Anneaux, idéaux et Z/nZ

Corrigé de l'exercice 1 : Inversibles de Z/nZ et calcul d'inverses

1. Une classe est inversible si sa ligne contient la case $\bar{1}$. Sur la table, on lit $\bar{1}\times\bar{1}=\bar{1}$, $\bar{3}\times\bar{7}=\overline{21}=\bar{1}$ et $\bar{9}\times\bar{9}=\overline{81}=\bar{1}$. En revanche, les lignes de 0, 2, 4, 5, 6 et 8 ne contiennent pas $\bar{1}$. Donc $(\mathbb{Z}/10\mathbb{Z})^{\times}=\{\bar{1},\overline{3},\overline{7},\bar{9}\}$**, avec** $\bar{3}^{-1}=\bar{7}$ **et** $\bar{9}^{-1}=\bar{9}$**.** Le cours donne le même résultat : les entiers de 0 à 9 premiers avec 10 sont 1, 3, 7 et 9.

2. Les inversibles correspondent aux entiers de $[\![0,19]\!]$ premiers avec $20=2^2\times5$. Ce sont les entiers impairs non multiples de 5. On obtient $\{\bar{1},\bar{3},\bar{7},\bar{9},\overline{11},\overline{13},\overline{17},\overline{19}\}$, soit $\varphi(20)=8$ éléments. Ensuite, $7\times3=21=20+1$. Donc $\bar{7}^{-1}=\bar{3}$ **dans** $\mathbb{Z}/20\mathbb{Z}$**.**

Questions 3 à 4

3. D'abord, $17\wedge60=1$, car 17 est premier et ne divise pas 60. L'algorithme d'Euclide donne :

$$60=3\times17+9,\ 17=1\times9+8,\ 9=1\times8+1.$$

On remonte ensuite les calculs :

$$1=9-8=9-(17-9)=2\times9-17=2(60-3\times17)-17=2\times60-7\times17.$$

Ainsi, $17\times(-7)\equiv1\,(\mathrm{mod}\,60)$. Donc $\overline{17}^{-1}=\overline{-7}=\overline{53}$**.** Vérification : $17\times53=901=15\times60+1$.

4. On a $\bar{6}\times\overline{10}=\overline{60}=\bar{0}$, alors que $\bar{6}\neq\bar{0}$ et $\overline{10}\neq\bar{0}$. Donc $\bar{6}$ **est un diviseur de zéro.** C'est cohérent avec le cours, puisque $6\wedge20=2>1$ et $20/2=10$.

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Point de méthode : vérifiez toujours un inverse modulaire par une multiplication ; c'est rapide et cela évite les erreurs de signe.

Corrigé de l'exercice 2 : Calculs de l'indicatrice d'Euler

1. On décompose chaque entier, puis on applique la multiplicativité et la formule $\varphi(p^k) = p^k - p^{k-1}$.
   - $360 = 2^3 \times 3^2 \times 5$, donc $\varphi(360) = (8-4)(9-3)(5-1) = 4 \times 6 \times 4$, soit $\varphi(360) = 96$.
   - $1001 = 7 \times 11 \times 13$, donc $\varphi(1001) = 6 \times 10 \times 12$, soit $\varphi(1001) = 720$.
   - $\varphi(2^{10}) = 2^{10} - 2^9 = 2^9$, soit $\varphi(1024) = 512$.
   - $343 = 7^3$, donc $\varphi(343) = 343 - 49$, soit $\varphi(343) = 294$.
2. On a $2026 = 2 \times 1013$, avec 2 et 1013 premiers distincts. Par multiplicativité, $\varphi(2026) = \varphi(2)\varphi(1013) = 1 \times 1012$. Donc $\varphi(2026) = 1012$.
3. Soit $n \geq 3$. Deux cas se présentent.
   - Si n a un facteur premier impair p, on écrit $n = p^\alpha m$ avec $p \wedge m = 1$. Alors $\varphi(n) = p^{\alpha-1}(p-1)\varphi(m)$, et $p-1$ est pair.
   - Sinon, $n = 2^k$ avec $k \geq 2$, car $n \geq 3$. Alors $\varphi(n) = 2^{k-1}$ est pair.

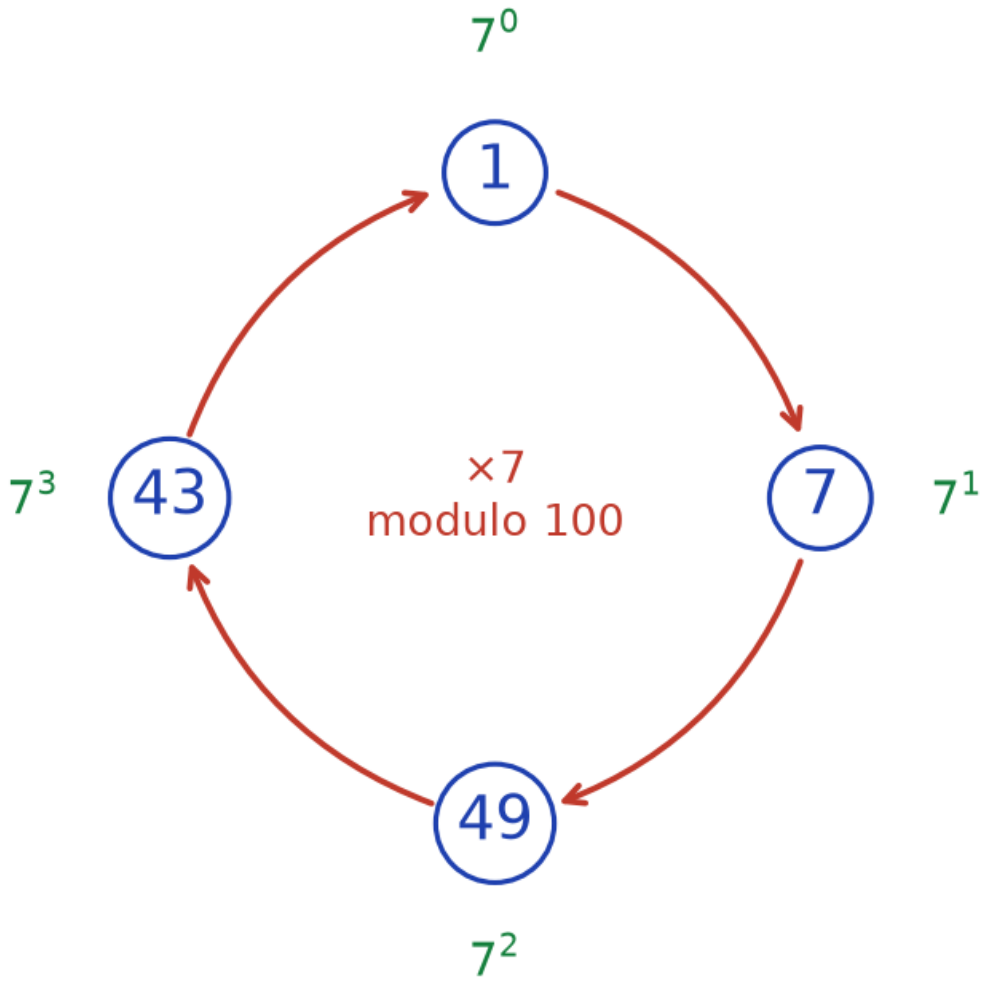
   Dans les deux cas, $\varphi(n)$ **est pair.**

Corrigé de l'exercice 3 : Puissances modulo n par le théorème d'Euler

1. Le nombre 7 est premier et ne divise pas 3. D'après le petit théorème de Fermat, $3^6 \equiv 1 \pmod 7$. Or $1000 = 166 \times 6 + 4$. Donc $3^{1000} \equiv 3^4 = 81 = 11 \times 7 + 4$. **Le reste vaut 4.**

2. De même, 13 est premier, donc $2^{12} \equiv 1 \pmod{13}$. Comme $100 = 8 \times 12 + 4$, on obtient $2^{100} \equiv 2^4 = 16 \equiv 3$. **Le reste vaut 3.**

3. On a $7^2 = 49$ et $7^4 = 49^2 = 2401 \equiv 1 \pmod{100}$. Ainsi, la classe de 7 est d'ordre 4 dans $(\mathbb{Z}/100\mathbb{Z})^\times$. Ensuite, $2026 = 4 \times 506 + 2$, donc $7^{2026} \equiv 7^2 = 49$. **Les deux derniers chiffres de 7^{2026} sont 4 et 9.** La figure ci-dessous montre ce cycle de longueur 4, bien plus court que $\varphi(100) = 40$.



4. Le chiffre des unités est le reste modulo 10. Or $13 \equiv 3 \pmod{10}$ et $3^4 = 81 \equiv 1 \pmod{10}$. Comme $2026 \equiv 2 \pmod 4$, on obtient $13^{2026} \equiv 3^2 = 9$. **Le chiffre des unités est 9.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

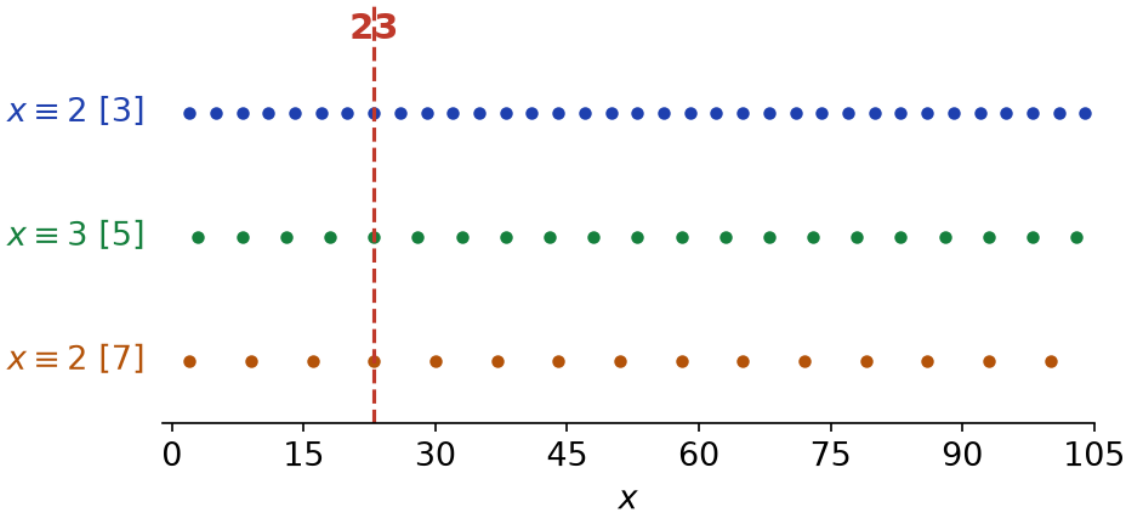
Point de méthode : le théorème d'Euler donne un exposant qui annule, mais pas forcément le plus petit ; cherchez d'abord une petite puissance égale à 1.

Corrigé de l'exercice 4 : Un système de trois congruences

1. Les entiers 3, 5 et 7 sont premiers deux à deux. En appliquant deux fois le théorème chinois, on obtient un isomorphisme $\mathbb{Z}/105\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Le triplet $(\bar{2}, \bar{3}, \bar{2})$ a donc un unique antécédent. Par conséquent, **les solutions forment une seule classe modulo 105.**

2. On part de la relation de Bézout $3 \times 2 + 5 \times (-1) = 1$. D'après la méthode du cours, $x_0 = 2 \times 5 \times (-1) + 3 \times 3 \times 2 = -10 + 18 = 8$. Vérification : $8 = 2 \times 3 + 2$ et $8 = 5 + 3$. Donc $x \equiv 8 \,(\mathrm{mod}\, 15)$**.**

3. Il reste à résoudre $x \equiv 8 \,(\mathrm{mod}\, 15)$ et $x \equiv 2 \,(\mathrm{mod}\, 7)$. On écrit $x = 8 + 15k$. Comme $15 \equiv 1 \,(\mathrm{mod}\, 7)$, on a $x \equiv 1 + k \,(\mathrm{mod}\, 7)$. La condition devient $k \equiv 1 \,(\mathrm{mod}\, 7)$, d'où $x = 8 + 15 = 23$ à 105 près. Donc $x \equiv 23 \,(\mathrm{mod}\, 105)$ **.** La figure ci-dessous confirme que 23 est le seul entier de $[\![0, 104]\!]$ qui vérifie les trois conditions.



4. Les solutions sont les $23 + 105j$. Or $23 + 105 \times 9 = 968 < 1000$ et $23 + 105 \times 10 = 1073$. **Le plus petit entier cherché est 1073.**

Corrigé de l'exercice 5 : Idéaux de Z et PGCD

1. D'après le cours, $12\mathbb{Z}+18\mathbb{Z}=(12\wedge 18)\mathbb{Z}$ et $12\mathbb{Z}\cap 18\mathbb{Z}=(12\vee 18)\mathbb{Z}$. Comme $12=2^2\times 3$ et $18=2\times 3^2$, on obtient $12\mathbb{Z}+18\mathbb{Z}=6\mathbb{Z}$ **et** $12\mathbb{Z}\cap 18\mathbb{Z}=36\mathbb{Z}$**.**

2. La somme vaut $(84\wedge 60\wedge 105)\mathbb{Z}$. D'abord, $84\wedge 60=12$. Ensuite, $12\wedge 105=3$. Donc $84\mathbb{Z}+60\mathbb{Z}+105\mathbb{Z}=3\mathbb{Z}$**.** Par ailleurs, $84=60+24$ et $60=2\times 24+12$. Ainsi, $12=60-2\times 24=60-2(84-60)=3\times 60-2\times 84$. **On peut prendre** $u=-2$ **et** $v=3$**.**

3. Si $a\mathbb{Z}\subset b\mathbb{Z}$, alors $a\in b\mathbb{Z}$, donc b divise a. Réciproquement, si $a=bc$, tout multiple $ak=b(ck)$ de a est un multiple de b. **Donc** $a\mathbb{Z}\subset b\mathbb{Z}\Leftrightarrow b\,|\,a$**.**

4. Un idéal de $\mathbb{Z}$ s'écrit $n\mathbb{Z}$ avec $n\in\mathbb{N}$. D'après la question précédente, $18\mathbb{Z}\subset n\mathbb{Z}$ si et seulement si n divise 18. **Les idéaux cherchés sont** $\mathbb{Z}$**,** $2\mathbb{Z}$**,** $3\mathbb{Z}$**,** $6\mathbb{Z}$**,** $9\mathbb{Z}$ **et** $18\mathbb{Z}$**.**

Corrigé de l'exercice 6 : Parties qui sont ou non des idéaux

1. La partie I_1 contient 0 et elle est stable par différence, car les conditions sont linéaires. Soit ensuite $A\in\mathbb{R}[X]$ et $P\in I_1$. On a $(AP)(1)=A(1)P(1)=0$ et $(AP)'(1)=A'(1)P(1)+A(1)P'(1)=0$. Donc I_1 est un idéal. De plus, $P(1)=P'(1)=0$ signifie que 1 est racine au moins double de P. Autrement dit, $(X-1)^2$ divise P. **Ainsi,** $I_1=(X-1)^2\,\mathbb{R}[X]$**.**

2. Le polynôme nul n'appartient pas à I_2. **Donc** I_2 **n'est pas un idéal**, ni même un sous-groupe.

3. La partie I_3 est un sous-groupe additif. Cependant, $X\in I_3$ et $X^2\times X=X^3\notin I_3$. L'absorption est en défaut, donc I_3 **n'est pas un idéal.**

4. La partie I_4 est le noyau du morphisme d'anneaux $P\to P(i)$ de $\mathbb{R}[X]$ dans $\mathbb{C}$. C'est donc un idéal. Pour le décrire, on écrit la division euclidienne $P=(X^2+1)Q+aX+b$ dans $\mathbb{R}[X]$. Alors $P(i)=ai+b$, avec a,b réels. Donc $P(i)=0$ équivaut à $a=b=0$. **Ainsi,** $I_4=(X^2+1)\,\mathbb{R}[X]$**.**

5. On a $2\in I_5$ et $3\in I_5$, mais $2+3=5$ n'est multiple ni de 2 ni de 3. **Donc** I_5 **n'est pas un idéal.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Corrigé de l'exercice 7 : Équations linéaires modulo n

1. L'équation a une solution si et seulement s'il existe $x, y \in \mathbb{Z}$ tels que $ax + ny = b$. Autrement dit, $b \in a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. C'est bien la condition $d \mid b$. Supposons-la réalisée et écrivons $a = da'$, $n = dn'$, $b = db'$. Alors $n \mid ax - b$ équivaut à $n' \mid a'x - b'$. Or $a' \wedge n' = 1$, donc a' est inversible modulo n'. Les solutions forment ainsi une classe $x_0 + n'\mathbb{Z}$. Modulo n, cette classe donne $x_0, x_0 + n', \ldots, x_0 + (d-1)n'$. **Il y a donc exactement d solutions modulo n.**

2. Ici $d = 6 \wedge 10 = 2$, qui divise 4. On se ramène à $3x \equiv 2 \pmod 5$. L'inverse de 3 modulo 5 est 2, donc $x \equiv 4 \pmod 5$. **Les solutions sont $x \equiv 4$ ou $x \equiv 9 \pmod{10}$.** Vérification : $24 \equiv 4$ et $54 \equiv 4$ modulo 10.

3. Ici $d = 6 \wedge 9 = 3$, qui ne divise pas 5. **L'équation n'a aucune solution.** On le voit aussi directement : $6x - 5$ n'est jamais multiple de 3.

Question 4

4. On a $133 = 7 \times 19$ et $91 = 7 \times 13$, donc $d = 7$, qui divise $35 = 7 \times 5$. L'équation équivaut à $13x \equiv 5 \pmod{19}$. Or $13 \times 3 = 39 = 2 \times 19 + 1$, donc l'inverse de 13 est 3. Ainsi, $x \equiv 15 \pmod{19}$. **Les solutions modulo 133 sont 15, 34, 53, 72, 91, 110 et 129.** Vérification : $91 \times 15 - 35 = 1330 = 10 \times 133$.

Corrigé de l'exercice 8 : Congruences à modules non premiers entre eux

1. Supposons que x soit solution. Comme d divise m et n, on a $x \equiv a$ et $x \equiv b$ modulo d, donc $a \equiv b \pmod d$. Réciproquement, écrivons $a - b = td$ et une relation de Bézout $mu + nv = d$. Alors $a - b = tmu + tnv$. Posons $x = a - tmu$. D'une part, $x \equiv a \pmod m$. D'autre part, $x = b + tnv \equiv b \pmod n$. Enfin, x et x' sont deux

solutions si et seulement si m et n divisent $x - x'$, c'est-à-dire si $m \vee n$ divise $x - x'$. **Les solutions forment donc une classe modulo $m \vee n$.**

2. Ici $d = 2$ et $3 \equiv 5 \pmod 2$: il y a des solutions, uniques modulo 12. Avec $4 \times (-1) + 6 \times 1 = 2$ et $t = (3-5)/2 = -1$, on obtient $x = 3 - (-1) \times 4 \times (-1) = -1$. **Les solutions sont les $x \equiv 11 \pmod{12}$.** Vérification : $11 = 2 \times 4 + 3 = 6 + 5$.

3. Ici $d = 2$, mais $1 \not\equiv 2 \pmod 2$. **Il n'y a aucune solution** : la première congruence impose x impair, la seconde x pair.

Question 4

4. Notons x le nombre de soldats. La condition « il en reste un par 2, 3, 4, 5 ou 6 » signifie que $x - 1$ est multiple de 2, 3, 4, 5 et 6, donc de leur PPCM 60. Ainsi, $x \equiv 1 \pmod{60}$ et $x \equiv 0 \pmod 7$. Comme $60 \wedge 7 = 1$, la solution est unique modulo 420. On écrit $x = 1 + 60k$, avec $60 \equiv 4 \pmod 7$. Il faut $4k \equiv -1 \equiv 6 \pmod 7$. L'inverse de 4 modulo 7 est 2, donc $k \equiv 12 \equiv 5$. D'où $x \equiv 301 \pmod{420}$. **La troupe compte 301 soldats**, seule solution inférieure à 400.

Corrigé de l'exercice 9 : Produit d'anneaux et idempotents

1. Comme $2 \wedge 3 = 1$, le théorème chinois fournit l'isomorphisme $\begin{matrix}\bar{k} \to (k \bmod 2,\\ ,k \bmod 3)\end{matrix}$. **Les images sont :** $0 \to (0,0)$, $1 \to (1,1)$, $2 \to (0,2)$, $3 \to (1,0)$, $4 \to (0,1)$, $5 \to (1,2)$.

2. Dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, on a $y + y = 0$ pour tout y. Supposons que f soit un isomorphisme depuis $\mathbb{Z}/4\mathbb{Z}$. Alors $f(\bar{2}) = f(\bar{1}) + f(\bar{1}) = 0 = f(\bar{0})$. Or $\bar{2} \neq \bar{0}$, ce qui contredit l'injectivité. **Les deux anneaux ne sont donc pas isomorphes**, bien qu'ils aient quatre éléments.

3. Les inversibles d'un produit sont les couples d'inversibles. Or $\mathbb{Z}^\times = \{-1, 1\}$. **Donc $(\mathbb{Z} \times \mathbb{Z})^\times = \{(1,1),, -1), (-1,1), (-1,-1)\}$.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

4. On a $(a,b)^2 = (a,b)$ si et seulement si $a^2 = a$ et $b^2 = b$. Dans l'anneau intègre A, l'égalité $a(a-1) = 0$ donne $a = 0$ ou $a = 1$. Il en va de même dans B. **Les idempotents sont $(0,0)$, $(1,0)$, $(0,1)$ et $(1,1)$.**

Question 5

5. D'abord, si I et J sont des idéaux, $I \times J$ est un sous-groupe, et $(a,b)(x,y) = (ax, by) \in I \times J$ pour $(x,y) \in I \times J$. C'est donc un idéal. Réciproquement, soit K un idéal de $A \times B$. On pose $I = \left\{ \begin{matrix} a \in A, \\ ,(a,0) \in K \end{matrix} \right\}$ et $J = \left\{ \begin{matrix} b \in B, \\ ,(0,b) \in K \end{matrix} \right\}$. Ce sont des idéaux, car $(x,0)(a,0) = (xa,0)$. Ensuite, si $(a,b) \in K$, alors $(1,0)(a,b) = (a,0) \in K$ et $(0,1)(a,b) = (0,b) \in K$. Donc $K \subset I \times J$. Enfin, si $a \in I$ et $b \in J$, alors $(a,b) = (a,0) + (0,b) \in K$. **Ainsi, $K = I \times J$.**

Point de méthode : dans un produit, les idempotents $(1,0)$ et $(0,1)$ permettent d'isoler chaque composante ; c'est l'outil clé de la question 5.

Corrigé de l'exercice 10 : Éléments nilpotents de Z/nZ

1. D'abord, $0 \in N$. Soit $x, y \in N$ avec $x^m = 0$ et $y^k = 0$. L'anneau est commutatif, donc la formule du binôme s'applique :

$$(x-y)^{m+k-1} = \sum_{j=0}^{m+k-1} ([\text{chooe?}]m+k-1\,,j)\, x^j\, (-y)^{m+k-1-j}.$$

Dans chaque terme, on a $j \geq m$ ou $m+k-1-j \geq k$. Chaque terme est donc nul, et $x - y \in N$. Enfin, pour $a \in A$, $(ax)^m = a^m x^m = 0$. **Donc N est un idéal de A.**

2. Supposons $\overline{k}$ nilpotent : il existe m tel que $n \mid k^m$. Chaque p_i divise alors k^m, donc k d'après le lemme d'Euclide. Les p_i étant distincts, leur produit r_n divise k. Réciproquement, si $r_n \mid k$, posons $m = \max \alpha_i$. Alors k^m est divisible par $p_1^m \cdots p_r^m$, donc par n.

Ainsi, $\overline{k}$ est nilpotent si et seulement si $r_n \mid k$.

3. On a $72 = 2^3 \times 3^2$, donc $r_{72} = 6$. **Les nilpotents sont $\overline{0}, \overline{6}, \overline{12}, \ldots, \overline{66}$, soit 12 éléments.** Par exemple, $6^3 = 216 = 3 \times 72$.

4. Le seul multiple de r_n dans $[\![0, n-1]\!]$ est 0 si et seulement si $r_n = n$. **Il n'y a aucun nilpotent non nul si et seulement si n est sans facteur carré**, comme 30 ou 105.

Corrigé de l'exercice 11 : Divisibilité dans l'anneau des entiers de Gauss

1. L'ensemble $\mathbb{Z}[i]$ contient 1 et il est stable par différence. De plus, $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$, avec des parties réelle et imaginaire entières. C'est donc un sous-anneau de $\mathbb{C}$. Comme sous-anneau d'un corps, il est commutatif, non nul et sans diviseur de zéro : $\mathbb{Z}[i]$ **est intègre.** Enfin, $N(a+ib) = a^2 + b^2 \in \mathbb{N}$, et $N(zw) = |zw|^2 = |z|^2 |w|^2 = N(z)N(w)$.

2. Si $zw = 1$, alors $N(z)N(w) = 1$ avec deux entiers naturels, donc $N(z) = 1$. Réciproquement, si $N(z) = 1$, alors $z\overline{z} = 1$ et $\overline{z} \in \mathbb{Z}[i]$. Ensuite, $a^2 + b^2 = 1$ impose $(a,b) \in \{(\pm 1, 0), (0, \pm 1)\}$. **Donc $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.**

3. On a $(1+i)^2 = 1 + 2i - 1 = 2i$, donc $-i(1+i)^2 = -2i^2 = 2$. Par ailleurs, $-i(1+i) = -i + 1 = 1 - i$. Comme $-i$ est inversible, $1+i$ **et** $1-i$ **sont associés.**

Questions 4 à 5

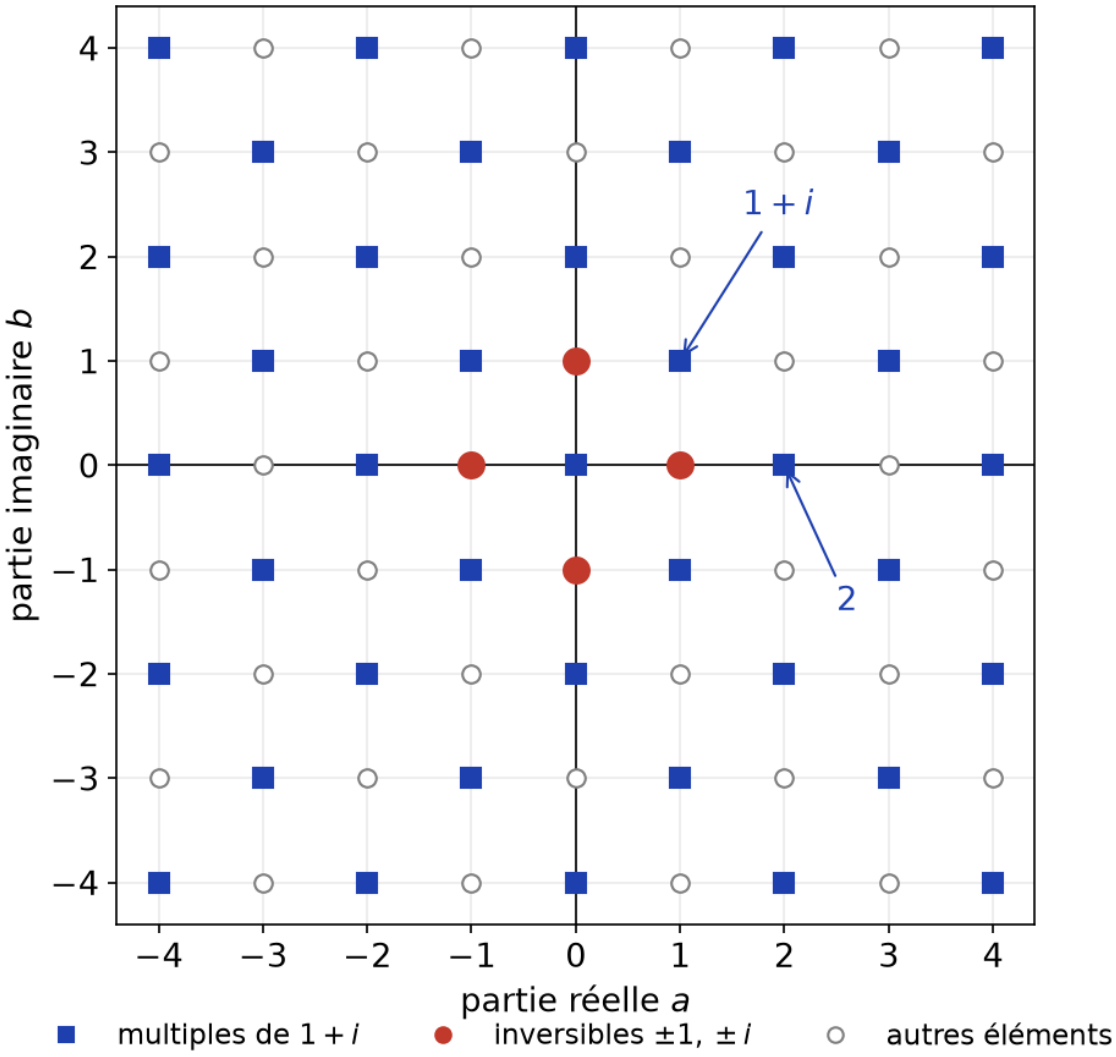
4. On calcule $\frac{5+5i}{3+i} = \frac{(5+5i)(3-i)}{10} = \frac{20+10i}{10} = 2+i$. **Donc $3+i$ divise $5+5i$, avec $5+5i = (3+i)(2+i)$.** En revanche, si $1+2i$ divisait 3, on aurait $N(1+2i) = 5$ qui diviserait $N(3) = 9$. C'est faux, donc $1+2i$ **ne divise pas 3.**

5. D'abord, $(1+i)(c+id) = (c-d) + i(c+d)$, et la somme $2c$ des parties est paire. Réciproquement, si $a+b$ est pair, alors $b-a$ l'est aussi, et

$$\frac{a+ib}{1+i} = \frac{(a+ib)(1-i)}{2} = \frac{a+b}{2} + i\,\frac{b-a}{2} \in \mathbb{Z}[i].$$

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Donc $(1+i)\mathbb{Z}[i] = \left\{ \begin{matrix} a+ib, \\ a+b \text{ pair} \end{matrix} \right\}$**.** La figure ci-dessous montre cet idéal : il forme un damier dans le réseau des entiers de Gauss.



Corrigé de l'exercice 12 : Noyaux de morphismes d'anneaux

1. On a $(P+Q)(i) = P(i)+Q(i)$, $(PQ)(i) = P(i)Q(i)$ et le polynôme constant 1 s'envoie sur 1. Donc θ est un morphisme d'anneaux. Il est surjectif, car $a+ib = \theta(a+bX)$. Enfin, l'exercice 6 a montré que $P(i) = 0$ si et seulement si X^2+1 divise P. **Donc** $\ker\theta = (X^2+1)\mathbb{R}[X]$**.**

2. L'application f est un morphisme d'anneaux, et $k \in \ker f$ si et seulement si 4 et 6 divisent

k. **Donc** $\ker f = 12\mathbb{Z}$**.** Ensuite, le couple $(\bar{1}, \bar{0})$ n'est pas atteint : il faudrait k impair et multiple de 6. **Donc** f **n'est pas surjective.** En effet, son image a 12 éléments, alors que l'anneau d'arrivée en a 24.

3. Supposons qu'un tel morphisme g existe. Alors $g(\bar{1}) = 1$, et $\bar{0} = \bar{1} + \ldots + \bar{1}$ (six termes). Ainsi, $0 = g(\bar{0}) = 6g(\bar{1}) = 6$, ce qui est absurde. **Il n'existe aucun morphisme d'anneaux de** $\mathbb{Z}/6\mathbb{Z}$ **dans** $\mathbb{Z}$**.**

4. Si $m \mid n$, l'application $k \bmod n \to k \bmod m$ est bien définie. En effet, $n \mid k - k'$ entraîne $m \mid k - k'$. C'est clairement un morphisme d'anneaux. Réciproquement, si g est un morphisme, alors $g(\bar{1}) = \bar{1}$. Par conséquent, $\bar{0} = g(n \cdot \bar{1}) = n \cdot \bar{1} = \bar{n}$ dans $\mathbb{Z}/m\mathbb{Z}$. **Donc** m **divise** n**.**

Corrigé de l'exercice 13 : Théorème de Wilson dans le corps F_p

1. On a $x^2 - 1 = (x-1)(x+1)$. Comme $\mathbb{F}_p$ est un corps, il est intègre. Donc $x^2 = \bar{1}$ équivaut à $x = \bar{1}$ ou $x = -\bar{1}$. **Les solutions sont** $\pm\bar{1}$, confondues lorsque $p = 2$.

2. Pour $p = 2$, on a $1! = 1 \equiv -1 \pmod 2$. Supposons ensuite p impair. Un élément x de $\mathbb{F}_p^\times$ est égal à son inverse si et seulement si $x^2 = \bar{1}$, c'est-à-dire $x = \pm\bar{1}$. Les $p-3$ autres éléments se regroupent donc en paires $\{x, x^{-1}\}$ de produit $\bar{1}$. Le produit de tous les éléments de $\mathbb{F}_p^\times$ vaut alors $\bar{1} \times (-\bar{1}) = -\bar{1}$. Or ce produit est la classe de $(p-1)!$. **Donc** $(p-1)! \equiv -1 \pmod p$**.**

3. Soit $n \geq 2$ non premier, et a un diviseur de n avec $1 < a < n$. Comme $a \leq n-1$, a divise $(n-1)!$. Si l'on avait $(n-1)! \equiv -1 \pmod n$, on aurait aussi cette congruence modulo a. On obtiendrait $0 \equiv -1 \pmod a$, ce qui est impossible pour $a \geq 2$. **Donc** $(n-1)! \not\equiv -1 \pmod n$**.**

4. On a $10! = 3\,628\,800 = 11 \times 329\,890 + 10$, donc $10! \equiv -1 \pmod{11}$, comme prévu. Ensuite, le théorème de Wilson donne $16! \equiv -1 \pmod{17}$. Or $16! = 16 \times 15!$ et $16 \equiv -1$. Ainsi, $-15! \equiv -1$, d'où $15! \equiv 1 \pmod{17}$**.**

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Corrigé de l'exercice 14 : PGCD de X^a - 1 et X^b - 1

1. La division euclidienne donne $X^6-1 = X^2(X^4-1)+X^2-1$. Ensuite, $X^4-1=(X^2+1)(X^2-1)$, avec un reste nul. Le dernier reste non nul est X^2-1, déjà unitaire. **Donc $(X^6-1)\wedge(X^4-1)=X^2-1$, avec $(X^6-1)-X^2(X^4-1)=X^2-1$.**

2. Les racines de X^6-1 sont les racines sixièmes de l'unité $\omega_k = e^{ik\pi/3}$, pour $0\leq k\leq 5$. Dans $\mathbb{C}[X]$, on a donc $X^6-1=\prod_{k=0}^{5}(X-\omega_k)$. Dans $\mathbb{R}[X]$, on regroupe les racines conjuguées. Les paires ω_1,ω_5 et ω_2,ω_4 donnent $X^2-2\cos(\pi/3)X+1$ et $X^2-2\cos(2\pi/3)X+1$. D'où :

$$X^6-1=(X-1)(X+1)(X^2-X+1)(X^2+X+1).$$

Les deux facteurs de degré 2 ont pour discriminant $-3<0$: ils sont irréductibles sur $\mathbb{R}$.

Questions 3 à 4

3. On écrit $X^a-1=X^r(X^{bq}-1)+(X^r-1)$. De plus, $X^{bq}-1=(X^b-1)(1+X^b+\ldots+X^{b(q-1)})$ lorsque $q\geq 1$, et $X^{bq}-1=0$ lorsque $q=0$. Dans les deux cas, il existe S tel que $X^a-1=(X^b-1)S+(X^r-1)$. Par conséquent, les diviseurs communs à X^a-1 et X^b-1 sont exactement ceux de X^b-1 et X^r-1. **Les deux PGCD sont donc égaux.**

4. Appliquons l'algorithme d'Euclide aux entiers a et b. La question 3 montre que le PGCD des polynômes ne change pas quand on remplace (a,b) par (b,r). Au bout du processus, le couple devient $(a\wedge b,0)$. On obtient alors $(X^{a\wedge b}-1)\wedge 0 = X^{a\wedge b}-1$. D'après le cours sur les idéaux de $\mathbb{K}[X]$, $(X^a-1)\mathbb{K}[X]+(X^b-1)\mathbb{K}[X]=(X^{a\wedge b}-1)\mathbb{K}[X]$. On retrouve la question 1, puisque $6\wedge 4=2$.

Corrigé de l'exercice 15 : Sous-algèbres de matrices

1. D'abord, $I_n \in \mathcal{T}_n$, et une combinaison linéaire de matrices triangulaires supérieures l'est encore. Soit ensuite $A, B \in \mathcal{T}_n$ et $i > j$. On a $(AB)_{ij} = \sum_k a_{ik} b_{kj}$. Si $k < i$, alors $a_{ik} = 0$. Sinon, $k \geq i > j$, donc $b_{kj} = 0$. Ainsi, $(AB)_{ij} = 0$. **Donc $\mathcal{T}_n$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{K})$.**

2. La matrice I_n commute avec A. De plus, si $M, N \in \mathcal{C}(A)$ et $\lambda \in \mathbb{K}$, alors $A(\lambda M + N) = \lambda AM + AN = (\lambda M + N)A$. Enfin, $A(MN) = (AM)N = (MA)N = M(AN) = M(NA) = (MN)A$. **Donc $\mathcal{C}(A)$ est une sous-algèbre.**

3. Soit $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$. On calcule $AM = \begin{pmatrix} x & y \\ 2z & 2t \end{pmatrix}$ et $MA = \begin{pmatrix} x & 2y \\ z & 2t \end{pmatrix}$. L'égalité impose $y = 2y$ et $2z = z$, donc $y = z = 0$. **Ainsi, $\mathcal{C}(A)$ est l'ensemble des matrices diagonales, de dimension 2.**

4. La trace de I_n vaut $n \neq 0$. **L'ensemble des matrices de trace nulle n'est donc pas une sous-algèbre.** Il n'est pas non plus stable par produit : $E_{12}E_{21} = E_{11}$ est de trace 1.

Corrigé de l'exercice 16 : Polynômes annulateurs et puissances d'une matrice

1. L'application $P \to P(M)$ est un morphisme d'algèbres de $\mathbb{R}[X]$ dans $\mathcal{M}_2(\mathbb{R})$. Son noyau est I. **Donc I est un idéal de $\mathbb{R}[X]$.**

2. Posons $N = M - I_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Un calcul direct donne $N^2 = 0$, donc $(X-1)^2 \in I$. L'idéal I est non nul, donc $I = P\,\mathbb{R}[X]$ avec P unitaire. Comme P divise $(X-1)^2$, on a $P \in \{1, X-1, (X-1)^2\}$. Or $P = 1$ est exclu, car $I_2 \neq 0$. De même, $P = X - 1$ est exclu, car $M \neq I_2$. **Donc $I = (X-1)^2\,\mathbb{R}[X]$.**

3. On écrit $X^n = (X-1)^2 Q + aX + b$. En évaluant en 1, on obtient $1 = a + b$. En dérivant puis en évaluant en 1, on obtient $n = a$, car 1 est racine double de $(X-1)^2 Q$. Le reste est donc $nX + 1 - n$. Comme $(X-1)^2$ annule M, il vient :

Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

$$M^n = nM + (1-n)I_2 = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Donc $M^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ **pour tout** $n \in \mathbb{N}$.

Question 4

4. L'ensemble $\mathbb{R}[M]$ est l'image d'un morphisme d'algèbres, donc une sous-algèbre. Pour tout P, on écrit $P = (X-1)^2 Q + aX + b$, d'où $P(M) = aM + bI_2$. Ainsi, $\mathbb{R}[M] = \mathrm{Vect}(I_2, M)$. Enfin, M n'est pas colinéaire à I_2. **Donc** $\dim \mathbb{R}[M] = 2$.

Point de méthode : pour calculer M^n, divisez X^n par un polynôme annulateur ; une racine multiple se traite en dérivant.

Corrigé de l'exercice 17 : Petit théorème de Fermat et nombre pseudo-premier

1. On teste les petits premiers : 341 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7. En revanche, $341 = 11 \times 31$.

2. Le nombre 11 est premier et ne divise pas 2. Le petit théorème de Fermat donne donc $2^{10} \equiv 1 \pmod{11}$. On le vérifie : $1024 = 93 \times 11 + 1$. Par ailleurs, $2^5 = 32 = 31 + 1$. **Donc** $2^5 \equiv 1 \pmod{31}$.

3. On a $340 = 34 \times 10 = 68 \times 5$. Ainsi, $2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$ et $2^{340} = (2^5)^{68} \equiv 1 \pmod{31}$. Comme 11 et 31 sont premiers entre eux, leur produit divise $2^{340} - 1$. **Donc** $2^{340} \equiv 1 \pmod{341}$. Pourtant, 341 n'est pas premier. **Le test proposé est donc faux** : la réciproque du petit théorème de Fermat est fausse.

4. On a $3^5 = 243 = 7 \times 31 + 26$, donc $3^5 \equiv -5$. Ainsi, $3^{10} \equiv 25 \pmod{31}$. Par ailleurs, $3^{30} \equiv 1 \pmod{31}$ par Fermat. Comme $340 = 11 \times 30 + 10$, on obtient $3^{340} \equiv 3^{10} \equiv 25 \pmod{31}$. Par conséquent, $3^{340} \not\equiv 1 \pmod{31}$, donc

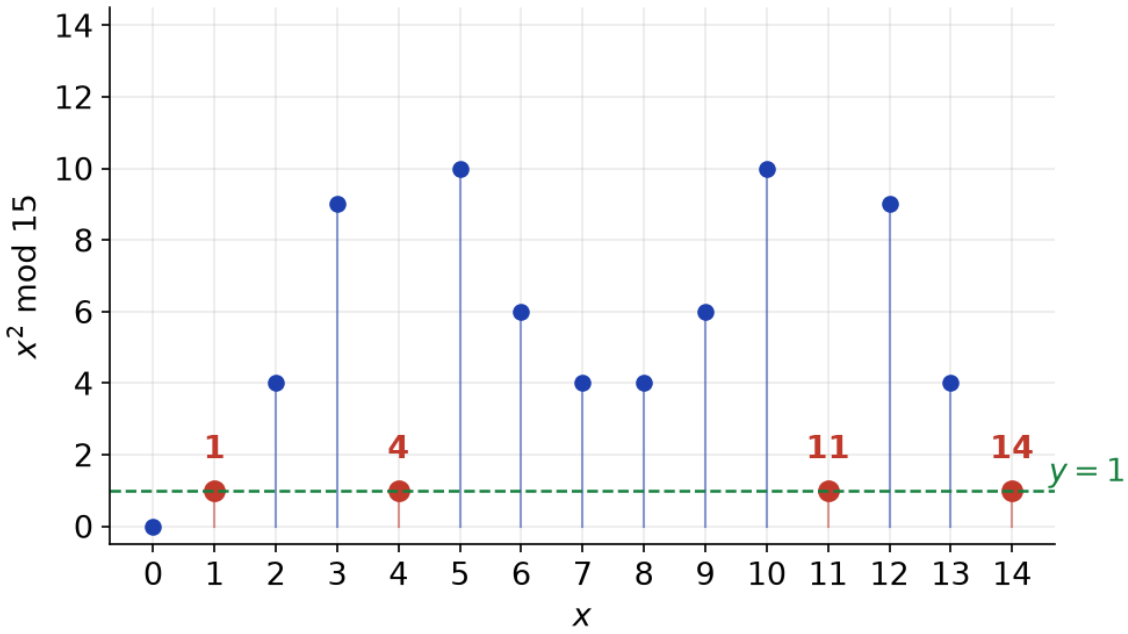
$3^{340} \not\equiv 1 \pmod{341}$. La base 3 prouve que 341 n'est pas premier.

Corrigé de l'exercice 18 : Racines carrées de 1 modulo n

1. Dans le corps $\mathbb{F}_p$, l'égalité $(x-1)(x+1)=0$ donne $x = \pm 1$. Comme p est impair, $1 \not\equiv -1 \pmod{p}$. **Il y a exactement deux solutions, $x \equiv 1$ et $x \equiv -1$.**

2. Un entier pair a un carré pair, donc il ne convient pas. Pour les impairs : $1^2 = 1$, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$ et $7^2 = 49 \equiv 1$. **Les solutions sont 1, 3, 5 et 7 modulo 8.** Le résultat de la question 1 est donc faux modulo 8. En effet, $\mathbb{Z}/8\mathbb{Z}$ n'est pas intègre.

3. Par le théorème chinois, $x^2 \equiv 1 \pmod{15}$ équivaut à $x^2 \equiv 1$ modulo 3 et modulo 5. Cela donne $x \equiv \pm 1 \pmod{3}$ et $x \equiv \pm 1 \pmod{5}$, soit quatre systèmes. Leurs solutions respectives sont 1, 14, 4 et 11. **Les solutions modulo 15 sont 1, 4, 11 et 14.** Par exemple, $4^2 = 16 \equiv 1$ et $11^2 = 121 = 8 \times 15 + 1$. La figure ci-dessous représente $x^2 \bmod 15$ et met ces quatre valeurs en évidence.



Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Questions 4 à 5

4. Comme $105 = 3 \times 5 \times 7$, il faut $x \equiv \pm 1$ modulo 3, 5 et 7. Il y a $2^3 = 8$ choix de signes, donc **8 solutions**. Par exemple, $x \equiv 1 \pmod{15}$ et $x \equiv -1 \pmod{7}$ donnent $x = 1 + 15k$ avec $1 + k \equiv 6 \pmod{7}$, soit $k = 5$ et $x = 76$. De même, on trouve 64 pour les signes $(+, -, +)$ et 71 pour $(-, +, +)$. Les opposés modulo 105 complètent la liste. **Les solutions sont 1, 29, 34, 41, 64, 71, 76 et 104.** Vérification : $76^2 = 5776 = 55 \times 105 + 1$.

5. Par le théorème chinois, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z}$. L'équation se résout composante par composante. Chaque composante admet exactement deux solutions distinctes, d'après la question 1. **Il y a donc exactement 2^r solutions modulo n.**

Corrigé de l'exercice 19 : L'équation φ(n) = 4

1. On écrit $n = p^\alpha m$ avec $\alpha \geq 1$ et $p \wedge m = 1$. Par multiplicativité, $\varphi(n) = p^{\alpha-1}(p-1)\varphi(m)$. **Donc $p-1$ divise $\varphi(n)$.**

2. Si n est premier, les entiers $1, \ldots, n-1$ sont premiers avec n, et n ne l'est pas. Donc $\varphi(n) = n - 1$. Réciproquement, supposons $\varphi(n) = n - 1$. Comme $n \wedge n = n \neq 1$, tous les entiers de $[\![1, n-1]\!]$ sont premiers avec n. Aucun d'eux, sauf 1, ne divise donc n. **Ainsi, n est premier.**

3. Soit n tel que $\varphi(n) = 4$; on a $n \geq 2$, car $\varphi(1) = 1$. Tout premier p divisant n vérifie $p - 1 \mid 4$, donc $p \in \{2, 3, 5\}$. De plus, $p^\alpha - 1$ divise 4, ce qui impose un exposant 1 pour 3 et 5, et au plus 3 pour 2. On écrit $n = 2^a 3^b 5^c$, avec $\varphi(2^a) \in \{1, 1, 2, 4\}$ pour $a = 0, 1, 2, 3$.

   - Si $c = 1$: il faut $\varphi(2^a)\, 2^b = 1$, donc $b = 0$ et $a \leq 1$. On obtient 5 et 10.
   - Si $c = 0$ et $b = 1$: il faut $\varphi(2^a) = 2$, donc $a = 2$. On obtient 12.
   - Si $c = b = 0$: il faut $\varphi(2^a) = 4$, donc $a = 3$. On obtient 8.

   Ainsi, **les solutions de $\varphi(n) = 4$ sont $n \in \{5, 8, 10, 12\}$.**

4. Supposons $\varphi(n) = 14$. Tout premier p divisant n vérifie $p - 1 \in \{1, 2, 7, 14\}$, donc $p \in \{2, 3, 8, 15\}$. Seuls 2 et 3 sont premiers. Ainsi, $n = 2^a 3^b$, et $\varphi(n) = \varphi(2^a)\varphi(3^b)$ n'a que 2 et 3 comme facteurs premiers. Or 7 divise 14. **L'équation $\varphi(n) = 14$ n'a donc aucune solution.**

Corrigé de l'exercice 20 : Formule de Gauss pour l'indicatrice d'Euler

1. Les fractions réduites sont $1/12$, $1/6$, $1/4$, $1/3$, $5/12$, $1/2$, $7/12$, $2/3$, $3/4$, $5/6$, $11/12$ et $1/1$. On compte 1 fraction de dénominateur 1, 1 de dénominateur 2, 2 de dénominateur 3, 2 de dénominateur 4, 2 de dénominateur 6 et 4 de dénominateur 12. **Ce sont bien $\varphi(1), \varphi(2), \varphi(3), \varphi(4), \varphi(6)$ et $\varphi(12)$.**

2. Supposons que k/n s'écrive a/d sous forme irréductible. Alors $kd = an$, donc $k = a\,n/d$, et $1 \leq k \leq n$ équivaut à $1 \leq a \leq d$. Réciproquement, si $1 \leq a \leq d$ et $a \wedge d = 1$, l'entier $k = a\,n/d$ vérifie $k/n = a/d$, fraction irréductible. L'application $a \to a\,n/d$ est donc une bijection entre $\left\{\begin{matrix} a \in [\![d]\!], \\ ,a\ [\backslash \text{wededge?}]\ d = 1 \end{matrix}\right\}$ et l'ensemble étudié. **Celui-ci a donc $\varphi(d)$ éléments.**

3. Chaque $k \in [\![1, n]\!]$ a un unique dénominateur réduit, qui divise n. Les ensembles de la question 2 forment ainsi une partition de $[\![1, n]\!]$. En comptant les éléments, **on obtient $\sum_{d \mid n} \varphi(d) = n$.**

4. Les diviseurs de p^k sont les p^j, $0 \leq j \leq k$. La formule donne $\sum_{j=0}^{k} \varphi(p^j) = p^k$ et $\sum_{j=0}^{k-1} \varphi(p^j) = p^{k-1}$. Par différence, $\varphi(p^k) = p^k - p^{k-1}$.

Corrigé de l'exercice 21 : Un idéal non principal de Z[X]

1. L'évaluation $P \to P(0)$ est un morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{Z}$. La surjection

canonique de $\mathbb{Z}$ sur $\mathbb{Z}/2\mathbb{Z}$ en est un aussi. Leur composée $\pi : P \to \overline{P(0)}$ est donc un morphisme d'anneaux. Son noyau est formé des P tels que $P(0)$ soit pair. **Ainsi,** $I = \ker \pi$ **est un idéal de** $\mathbb{Z}[X]$**.**

2. D'abord, un polynôme $2A + XB$ a pour coefficient constant $2A(0)$, qui est pair. Donc $2\mathbb{Z}[X] + X\mathbb{Z}[X] \subset I$. Réciproquement, soit $P \in I$, avec $P(0) = 2c$. Le polynôme $P - P(0)$ s'annule en 0, donc s'écrit XQ avec $Q \in \mathbb{Z}[X]$. Ainsi, $P = 2c + XQ$. **Donc** $I = 2\mathbb{Z}[X] + X\mathbb{Z}[X]$**.**

3. Supposons $I = D\,\mathbb{Z}[X]$. Comme $2 \in I$, il existe Q tel que $2 = DQ$. Les degrés imposent $\deg D = 0$, donc D est un entier qui divise 2. Si $D = \pm 1$, alors $I = \mathbb{Z}[X]$, ce qui est faux puisque $1 \notin I$. Si $D = \pm 2$, alors $X \in I$ s'écrirait $2Q$. Son coefficient dominant 1 serait pair, ce qui est absurde. **Donc** I **n'est pas principal.**

4. Dans $\mathbb{K}[X]$, on divise par un polynôme de I de degré minimal. Cette division exige que son coefficient dominant soit inversible. Or ici, les éléments de I de degré minimal sont les constantes paires non nulles. Par exemple, on ne peut pas écrire $X = 2Q + R$ avec R constant dans $\mathbb{Z}[X]$. **La division euclidienne par 2 est impossible dans** $\mathbb{Z}[X]$**, et la démonstration échoue.**

Corrigé de l'exercice 22 : Problème, le chiffrement RSA

1. Les premiers p et q sont distincts, donc premiers entre eux. Par multiplicativité, $\varphi(n) = (p-1)(q-1)$**.** Ensuite, $e \wedge \varphi(n) = 1$, donc $\overline{e}$ est inversible dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Un représentant $d \in [\![1, \varphi(n)]\!]$ de son inverse convient.

2. On a $n = 143$ et $\varphi(n) = 10 \times 12 = 120$. De plus, $7 \wedge 120 = 1$. La division $120 = 17 \times 7 + 1$ donne $7 \times (-17) \equiv 1 \,(\mathrm{mod}\, 120)$. Or $-17 \equiv 103$. **Donc** $d = 103$**.** Vérification : $7 \times 103 = 721 = 6 \times 120 + 1$.

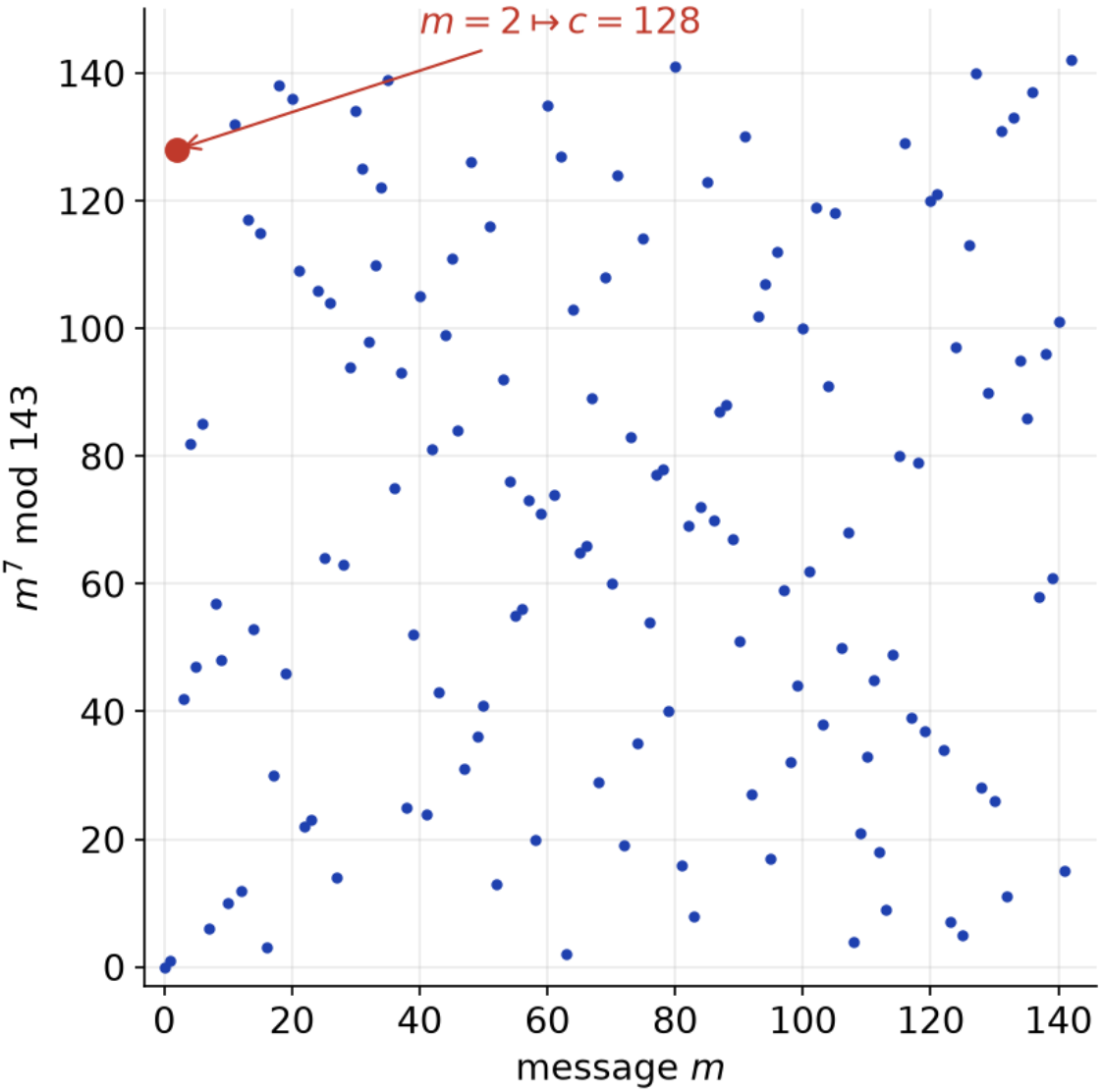
3. On a $2^7 = 128 < 143$. **Le message chiffré est** $c = 128$**.**

4. Comme $ed \equiv 1 \,(\mathrm{mod}\, \varphi(n))$ et $ed \geq 1$, on écrit $ed = 1 + k\varphi(n)$ avec $k \in \mathbb{N}$. Si $m \wedge n = 1$, le théorème d'Euler donne $m^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\,)n$. Par conséquent, $m^{ed} = m \times (m^{\varphi(n)})^k \equiv m \,(\mathrm{mod}\,)n$. **Donc** $m^{ed} \equiv m \,(\mathrm{mod}\,)n$**.**

Questions 5 à 6

5. Si p divise m, les deux membres sont multiples de p, car $ed \geq 1$. Sinon, le petit théorème de Fermat donne $m^{p-1} \equiv 1 \pmod{p}$. Comme $ed = 1 + k(p-1)(q-1)$, il vient $m^{ed} = m \times (m^{p-1})^{k(q-1)} \equiv m \pmod{p}$. Le même raisonnement vaut modulo q. Enfin, p et q sont premiers entre eux, donc pq divise $m^{ed} - m$. **Ainsi,** $m^{ed} \equiv m \pmod{n}$ **pour tout** $m \in \mathbb{Z}$ **.**

6. Posons $F(x) = x^e$ et $G(x) = x^d$ sur $\mathbb{Z}/n\mathbb{Z}$. D'après la question 5, $G(F(x)) = x^{ed} = x$ et $F(G(x)) = x^{de} = x$. **Donc** F **est une bijection de réciproque** $G : x \to x^d$**.** La figure ci-dessous représente $m \to m^7 \bmod 143$: chaque valeur est atteinte une seule fois.



Téléchargé depuis https://mathovore.fr - Mathovore site de maths.

Question 7

7. Modulo 11, on a $128 \equiv 7$ et $7^{10} \equiv 1$. Comme $103 = 10 \times 10 + 3$, il vient $128^{103} \equiv 7^3 = 343 = 31 \times 11 + 2 \equiv 2$. Modulo 13, on a $128 = 9 \times 13 + 11 \equiv -2$ et $(-2)^{12} \equiv 1$. Comme $103 = 8 \times 12 + 7$, il vient $128^{103} \equiv (-2)^7 = -128 \equiv -11 \equiv 2$. Par le théorème chinois, $128^{103} \equiv 2 \pmod{143}$ **: on retrouve le message** $m = 2$ **.**

Point de méthode : pour une grande puissance modulo pq, calculez séparément modulo p et modulo q, puis recollez par le théorème chinois.

Revenir aux énoncés des exercices

Pour aller plus loin en maths spé

- Le cours : anneaux, idéaux et Z/nZ, cours de maths spé
- Les énoncés : exercices de maths spé sur anneaux, idéaux et Z/nZ
- À maîtriser avant : Compléments sur les groupes : groupes monogènes et ordre
- Chapitre précédent : Compléments sur les groupes : groupes monogènes et ordre
- Chapitre suivant : Éléments propres et polynôme caractéristique
- Tester vos connaissances : QCM de maths spé par chapitre
- Le sommaire : tous les chapitres de maths spé et les chapitres de maths sup