z}$ est tel que $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ soit nilpotent si et seulement si :
$$\mathrm{rad}(n) := p_1 \dots p_s \mid a.$$
2. L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ possède exactement 2^s éléments idempotents.

Démonstration. Utilisons encore une fois le théorème des restes chinois. En utilisant le même calcul qu'en proposition 2.44, on a que $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ est nilpotent (resp. idempotent) si et seulement si $\overline{a} \in \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$ est nilpotent (resp. idempotent) pour tout $i \in [\![1, s]\!]$. Or, $\overline{a} \in \frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}$ est nilpotent (resp. idempotent) si et seulement si p^α divise a^k pour un certain $k \in \mathbb{N}^*$ (resp. p^α divise $a^2 - a$), ce qui est vérifié si et seulement si p divise a (resp. p^α divise $a^2 - a$, et puisque a et $a-1$ sont premiers entre eux, si et seulement si p^α divise a ou p^α divise $a-1$, i.e. $\overline{a} \in \{0, 1\}$ en tant qu'élément de $\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}$).

1. Ainsi, $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ est nilpotent si et seulement si p_i divise a pour tout $i \in [\![1, s]\!]$, et donc étant donné que les p_i sont premiers distincts, cela est vérifié si et seulement si $p_1 \dots p_s$ divise a, ce qui est bien ce que l'on voulait !
2. La discussion précédente montre alors que $\overline{a} \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ est idempotent si et seulement si $a \equiv 0 \ [p_i^{\alpha_i}]$ ou $a \equiv 1 \ [p_i^{\alpha_i}]$ pour tout $i \in [\![1, s]\!]$. Et, étant donné que l'application ψ des restes chinois est bijective, il y a donc exactement 2^s éléments idempotents dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (qui sont les $\psi^{-1}(\varepsilon_1, \dots, \varepsilon_s)$ où $\varepsilon_i \in \{0, 1\}$ pour tout $i \in [\![1, s]\!]$.

□

Ces résultats n'ont pas l'air passionnants mais peuvent potententiellement faire l'objet de questions du jury. Passons à des résultats peut-être plus fondamentaux, concernant la structure des inversibles de $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

Théorème 2.46. 1. Soit p un nombre premier impair et $\alpha \geqslant 1$. Alors :

$$\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{p^{\alpha-1}(p-1)\mathbb{Z}}.$$

2. Si $\alpha \geqslant 2$, on a :

$$\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}}$$

3. $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est cyclique si et seulement si $n \in \{2, 4\}$ ou $n = p^\alpha$ avec p premier impair, ou $n = 2p^\alpha$.

Démonstration. 1. **Étape 1 : cas $\alpha = 1$**

Pour montrer que $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ est cyclique, on utilise le fait que, si e désigne l'exposant de ce groupe, alors $X^e - 1$ admet tous les éléments de ce groupe comme racines. Ainsi, étant donné que $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps (en particulier il est intègre), on a que $e \geqslant p-1$. Or, e divise l'odre du groupe, donc $e \leqslant p-1$. On a donc $e = p-1$. Or, il existe un élément du groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ d'ordre e, donc d'ordre $p-1$, ce qui conclut. Prenons alors dans la suite $\alpha \geqslant 2$

Étape 2 : Détermination d'un élément d'ordre $p^{\alpha-1}$ dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$

On montre par récurrence sur $k \in \mathbb{N}$ la propriété suivante :

$$\forall k \in \mathbb{N},\ \exists \lambda_k \in \mathbb{N},\ \lambda_k \wedge p = 1, \quad (1+p)^{p^k} = 1 + p^{k+1}\lambda_k.$$

En effet, pour $k = 0$, c'est clair ($\lambda_0 = 1$). Maintenant, si $k \in \mathbb{N}$, on a :

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p = \left(1 + p^{k+1}\lambda_k\right)^p = \sum_{i=0}^{p} \binom{p}{i} \lambda_k^i p^{(k+1)i} = 1 + p^{k+2} \underbrace{\left(\lambda_k + \sum_{i=2}^{p} \frac{1}{p}\binom{p}{i} \lambda_k^i p^{(k+1)(i-1)}\right)}_{\equiv \lambda_k \not\equiv 0\ [p]},$$

ce qui montre que la propriété est bien héréditaire. On observe alors que $\overline{1+p} \in \left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ est d'ordre $p^{\alpha-1}$.

Étape 3 : Conclusion

Prenons un entier $g \in [\![1, p-1]\!]$ tel que $\overline{g} \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ soit un générateur de ce groupe. Posons alors $y = g^{p^{\alpha-1}}$. On a bien que $g^{p^{\alpha-1}}$ est premier avec p^α car g est premier avec p. Maintenant, par le théorème de Lagrange, on a que $y^{p-1} = g^{p^{\alpha-1}(p-1)} \equiv 1\ [p^\alpha]$. Ainsi, $r := \mathrm{o}(y)$ divise $p-1$ (l'ordre étant dans le groupe $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$). Or, en écrivant $y = g \times g^{p^{\alpha-1}-1}$, on observe que $y \equiv g\ [p]$ étant donné que $p-1$ divise $p^{\alpha-1}-1$. Or, $y^r \equiv 1\ [p^\alpha]$ et donc, par primalité de p, p divise $y^r - 1$. Ainsi, $y^r \equiv g^r \equiv 1\ [p]$. L'ordre de g dans $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$ étant $p-1$, on a donc que $p-1$ divise r, donc $r = p-1$. Ainsi, étant donné que $p-1$ et $p^{\alpha-1}$ sont premiers entre eux, on a que $\overline{y}\overline{1+p}$ est d'ordre $p^{\alpha-1}(p-1)$ dans $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$. Ce groupe est donc cyclique !

2. Pour $\alpha = 2$, c'est clair. Prenons alors $\alpha \geqslant 3$. On va alors, comme dans le cas p premier impair, trouver un élément d'ordre $2^{\alpha-2}$ et un autre d'ordre 2. Cependant, étant donné que ces deux nombres ne sont pas premiers entre eux, on retrouvera un produit direct et non plus un groupe cyclique. On montre que 5 est un

élément d'ordre $2^{\alpha-2}$ de $\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$, en montrant, par récurrence, que :

$$\forall k \in \mathbb{N},\ \exists \lambda_k \text{ impair}, \quad 5^{2^k} = 1 + 2^{k+2}\lambda_k.$$

Montrons alors que l'application :

$$\begin{array}{rccc} \mu & : & \langle 5\rangle \times \langle -1\rangle & \longrightarrow & \left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times \\ & & (u,v) & \longmapsto & uv \end{array}$$

est un isomorphisme. Déjà, μ est un morphisme de groupes et est bien défini. Ensuite, μ est injectif. En effet, si $u, u' \in \langle 5\rangle$ et $v, v' \in \{-1, 1\}$ sont tels que :

$$uu' = vv',$$

avec $u \neq u'$, alors $vv' = -1$ et on a que $5^k \equiv -1\ [2^\alpha]$ pour un certain $k \in \mathbb{N}$ (ici, $5^k = uu'$). Ainsi, il existe $l \in \mathbb{Z}$ tel que :

$$5^k = -1 + l \times 2^\alpha.$$

En réduisant modulo 4, on aurait alors $-1 \equiv 1\ [4]$, **ABSURDE !** Ainsi, $u = u'$ et donc $v = v'$. μ est donc injective, et, par cardinalité, μ est bijective, donc est un isomorphisme. Ainsi :

$$\left(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times \simeq \langle 5\rangle \times \langle -1\rangle \simeq \frac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}},$$

ce qui conclut !

3. En écrivant $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, on a, là encore, par le théorème chinois :

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \simeq \prod_{i=1}^{s} \left(\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}\right)^\times.$$

Si n est impair, on a alors :

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \simeq \prod_{i=1}^{s} \left(\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}\right)^\times \simeq \prod_{i=1}^{s} \frac{\mathbb{Z}}{p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}}$$

Ainsi, étant donné que $p_i - 1$ est pair pour tout $i \in [\![1, s]\!]$, si $s \geqslant 2$, alors le théorème chinois interdit également d'avoir l'isomorphisme :

$$\prod_{i=1}^{s} \frac{\mathbb{Z}}{p_i^{\alpha_i-1}(p_i-1)\mathbb{Z}} \simeq \frac{\mathbb{Z}}{\left(\prod_{i=1}^{s} p^{\alpha_i-1}(p_i-1)\right)\mathbb{Z}}$$

car les facteurs ne sont pas premiers entre eux. Ainsi, si n est impair et est tel que $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ soit cyclique, alors $n = p^\alpha$ pour un certain nombre premier p impair. Maintenant, si $p_1 = 2$, alors, ou bien $n = 2^\alpha$ et alors, si $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est cyclique, cela force à ce que $\alpha = 1$ ou $\alpha = 2$ d'après ce qu'on a vu. Si $p_1 = 2$ et $s \geqslant 2$, alors, en réitérant l'argument du cas n impair, on a que n s'écrit $2^\alpha p^\beta$ pour un certain nombre premier impair p. Si $\alpha \geqslant 2$, on a :

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}} \times \frac{\mathbb{Z}}{p^{\alpha-1}(p-1)\mathbb{Z}}$$

qui n'est pas cyclique étant donné que $p - 1$ est pair (donc n'est pas premier avec 2). Ainsi, on a $\alpha = 1$ et

on a bien que si $n = 2p^\alpha$, le groupe $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est cyclique, car isomorphe à $\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ par théorème chinois, ce qui termine la preuve !

□

Le théorème chinois a vraiment plein d'applications ! J'en donnerai une dernière concernant les nombres de Carmichaël :

Définition 2.47 (Nombre de Carmichaël)**.** Un entier $n \geqslant 2$ est dit de *Carmichaël* s'il n'est pas premier et vérifie :

$$\forall a \in \mathbb{Z}, \quad a^n \equiv a\ [n].$$

Autrement dit, c'est un nombre qui n'est pas premier mais ne possède aucun témoin de non-primalité de Fermat dans $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$.

On peut caractériser les nombres de Carmichaël grâce à la proposition suivante :

Théorème 2.48 (Critère de Korselt)**.** Un entier n est de Carmichaël si et seulement si n est sans facteur carré et, pour tout nombre premier p divisant n, $p-1$ divise $n-1$.

Démonstration. **Étape 1 : Un nombre de Carmichaël est sans facteur carré**
Soit n un nombre de Carmichaël. Supposons qu'il existe p premier tel que p^2 divise n. Alors, puisque n est de Carmichaël, n divise $p^n - p$, donc p^2 divise $p^n - p$ et, puisque $n \geqslant 2$, on a que p^2 divise p ! **ABSURDE !**

Étape 2 : Théorème chinois et conclusion
Écrivons $n = p_1 \dots p_s$ avec $s \geqslant 2$. Supposons que n soit de Carmichaël. Alors pour tout $a \in \mathbb{Z}$, $a^n \equiv a\ [n]$. En particulier, en posant b un entier vérifiant :

$$\forall i \in [\![1, s]\!], \quad b \equiv b_i\ [p_i]$$

avec b_i d'ordre $p_i - 1$ dans $\left(\frac{\mathbb{Z}}{p_i\mathbb{Z}}\right)^\times$ (il existe grâce au théorème chinois !) on a :

$$b^n \equiv b\ [n], \quad \text{et donc} \quad \forall i \in [\![1, s]\!], \quad b^n \equiv b_i^n \equiv b_i\ [p_i].$$

Ainsi, l'ordre de b_i, qui est $p_i - 1$ divise $n - 1$ pour tout i ! Réciproquement, si $p_i - 1$ divise $n - 1$ pour tout i, montrons que n est de Carmichaël. Étant donné que :

$$\forall i \in [\![1, s]\!],\ \forall a \in \mathbb{Z} \text{ tel que } a \wedge p_i = 1, \quad a^{p_i - 1} \equiv 1\ [p_i]$$

on a :

$$\forall i \in [\![1, s]\!],\ \forall a \in \mathbb{Z} \text{ tel que } a \wedge p_i = 1, \quad a^{n-1} \equiv 1\ [p_i].$$

Cela assure :

$$\forall i \in [\![1, s]\!],\ \forall a \in \mathbb{Z}, \quad a^n \equiv a\ [p_i].$$

Ainsi, par théorème chinois, on a :

$$\forall a \in \mathbb{Z}, \quad a^n \equiv a\ [n]$$

ce qui montre bien que n est de Carmichaël et cela conclut ! □