Plaquette 5 – L'anneau Z/nZ, théorème chinois et corps finis

Structures algébriques — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

L'anneau $\mathbb{Z}/n\mathbb{Z}$.

- $\overline{k}$ est **inversible** si et seulement si $k \wedge n = 1$; l'inverse se calcule par une relation de Bézout $uk + vn = 1$: $\overline{k}^{-1} = \overline{u}$.
- $\mathbb{Z}/n\mathbb{Z}$ est un **corps** $\Leftrightarrow$ il est intègre $\Leftrightarrow$ n est premier.
- **Équation** $\overline{a}x = \overline{b}$, avec $d = a \wedge n$: solutions si et seulement si $d \mid b$; il y en a alors d.
- **Théorème chinois** : si $m \wedge m' = 1$, l'application suivante est un isomorphisme d'anneaux :
$$\mathbb{Z}/mm'\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z}, \qquad k \bmod mm' \mapsto (k \bmod m,\ k \bmod m')$$
- **Indicatrice d'Euler** : $\varphi(n) = \mathrm{card}(\mathbb{Z}/n\mathbb{Z})^\times$; $\varphi(mm') = \varphi(m)\varphi(m')$ si $m \wedge m' = 1$; $\varphi(p^k) = p^k - p^{k-1}$.
- **Fermat-Euler** : $a^{\varphi(n)} \equiv 1 \pmod{n}$ si $a \wedge n = 1$; $a^p \equiv a \pmod{p}$ pour p premier.
- **Dans un corps**, un polynôme non nul de degré d a au plus d racines, et $xy = 0 \Rightarrow x = 0$ ou $y = 0$.

Correction de l'exercice 1 – Équations du premier degré modulo n

On regarde d'abord si $\overline{a}$ est inversible, via $d = a \wedge n$. La règle :

$$\overline{a}x = \overline{b} \text{ a des solutions} \Leftrightarrow d \mid b, \quad \text{et il y en a alors } d$$

- **a)** $7 \wedge 12 = 1$: $\overline{7}$ est inversible, et $7 \times 7 = 49 = 4 \times 12 + 1$ donne $\overline{7}^{-1} = \overline{7}$. Donc $x = \overline{7} \times \overline{3} = \overline{21} = \overline{9}$. Contrôle : $7 \times 9 = 63 = 60 + 3$ ✓.
- **b)** $d = 4 \wedge 10 = 2$ divise 6. On traduit : $10 \mid 4x - 6 \Leftrightarrow 5 \mid 2x - 3$, soit $\overline{2}x = \overline{3}$ dans $\mathbb{Z}/5\mathbb{Z}$; $\overline{2}^{-1} = \overline{3}$, donc $x \equiv 9 \equiv 4 \pmod{5}$. Modulo 10 : $x \in \{\overline{4}, \overline{9}\}$, deux solutions. Contrôle : $16 \equiv 6$ et $36 \equiv 6 \pmod{10}$ ✓.
- **c)** $d = 6 \wedge 9 = 3$ ne divise pas 4 : **aucune solution** ($6x - 4$ n'est jamais multiple de 3).
- **d)** $d = 15 \wedge 21 = 3$ divise 9 : on simplifie en $5x \equiv 3 \pmod{7}$. $\overline{5}^{-1} = \overline{3}$ dans $\mathbb{Z}/7\mathbb{Z}$ ($15 = 14 + 1$), donc $x \equiv 9 \equiv 2 \pmod{7}$: $x \in \{\overline{2}, \overline{9}, \overline{16}\}$ dans $\mathbb{Z}/21\mathbb{Z}$. Contrôle : $15 \times 2 = 30 \equiv 9 \pmod{21}$ ✓.

Piège : dans b), « diviser par 2 » l'égalité $\overline{4}x = \overline{6}$ n'est pas permis dans $\mathbb{Z}/10\mathbb{Z}$ ($\overline{2}$ n'y est pas inversible) ; on revient à la divisibilité dans $\mathbb{Z}$, où l'on divise **aussi le module**.

Réponse. a) $x = \overline{9}$ · b) $x \in \{\overline{4}, \overline{9}\}$ · c) aucune solution · d) $x \in \{\overline{2}, \overline{9}, \overline{16}\}$.

Correction de l'exercice 2 – Équations du second degré dans Z/pZ

a) $\mathbb{Z}/p\mathbb{Z}$ est un corps et $\overline{4a} \neq \overline{0}$ car p est impair : on peut multiplier par $4a$ (et diviser par $2a$). On développe :

$$4a\left(ax^2 + bx + c\right) = (2ax + b)^2 - \left(b^2 - 4ac\right)$$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— donc les solutions sont les $x = \frac{-b \pm \delta}{2a}$, où δ parcourt les racines carrées de Δ : deux solutions si Δ est un carré non nul, une si $\Delta = \overline{0}$, aucune si Δ n'est pas un carré.

b) Dans $\mathbb{Z}/7\mathbb{Z}$: $\Delta = 1 - 4 = -3 = \overline{4} = \overline{2}^2$. Avec $\overline{2}^{-1} = \overline{4}$:

— $x = (-1+2) \times 4 = \overline{4}$ ou $x = (-1-2) \times 4 = -12 \equiv \overline{2}$. Contrôle : $4 + 2 + 1 = 7$ et $16 + 4 + 1 = 21$, tous deux $\equiv 0$ ✓.

— Dans $\mathbb{Z}/5\mathbb{Z}$: $\Delta = -3 = \overline{2}$. Les carrés modulo 5 sont $\overline{0}, \overline{1}, \overline{4}$: $\overline{2}$ n'en est pas un, **aucune solution**. Contrôle direct : pour $x = 0, 1, 2, 3, 4$, $x^2 + x + 1$ vaut $1, 3, 7, 13, 21$, soit $1, 3, 2, 3, 1$ modulo 5 ✓.

c) $1^2 = 1$, $3^2 = 9$, $5^2 = 25$, $7^2 = 49$ sont tous $\equiv 1 \pmod 8$, les carrés pairs non : **quatre** solutions $\overline{1}, \overline{3}, \overline{5}, \overline{7}$.

— Ce n'est pas contradictoire : « au plus 2 racines pour un degré 2 » suppose un **corps** (ou un anneau intègre). Dans $\mathbb{Z}/8\mathbb{Z}$, $(x-1)(x+1) = \overline{0}$ n'impose pas un facteur nul : $\overline{2} \times \overline{4} = \overline{0}$ pour $x = \overline{3}$.

Réponse. Forme canonique valable pour p impair ; dans $\mathbb{Z}/7\mathbb{Z}$: $x \in \{\overline{2}, \overline{4}\}$; dans $\mathbb{Z}/5\mathbb{Z}$: aucune ; $x^2 = \overline{1}$ a quatre solutions dans $\mathbb{Z}/8\mathbb{Z}$ (non intègre).

Correction de l'exercice 3 – Le théorème chinois

a) Si $k \equiv k' \pmod{mm'}$, alors m et m' divisent $k - k'$: les images sont égales, ψ est bien défini. Il respecte somme, produit et unité, qui se calculent composante par composante.

b) Si $\psi(\overline{k}) = (\overline{0}, \overline{0})$, alors $m \mid k$ et $m' \mid k$, donc $\operatorname{ppcm}(m, m') = mm'$ divise k (car $m \wedge m' = 1$) : le noyau est nul, ψ est injectif. Les deux ensembles ont mm' éléments : ψ est bijectif, c'est un **isomorphisme d'anneaux**.

$$\mathbb{Z}/mm'\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z} \qquad (m \wedge m' = 1)$$

c) $u'm' = 1 - um \equiv 1 \pmod m$ et $um \equiv 0 \pmod m$, donc $k \equiv a \pmod m$. Symétriquement $um \equiv 1 \pmod{m'}$ et $k \equiv b \pmod{m'}$.

d) On procède en deux temps.

— Modulo 3 et 5 : $2 \times 3 - 1 \times 5 = 1$, donc $u = 2$, $u' = -1$, et $k = 3 \times 2 \times 3 + 2 \times (-1) \times 5 = 18 - 10 = 8$. Vérification : $8 \equiv 2 \pmod 3$, $8 \equiv 3 \pmod 5$ ✓. Les solutions sont les $x \equiv 8 \pmod{15}$.

— Modulo 15 et 7 : $x = 8 + 15t \equiv 1 + t \pmod 7$ doit valoir 2, donc $t \equiv 1 \pmod 7$, et $x = 23$.

Contrôle : $23 = 7 \times 3 + 2 = 5 \times 4 + 3 = 3 \times 7 + 2$ ✓. Les solutions sont les $23 + 105k$; la plus petite est 23.

Réponse. ψ isomorphisme d'anneaux ; $k = bum + au'm'$; le plus petit entier cherché est 23 (solutions $23 + 105\mathbb{Z}$).

Correction de l'exercice 4 – Indicatrice d'Euler

a) Un isomorphisme d'anneaux envoie les inversibles sur les inversibles. Par le théorème chinois :

$$(\mathbb{Z}/mm'\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/m'\mathbb{Z})^\times$$

— et les cardinaux donnent $\varphi(mm') = \varphi(m)\varphi(m')$.

b) Parmi $0, 1, \ldots, p^k - 1$, un entier n'est pas premier avec p^k si et seulement s'il est multiple de p : il y en a p^{k-1}. Donc $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

c) On décompose $n = \prod p_i^{k_i}$ (facteurs deux à deux premiers entre eux) et on applique a)

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

puis b) :

— $\varphi(n) = \prod p_i^{k_i}\left(1 - \frac{1}{p_i}\right) = n\prod\left(1 - \frac{1}{p_i}\right)$.

— $360 = 2^3 \times 3^2 \times 5$: $\varphi(360) = 4 \times 6 \times 4 = 96$.

— $1\,001 = 7 \times 11 \times 13$: $\varphi(1\,001) = 6 \times 10 \times 12 = 720$.

d) Pour $n \geq 3$, $\overline{k} \mapsto -\overline{k}$ est une involution de $(\mathbb{Z}/n\mathbb{Z})^\times$ sans point fixe : $\overline{k} = -\overline{k}$ donnerait $n \mid 2k$, puis, k étant premier avec n, $n \mid 2$. Les inversibles se regroupent donc en paires $\{\overline{k}, -\overline{k}\}$, et leur nombre est pair.

— Contrôle : $\varphi(360) = 96$ et $\varphi(1\,001) = 720$ sont bien pairs.

Réponse. φ multiplicative ; $\varphi(p^k) = p^k - p^{k-1}$; $\varphi(n) = n\prod(1 - \frac{1}{p})$; $\varphi(360) = 96$, $\varphi(1\,001) = 720$; $\varphi(n)$ pair pour $n \geq 3$.

Correction de l’exercice 5 – Le théorème de Wilson

a) $x = x^{-1} \Leftrightarrow x^2 = \overline{1} \Leftrightarrow (x - \overline{1})(x + \overline{1}) = \overline{0}$. Le corps $\mathbb{Z}/p\mathbb{Z}$ étant **intègre** :

$$x^2 = \overline{1} \Leftrightarrow x = \overline{1} \text{ ou } x = -\overline{1}$$

b) Pour $p = 2$: $1! \equiv -1 \pmod 2$. Pour p impair, $\overline{1} \neq -\overline{1}$. Les éléments de $\{\overline{2}, \ldots, \overline{p-2}\}$ sont distincts de leur inverse, qui est dans le même ensemble : ils se regroupent en paires $\{x, x^{-1}\}$ de produit $\overline{1}$. Il reste $\overline{1}$ et $-\overline{1}$, d’où

$$\overline{(p-1)!} = \overline{1} \times (-\overline{1}) \times \overline{1}^{(p-3)/2} = -\overline{1}$$

c) $6! = 720 = 7 \times 103 - 1$: $720 \equiv -1 \pmod 7$ ✓. $10! = 3\,628\,800 = 11 \times 329\,891 - 1$: $10! \equiv -1 \pmod{11}$ ✓.

d) Si n n’est pas premier, $n = ab$ avec $1 < a < n$. Alors a figure parmi $1, \ldots, n-1$, donc $a \mid (n-1)!$. Si l’on avait $(n-1)! = qn - 1$, alors a diviserait $qn - (n-1)! = 1$: absurde.

Bilan : Wilson caractérise les nombres premiers, mais ce critère est inutilisable en pratique ($(n-1)!$ est gigantesque).

Réponse. $x^2 = \overline{1} \Leftrightarrow x = \pm\overline{1}$; $(p-1)! \equiv -1 \pmod p$; $720 \equiv -1$ (7), $10! \equiv -1$ (11) ; réciproque vraie.

Correction de l’exercice 6 – Clé de contrôle de l’ISBN

a) Avec $(a_1, \ldots, a_9) = (2, 0, 7, 0, 3, 6, 0, 0, 2)$:

$$\sum_{i=1}^{9} i\,a_i = 2 + 21 + 15 + 36 + 18 = 92$$

— il faut $92 + 10a_{10} \equiv 0 \pmod{11}$. Or $92 = 88 + 4 \equiv 4$ et $10 \equiv -1$: $4 - a_{10} \equiv 0$, donc $a_{10} = 4$. Contrôle : $92 + 40 = 132 = 12 \times 11$ ✓.

b) Si a_i devient $a_i' \neq a_i$, la somme varie de $i(a_i' - a_i)$, avec $1 \leq i \leq 10$ et $0 < |a_i' - a_i| \leq 10$. Aucun des deux facteurs n’est multiple de 11, et $\mathbb{Z}/11\mathbb{Z}$ est **intègre** : $\overline{i}\,\overline{(a_i' - a_i)} \neq \overline{0}$. La nouvelle somme n’est plus $\equiv 0$: erreur détectée.

c) Échanger a_i et a_j ($i < j$) fait varier la somme de $ia_j + ja_i - ia_i - ja_j = (j - i)(a_i - a_j)$. Les deux facteurs sont non nuls et strictement inférieurs à 11 en valeur absolue : par intégrité, la variation est non nulle modulo 11.

d) Tout repose sur l’intégrité de $\mathbb{Z}/11\mathbb{Z}$ (11 premier). Modulo 10, $\overline{2} \times \overline{5} = \overline{0}$: avec des poids i, un 5 remplacé par un 7 en position 5 change la somme de $5 \times 2 = 10 \equiv 0$, erreur **invisible**. Le prix à payer est la clé « X » pour 10.

Réponse. $a_{10} = 4$; toute erreur simple et toute transposition sont détectées car $\mathbb{Z}/11\mathbb{Z}$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s’expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

est intègre ; modulo 10, $\overline{2}\times\overline{5}=\overline{0}$ masquerait des erreurs.

Correction de l'exercice 7 – Le chiffrement RSA en miniature

a) $\varphi(143)=\varphi(11)\varphi(13)=10\times12=120$. On cherche $7d\equiv1 \pmod{120}$; Euclide : $120=17\times7+1$, donc $1=120-17\times7$ et $d\equiv-17\equiv103$. Contrôle : $7\times103=721=6\times120+1$ ✓.

b) $ed=1+k\varphi(n)=1+k(p-1)(q-1)$ avec $k\geq0$.

— Si $p\mid m$: les deux membres sont nuls modulo p.

— Sinon, Fermat donne $m^{p-1}\equiv1$, donc $m^{ed}=m\left(m^{p-1}\right)^{k(q-1)}\equiv m \pmod{p}$.

De même modulo q. Ainsi p et q divisent $m^{ed}-m$, donc $pq=n$ aussi (premiers entre eux) :

$$m^{ed}\equiv m \pmod{n}$$

c) $2^7=128<143$: $c=128$.

d) Modulo 11 : $128=121+7\equiv7$, et $7^{10}\equiv1$ ramène l'exposant 103 à 3 : $7^3=343=341+2\equiv2$.

— Modulo 13 : $128=117+11\equiv-2$, et $103=8\times12+7$: $(-2)^7=-128=-130+2\equiv2$.

— Le résultat vaut 2 modulo 11 et modulo 13, donc 2 modulo 143 : on retrouve $m=2$ ✓.

Sécurité : connaître d revient à connaître $\varphi(n)$, donc à factoriser n. Avec n de plusieurs centaines de chiffres, c'est hors de portée.

Réponse. $\varphi(n)=120$, $d=103$; $m^{ed}\equiv m$ (n) ; $c=128$; $128^{103}\equiv2 \pmod{143}$.

Correction de l'exercice 8 – Un corps à quatre éléments

a) $A^2=\begin{pmatrix}0+1 & 0+1\\ 0+1 & 1+1\end{pmatrix}=\begin{pmatrix}\overline{1} & \overline{1}\\ \overline{1} & \overline{0}\end{pmatrix}$, et $A+I_2=\begin{pmatrix}\overline{1} & \overline{1}\\ \overline{1} & \overline{0}\end{pmatrix}$: égalité.

b) Les coefficients sont modulo 2, donc $M+M=0$ pour toute matrice. On note $B=A+I_2$.

— Addition : $I_2+A=B$, $I_2+B=A$, $A+B=I_2$, et $X+X=0$.

— Produit : $A^2=B$; $AB=A^2+A=B+A=I_2$; $B^2=A^2+2A+I_2=B+I_2=A$.

Toutes les sommes et tous les produits restent dans F_4, qui contient I_2 : sous-anneau. Il est commutatif (tout est polynôme en A). Enfin :

$$I_2^{-1}=I_2,\qquad A^{-1}=B,\qquad B^{-1}=A$$

— tout élément non nul est inversible : F_4 est un **corps** à 4 éléments.

c) $(\mathrm{F}_4,+)$: trois éléments d'ordre 2 ($X+X=0$), c'est le groupe de Klein. $(\mathrm{F}_4^*,\times)=\{I_2,A,A^2=B\}$ avec $A^3=AB=I_2$: cyclique d'ordre 3, engendré par A.

d) Dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{2}\times\overline{2}=\overline{0}$: $\overline{2}$ est diviseur de zéro, pas un corps. De plus $(\mathbb{Z}/4\mathbb{Z},+)$ est cyclique alors que $(\mathrm{F}_4,+)$ ne l'est pas : les deux anneaux ne sont même pas isomorphes comme groupes additifs.

Remarque : A est une racine de X^2+X+1, qui n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$; on a « ajouté » une racine comme on ajoute i à $\mathbb{R}$.

Réponse. $A^2=A+I_2$; F_4 est un corps ($A^{-1}=A+I_2$) ; groupe additif de Klein, groupe multiplicatif cyclique d'ordre 3 ; $\mathbb{Z}/4\mathbb{Z}$ n'est pas un corps.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 9 – Un corps à neuf éléments

a) Les carrés modulo 3 sont $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1$: ils valent $\overline{0}$ ou $\overline{1}$. Une somme de deux d'entre eux vaut $\overline{0}$, $\overline{1}$ ou $\overline{2}$, et vaut $\overline{0}$ seulement si les deux sont nuls.

b) Comme dans $\mathbb{C}$, on multiplie par le conjugué :

$$(a + b\,\mathrm{i})(a - b\,\mathrm{i}) = a^2 + b^2$$

— si $a + b\,\mathrm{i} \neq 0$, $a^2 + b^2 \neq \overline{0}$ par a), donc inversible dans le corps $\mathbb{Z}/3\mathbb{Z}$, et $(a + b\,\mathrm{i})^{-1} = (a^2 + b^2)^{-1}(a - b\,\mathrm{i})$. K est un corps à 9 éléments.

— Pour $\overline{1} + \mathrm{i}$: $a^2 + b^2 = \overline{2}$, d'inverse $\overline{2}$ ($2 \times 2 = 4 \equiv 1$), donc $(\overline{1} + \mathrm{i})^{-1} = \overline{2}(\overline{1} - \mathrm{i}) = \overline{2} + \mathrm{i}$. Contrôle : $(1 + \mathrm{i})(2 + \mathrm{i}) = 2 + \mathrm{i} + 2\mathrm{i} - 1 = 1 + 3\mathrm{i} = \overline{1}$ ✓.

c) Avec $z = \overline{1} + \mathrm{i}$: $z^2 = 1 + 2\mathrm{i} - 1 = \overline{2}\mathrm{i}$, $z^4 = (\overline{2}\mathrm{i})^2 = 4\mathrm{i}^2 = -4 \equiv \overline{2}$, donc $z^8 = \overline{4} = \overline{1}$. L'ordre de z divise 8 mais pas 4 ($z^4 = \overline{2} \neq \overline{1}$) : il vaut $8 = \mathrm{card}\mathrm{K}^*$, et z engendre K^*, qui est **cyclique**.

d) Modulo 5 : $(\overline{2} + \mathrm{i})(\overline{2} - \mathrm{i}) = 4 + 1 = \overline{5} = \overline{0}$, avec deux facteurs non nuls : l'anneau obtenu n'est pas intègre, donc pas un corps. La différence vient de ce que -1 est un carré modulo 5 ($2^2 = 4 \equiv -1$) mais pas modulo 3.

Réponse. Les carrés modulo 3 sont $\overline{0}, \overline{1}$; K est un corps à 9 éléments, $(\overline{1} + \mathrm{i})^{-1} = \overline{2} + \mathrm{i}$; $\overline{1} + \mathrm{i}$ d'ordre 8 ; modulo 5, $(\overline{2} + \mathrm{i})(\overline{2} - \mathrm{i}) = \overline{0}$.

Correction de l'exercice 10 – Sous-corps de C

a) K contient 1, donc les $n = 1 + \ldots + 1$ et leurs opposés : $\mathbb{Z} \subset K$. Pour $q \neq 0$, $q^{-1} \in K$, puis $\frac{p}{q} = p\,q^{-1} \in K$. Donc

$$\mathbb{Q} \subset K \quad \text{pour tout sous-corps } K \text{ de } \mathbb{C}$$

b) Soit (K_j) une famille de sous-corps et $K = \bigcap K_j$. $1 \in K$; si $x, y \in K$, $x - y$ et xy sont dans chaque K_j, donc dans K ; si $x \in K \setminus \{0\}$, x^{-1} est dans chaque K_j. C'est un sous-corps.

c) $\mathbb{Q}(\mathrm{i})$ contient 1, est stable par différence, et par produit : $(a + \mathrm{i}b)(c + \mathrm{i}d) = (ac - bd) + \mathrm{i}(ad + bc)$. Pour $z = a + \mathrm{i}b \neq 0$:

— $z^{-1} = \dfrac{\overline{z}}{|z|^2} = \dfrac{a}{a^2 + b^2} - \mathrm{i}\dfrac{b}{a^2 + b^2}$, à coefficients rationnels : c'est un sous-corps.

— Un sous-corps K contenant i contient $\mathbb{Q}$ (par a)), donc tous les $a + \mathrm{i}b$ avec a, b rationnels : $\mathbb{Q}(\mathrm{i}) \subset K$.

Exemple : $\dfrac{1}{2 + \mathrm{i}} = \dfrac{2 - \mathrm{i}}{5} = \dfrac{2}{5} - \dfrac{1}{5}\mathrm{i} \in \mathbb{Q}(\mathrm{i})$.

d) Non : $2 \in \mathbb{Z}[\mathrm{i}]$ mais $\frac{1}{2} \notin \mathbb{Z}[\mathrm{i}]$ (et plus généralement, seuls ± 1, $\pm\mathrm{i}$ y sont inversibles). $\mathbb{Q}(\mathrm{i})$ est le plus petit corps contenant $\mathbb{Z}[\mathrm{i}]$.

Réponse. $\mathbb{Q} \subset K$; intersection de sous-corps = sous-corps ; $\mathbb{Q}(\mathrm{i})$ est le plus petit sous-corps contenant i ; $\mathbb{Z}[\mathrm{i}]$ n'est pas un corps.

Correction de l'exercice 11 – Générateurs de (Z/11Z)* et échange de clés

a) Par Lagrange, l'ordre de $\overline{2}$ divise $\mathrm{card}G = 10$: c'est 1, 2, 5 ou 10. On teste les diviseurs stricts :

$$2^1 = 2, \qquad 2^2 = 4, \qquad 2^5 = 32 = 33 - 1 \equiv -1$$

— aucun ne vaut 1 : $\overline{2}$ est d'ordre 10 et engendre G.

b) $G \simeq \mathbb{Z}/10\mathbb{Z}$ par $\overline{k} \mapsto \overline{2}^k$; les générateurs sont les $\overline{2}^k$ avec $k \wedge 10 = 1$, soit $k \in \{1, 3, 7, 9\}$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

:

— $2^1 = 2$, $2^3 = 8$, $2^7 = 128 = 121 + 7 \equiv 7$, $2^9 = 512 = 506 + 6 \equiv 6$. Générateurs : $\overline{2}, \overline{6}, \overline{7}, \overline{8}$ ($\varphi(10) = 4$ générateurs).

c) Puissances successives : $2, 4, 8, 16 \equiv 5$: $k = 4$. Contrôle : $2^4 = 16 = 11 + 5$ ✓.

d) $A = 2^3 = 8$ et $B = 2^4 \equiv 5$.

— Alice calcule $B^a = 5^3 = 125 = 121 + 4 \equiv 4$.

— Bob calcule $A^b = 8^4 = 4\,096 = 372 \times 11 + 4 \equiv 4$.

Les deux obtiennent 4, car $B^a = g^{ab} = A^b$. Un espion connaît g, A, B ; pour retrouver la clé, il doit résoudre un logarithme discret comme en c), infaisable pour des p de plusieurs centaines de chiffres.

Réponse. $\overline{2}$ d'ordre 10 ; générateurs $\overline{2}, \overline{6}, \overline{7}, \overline{8}$; $k = 4$; $A = 8$, $B = 5$, clé commune 4.

Correction de l'exercice 12 – Le chiffrement affine

a) Si a est inversible, $y = ax + b \Leftrightarrow x = a^{-1}(y - b)$: bijection. Si a n'est pas inversible, a est diviseur de zéro ($\mathbb{Z}/26\mathbb{Z}$, exercice des diviseurs de zéro) : $ac = \overline{0}$ avec $c \neq \overline{0}$, et $f_{a,b}(c) = f_{a,b}(\overline{0})$, pas injective.

— a inversible $\Leftrightarrow a \wedge 26 = 1$: $\varphi(26) = \varphi(2)\varphi(13) = 12$ choix, et 26 choix de b : $12 \times 26 = 312$ clés.

b) $f_{a,b} \circ f_{c,d}(x) = a(cx + d) + b = acx + (ad + b)$, avec ac inversible ; id $= f_{1,0}$; la réciproque $x \mapsto a^{-1}x - a^{-1}b$ est encore affine. C'est un sous-groupe du groupe des permutations de $\mathbb{Z}/26\mathbb{Z}$.

c) $M = 12$, $A = 0$, $T = 19$, $H = 7$, et $y = 5x + 8$ modulo 26 :

— M : $68 = 52 + 16 \to 16 = Q$; A : $8 = I$; T : $103 = 78 + 25 \to 25 = Z$; H : $43 = 26 + 17 \to 17 = R$.

MATH devient QIZR.

d) $5 \times 21 = 105 = 4 \times 26 + 1$, donc $\overline{5}^{-1} = \overline{21}$ et

$$x = 21\,(y - 8) \bmod 26$$

— Q : $21 \times 8 = 168 = 156 + 12 \to M$; I : $0 \to A$; Z : $21 \times 17 = 357 = 338 + 19 \to T$; R : $21 \times 9 = 189 = 182 + 7 \to H$. On retrouve MATH ✓.

Faiblesse : chaque lettre est toujours chiffrée de la même façon ; une analyse des fréquences (le E est la lettre la plus courante) casse le code.

Réponse. Bijection $\Leftrightarrow a \wedge 26 = 1$, 312 clés ; groupe pour $\circ$; MATH $\to$ QIZR ; déchiffrement $x = 21(y - 8)$.

Correction de l'exercice 13 – Calculs de restes

On calcule dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ adapté, en réduisant l'exposant grâce à l'ordre de l'élément.

a) Modulo 10 : $7^2 = 49 \equiv 9$, $7^4 \equiv 81 \equiv 1$. Comme $2026 = 4 \times 506 + 2$,

$$7^{2026} = \left(7^4\right)^{506} \times 7^2 \equiv 9 \pmod{10}$$

— le dernier chiffre est 9.

b) $3^{10} = 59\,049 \equiv 49 \pmod{100}$, puis $3^{20} \equiv 49^2 = 2\,401 \equiv 1$. Donc $3^{100} = \left(3^{20}\right)^5 \equiv 1$: les deux derniers chiffres sont 01.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) Modulo 7 : $3^{2n+1} = 3 \times 9^n \equiv 3 \times 2^n$ car $9 \equiv 2$, et $2^{n+2} = 4 \times 2^n$. La somme vaut $7 \times 2^n \equiv 0$: 7 la divise.

— Contrôle pour $n = 1$: $3^3 + 2^3 = 27 + 8 = 35 = 5 \times 7$ ✓.

d) Par Fermat, $2^{12} \equiv 1 \pmod{13}$: il suffit de connaître 2^{10} modulo 12.
$2^{10} = 1\,024 = 85 \times 12 + 4$, donc $2^{2^{10}} \equiv 2^4 = 16 \equiv 3 \pmod{13}$.

Méthode : l'exposant se réduit modulo l'**ordre** (ou modulo $p-1$, jamais modulo p).

Réponse. a) 9 · b) 01 · c) $3^{2n+1} + 2^{n+2} \equiv 7 \times 2^n \equiv 0$ (7) · d) 3.

Correction de l'exercice 14 – Morphismes d'anneaux entre les Z/nZ

a) Un sous-anneau contient $\overline{1}$, donc $\overline{1} + \ldots + \overline{1} = \overline{k}$ pour tout k : c'est $\mathbb{Z}/n\mathbb{Z}$ entier.

b) Si f existe, $f(\overline{1}) = \overline{1}$, donc $f(\overline{k}) = \overline{k}$ (image de k modulo m) : f est unique. De plus

$$\overline{0} = f(\overline{0}) = f(\overline{n}) = n \cdot \overline{1} \quad \text{dans } \mathbb{Z}/m\mathbb{Z}$$

— donc $m \mid n$. Réciproquement, si $m \mid n$, $k \bmod n \mapsto k \bmod m$ est bien défini ($n \mid k - k' \Rightarrow m \mid k - k'$) et respecte les deux lois et l'unité.

c) $4 \mid 12$: oui, la réduction $k \bmod 12 \mapsto k \bmod 4$. $12 \nmid 4$: **non** de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ — en effet $f(\overline{1}+\overline{1}+\overline{1}+\overline{1}) = f(\overline{0}) = \overline{0}$ exigerait $\overline{4} = \overline{0}$ dans $\mathbb{Z}/12\mathbb{Z}$.

— Remarque : il existe bien des morphismes de **groupes** $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ (comme $\overline{k} \mapsto \overline{3k}$), mais aucun n'envoie $\overline{1}$ sur $\overline{1}$.

d) Un morphisme $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Q}$ donnerait $0 = f(\overline{0}) = f(p \cdot \overline{1}) = p \cdot 1 = p$ dans $\mathbb{Q}$: absurde. Un morphisme $g : \mathbb{Q} \to \mathbb{Z}/p\mathbb{Z}$ vérifierait $g(p) = p \cdot \overline{1} = \overline{0}$, mais p est inversible dans $\mathbb{Q}$, donc $g(p)g\left(\frac{1}{p}\right) = g(1) = \overline{1}$: absurde.

Réponse. Seul sous-anneau : lui-même ; morphisme $\mathbb{Z}/n \to \mathbb{Z}/m \Leftrightarrow m \mid n$, unique ; oui de $\mathbb{Z}/12$ vers $\mathbb{Z}/4$, non dans l'autre sens ; aucun morphisme entre $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Q}$.

Correction de l'exercice 15 – Synthèse : racines carrées de 1 modulo n

a) $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc intègre : $(x-\overline{1})(x+\overline{1}) = \overline{0} \Leftrightarrow x = \pm\overline{1}$, et $\overline{1} \neq -\overline{1}$ car $p \neq 2$. Deux solutions.

b) L'isomorphisme d'anneaux $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ transforme l'équation en un système : $x^2 = \overline{1}$ dans chacune des composantes.

$$x^2 \equiv 1\ (15) \Leftrightarrow \begin{cases} x \equiv \pm 1 \pmod 3 \\ x \equiv \pm 1 \pmod 5 \end{cases}$$

— $2 \times 2 = 4$ couples de signes, donc 4 solutions : $(1,1) \to 1$, $(-1,-1) \to 14$, $(1,-1) \to 4$ ($4 \equiv 1 \bmod 3$, $4 \equiv -1 \bmod 5$), $(-1,1) \to 11$.

— Contrôle : $4^2 = 16$, $11^2 = 121 = 8 \times 15 + 1$, $14^2 = 196 = 13 \times 15 + 1$ ✓. Solutions : $\overline{1}, \overline{4}, \overline{11}, \overline{14}$.

c) Chaque facteur premier impair apporte un choix de signe indépendant : $2^3 = 8$ solutions modulo 105 (ce sont $1, 29, 34, 41, 64, 71, 76, 104$), et $2^2 = 4$ modulo pq.

d) $n \mid (x-1)(x+1)$. Si $d = 1$, alors $n \mid x+1$ (Gauss), soit $x = -\overline{1}$: exclu. Si $d = n$, alors $x = \overline{1}$: exclu. Donc $1 < d < n$.

— $n = 15$, $x = 4$: $3 \wedge 15 = 3$. $x = 11$: $10 \wedge 15 = 5$. On retrouve $15 = 3 \times 5$ ✓.

e) Le PGCD se calcule très vite (Euclide) : une racine non triviale de $\overline{1}$ fournit donc immédiatement un facteur de n. Réciproquement, pour $n = pq$ inconnu, trouver une telle racine est aussi difficile que factoriser — c'est sur cette difficulté que reposent des

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

cryptosystèmes comme celui de Rabin.

Réponse. Deux solutions modulo p ; modulo 15 : $\overline{1}, \overline{4}, \overline{11}, \overline{14}$; 8 modulo 105, 4 modulo pq ; $(x-1) \wedge n$ est un diviseur strict : 3 et 5 pour $n = 15$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).