Plaquette 4 – Congruences, Z/nZ, théorèmes d'Euler et de Wilson

Arithmétique dans Z — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Congruences et $\mathbb{Z}/n\mathbb{Z}$.

— $a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$; compatible avec $+$, $\times$ et les puissances.

— **Inversibles** : $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$; si $au + nv = 1$, alors $\overline{a}^{-1} = \overline{u}$. $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ premier.

— **Indicatrice d'Euler** : $\varphi(n) = \mathrm{card}\{k \in [\![1, n]\!],\ k \wedge n = 1\}$, et si $n = \prod p_i^{\alpha_i}$,

$$\varphi(n) = n \prod_i \left(1 - \frac{1}{p_i}\right)$$

— **Théorème d'Euler** : si $a \wedge n = 1$, alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

— **Ordre** : le plus petit $k \geq 1$ tel que $a^k \equiv 1$; il divise $\varphi(n)$, et $a^m \equiv 1 \Leftrightarrow \mathrm{ord}(a) \mid m$.

— **Wilson** : p premier $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.

— **Théorème chinois** : si $m \wedge n = 1$, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$; en particulier $\varphi(mn) = \varphi(m)\varphi(n)$.

Correction de l'exercice 1 – Critères de divisibilité par 9, 11, 7 et 13

a) On réduit la base avant de calculer : $10 \equiv 1 \pmod{9}$ et $10 \equiv -1 \pmod{11}$, donc $10^k \equiv 1$ et $10^k \equiv (-1)^k$ respectivement. Par compatibilité avec les sommes et les produits :

$$N \equiv \sum_k c_k \pmod{9}, \qquad N \equiv \sum_k (-1)^k c_k \pmod{11}$$

b) $7 \times 11 \times 13 = 77 \times 13 = 1001$, donc $1000 = 1001 - 1 \equiv -1$ modulo chacun de ces trois nombres. En écrivant $N = \sum_j T_j 1000^j$ avec des tranches T_j de trois chiffres :

$$N \equiv T_0 - T_1 + T_2 - \ldots \pmod{7, 11, 13}$$

c) Somme des chiffres $= 45$, donc $N \equiv 0 \pmod{9}$.

— Somme alternée (depuis les unités) : $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$, donc $N \equiv 5 \pmod{11}$.

— Tranches : $789 - 456 + 123 = 456$. Or $456 = 7 \times 65 + 1 = 11 \times 41 + 5 = 13 \times 35 + 1$.

Restes : 0 modulo 9, 5 modulo 11 (cohérent avec a)), 1 modulo 7, 1 modulo 13.

Piège : la somme alternée commence par le chiffre des **unités** avec le signe $+$; partir de la gauche change le signe quand le nombre de chiffres est pair.

Réponse. $123\,456\,789 \equiv 0$ (9), $\equiv 5$ (11), $\equiv 1$ (7), $\equiv 1$ (13).

Correction de l'exercice 2 – Sommes de trois carrés

a) $x \in \{0, \ldots, 7\}$ donne $x^2 \equiv 0, 1, 4, 1, 0, 1, 4, 1$: les carrés modulo 8 sont 0, 1, 4. Les impairs ont tous le carré 1, les multiples de 4 le carré 0, les autres pairs le carré 4.

b) En sommant trois valeurs de $\{0, 1, 4\}$: $0, 1, 2, 3, 4, 5, 6$ $(= 1+1+4)$ et $8 \equiv 0$, $9 \equiv 1$, $12 \equiv 4$. Jamais 7 :

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).

$$a^2 + b^2 + c^2 \not\equiv 7 \pmod 8$$

c) $2023 = 8 \times 252 + 7$: ce n'est pas une somme de trois carrés.

d) Supposons $4^m(8k+7) = a^2 + b^2 + c^2$ avec $m \geq 1$ minimal (le cas $m = 0$ est c)). Le membre de gauche est $\equiv 0 \pmod 4$. Modulo 4, les carrés valent 0 (pair) ou 1 (impair) ; une somme de trois d'entre eux n'est nulle modulo 4 que si **les trois** sont nuls, donc a, b, c pairs. Alors

$$4^{m-1}(8k+7) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$$

— contredit la minimalité de m.

Remarque : le théorème de Gauss-Legendre affirme la réciproque — tous les autres entiers sont sommes de trois carrés.

Réponse. Carrés modulo 8 : $0, 1, 4$; une somme de trois carrés n'est jamais $\equiv 7 \pmod 8$; $4^m(8k+7)$ n'en est jamais une.

Correction de l'exercice 3 – Inversibles de Z/nZ

a) $\overline{a}$ inversible $\Leftrightarrow \exists u,\ au \equiv 1 \pmod n \Leftrightarrow \exists u, v,\ au + nv = 1$. Par le **théorème de Bézout**, cette dernière condition équivaut à

$$a \wedge n = 1$$

b) Les $a \in \{0, \ldots, 11\}$ premiers avec 12 sont $1, 5, 7, 11$. Or $5^2 = 25 \equiv 1$, $7^2 = 49 \equiv 1$, $11^2 = 121 \equiv 1 \pmod{12}$: **chacun est son propre inverse**.

c) Euclide : $101 = 5 \times 17 + 16$, $17 = 16 + 1$. Remontée : $1 = 17 - 16 = 17 - (101 - 5 \times 17) = 6 \times 17 - 101$.

— Donc $\overline{17}^{-1} = \overline{6}$. Contrôle : $17 \times 6 = 102 = 101 + 1$ ✓.

— $17x \equiv 5 \Leftrightarrow x \equiv 6 \times 5 = 30 \pmod{101}$. Contrôle : $17 \times 30 = 510 = 5 \times 101 + 5$ ✓.

d) $\mathbb{Z}/n\mathbb{Z}$ (avec $n \geq 2$) est un corps si et seulement si tout $\overline{a} \neq \overline{0}$ est inversible, c'est-à-dire $a \wedge n = 1$ pour tout $1 \leq a \leq n-1$: cela signifie que n n'a aucun diviseur entre 2 et $n-1$, donc que n est premier.

Piège : dans $\mathbb{Z}/12\mathbb{Z}$, $\overline{3} \times \overline{4} = \overline{0}$ alors qu'aucun n'est nul — on ne peut pas « simplifier » une congruence par un non-inversible.

Réponse. Inversible $\Leftrightarrow a \wedge n = 1$; $(\mathbb{Z}/12\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, chacun son inverse ; $\overline{17}^{-1} = \overline{6}$, $x \equiv 30 \pmod{101}$.

Correction de l'exercice 4 – Théorème chinois : trois congruences et modules non premiers entre eux

a) $N = 3 \times 5 \times 7 = 105$. On cherche e_1 multiple de 35 avec $e_1 \equiv 1 \pmod 3$: $35 \equiv 2$, $70 \equiv 1$, donc $e_1 = 70$. De même e_2 multiple de 21, $\equiv 1 \pmod 5$: $21 \equiv 1$, $e_2 = 21$. Et e_3 multiple de 15, $\equiv 1 \pmod 7$: $15 \equiv 1$, $e_3 = 15$. Alors

$$x \equiv 2e_1 + 3e_2 + 2e_3 = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}$$

— Contrôle : $23 = 7 \times 3 + 2 = 4 \times 5 + 3 = 3 \times 7 + 2$ ✓. Le théorème chinois garantit l'unicité modulo 105.

b) $6 \wedge 8 = 2$: le théorème ne s'applique pas tel quel. Une solution vérifierait $x \equiv 3 \equiv 1 \pmod 2$ et $x \equiv 5 \equiv 1 \pmod 2$: **compatible**.

— $x = 3 + 6k$ et $3 + 6k \equiv 5 \pmod 8$, soit $6k \equiv 2 \pmod 8$, c'est-à-dire $3k \equiv 1 \pmod 4$, d'où $k \equiv 3 \pmod 4$.

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).

— $x = 3 + 6(3 + 4j) = 21 + 24j$: $x \equiv 21 \pmod{24}$, et $24 = \text{ppcm}(6, 8)$.

c) $x \equiv 3 \pmod 6$ impose x impair ; $x \equiv 4 \pmod 8$ impose x pair : **aucune solution**.

Règle : $x \equiv a\ (m)$, $x \equiv b\ (n)$ a des solutions si et seulement si $a \equiv b \pmod{m \wedge n}$; elles forment alors une classe modulo $\text{ppcm}(m, n)$.

Réponse. a) $x \equiv 23 \pmod{105}$. b) $x \equiv 21 \pmod{24}$. c) Aucune solution.

Correction de l'exercice 5 – Calendrier et congruences modulo 7

a) $365 = 52 \times 7 + 1 \equiv 1 \pmod 7$ et $366 \equiv 2 \pmod 7$: un an plus tard, la date avance d'un jour, ou de deux si l'on franchit un 29 février.

— Du 29/09/2026 au 29/09/2027 : pas de 29 février, décalage 1 : **mercredi**.

— Du 29/09/2027 au 29/09/2028 : on franchit le 29/02/2028, décalage 2 : **vendredi**.

b) Chaque année apporte 1, plus 1 par 29 février :

$$D(y) \equiv (y - 2026) + b(y) \pmod 7$$

c) On cherche le premier $y > 2026$ avec $D(y) \equiv 0 \pmod 7$. On tabule $(y - 2026) + b(y)$:

— 2027 : 1 ; 2028 : $2 + 1 = 3$; 2029 : 4 ; 2030 : 5 ; 2031 : 6 ; 2032 : $6 + 2 = 8 \equiv 1$;

— 2033 : $9 \equiv 2$; 2034 : 3 ; 2035 : 4 ; 2036 : $10 + 3 = 13 \equiv 6$; 2037 : $11 + 3 = 14 \equiv 0$.

Le 29 septembre 2037 sera un **mardi**, onze ans plus tard.

Remarque : le calendrier grégorien se répète exactement tous les 400 ans, car 400 ans comptent 146 097 jours, et $146\,097 = 7 \times 20\,871$.

Réponse. 2027 : mercredi ; 2028 : vendredi ; $D(y) \equiv (y - 2026) + b(y) \pmod 7$; de nouveau mardi en 2037.

Correction de l'exercice 6 – Chiffrement affine

a) On applique $y = 5x + 8$ puis on réduit modulo 26 :

— M : $5 \times 12 + 8 = 68 \equiv 16$, lettre Q ;

— A : 8, lettre I ;

— T : $5 \times 19 + 8 = 103 \equiv 25$, lettre Z ;

— H : $43 \equiv 17$, lettre R ;

— S : $98 \equiv 20$, lettre U.

MATHS devient **QIZRU**.

b) $5 \wedge 26 = 1$: $\overline{5}$ est inversible modulo 26. Bézout : $26 = 5 \times 5 + 1$, donc $1 = 26 - 5 \times 5$ et $5^{-1} \equiv -5 \equiv 21$. Contrôle : $5 \times 21 = 105 = 4 \times 26 + 1$ ✓. Alors

$$y \equiv 5x + 8 \Leftrightarrow x \equiv 21(y - 8) \pmod{26}$$

— Contrôle sur $Q = 16$: $21 \times 8 = 168 = 6 \times 26 + 12$, on retrouve M ✓.

c) $4 \wedge 26 = 2$: $x \mapsto 4x + 8$ n'est pas injective, par exemple $x = 0$ et $x = 13$ donnent tous deux 8 ; le message ne serait pas déchiffrable. Les clés utilisables sont les (a, b) avec $a \wedge 26 = 1$: $\varphi(26) = 12$ choix de a et 26 de b, soit 312 clés — trop peu pour résister à une recherche exhaustive.

Réponse. QIZRU ; $x \equiv 21(y - 8) \pmod{26}$; il faut $a \wedge 26 = 1$: 312 clés.

Correction de l'exercice 7 – Clé de contrôle ISBN-10

a) Poids $10, 9, \ldots, 2$ sur les neuf premiers chiffres $0, 3, 0, 6, 4, 0, 6, 1, 5$:

$$0 + 27 + 0 + 42 + 24 + 0 + 24 + 3 + 10 = 130$$

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).

— On veut $130 + x_{10} \equiv 0 \pmod{11}$. Or $130 = 11 \times 11 + 9$, donc $x_{10} \equiv -9 \equiv 2$: ISBN 0-306-40615-2.

b) Si le chiffre x_i est remplacé par $x_i' \neq x_i$, la somme varie de $(11-i)(x_i' - x_i)$. Les deux facteurs sont non nuls et strictement compris entre -11 et 11 ; comme 11 est **premier**, par le lemme d'Euclide :

$$11 \nmid (11-i)(x_i' - x_i)$$

— la somme n'est plus multiple de 11 : l'erreur est détectée.

c) Échanger x_i et x_{i+1} fait varier la somme de $(11-i)(x_{i+1} - x_i) + (10-i)(x_i - x_{i+1}) = x_{i+1} - x_i$, non nul et compris entre -10 et 10 : non multiple de 11, erreur détectée.

— Avec le module 10 et des poids, certains poids ne seraient pas inversibles (un poids 2 ne distingue pas x de $x+5$) : 10 n'est pas premier. C'est le prix du « chiffre » X.

Réponse. Clé 2 ; détecte toute erreur simple et toute transposition voisine grâce à la primalité de 11.

Correction de l'exercice 8 – Indicatrice d'Euler

a) Tout $k \in [\![1, p-1]\!]$ est premier avec p : $\varphi(p) = p - 1$. Pour p^k : un entier n'est **pas** premier avec p^k si et seulement s'il est multiple de p ; il y a p^{k-1} multiples de p dans $[\![1, p^k]\!]$, donc

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

b) Avec $n = \prod p_i^{\alpha_i}$, les $p_i^{\alpha_i}$ sont deux à deux premiers entre eux ; la multiplicativité donne

$$\varphi(n) = \prod_i p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) = n\prod_i\left(1 - \frac{1}{p_i}\right)$$

c) $100 = 2^2 \times 5^2$: $\varphi(100) = 100 \times \frac{1}{2} \times \frac{4}{5} = 40$.

— $360 = 2^3 \times 3^2 \times 5$: $\varphi(360) = 360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96$.

— $143 = 11 \times 13$: $\varphi(143) = 10 \times 12 = 120$.

d) Si $k \wedge n = 1$, alors $(n-k) \wedge n = 1$: les entiers premiers avec n se groupent en paires $\{k, n-k\}$. Une paire n'est réduite à un élément que si $k = \frac{n}{2}$, et alors $k \wedge n = \frac{n}{2} \geq 2$ pour $n \geq 4$; pour $n = 3$, $\varphi(3) = 2$. Donc $\varphi(n)$ est pair.

Réponse. $\varphi(p^k) = p^k - p^{k-1}$; $\varphi(100) = 40$, $\varphi(360) = 96$, $\varphi(143) = 120$; $\varphi(n)$ pair pour $n \geq 3$.

Correction de l'exercice 9 – Théorème d'Euler et derniers chiffres

a) a et r_i sont inversibles modulo n, donc ar_i aussi : $\overline{ar_i}$ est l'un des $\overline{r}_j$. L'application $\overline{x} \mapsto \overline{ax}$ est **injective** ($\overline{ax} = \overline{ay} \Rightarrow \overline{x} = \overline{y}$ en multipliant par $\overline{a}^{-1}$), donc bijective sur cet ensemble fini.

b) Les deux produits contiennent les mêmes classes dans un autre ordre :

$$\prod_i (ar_i) \equiv \prod_i r_i \pmod{n}, \qquad \text{soit} \qquad a^{\varphi(n)}P \equiv P, \quad P = \prod_i r_i$$

— P est inversible modulo n (produit d'inversibles) : on simplifie, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

c) Deux derniers chiffres = reste modulo 100. $7 \wedge 100 = 1$ et $\varphi(100) = 40$; $2026 = 40 \times 50 + 26$, donc $7^{2026} \equiv 7^{26}$. On remarque mieux : $7^4 = 2401 \equiv 1 \pmod{100}$, et $2026 = 4 \times 506 + 2$, donc

$$7^{2026} \equiv 7^2 = 49 \pmod{100}$$

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).

— Pour 3 : $3^{20} \equiv 1 \pmod{100}$ ($3^5 = 243 \equiv 43$, $43^2 = 1849 \equiv 49$, $49^2 = 2401 \equiv 1$). $2026 = 20 \times 101 + 6$, donc $3^{2026} \equiv 3^6 = 729 \equiv 29$.

Les deux derniers chiffres sont 49 et 29.

Réflexe : Euler donne un exposant qui marche ; l'**ordre** réel (4 pour 7, 20 pour 3) peut être plus petit, et le calcul plus court.

Réponse. $a^{\varphi(n)} \equiv 1 \pmod{n}$; 7^{2026} finit par 49, 3^{2026} par 29.

Correction de l'exercice 10 – Ordre multiplicatif et développement décimal périodique

a) Soit $k = \mathrm{ord}(a)$ et $m = kq + r$ la division euclidienne, $0 \leq r < k$. Alors

$$a^m = (a^k)^q a^r \equiv a^r \pmod{n}$$

— Si $a^m \equiv 1$, alors $a^r \equiv 1$ avec $0 \leq r < k$: par minimalité de k, $r = 0$, donc $k \mid m$. La réciproque est immédiate.

— Par Euler, $a^{\varphi(n)} \equiv 1$, donc $k \mid \varphi(n)$.

b) Modulo 7 : $2, 4, 8 \equiv 1$: ordre 3 (qui divise bien $\varphi(7) = 6$). Modulo 11 : l'ordre divise 10, on teste $2^1 = 2$, $2^2 = 4$, $2^5 = 32 \equiv -1$: aucun ne vaut 1, donc l'ordre est 10.

c) On teste les diviseurs de $p - 1$:

— $p = 7$: $10 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$; l'ordre divise 6 et vaut ni 1, ni 2, ni 3 : **période** 6 ($\frac{1}{7} = 0,\overline{142857}$).

— $p = 13$: $10^2 = 100 \equiv 9$, $10^3 \equiv 90 \equiv 12 \equiv -1$, donc $10^6 \equiv 1$, et $10^1, 10^2, 10^3 \not\equiv 1$: **période** 6.

— $p = 41$: $10^5 = 100\,000 = 41 \times 2439 + 1$: l'ordre divise 5 et n'est pas 1 : **période** 5 ($\frac{1}{41} = 0,\overline{02439}$).

Réponse. $\mathrm{ord}(a) \mid m \Leftrightarrow a^m \equiv 1$; $\mathrm{ord}_7(2) = 3$, $\mathrm{ord}_{11}(2) = 10$; périodes 6, 6, 5.

Correction de l'exercice 11 – Racines carrées de 1 modulo n

a) On factorise :

$$x^2 - 1 = (x - 1)(x + 1) \equiv 0 \pmod{p}$$

— p premier divise un produit, donc l'un des facteurs (**lemme d'Euclide**) : $x \equiv 1$ ou $x \equiv -1$. Réciproquement ces deux classes conviennent (et sont distinctes si $p \neq 2$).

b) Les carrés modulo 8 : $1^2 = 1$, $3^2 = 9 \equiv 1$, $5^2 = 25 \equiv 1$, $7^2 = 49 \equiv 1$. Quatre solutions : $x \equiv 1, 3, 5, 7 \pmod{8}$, soit tous les impairs. L'argument de a) échoue car 8 n'est pas premier : $8 \mid (x - 1)(x + 1)$ sans diviser un facteur, par exemple $x = 3$ donne 2×4.

c) $15 = 3 \times 5$ avec $3 \wedge 5 = 1$: $x^2 \equiv 1 \pmod{15} \Leftrightarrow x^2 \equiv 1 \pmod{3}$ et $x^2 \equiv 1 \pmod{5}$, soit $x \equiv \pm 1 \pmod{3}$ et $x \equiv \pm 1 \pmod{5}$ d'après a). Quatre combinaisons, chacune une classe modulo 15 :

— $(1, 1) \to 1$; $(-1, -1) \to 14$; $(1, -1) \to 4$; $(-1, 1) \to 11$.

Contrôle : $4^2 = 16 \equiv 1$ et $11^2 = 121 = 8 \times 15 + 1$ ✓.

Conséquence : un module n avec plus de deux racines carrées de 1 n'est pas premier — c'est l'idée du test de primalité de Miller-Rabin.

Réponse. Modulo p premier : ± 1 ; modulo 8 : $1, 3, 5, 7$; modulo 15 : $1, 4, 11, 14$.

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 12 – Théorème de Wilson

a) $\mathbb{Z}/p\mathbb{Z}$ est un corps : chaque $\overline{a} \neq \overline{0}$ a un inverse. D'après l'exercice précédent, $\overline{a} = \overline{a}^{-1} \Leftrightarrow a^2 \equiv 1 \Leftrightarrow a \equiv \pm 1$. Les autres éléments se groupent en paires $\{\overline{a}, \overline{a}^{-1}\}$ de produit $\overline{1}$. D'où

$$(p-1)! \equiv 1 \times (-1) \times \prod_{\text{paires}} \overline{1} = -1 \pmod{p}$$

— Pour $p = 11$: paires $\{2,6\}$, $\{3,4\}$, $\{5,9\}$, $\{7,8\}$ (car 12, 12, 45, 56 sont $\equiv 1$), et restent 1, 10. Donc $10! \equiv 10 \equiv -1 \pmod{11}$ ✓.

b) Soit d un diviseur de n avec $1 < d < n$. Alors $d \leq n-1$ divise $(n-1)!$. Si l'on avait $(n-1)! \equiv -1 \pmod{n}$, on aurait $d \mid (n-1)! + 1$, donc $d \mid 1$: absurde.

— Contrôle : $3! = 6 \equiv 2 \pmod{4}$; $5! = 120 \equiv 0 \pmod{6}$; $8! = 40320 \equiv 0 \pmod{9}$.

c) $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1 \pmod{n}$. C'est un critère exact mais **inutilisable** : calculer $(n-1)!$ modulo n demande $n-2$ multiplications, bien plus que les $\sqrt{n}$ essais de division.

Réponse. $(p-1)! \equiv -1 \pmod{p}$; faux pour n composé ; critère exact mais trop coûteux.

Correction de l'exercice 13 – Générateurs du groupe des inversibles

a) Puissances de 3 modulo 7 : $3, 2, 6, 4, 5, 1$. Les six inversibles sont atteints : 3 est d'ordre $6 = \varphi(7)$.

— Si g est un générateur, g^k est d'ordre $\frac{6}{k \wedge 6}$; il est générateur si et seulement si $k \wedge 6 = 1$, soit $k \in \{1, 5\}$. Les générateurs sont 3 et $3^5 \equiv 5$.

b) Les inversibles modulo 8 sont $1, 3, 5, 7$, et chacun vérifie $x^2 \equiv 1$ (exercice 11). Tous sont d'ordre 1 ou 2, jamais $\varphi(8) = 4$: pas de générateur.

c) Même raisonnement : 2 est d'ordre 10 (exercice 10), donc 2^k est générateur si et seulement si

$$k \wedge 10 = 1 \Leftrightarrow k \in \{1, 3, 7, 9\}$$

— $2^1 = 2$, $2^3 = 8$, $2^7 = 128 = 11 \times 11 + 7 \equiv 7$, $2^9 = 512 = 46 \times 11 + 6 \equiv 6$.

Générateurs : $2, 6, 7, 8$ — il y en a $\varphi(10) = 4$.

Remarque : pour p premier, $(\mathbb{Z}/p\mathbb{Z})^*$ a toujours un générateur (il est **cyclique**), et exactement $\varphi(p-1)$ générateurs ; c'est un théorème plus difficile.

Réponse. Modulo 7 : 3 et 5 ; modulo 8 : aucun ; modulo 11 : $2, 6, 7, 8$.

Correction de l'exercice 14 – Un chiffrement RSA à la main

a) $\varphi(143) = 10 \times 12 = 120$; $7 \wedge 120 = 1$. Euclide : $120 = 17 \times 7 + 1$, donc $1 = 120 - 17 \times 7$ et $7^{-1} \equiv -17 \equiv 103 \pmod{120}$. Contrôle : $7 \times 103 = 721 = 6 \times 120 + 1$ ✓. Donc $d = 103$.

b) Carrés successifs modulo 143 : $9^2 = 81$, $9^4 = 6561 = 45 \times 143 + 126 \equiv 126$. Puis $9^7 = 9^4 \times 9^2 \times 9$:

$$126 \times 81 = 10206 \equiv 53, \qquad 53 \times 9 = 477 \equiv 48 \pmod{143}$$

— Donc $c = 48$.

c) $ed = 1 + k\varphi(n)$, donc pour $m \wedge n = 1$, par **Euler** : $c^d \equiv m^{ed} = m\left(m^{\varphi(n)}\right)^k \equiv m \pmod{n}$.

— Vérification par le théorème chinois : modulo 11, $48 \equiv 4$ et $103 \equiv 3 \pmod{10}$, donc $48^{103} \equiv 4^3 = 64 \equiv 9$. Modulo 13, $48 \equiv 9$ et $103 \equiv 7 \pmod{12}$, donc $48^{103} \equiv 9^7$; or

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).

$9^2 \equiv 3$, $9^4 \equiv 9$, $9^7 \equiv 9 \times 3 \times 9 = 243 \equiv 9$.

— $x \equiv 9$ modulo 11 et modulo 13 donne $x \equiv 9 \pmod{143}$: on retrouve $m = 9$ ✓.

d) Connaître d revient à connaître $\varphi(n) = (p-1)(q-1)$, donc p et q ($p + q = n - \varphi(n) + 1$ et $pq = n$). Avec n de plus de 600 chiffres, aucune méthode connue ne factorise n en un temps raisonnable.

Réponse. $\varphi(n) = 120$, $d = 103$; $c = 48$; $48^{103} \equiv 9 \pmod{143}$.

Correction de l’exercice 15 – Synthèse : n puissance 13 moins n

a) $2730 = 2 \times 1365 = 2 \times 3 \times 455 = 2 \times 3 \times 5 \times 91 = 2 \times 3 \times 5 \times 7 \times 13$.

b) Si $p \mid n$, c’est évident. Sinon, par le **petit théorème de Fermat**,

$$n^{p-1} \equiv 1 \pmod{p}$$

— et $p - 1 \mid 12$ donne $n^{12} = \left(n^{p-1}\right)^{12/(p-1)} \equiv 1$, donc $n^{13} \equiv n \pmod{p}$.

c) Les premiers p avec $p - 1 \mid 12$: $p - 1 \in \{1, 2, 3, 4, 6, 12\}$, soit $p \in \{2, 3, 4, 5, 7, 13\}$, dont les premiers sont $2, 3, 5, 7, 13$ (4 n’est pas premier). Chacun divise $n^{13} - n$ d’après b). Ils sont deux à deux premiers entre eux, donc leur produit 2730 divise $n^{13} - n$ (corollaire de Gauss).

d) $11 - 1 = 10$ ne divise pas 12 : aucune raison que $11 \mid n^{13} - n$. Pour $n = 2$: $2^{13} - 2 = 8190 = 3 \times 2730$, et $8190 = 11 \times 744 + 6$: non multiple de 11. Le résultat est faux avec 2730×11.

Remarque : 2730 est le plus grand entier divisant tous les $n^{13} - n$, puisque $8190 = 3 \times 2730$ et $3^{13} - 3 = 1\,594\,320 = 584 \times 2730$, avec $3 \wedge 584 = 1$.

Réponse. $2730 = 2 \times 3 \times 5 \times 7 \times 13$; Fermat donne $p \mid n^{13} - n$ pour ces cinq premiers ; faux pour 2730×11 ($n = 2$).

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).