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

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

Exercices

Méthode

Calculer **modulo** n, c'est remplacer chaque nombre par un représentant commode ($10 \equiv -1 \pmod{11}$, $7^4 \equiv 1 \pmod{100}$) avant de calculer. Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{a}$ est **inversible** si et seulement si $a \wedge n = 1$ — l'inverse se lit sur une relation de Bézout. Les inversibles forment un groupe à $\varphi(n)$ éléments, d'où le **théorème d'Euler** $a^{\varphi(n)} \equiv 1$, qui généralise Fermat et fonde le chiffrement RSA.

Exercice 1 – Critères de divisibilité par 9, 11, 7 et 13

Soit $N = \sum_{k=0}^{m} c_k 10^k$ un entier écrit en base 10.

a) Montrer que $N \equiv \sum c_k \pmod{9}$ et $N \equiv \sum (-1)^k c_k \pmod{11}$.

b) Vérifier que $1001 = 7 \times 11 \times 13$ et que $1000 \equiv -1$ modulo 7, 11 et 13. En déduire un critère utilisant la somme alternée des **tranches de trois chiffres**.

c) Appliquer à $N = 123\,456\,789$: restes modulo 9, 11, 7 et 13.

Exercice 2 – Sommes de trois carrés

a) Dresser la table des carrés modulo 8.

b) Quelles sont les valeurs possibles de $a^2 + b^2 + c^2$ modulo 8 ?

c) En déduire qu'aucun entier de la forme $8k + 7$ n'est somme de trois carrés d'entiers. Application : 2023.

d) Montrer plus généralement que $4^m(8k + 7)$ n'est jamais somme de trois carrés (on pourra, par l'absurde, considérer un contre-exemple avec m minimal et étudier la parité de a, b, c modulo 4).

Exercice 3 – Inversibles de Z/nZ

a) Montrer que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

b) Lister les inversibles de $\mathbb{Z}/12\mathbb{Z}$ et donner l'inverse de chacun.

c) Calculer l'inverse de $\overline{17}$ dans $\mathbb{Z}/101\mathbb{Z}$ et résoudre $17x \equiv 5 \pmod{101}$.

d) Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Exercice 4 – Théorème chinois : trois congruences et modules non premiers entre eux

a) Résoudre le système de Sunzi (IIIe siècle) : $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$, en construisant des entiers e_1, e_2, e_3 tels que $e_i \equiv 1$ modulo le i-ème module et $\equiv 0$ modulo les deux autres.

b) Le système $x \equiv 3 \pmod{6}$, $x \equiv 5 \pmod{8}$ a-t-il des solutions ? Les déterminer.

c) Même question pour $x \equiv 3 \pmod{6}$, $x \equiv 4 \pmod{8}$.

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).

Exercice 5 – Calendrier et congruences modulo 7

Le mardi 29 septembre 2026 sert de référence. Une année non bissextile compte 365 jours, une bissextile 366 ; entre 2027 et 2040, les années bissextiles sont 2028, 2032, 2036 et 2040.

a) Quel jour de la semaine sera le 29 septembre 2027 ? le 29 septembre 2028 ?

b) Soit $D(y)$ le décalage (en jours de la semaine) entre le 29 septembre 2026 et le 29 septembre de l'année y. Exprimer $D(y)$ modulo 7 en fonction de $y-2026$ et du nombre $b(y)$ de 29 février rencontrés.

c) En quelle année le 29 septembre retombera-t-il pour la première fois un mardi ?

Exercice 6 – Chiffrement affine

On code les lettres $A, B, \ldots, Z$ par $0, 1, \ldots, 25$ et on chiffre la lettre x en $y \equiv 5x + 8 \pmod{26}$.

a) Chiffrer le mot MATHS ($M = 12$, $T = 19$, $H = 7$, $S = 18$).

b) Justifier que ce chiffrement est **inversible** et donner la formule de déchiffrement.

c) Pourquoi la clé $y \equiv 4x + 8$ serait-elle inutilisable ? Combien de clés (a, b) sont utilisables ?

Exercice 7 – Clé de contrôle ISBN-10

Un ISBN-10 est une suite de chiffres $x_1 x_2 \ldots x_{10}$ (où x_{10} peut valoir 10, noté X) telle que

$$\sum_{i=1}^{10} (11-i)\,x_i \equiv 0 \pmod{11}$$

a) Calculer la clé x_{10} de l'ISBN commençant par 0-306-40615.

b) Montrer que le code détecte toute erreur sur **un seul** chiffre.

c) Montrer qu'il détecte aussi l'échange de deux chiffres voisins distincts. Pourquoi a-t-on choisi le module 11 plutôt que 10 ?

Exercice 8 – Indicatrice d'Euler

On note $\varphi(n)$ le nombre d'entiers de $[\![1, n]\!]$ premiers avec n.

a) Calculer $\varphi(p)$ et $\varphi(p^k)$ pour p premier et $k \geq 1$.

b) On admet que $\varphi(mn) = \varphi(m)\varphi(n)$ si $m \wedge n = 1$ (conséquence du théorème chinois). En déduire la formule $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$.

c) Calculer $\varphi(100)$, $\varphi(360)$ et $\varphi(143)$.

d) Montrer que $\varphi(n)$ est pair pour $n \geq 3$.

Exercice 9 – Théorème d'Euler et derniers chiffres

Soit $n \geq 2$ et a premier avec n. On note $r_1, \ldots, r_{\varphi(n)}$ les entiers de $[\![1, n]\!]$ premiers avec n.

a) Montrer que $x \mapsto ax$ permute les classes $\overline{r}_1, \ldots, \overline{r}_{\varphi(n)}$ dans $\mathbb{Z}/n\mathbb{Z}$.

b) En comparant $\prod_i r_i$ et $\prod_i (a r_i)$ modulo n, démontrer le théorème d'Euler :

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).

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

c) Déterminer les deux derniers chiffres de 7^{2026}, puis de 3^{2026}.

Exercice 10 – Ordre multiplicatif et développement décimal périodique

Pour $a \wedge n = 1$, l'**ordre** de a modulo n est le plus petit $k \geq 1$ tel que $a^k \equiv 1 \pmod{n}$.

a) Montrer que $a^m \equiv 1 \pmod{n} \Leftrightarrow \mathrm{ord}(a) \mid m$, et en déduire que $\mathrm{ord}(a)$ divise $\varphi(n)$.

b) Calculer l'ordre de 2 modulo 7 et modulo 11.

c) Soit $p \neq 2, 5$ premier. On admet que la période du développement décimal de $\frac{1}{p}$ est l'ordre de 10 modulo p. Déterminer la période de $\frac{1}{7}$, $\frac{1}{13}$, $\frac{1}{41}$, sans poser de division.

Exercice 11 – Racines carrées de 1 modulo n

a) Soit p premier. Montrer que les solutions de $x^2 \equiv 1 \pmod{p}$ sont exactement $x \equiv \pm 1$.

b) Résoudre $x^2 \equiv 1 \pmod{8}$. Quelle propriété de a) tombe en défaut, et pourquoi ?

c) À l'aide du théorème chinois, résoudre $x^2 \equiv 1 \pmod{15}$.

Exercice 12 – Théorème de Wilson

a) Soit $p \geq 3$ premier. En regroupant chaque élément de $\{\overline{1}, \ldots, \overline{p-1}\}$ avec son inverse, montrer que $(p-1)! \equiv -1 \pmod{p}$. Vérifier pour $p = 11$ en écrivant les paires.

b) Soit $n \geq 2$ composé. Montrer que $(n-1)! \not\equiv -1 \pmod{n}$. (Pour $n > 4$, on peut même montrer $(n-1)! \equiv 0$.)

c) En déduire un critère de primalité. Est-il utilisable en pratique ?

Exercice 13 – Générateurs du groupe des inversibles

On dit que g est un **générateur** de $(\mathbb{Z}/n\mathbb{Z})^*$ si son ordre vaut $\varphi(n)$, c'est-à-dire si ses puissances décrivent tous les inversibles.

a) Montrer que 3 est un générateur de $(\mathbb{Z}/7\mathbb{Z})^*$ en écrivant ses puissances. Trouver tous les générateurs.

b) Montrer que $(\mathbb{Z}/8\mathbb{Z})^*$ n'a pas de générateur.

c) Trouver tous les générateurs de $(\mathbb{Z}/11\mathbb{Z})^*$, sachant que 2 en est un (exercice 10). Combien y en a-t-il ?

Exercice 14 – Un chiffrement RSA à la main

Alice choisit $p = 11$, $q = 13$, $n = pq = 143$ et l'exposant public $e = 7$.

a) Calculer $\varphi(n)$ et vérifier que $e \wedge \varphi(n) = 1$. Déterminer l'exposant secret $d \in [\![1, \varphi(n)]\!]$ tel que $ed \equiv 1 \pmod{\varphi(n)}$.

b) Bob chiffre le message $m = 9$ en $c \equiv m^e \pmod{n}$. Calculer c par exponentiation rapide.

c) Montrer que $c^d \equiv m \pmod{n}$ pour tout m premier avec n (on utilisera Euler), puis

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).

vérifier le déchiffrement de c à l'aide du théorème chinois.

d) Pourquoi la sécurité repose-t-elle sur la difficulté de factoriser n ?

Exercice 15 – Synthèse : n puissance 13 moins n

a) Décomposer 2730 en facteurs premiers.

b) Soit p premier tel que $p-1$ divise 12. Montrer que $p \mid n^{13}-n$ pour tout $n \in \mathbb{Z}$.

c) En déduire que 2730 divise $n^{13}-n$ pour tout $n \in \mathbb{Z}$.

d) Le résultat reste-t-il vrai en remplaçant 2730 par 2730×11 ? Vérifier avec $n = 2$.

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).