

Arithmétique et $\mathbb{Z}/n\mathbb{Z}$

Corrigé de l'exercice 1 : Relations d'équivalence et classes

1. D'abord, $a^2 - a^2 = 0$ est divisible par 5 : la relation est réflexive. Ensuite, si $5 \mid a^2 - b^2$, alors 5 divise son opposé $b^2 - a^2$: elle est symétrique. Enfin, si $5 \mid a^2 - b^2$ et $5 \mid b^2 - c^2$, alors 5 divise la somme $a^2 - c^2$: elle est transitive. **Donc $\mathcal{R}$ est une relation d'équivalence.**

2. On factorise : $a^2 - b^2 = (a - b)(a + b)$. Comme 5 est premier, le lemme d'Euclide donne : $5 \mid (a - b)(a + b)$ si et seulement si $5 \mid a - b$ ou $5 \mid a + b$. Autrement dit, $a \mathcal{R} b \Leftrightarrow a \equiv \pm b \pmod{5}$. Les classes se lisent alors sur les restes modulo 5, et la figure de l'énoncé le confirme :

- la classe de 0 est $5\mathbb{Z}$;
- la classe de 1 réunit les entiers congrus à 1 ou à 4 modulo 5 ;
- la classe de 2 réunit les entiers congrus à 2 ou à 3 modulo 5.

L'ensemble quotient $\mathbb{Z}/\mathcal{R}$ a donc 3 éléments, qui correspondent aux trois valeurs 0, 1, 4 de a^2 modulo 5.

3. Pour $\mathcal{S}$: on a $a \mid a$ (même pour $a = 0$, car $0 = 0 \times 1$), donc $\mathcal{S}$ est réflexive. De plus, si $a \mid b$ et $b \mid c$, alors $a \mid c$: elle est transitive. En revanche, $1 \mid 2$ mais $2 \nmid 1$: elle n'est pas symétrique. Pour $\mathcal{T}$: elle est réflexive ($|a - a| = 0$) et symétrique ($|a - b| = |b - a|$). Cependant, $0 \mathcal{T} 1$ et $1 \mathcal{T} 2$, alors que $|0 - 2| = 2 > 1$. **Aucune des deux n'est une relation d'équivalence : $\mathcal{S}$ n'est pas symétrique, $\mathcal{T}$ n'est pas transitive.**

4. Existence : soit $x \in \mathbb{R}$ et $y = x - \lfloor x \rfloor$. Alors $y \in [0, 1[$ et $x - y = \lfloor x \rfloor \in \mathbb{Z}$.
Unicité : si $y, y' \in [0, 1[$ sont dans la même classe, alors $y - y'$ est un entier. Or $|y - y'| < 1$, donc $y = y'$. **Chaque classe contient exactement un réel de $[0, 1[$, la**

partie fractionnaire de ses éléments.

Corrigé de l'exercice 2 : Congruences et critères de divisibilité

1. Écrivons $N = \sum_{i=0}^k a_i \cdot 10^i$. Comme $10 \equiv 1 \pmod{9}$, la compatibilité avec les puissances donne $10^i \equiv 1$. Par conséquent, $N \equiv \sum a_i \pmod{9}$. Pour 123456789, la somme des chiffres vaut $45 = 5 \times 9$. **Le reste de 123456789 modulo 9 est 0.**
2. De même, $10 \equiv -1 \pmod{11}$, donc $10^i \equiv (-1)^i$. Ainsi $N \equiv \sum (-1)^i a_i \pmod{11}$. En partant des unités : $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$. **Le reste de 123456789 modulo 11 est 5.**
3. La somme des chiffres de 2026 vaut 10, donc $2026 \equiv 10 \equiv 1 \pmod{9}$. Par suite, $2026^{2026} \equiv 1^{2026} = 1$. **Le reste cherché est 1.**
4. On a $7 \times 11 = 77$ et $77 \times 13 = 1001$. Ensuite, $1000 = 1001 - 1$, donc $1000 \equiv -1$ modulo 7, 11 et 13. On en déduit :
$$123456 = 123 \times 1000 + 456 \equiv -123 + 456 = 333.$$
Or $333 = 7 \times 47 + 4$ et $333 = 13 \times 25 + 8$. **Donc $123456 \equiv 4 \pmod{7}$ et $123456 \equiv 8 \pmod{13}$.**

Point de méthode : pour un critère de divisibilité par n , on cherche une puissance de 10 congrue à ± 1 modulo n .

Corrigé de l'exercice 3 : Calculs dans $\mathbb{Z}/12\mathbb{Z}$

1. D'après le cours, $\bar{k}$ est inversible si et seulement si $\text{pgcd}(k, 12) = 1$. Les inversibles sont

donc $\bar{1}, \bar{5}, \bar{7}, \bar{11}$. De plus, $5^2 = 25 = 2 \times 12 + 1$, $7^2 = 49 = 4 \times 12 + 1$ et $11^2 = 121 = 10 \times 12 + 1$. **Chaque inversible de $\mathbb{Z}/12\mathbb{Z}$ est son propre inverse.**

2. Les classes non nulles et non inversibles sont $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}, \bar{10}$. On a successivement :

$$2 \times 6 = 12, 3 \times 4 = 12, 8 \times 3 = 24, 9 \times 4 = 36, 10 \times 6 = 60.$$

Ainsi $\bar{2}\bar{6} = \bar{3}\bar{4} = \bar{8}\bar{3} = \bar{9}\bar{4} = \bar{10}\bar{6} = \bar{0}$, ce qui règle aussi le cas de $\bar{4}$ et de $\bar{6}$. **Toutes ces classes sont des diviseurs de zéro.** La table ci-dessous le montre : les lignes des inversibles (numéros en bleu) contiennent un seul $\bar{1}$ et aucun $\bar{0}$ hors de la première colonne.

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

■ produit $\bar{0}$ ■ produit $\bar{1}$

3. L'équation équivaut à $\bar{5}x = \bar{7}$. On multiplie par $\bar{5}^{-1} = \bar{5}$: $x = \overline{35} = \overline{11}$. Vérification : $5 \times 11 + 3 = 58 = 4 \times 12 + 10$. **L'unique solution est $x = \overline{11}$.**
4. On a $12 \mid 4x - 8$ si et seulement si $3 \mid x - 2$. **Les solutions de $\bar{4}x = \bar{8}$ sont $\bar{2}, \bar{5}, \bar{8}, \overline{11}$.** En revanche, $4x$ modulo 12 ne prend que les valeurs 0, 4, 8. Autrement dit, $\text{pgcd}(4, 12) = 4$ ne divise pas 6. **L'équation $\bar{4}x = \bar{6}$ n'a pas de solution.**
5. Comme $\bar{7}^2 = \bar{1}$, on obtient $\bar{7}^{100} = (\bar{7}^2)^{50} = \bar{1}$. De même, $\bar{5}^{2027} = (\bar{5}^2)^{1013} \times \bar{5} = \bar{5}$. **Donc $\bar{7}^{100} = \bar{1}$ et $\bar{5}^{2027} = \bar{5}$.**

Corrigé de l'exercice 4 : Opérations bien définies sur le quotient

1. On écrit $ab - a'b' = a(b - b') + b'(a - a')$. Les deux termes sont des multiples de n .
Donc $ab \equiv a'b' \pmod{n}$.
2. Les entiers 0 et 3 ont la même classe modulo 3. Pourtant, $2^0 = 1$ et $2^3 = 8 \equiv 2 \pmod{3}$. La formule donnerait donc deux valeurs différentes pour la même classe : **elle ne définit pas une application sur $\mathbb{Z}/3\mathbb{Z}$.** En revanche, $2 \equiv -1 \pmod{3}$, donc $2^x \equiv (-1)^x \pmod{3}$. Cette valeur ne dépend que de la parité de x . **Ainsi $\overline{2^x}^{(3)}$ ne dépend que de $\bar{x}^{(2)}$.**
3. Bonne définition : si $x \equiv x' \pmod{6}$, alors $6 \mid x - x'$, donc $3 \mid x - x'$. Notons f l'application obtenue. Ensuite, f respecte les lois, car celles-ci se calculent sur les représentants : $f(\bar{x} + \bar{y}) = \overline{x+y}^{(3)} = f(\bar{x}) + f(\bar{y})$, et de même pour le produit. De plus, $f(\bar{1}) = \bar{1}$. Elle est surjective, car $\bar{0}, \bar{1}, \bar{2}$ sont atteints. Enfin, $f(\bar{x}) = \bar{0}$ si et seulement si $3 \mid x$. **Le noyau est $\{\bar{0}, \bar{3}\}$.**
4. On a $\bar{0}^{(3)} = \bar{3}^{(3)}$, mais $\bar{0}^{(6)} \neq \bar{3}^{(6)}$. **La formule dépend du représentant : l'application n'est pas bien définie.**
5. Si $m \mid n$ et $x \equiv x' \pmod{n}$, alors $m \mid n \mid x - x'$: l'application est bien définie. Réciproquement, supposons-la bien définie. Comme $\bar{0}^{(n)} = \bar{n}^{(n)}$, on doit avoir $\bar{0}^{(m)} = \bar{n}^{(m)}$, c'est-à-dire $m \mid n$. **L'application est bien définie si et seulement si $m \mid n$.**

Point de méthode : pour tester la bonne définition, on compare les images de deux représentants d'une même classe, souvent 0 et n .

Corrigé de l'exercice 5 : Inverse d'une classe par Bézout

1. Le nombre 17 est premier et ne divise pas 60 , donc $\text{pgcd}(17, 60) = 1$ et $\overline{17}$ est inversible. Algorithme d'Euclide : $60 = 3 \times 17 + 9$, $17 = 1 \times 9 + 8$, $9 = 1 \times 8 + 1$. On remonte ensuite :

$$\begin{aligned} 1 &= 9 - 8 = 9 - (17 - 9) = 2 \times 9 - 17 \\ &= 2(60 - 3 \times 17) - 17 = 2 \times 60 - 7 \times 17. \end{aligned}$$

Donc $\overline{17}^{-1} = \overline{-7} = \overline{53}$. Vérification : $17 \times 53 = 901 = 15 \times 60 + 1$. **L'inverse de $\overline{17}$ est $\overline{53}$.**

2. On multiplie par $\overline{53}$: $x \equiv 5 \times 53 = 265 = 4 \times 60 + 25$. Vérification : $17 \times 25 = 425 = 7 \times 60 + 5$. **Les solutions sont les $x \equiv 25 \pmod{60}$.**

3. Euclide : $101 = 4 \times 23 + 9$, $23 = 2 \times 9 + 5$, $9 = 5 + 4$, $5 = 4 + 1$. En remontant :

$$\begin{aligned} 1 &= 5 - 4 = 2 \times 5 - 9 = 2 \times 23 - 5 \times 9 \\ &= 2 \times 23 - 5(101 - 4 \times 23) = 22 \times 23 - 5 \times 101. \end{aligned}$$

Ainsi $\overline{23}^{-1} = \overline{22}$, car $23 \times 22 = 506 = 5 \times 101 + 1$. Par conséquent, $x \equiv 22 \times 7 = 154 \equiv 53$. Vérification : $23 \times 53 = 1219 = 12 \times 101 + 7$. **L'inverse est $\overline{22}$ et la solution est $x \equiv 53 \pmod{101}$.**

4. On a $\text{pgcd}(21, 60) = 3 \neq 1$. De plus, $21 \times 20 = 420 = 7 \times 60$, donc $\overline{21} \overline{20} = \overline{0}$. **La classe $\overline{21}$ n'est pas inversible : c'est un diviseur de zéro.**

Corrigé de l'exercice 6 : Équations linéaires modulo n

1. Condition nécessaire : si $ax = b + kn$, alors d divise $ax - kn = b$. Condition suffisante : si $d \mid b$, écrivons $a = da_1$, $b = db_1$, $n = dn_1$, avec $\text{pgcd}(a_1, n_1) = 1$. Alors $n \mid ax - b$ équivaut à $n_1 \mid a_1 x - b_1$. Comme a_1 est inversible modulo n_1 , cela équivaut à $x \equiv x_0 \pmod{n_1}$, où $x_0 = a_1^{-1} b_1$. Enfin, les solutions modulo n sont $x_0, x_0 + n_1, \dots, x_0 + (d-1)n_1$. **Il y a des solutions si et seulement si $d \mid b$, et alors exactement d solutions modulo n .**
2. Ici $d = \text{pgcd}(6, 15) = 3$, qui divise 9. On divise par 3 : $2x \equiv 3 \pmod{5}$. L'inverse de 2 modulo 5 est 3, donc $x \equiv 9 \equiv 4 \pmod{5}$. Vérification : $6 \times 4 = 24 = 15 + 9$. **Les solutions modulo 15 sont 4, 9 et 14.**
3. Cette fois, 3 ne divise pas 10. **L'équation $6x \equiv 10 \pmod{15}$ n'a aucune solution.**
4. On a $\text{pgcd}(14, 35) = 7$, qui divise 21. On divise par 7 : $2x \equiv 3 \pmod{5}$, donc $x \equiv 4 \pmod{5}$. Vérification : $14 \times 4 = 56 = 35 + 21$. **Les sept solutions modulo 35 sont 4, 9, 14, 19, 24, 29, 34.**

Corrigé de l'exercice 7 : $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier

1. Si n n'est pas premier, on écrit $n = rs$ avec $1 < r, s < n$. Alors $\bar{r} \neq \bar{0}$, $\bar{s} \neq \bar{0}$, et pourtant $\bar{r}\bar{s} = \bar{n} = \bar{0}$. **L'anneau n'est pas intègre, donc ce n'est pas un corps**, car un corps est intègre.
2. Soit $\bar{a} \neq \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Alors $p \nmid a$ et, p étant premier, $\text{pgcd}(a, p) = 1$. Le théorème de Bézout donne $au + pv = 1$, donc $\bar{a}\bar{u} = \bar{1}$. **Toute classe non nulle est inversible : $\mathbb{Z}/p\mathbb{Z}$ est un corps.**
3. On a $x^2 - \bar{1} = (x - \bar{1})(x + \bar{1})$. Dans un corps, un produit nul a un facteur nul. **Donc $x^2 = \bar{1}$ équivaut à $x = \bar{1}$ ou $x = -\bar{1}$.**
4. Pour $p = 2$, $1! = 1 \equiv -1 \pmod{2}$. Supposons ensuite p impair. Dans le groupe $\mathbb{F}_p^\times$,

l'égalité $x = x^{-1}$ équivaut à $x^2 = 1$, donc à $x = \pm 1$. Les autres éléments se regroupent en paires $\{x, x^{-1}\}$ de produit 1. Par conséquent, le produit de tous les éléments de $\mathbb{F}_p^\times$ vaut $1 \times (-1) = -1$. **Ainsi** $(p-1)! \equiv -1 \pmod{p}$.

5. Le théorème de Wilson avec $p = 11$ donne $10! \equiv -1 \equiv 10 \pmod{11}$. De plus, $10! = 10 \times 9!$ et $10 \equiv -1$. Donc $-9! \equiv -1$, soit $9! \equiv 1$. On peut vérifier : $9! = 362880 = 32989 \times 11 + 1$. **Donc** $10! \equiv 10$ **et** $9! \equiv 1 \pmod{11}$.
6. Soit n non premier, et r un diviseur de n avec $1 < r < n$. Comme $r \leq n-1$, r divise $(n-1)!$. Supposons par l'absurde $n \mid (n-1)! + 1$. Alors r divise $(n-1)! + 1$, donc r divise la différence, qui vaut 1. C'est absurde. **Par conséquent**, $(n-1)! \not\equiv -1 \pmod{n}$: **le théorème de Wilson caractérise les nombres premiers.**

Corrigé de l'exercice 8 : Calculs d'indicatrice d'Euler

1. D'abord, 97 est premier, donc $\varphi(97) = 96$. Ensuite, $\varphi(2^{10}) = 2^{10} - 2^9 = 512$. De plus, $100 = 2^2 \times 5^2$, d'où $\varphi(100) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40$. Enfin, $360 = 2^3 \times 3^2 \times 5$, d'où $\varphi(360) = 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96$. **On trouve** 96, 512, 40 **et** 96.
2. Soit $n \geq 3$. Si n a un facteur premier impair p , avec p^k la plus grande puissance de p divisant n , alors $\varphi(n) = \varphi(p^k) \varphi(n/p^k)$ par multiplicativité. Or $\varphi(p^k) = p^{k-1}(p-1)$ est pair. Sinon, $n = 2^k$ avec $k \geq 2$, et $\varphi(n) = 2^{k-1}$ est pair. **Dans tous les cas, $\varphi(n)$ est pair.**
3. Soit n tel que $\varphi(n) = 4$, et p^k une puissance exacte d'un premier p dans n . Par multiplicativité, $p^{k-1}(p-1)$ divise 4. Ainsi $p-1 \mid 4$, donc $p \in \{2, 3, 5\}$. De plus, 3^{k-1} et 5^{k-1} divisent 4, ce qui impose $k \leq 1$ pour 3 et 5. Pour 2, $2^{k-1} \mid 4$ impose $k \leq 3$. On écrit donc $n = 2^a 3^b 5^c$ avec $a \leq 3$ et $b, c \leq 1$. Les valeurs de $\varphi(2^a)$ sont 1, 1, 2, 4 pour $a = 0, 1, 2, 3$; de plus $\varphi(3) = 2$ et $\varphi(5) = 4$. On examine les cas :
 - si $c = 1$, il faut $b = 0$ et $\varphi(2^a) = 1$, donc $n \in \{5, 10\}$;
 - si $c = 0$ et $b = 1$, il faut $\varphi(2^a) = 2$, donc $n = 12$;
 - si $b = c = 0$, il faut $\varphi(2^a) = 4$, donc $n = 8$.

Les entiers cherchés sont 5, 8, 10 et 12.

Corrigé de l'exercice 9 : Somme des indicatrices des diviseurs

1. Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. Leurs indicatrices valent 1, 1, 2, 2, 2, 4. **La somme vaut 12.**

2. Les diviseurs de p^k sont les p^j , $0 \leq j \leq k$. La somme est télescopique :

$$\sum_{j=0}^k \varphi(p^j) = 1 + \sum_{j=1}^k (p^j - p^{j-1}) = 1 + p^k - 1 = p^k.$$

La formule est vraie pour $n = p^k$.

3. Soit $k \in A_d$. Comme n/d divise k , on écrit $k = (n/d)j$ avec $j = kd/n \in \mathbb{N}$. De plus, $1 \leq k \leq n$ donne $1 \leq j \leq d$. Ensuite,

$\text{pgcd}(k, n) = \text{pgcd}\left(\frac{n}{d}j, \frac{n}{d}d\right) = \frac{n}{d}\text{pgcd}(j, d)$. Cette quantité vaut n/d , donc $\text{pgcd}(j, d) = 1$. Réciproquement, si $1 \leq j \leq d$ et $\text{pgcd}(j, d) = 1$, le même calcul montre que $k = jn/d$ appartient à A_d . Les deux applications $k \rightarrow kd/n$ et $j \rightarrow jn/d$ sont réciproques. **C'est une bijection, et $\text{card } A_d = \varphi(d)$.**

4. Pour tout $k \in \{1, \dots, n\}$, $\text{pgcd}(k, n)$ est un diviseur de n . Il s'écrit donc n/d pour un unique diviseur d . Ainsi les A_d forment une partition de $\{1, \dots, n\}$. En comptant les éléments, $n = \sum_{d|n} \text{card } A_d$. **Donc $\sum_{d|n} \varphi(d) = n$.**

Corrigé de l'exercice 10 : Exponentiation rapide

1. On a $45 = 32 + 8 + 4 + 1$, soit $45 = (101101)_2$ en base 2. Calculons les carrés successifs modulo 23 :

$$3^1 = 3, 3^2 = 9, 3^4 = 81 \equiv 12, 3^8 \equiv 144 \equiv 6, 3^{16} \equiv 36 \equiv 13, 3^{32} \equiv 169 \equiv 8.$$

Ensuite, $3^{45} = 3^{32} \times 3^8 \times 3^4 \times 3$. Or $8 \times 6 = 48 \equiv 2$, puis $2 \times 12 = 24 \equiv 1$, puis $1 \times 3 = 3$. Vérification par Fermat : $3^{22} \equiv 1$ et $45 = 2 \times 22 + 1$, donc $3^{45} \equiv 3$.
Ainsi $3^{45} \equiv 3 \pmod{23}$.

- Comme 7 est premier, $3^6 \equiv 1 \pmod{7}$. Or $100 = 16 \times 6 + 4$, donc $3^{100} \equiv 3^4 = 81 = 11 \times 7 + 4$. De même, $2^{12} \equiv 1 \pmod{13}$ et $1000 = 83 \times 12 + 4$. Donc $2^{1000} \equiv 2^4 = 16 \equiv 3$. **On trouve** $3^{100} \equiv 4 \pmod{7}$ et $2^{1000} \equiv 3 \pmod{13}$.
- On calcule modulo 100 : $7^2 = 49$ et $7^4 = 2401 \equiv 1$. Or $2026 = 4 \times 506 + 2$. Donc $7^{2026} \equiv 7^2 = 49$. **Les deux derniers chiffres de 7^{2026} sont 49.**
- Le nombre 19 est premier et ne divise pas 5, donc $5^{18} \equiv 1$. Comme $117 = 6 \times 18 + 9$, on a $5^{117} \equiv 5^9$. Ensuite, $5^2 = 25 \equiv 6$, $5^4 \equiv 36 \equiv 17$, $5^8 \equiv 17^2 = 289 = 15 \times 19 + 4 \equiv 4$. Enfin, $5^9 \equiv 4 \times 5 = 20 \equiv 1$. **Donc** $5^{117} \equiv 1 \pmod{19}$.

Point de méthode : réduisez toujours l'exposant avant de lancer les carrés successifs, et réduisez chaque produit intermédiaire.

Corrigé de l'exercice 11 : Petit théorème de Fermat et divisibilité

- On a $42 = 2 \times 3 \times 7$. D'abord, Fermat donne $n^7 \equiv n \pmod{7}$. Ensuite, modulo 3, $n^3 \equiv n$, donc $n^7 = n^3 \times n^3 \times n \equiv n^3 \equiv n$. Enfin, modulo 2, $n^2 \equiv n$, donc $n^7 \equiv n$. Ainsi 2, 3 et 7 divisent $n^7 - n$. Ces nombres sont deux à deux premiers entre eux, donc leur produit divise aussi $n^7 - n$. **Pour tout n , $42 \mid n^7 - n$.**
- On a $2026 = 184 \times 11 + 2$, donc $2026^{2026} \equiv 2^{2026} \pmod{11}$. Par Fermat, $2^{10} \equiv 1$, et $2026 = 202 \times 10 + 6$. Donc $2^{2026} \equiv 2^6 = 64 = 5 \times 11 + 9$. **Le reste est 9.**
- On a $2^{10} = 1024 = 3 \times 341 + 1$, donc $2^{10} \equiv 1 \pmod{341}$. Par conséquent, $2^{340} = (2^{10})^{34} \equiv 1$. Pourtant, $341 = 11 \times 31$ n'est pas premier. **La réciproque du petit théorème de Fermat est donc fausse :** on dit que 341 est pseudo-premier en base 2.

4. D'après la seconde forme du petit théorème de Fermat, $x^p \equiv x \pmod{p}$ pour tout entier x .
 En l'appliquant à $a+b$, à a et à b : $(a+b)^p \equiv a+b \equiv a^p + b^p$. **Donc**
 $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Corrigé de l'exercice 12 : Théorème d'Euler et derniers chiffres

- On a $1000 = 2^3 \times 5^3$, donc $\varphi(1000) = 1000 \times \frac{1}{2} \times \frac{4}{5} = 400$. Comme $\text{pgcd}(3, 1000) = 1$, le théorème d'Euler donne $3^{400} \equiv 1 \pmod{1000}$. Or $2026 = 5 \times 400 + 26$, donc $3^{2026} \equiv 3^{26}$. Ensuite, $3^{10} = 59049 \equiv 49$ et $3^{20} \equiv 49^2 = 2401 \equiv 401$. Enfin, $3^6 = 729$, d'où $3^{26} \equiv 401 \times 729 = 292329 \equiv 329$. **Les trois derniers chiffres de 3^{2026} sont 329.**
- On a $\varphi(10) = 4$ et $7^4 = 2401 \equiv 1 \pmod{10}$. Il suffit donc de connaître 7^7 modulo 4. Or $7 \equiv -1 \pmod{4}$, donc $7^7 \equiv -1 \equiv 3$. Écrivons $7^7 = 4q + 3$. Alors $7^{7^7} = (7^4)^q \times 7^3 \equiv 343 \equiv 3 \pmod{10}$. **Le chiffre des unités est 3.**
- Soit a premier avec 10. D'une part, a est impair, donc $a^2 \equiv 1 \pmod{4}$ et $a^{20} \equiv 1 \pmod{4}$. D'autre part, a est premier avec 25 et $\varphi(25) = 20$, donc $a^{20} \equiv 1 \pmod{25}$. Comme 4 et 25 sont premiers entre eux, le théorème chinois donne $a^{20} \equiv 1 \pmod{100}$. **L'exposant $20 = \text{ppcm}(\varphi(4), \varphi(25))$ suffit, alors que $\varphi(100) = \varphi(4)\varphi(25) = 40$ est un multiple strict.**

Corrigé de l'exercice 13 : Système de congruences à modules premiers entre eux

- Les modules 3, 5, 7 sont deux à deux premiers entre eux et $N = 105$. On construit trois entiers e_1, e_2, e_3 , chacun congru à 1 modulo un module et à 0 modulo les deux autres :
 - $35 \equiv 2 \pmod{3}$ et $2 \times 2 = 4 \equiv 1$, d'où $e_1 = 35 \times 2 = 70$;
 - $21 \equiv 1 \pmod{5}$, d'où $e_2 = 21$;

◦ $15 \equiv 1 \pmod{7}$, d'où $e_3 = 15$.

Ensuite, $x_0 = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233 \equiv 23 \pmod{105}$. Vérification :
 $23 = 7 \times 3 + 2 = 4 \times 5 + 3 = 3 \times 7 + 2$. **Les solutions sont les**
 $x \equiv 23 \pmod{105}$.

- Les congruences modulo 3 et 7 disent que 3 et 7 divisent $x - 2$. Comme ils sont premiers entre eux, $21 \mid x - 2$. On écrit donc $x = 2 + 21k$. Ensuite, $x \equiv 3 \pmod{5}$ donne $21k \equiv 1$, soit $k \equiv 1 \pmod{5}$. **On retrouve** $x = 23 + 105j$.
- Les solutions sont $23 + 105j$: 23, 128, 233, 338, etc. **Le groupe compte 233 personnes.**

Corrigé de l'exercice 14 : Système de congruences à modules non premiers entre eux

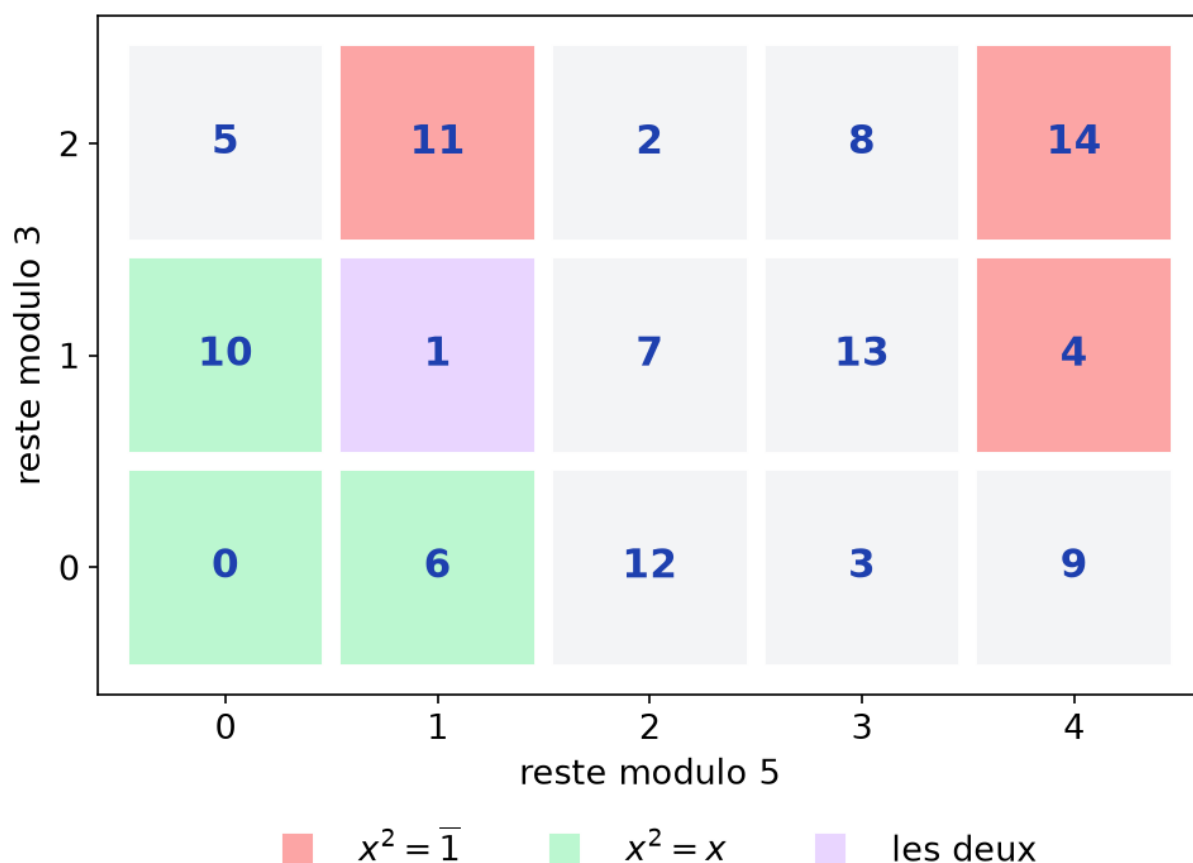
- Condition nécessaire : si $x = a + mu = b + nv$, alors $a - b = nv - mu$ est divisible par d . Condition suffisante : supposons $b - a = dt$. Par Bézout, il existe u, v avec $mu + nv = d$. Posons $x = a + mut$. Alors $x \equiv a \pmod{m}$. De plus, $x - b = mut - dt = (mu - d)t = -nvt$, donc $x \equiv b \pmod{n}$. **Le système est résoluble si et seulement si** $a \equiv b \pmod{d}$.
- Si x et x' sont solutions, m et n divisent $x - x'$. Donc leur ppcm ℓ divise $x - x'$. Réciproquement, $x + k\ell$ est encore solution. **Les solutions forment une unique classe modulo** $\text{ppcm}(m, n)$.
- Ici $d = 6$ et $5 \equiv 11 \pmod{6}$: le système est résoluble. On pose $x = 5 + 12k$. Alors $12k \equiv 6 \pmod{18}$, soit $2k \equiv 1 \pmod{3}$, soit $k \equiv 2 \pmod{3}$. Avec $k = 2$, $x = 29$. Vérification : $29 = 2 \times 12 + 5 = 18 + 11$. **Les solutions sont les** $x \equiv 29 \pmod{36}$.
- Ici $d = \text{pgcd}(6, 4) = 2$, et $1 \not\equiv 2 \pmod{2}$. Concrètement, la première équation impose x impair, la seconde x pair. **Le système n'a pas de solution.**

Corrigé de l'exercice 15 : Isomorphisme chinois dans $\mathbb{Z}/15\mathbb{Z}$

1. Les entiers 3 et 5 sont premiers entre eux et $15 = 3 \times 5$. **Le théorème chinois affirme exactement que ψ est un isomorphisme d'anneaux.**
2. On cherche x avec $x \equiv 2 \pmod{3}$ et $x \equiv 4 \pmod{5}$. Les candidats modulo 15 sont 4, 9, 14. Seul $14 = 4 \times 3 + 2$ convient. **L'antécédent est $\overline{14}$.**
3. Un couple est inversible si et seulement si ses deux composantes le sont. D'où $\varphi(15) = \varphi(3)\varphi(5) = 2 \times 4 = 8$. **Les inversibles de $\mathbb{Z}/15\mathbb{Z}$ sont $\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}$.**
4. Via ψ , l'équation devient $u^2 = 1$ dans $\mathbb{F}_3$ et $v^2 = 1$ dans $\mathbb{F}_5$. Ces deux corps donnent chacun ± 1 , soit quatre couples. Ensuite, on remonte :
 - $(1, 1) \rightarrow 1$ et $(-1, -1) \rightarrow 14$;
 - $(1, -1) : x \equiv 1 \pmod{3}, x \equiv 4 \pmod{5}$, donc $x = 4$;
 - $(-1, 1) : x \equiv 2 \pmod{3}, x \equiv 1 \pmod{5}$, donc $x = 11$.

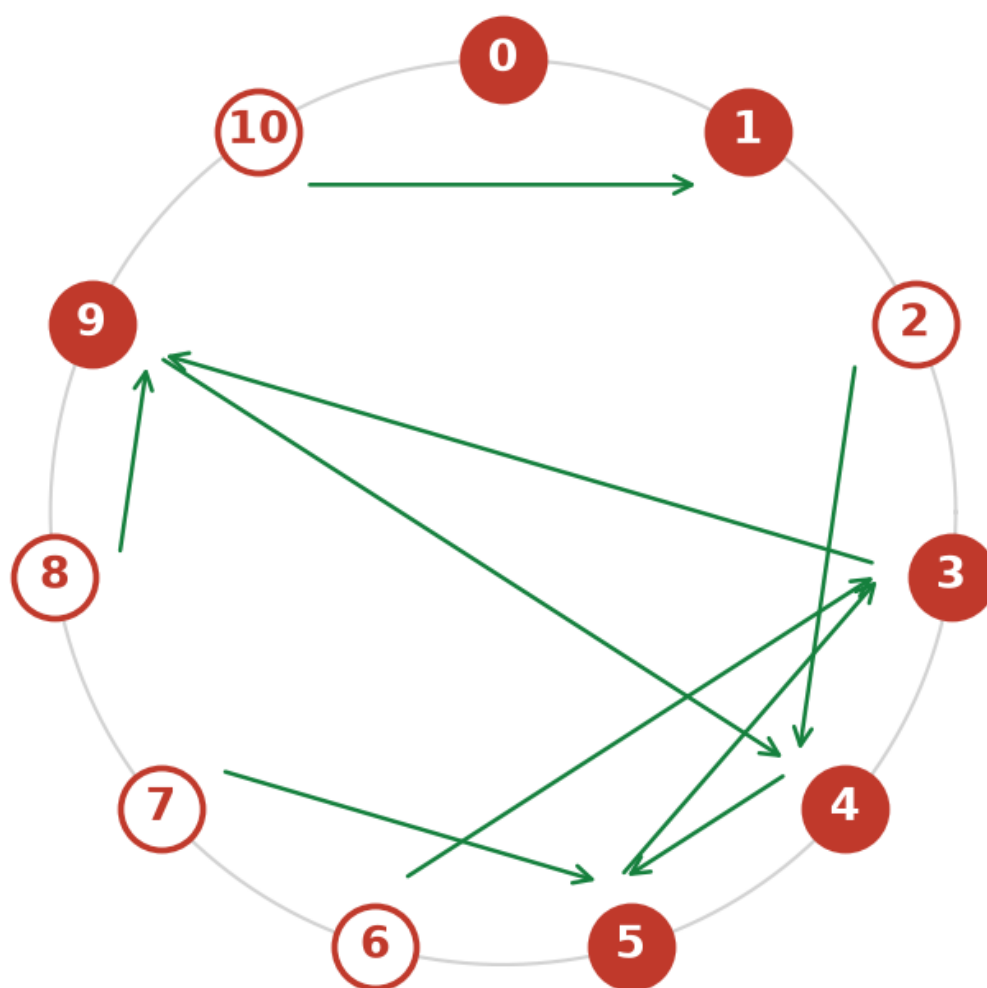
Vérification : $4^2 = 16 = 15 + 1$ et $11^2 = 121 = 8 \times 15 + 1$. **Il y a quatre solutions :** $\overline{1}, \overline{4}, \overline{11}, \overline{14}$. Dans un corps, un polynôme de degré 2 a au plus deux racines. Ici, ce n'est pas contradictoire, car $\mathbb{Z}/15\mathbb{Z}$ n'est pas intègre.

5. Dans un corps, $x^2 = x$ équivaut à $x(x - 1) = 0$, soit $x \in \{0, 1\}$. Les quatre couples donnent : $(0, 0) \rightarrow 0$, $(1, 1) \rightarrow 1$, $(1, 0) \rightarrow 10$ et $(0, 1) \rightarrow 6$. Vérification : $6^2 = 36 = 2 \times 15 + 6$ et $10^2 = 100 = 6 \times 15 + 10$. **Les solutions de $x^2 = x$ sont $\overline{0}, \overline{1}, \overline{6}, \overline{10}$.** La grille ci-dessous place chaque classe selon ses deux restes et fait apparaître ces solutions.



Corrigé de l'exercice 16 : Carrés dans $\mathbb{F}_{11}$

- Comme $(-x)^2 = x^2$, il suffit de calculer les carrés de 0 à 5 :
 $0, 1, 4, 9, 16 \equiv 5, 25 \equiv 3$. **Les carrés de $\mathbb{F}_{11}$ sont 0, 1, 3, 4, 5, 9, dont 5 non nuls,**
 conformément à la formule $\frac{11-1}{2} = 5$. La figure ci-dessous montre les deux flèches arrivant sur
 chaque carré non nul.



● carré dans $\mathbb{F}_{11}$ ○ non carré

2. Ici $\frac{p-1}{2} = 5$. D'une part, $3^5 = 243 = 22 \times 11 + 1$, donc $3^5 = 1$: 3 est un carré, et en effet $5^2 = 3$. D'autre part, $2^5 = 32 = 2 \times 11 + 10$, donc $2^5 = -1$. **Le critère d'Euler annonce que 3 est un carré et que 2 n'en est pas un, ce que confirme la liste.**

3. On a $4^2 = 16 \equiv 5$ et $7^2 = 49 = 4 \times 11 + 5$. Dans un corps, l'équation a au plus deux racines. **Les solutions de $x^2 = 5$ sont $\bar{4}$ et $\bar{7}$.**

4. Comme 2 est inversible, on écrit $4(x^2 + x + c) = (2x + 1)^2 - (1 - 4c)$. Pour $c = -1$, $\Delta = 1 + 4 = 5 = 4^2$. Donc $2x + 1 = \pm 4$. Or $2^{-1} = 6$, car $12 \equiv 1$. Ainsi $x = 3 \times 6 = 18 \equiv 7$ ou $x = -5 \times 6 = -30 \equiv 3$. Vérification : $49 + 7 - 1 = 55$

et $9 + 3 - 1 = 11$. Les solutions de $x^2 + x - 1 = 0$ sont $\bar{3}$ et $\bar{7}$. Pour $c = 1$, $\Delta = -3 \equiv 8$, qui n'est pas un carré d'après la liste. L'équation $x^2 + x + 1 = 0$ n'a pas de solution dans $\mathbb{F}_{11}$.

Corrigé de l'exercice 17 : Critère d'Euler et produit de non-carrés

1. L'application $s : x \rightarrow x^2$ est un morphisme du groupe commutatif $\mathbb{F}_p^\times$ dans lui-même. Son image C est donc un sous-groupe. Son noyau est $\{x \mid x^2 = 1\} = \{1, -1\}$, qui a deux éléments car p est impair. Chaque élément de C a donc exactement deux antécédents. **Par conséquent**, $\text{card } C = \frac{p-1}{2}$.
2. Soit $b = a^{\frac{p-1}{2}}$. Par Fermat, $b^2 = 1$, donc $b = \pm 1$. Si $a = x^2$, alors $b = x^{p-1} = 1$. Ainsi les $\frac{p-1}{2}$ éléments de C sont racines de $X^{\frac{p-1}{2}} - 1$. Or ce polynôme a au plus $\frac{p-1}{2}$ racines dans le corps $\mathbb{F}_p$. Ses racines sont donc exactement les éléments de C . **Un carré vérifie $b = 1$ et un non-carré vérifie $b = -1$.**
3. Notons $\chi(a) = a^{\frac{p-1}{2}} \in \{1, -1\}$. Clairement, $\chi(ab) = \chi(a)\chi(b)$. Si a et b ne sont pas des carrés, $\chi(ab) = (-1)(-1) = 1$. Si a est un carré et b non, $\chi(ab) = -1$. **Le produit de deux non-carrés est un carré ; le produit d'un carré par un non-carré n'en est pas un.**
4. Ici $\frac{p-1}{2} = 3$. D'abord, $2^3 = 8 \equiv 1 : 2$ est un carré, en effet $3^2 = 9 \equiv 2$. Ensuite, $3^3 = 27 = 3 \times 7 + 6 \equiv -1$ et $6^3 \equiv (-1)^3 = -1 : 3$ ni 6 ne sont des carrés. Enfin, $3 \times 6 = 18 \equiv 4 = 2^2$, qui est un carré, alors que $2 \times 3 = 6$ n'en est pas un. **Dans $\mathbb{F}_7$, seul 2 est un carré parmi $2, 3, 6$, et la règle de la question 3 est vérifiée.**

Corrigé de l'exercice 18 : -1 est-il un carré modulo p ?

1. D'après le critère d'Euler, -1 est un carré si et seulement si $(-1)^{\frac{p-1}{2}} = 1$ dans $\mathbb{F}_p$. Comme $1 \neq -1$ pour p impair, cela équivaut à $\frac{p-1}{2}$ pair. **Donc -1 est un carré modulo p si et seulement si $p \equiv 1 \pmod{4}$.**

2. On regroupe les facteurs de $(p-1)!$ par paires k et $p-k$, pour $1 \leq k \leq \frac{p-1}{2}$. Or $k(p-k) \equiv -k^2 \pmod{p}$. Par conséquent,

$$(p-1)! = \prod_{k=1}^{\frac{p-1}{2}} k(p-k) \equiv (-1)^{\frac{p-1}{2}} A^2 \pmod{p}.$$

Le théorème de Wilson donne alors $-1 \equiv (-1)^{\frac{p-1}{2}} A^2$. On multiplie par $(-1)^{\frac{p-1}{2}}$. On obtient $A^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

3. Si $p \equiv 1 \pmod{4}$, alors $\frac{p+1}{2}$ est impair, donc $A^2 \equiv -1$. Pour $p = 13$, $A = 6! = 720 = 55 \times 13 + 5$. Vérification : $5^2 = 25 = 2 \times 13 - 1$. **Une racine carrée de -1 modulo p est $(\frac{p-1}{2})!$; pour $p = 13$, c'est 5 .**

4. Supposons par l'absurde que $p_1, \dots, p_r$ soient tous les premiers congrus à 1 modulo 4 (il y en a, par exemple 5). Posons $N = (2p_1 \dots p_r)^2 + 1 > 1$, et soit q un facteur premier de N . D'abord, N est impair, donc q aussi. Ensuite, $(2p_1 \dots p_r)^2 \equiv -1 \pmod{q}$, donc -1 est un carré modulo q . D'après la question 1, $q \equiv 1 \pmod{4}$. Ainsi $q = p_i$ pour un certain i . Mais alors q divise N et $(2p_1 \dots p_r)^2$, donc $q \mid 1$. C'est absurde. **Il existe donc une infinité de nombres premiers congrus à 1 modulo 4 .**

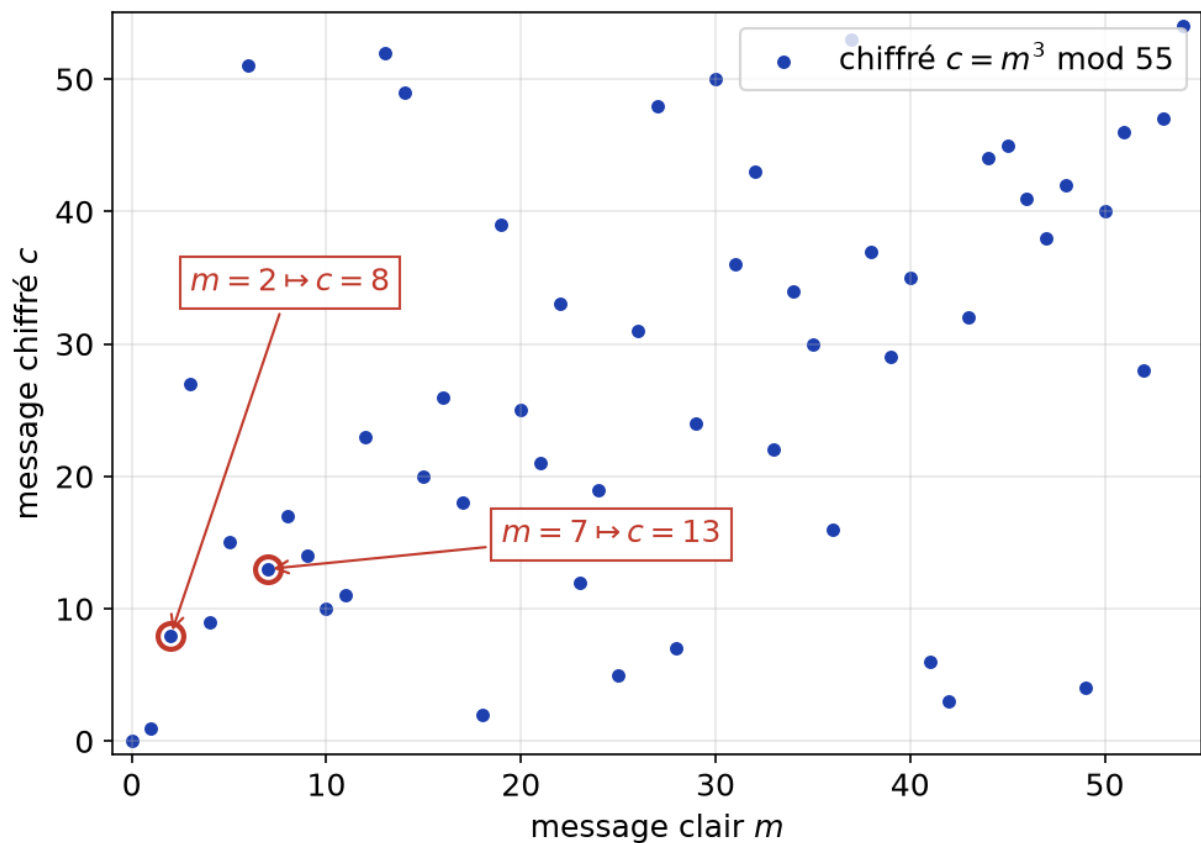
Corrigé de l'exercice 19 : Un chiffrement RSA à la main

1. On a $n = 5 \times 11 = 55$ et $\varphi(n) = 4 \times 10 = 40$. Comme $3 \nmid 40$ et 3 est premier, $\text{pgcd}(3, 40) = 1$. **Donc $n = 55$, $\varphi(n) = 40$, et $e = 3$ convient.**

2. On a $40 = 13 \times 3 + 1$, donc $1 = 40 - 13 \times 3$. Ainsi $3^{-1} \equiv -13 \equiv 27 \pmod{40}$. Vérification : $3 \times 27 = 81 = 2 \times 40 + 1$. **La clé privée est $d = 27$.**

3. On calcule $2^3 = 8$ et $7^3 = 343 = 6 \times 55 + 13$. **Les messages 2 et 7 sont chiffrés**

en 8 et 13. La figure ci-dessous montre le chiffrement de tous les messages : la répartition paraît désordonnée, mais chaque valeur est atteinte une seule fois.



4. Modulo 5 : $13 \equiv 3$, et $3^4 \equiv 1$ par Fermat. Or $27 = 6 \times 4 + 3$, donc $13^{27} \equiv 3^3 = 27 \equiv 2$. Modulo 11 : $13 \equiv 2$, et $2^{10} \equiv 1$. Or $27 = 2 \times 10 + 7$, donc $13^{27} \equiv 2^7 = 128 = 11 \times 11 + 7 \equiv 7$. Il reste à résoudre $x \equiv 2 \pmod{5}$, $x \equiv 7 \pmod{11}$. Le nombre 7 convient, et la solution est unique modulo 55 par le théorème chinois. **Le message déchiffré est $m = 7$** , comme attendu.
5. Connaissant p et q , on calcule $\varphi(n) = (p-1)(q-1)$. Ensuite, l'algorithme d'Euclide étendu donne $d = e^{-1} \bmod \varphi(n)$, exactement comme à la question 2. **La sécurité repose donc sur la difficulté de factoriser n .**

Corrigé de l'exercice 20 : Correction du RSA et factorisation

1. Écrivons $ed = 1 + k(p-1)(q-1)$ avec $k \in \mathbb{N}$. Travaillons d'abord modulo p . Si $p \mid m$, alors $m^{ed} \equiv 0 \equiv m$. Sinon, Fermat donne $m^{p-1} \equiv 1$, donc $m^{ed} = m(m^{p-1})^{k(q-1)} \equiv m$. Le même raisonnement vaut modulo q . Ainsi p et q divisent $m^{ed} - m$. Comme ils sont premiers entre eux, pq divise $m^{ed} - m$. **Donc** $m^{ed} \equiv m \pmod{n}$ **pour tout entier** m .
2. Posons $f(x) = x^e$ et $g(x) = x^d$ sur $\mathbb{Z}/n\mathbb{Z}$. D'après la question 1, $g(f(x)) = x^{ed} = x$ et $f(g(x)) = x^{de} = x$. **Ainsi f est bijective, de réciproque** $x \rightarrow x^d$.
3. On a $\varphi(n) = (p-1)(q-1) = n - (p+q) + 1$. Donc $p+q = 391 - 352 + 1 = 40$ et $pq = 391$. Les nombres p et q sont les racines de $X^2 - 40X + 391$. Le discriminant vaut $1600 - 1564 = 36$, donc les racines sont $\frac{40 \pm 6}{2}$. **On trouve** $p = 17$ **et** $q = 23$; en effet $17 \times 23 = 391$ et $16 \times 22 = 352$.
4. On a $352 = 2^5 \times 11$, qui n'est pas divisible par 3 . Donc $e = 3$ convient. Ensuite, $352 = 117 \times 3 + 1$, donc $3 \times (-117) \equiv 1 \pmod{352}$. Ainsi $d = 352 - 117 = 235$. Vérification : $3 \times 235 = 705 = 2 \times 352 + 1$. **La clé privée est** $d = 235$.

Corrigé de l'exercice 21 : Problème : ordre multiplicatif et nombres de Carmichael

1. Comme $\text{pgcd}(a, n) = 1$, le théorème d'Euler donne $a^{\varphi(n)} \equiv 1 \pmod{n}$, avec $\varphi(n) \geq 1$. **L'ensemble contient $\varphi(n)$, il est donc non vide, et $\omega(a)$ existe.**
2. Soit $k \geq 0$. La division euclidienne donne $k = q\omega(a) + r$ avec $0 \leq r < \omega(a)$. Ensuite, $a^k = (a^{\omega(a)})^q a^r \equiv a^r$. Si $r = 0$, on obtient $a^k \equiv 1$. Si $r \geq 1$, alors $a^r \not\equiv 1$ par minimalité de $\omega(a)$. Donc $a^k \equiv 1$ si et seulement si $r = 0$. **Ainsi $a^k \equiv 1 \Leftrightarrow \omega(a) \mid k$; avec $k = \varphi(n)$, on obtient $\omega(a) \mid \varphi(n)$.**
3. Ici $\varphi(11) = 10$, donc $\omega(2) \in \{1, 2, 5, 10\}$. Or $2^1 = 2$, $2^2 = 4$ et $2^5 = 32 \equiv 10$. Aucune de ces valeurs ne vaut 1 . **Donc l'ordre de 2 modulo 11 est 10**. Sur la figure de

l'énoncé, en partant de 1, on parcourt 1, 2, 4, 8, 5, 10, 9, 7, 3, 6 avant de revenir à 1.
Autrement dit, les puissances de 2 décrivent tout $(\mathbb{Z}/11\mathbb{Z})^\times$: 2 engendre ce groupe.

4. De même, $\omega(3) \in \{1, 2, 5, 10\}$. On a $3 \not\equiv 1$, $3^2 = 9 \not\equiv 1$ et $3^5 = 243 = 22 \times 11 + 1$. **L'ordre de 3 modulo 11 est 5.**
5. Posons $x = 1/p$. Comme $p \nmid 10$, le développement décimal de x est illimité. La suite des chiffres est invariante par décalage de k rangs si et seulement si $10^k x$ et x ont la même partie fractionnaire. Cela équivaut à $10^k x - x \in \mathbb{Z}$, c'est-à-dire $p \mid 10^k - 1$. La plus petite période est donc le plus petit $k \geq 1$ tel que $10^k \equiv 1 \pmod{p}$. Pour $p = 7$:
 $10 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, et $3^6 \equiv 1$, donc l'ordre vaut 6. On a bien
 $1/7 = 0,142857\,142857\dots$ Pour $p = 13$: $10^2 \equiv 9$, $10^3 \equiv 10 \equiv -3$,
 $10^4 \equiv -10 \equiv 3$, et $10^6 \equiv 1$. L'ordre divise 12 et vaut 6. On a bien
 $1/13 = 0,076923\,076923\dots$ **Dans les deux cas, la période est 6, égale à l'ordre de 10.**
6. Soit a premier avec 561. Alors a est premier avec 3, 11 et 17. Par Fermat,
 $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$ et $a^{16} \equiv 1 \pmod{17}$. Or
 $560 = 2 \times 280 = 10 \times 56 = 16 \times 35$. Donc $a^{560} \equiv 1$ modulo 3, 11 et 17. Ces modules sont deux à deux premiers entre eux. **Par le théorème chinois, $a^{560} \equiv 1 \pmod{561}$**
 .
7. Le nombre 561 est composé, mais il passe le test de Fermat pour toute base première avec lui. Un tel entier s'appelle un nombre de Carmichael. **Le test « $a^{n-1} \equiv 1$ » permet de prouver qu'un nombre est composé quand il échoue, mais son succès ne prouve jamais la primalité.**

Point de méthode : l'ordre divise $\varphi(n)$, donc on ne teste que les diviseurs de $\varphi(n)$. Pour prouver que l'ordre vaut $\varphi(n)$, il suffit de vérifier $a^{\varphi(n)/q} \not\equiv 1$ pour chaque premier q divisant $\varphi(n)$.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en L2

- Le cours : [arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$, cours de maths en L2](#)

- Les énoncés : [exercices de maths en L2 sur arithmétique et \$\mathbb{Z}/n\mathbb{Z}\$](#)
- Chapitre précédent : [Polynômes d'endomorphismes et trigonalisation](#)
- Chapitre suivant : [Groupes, sous-groupes et morphismes](#)
- Tester vos connaissances : [QCM de maths en L2 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L2](#) et la [licence de maths de L1 à L3](#)