Plaquette 4 – Congruences, anneaux Z/nZ et applications

Arithmétique dans Z — Licence 1 (L1)

Exercices

Méthode

On calcule **modulo** n : réduire les puissances grâce à un exposant qui ramène à 1 (Fermat, Euler, ordre), inverser un nombre par **Bézout**, recoller des congruences par le **théorème chinois**, et éliminer des équations impossibles en regardant les **restes des carrés et des cubes**. On termine par des applications concrètes : calendrier, cryptographie RSA, clés de contrôle.

Exercice 1 – Réduire une grande puissance

a) Calculer 7^4 modulo 100. En déduire les deux derniers chiffres de 7^{2026}.

b) Déterminer le reste de la division de 3^{2026} par 7.

c) Déterminer le chiffre des unités de 2^{2026} et de 2026^{2026}.

d) Expliquer pourquoi, dans chaque cas, on cherche d'abord un exposant k tel que $a^k \equiv 1$.

Exercice 2 – Indicatrice d'Euler

a) Justifier que $\varphi(p^k) = p^k - p^{k-1}$ pour p premier et $k \geq 1$.

b) En admettant que φ est multiplicative, calculer $\varphi(100)$ et $\varphi(360)$.

c) Démontrer le **théorème d'Euler** : si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.
(Indication : si $r_1, \ldots, r_m$ sont les inversibles modulo n, les $ar_1, \ldots, ar_m$ en sont une permutation.)

d) Retrouver le résultat de l'exercice précédent, $7^{2026} \equiv 49 \pmod{100}$, à l'aide d'Euler.

Exercice 3 – Inverse modulaire par Bézout

a) Justifier que 17 est inversible modulo 31.

b) Déterminer une relation de Bézout entre 17 et 31 par l'algorithme d'Euclide, et en déduire l'inverse de 17 modulo 31.

c) Résoudre $17x \equiv 5 \pmod{31}$.

d) Résoudre le système $17x + 3y \equiv 1$, $x - y \equiv 0 \pmod{31}$.

Exercice 4 – Le problème de Sunzi

« Un nombre laisse le reste 2 quand on le divise par 3, le reste 3 par 5, et le reste 2 par 7. Quel est-il ? » (Sunzi, III^{e} siècle)

a) Justifier par le théorème chinois qu'il existe une unique solution modulo 105.

b) Trouver e_1, e_2, e_3 tels que $e_1 \equiv 1$ [3], $e_1 \equiv 0$ [5], $e_1 \equiv 0$ [7], et de même pour e_2 (rôle de 5) et e_3 (rôle de 7).

c) En déduire la solution $x = 2e_1 + 3e_2 + 2e_3$ réduite modulo 105.

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).

d) Une armée compte entre 1 000 et 1 100 soldats ; rangés par 3, il en reste 2 ; par 5, il en reste 3 ; par 7, il en reste 2. Combien sont-ils ?

Exercice 5 – Sommes de carrés impossibles

a) Déterminer les restes possibles d'un carré modulo 4, puis modulo 8.

b) Montrer qu'un entier $n \equiv 3 \pmod 4$ n'est jamais somme de deux carrés.

c) Montrer qu'un entier $n \equiv 7 \pmod 8$ n'est jamais somme de trois carrés. Donner les trois plus petits exemples.

d) Montrer que l'équation $x^2 - 3y^2 = 2$ n'a pas de solution entière (raisonner modulo 3).

Exercice 6 – Ordre d'un élément

Soit $n \geq 2$ et a premier avec n. L'**ordre** de a modulo n est le plus petit $k \geq 1$ tel que $a^k \equiv 1 \pmod n$.

a) Justifier l'existence de l'ordre.

b) Soit d l'ordre de a. Montrer que $a^m \equiv 1 \Leftrightarrow d \mid m$ (division euclidienne de m par d). En déduire que d divise $\varphi(n)$.

c) Calculer l'ordre de chaque élément $1, \ldots, 6$ modulo 7. Lesquels sont des **générateurs** (d'ordre 6) ?

d) Quel est l'ordre de 10 modulo 7 ? En déduire la période du développement décimal de $\frac{1}{7}$.

Exercice 7 – Racine carrée de -1 modulo p

Soit p un nombre premier impair.

a) On a vu que si $x^2 \equiv -1 \pmod p$ a une solution, alors $p \equiv 1 \pmod 4$. On montre la réciproque. En utilisant le théorème de Wilson, montrer que

$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2} \right)! \right)^2 \pmod p$ (associer k et $p-k$).

b) En déduire que si $p \equiv 1 \pmod 4$, alors $x = \left(\frac{p-1}{2} \right)!$ vérifie $x^2 \equiv -1 \pmod p$.

c) Application : $p = 13$. Calculer x modulo 13 et vérifier.

d) Conclure : -1 est un carré modulo p si et seulement si $p \equiv 1 \pmod 4$.

Exercice 8 – Chiffrement RSA miniature

Alice choisit $p = 5$, $q = 11$, $n = pq = 55$ et l'exposant public $e = 3$.

a) Calculer $\varphi(n)$ et vérifier que $e \wedge \varphi(n) = 1$.

b) Déterminer l'exposant secret d, inverse de e modulo $\varphi(n)$.

c) Bob chiffre le message $m = 7$ en $c = m^e \bmod n$. Calculer c.

d) Alice déchiffre en calculant $c^d \bmod n$. Vérifier qu'elle retrouve 7, puis justifier en général que $m^{ed} \equiv m \pmod n$ lorsque $m \wedge n = 1$.

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 9 – Critère de divisibilité par 7

Tout entier $n \geq 10$ s'écrit $n = 10a + b$ avec $b \in \{0, \dots, 9\}$ (chiffre des unités).

a) Montrer que $7 \mid 10a + b \Leftrightarrow 7 \mid a - 2b$ (on remarquera que $-2 \times 10 \equiv 1 \pmod 7$).

b) Tester la divisibilité de 2 023 et de 4 165 par 7 en itérant le critère.

c) Établir un critère analogue pour 13 : $13 \mid 10a + b \Leftrightarrow 13 \mid a + 4b$.

d) Montrer que $1\,001 = 7 \times 11 \times 13$ et en déduire un critère simultané pour 7, 11 et 13 par tranches de trois chiffres.

Exercice 10 – Calendrier perpétuel

Le 28 septembre 2026 est un lundi. On numérote les jours de la semaine de 0 (lundi) à 6 (dimanche).

a) Justifier qu'une année non bissextile décale le jour de la semaine d'une date de 1, et une année bissextile de 2 (quand le 29 février est franchi).

b) Quel jour sera le 28 septembre 2030 ? (Seule 2028 est bissextile entre les deux dates.)

c) Quel jour de la semaine tombera le 28 septembre 2126, cent ans plus tard ? (On compte 24 années bissextiles dans l'intervalle.)

d) Montrer qu'une date donnée retombe le même jour de la semaine au bout de 400 ans (cycle grégorien de 146 097 jours).

Exercice 11 – Suites périodiques modulo m

a) Soit $f : \{0, \dots, m-1\} \to \{0, \dots, m-1\}$ et $u_{n+1} = f(u_n)$. Montrer que la suite (u_n) est **périodique à partir d'un certain rang** (principe des tiroirs).

b) Pour la suite de Fibonacci modulo 3 ($F_0 = 0$, $F_1 = 1$, $F_{n+2} \equiv F_{n+1} + F_n$), le couple (F_n, F_{n+1}) ne peut prendre que 9 valeurs. En déduire que la suite est périodique, puis calculer sa période.

c) En déduire le reste de F_{2026} modulo 3.

d) Pour quels n le nombre F_n est-il divisible par 3 ?

Exercice 12 – Nombres pseudo-premiers

a) Vérifier que $341 = 11 \times 31$ et que $2^{10} \equiv 1 \pmod{341}$.

b) En déduire que $2^{340} \equiv 1 \pmod{341}$. Que peut-on en conclure sur la réciproque du petit théorème de Fermat ?

c) Calculer 3^{340} modulo 11 et modulo 31 (Fermat), puis dire si $3^{340} \equiv 1 \pmod{341}$.

d) Expliquer pourquoi le « test de Fermat » avec plusieurs bases est un test de **non-primalité** et non de primalité.

Exercice 13 – Diviseurs de zéro dans Z/12Z

On travaille dans $\mathbb{Z}/12\mathbb{Z}$.

a) Donner deux classes non nulles dont le produit est nul. L'anneau est-il intègre ?

b) Déterminer les éléments inversibles et leurs inverses. Vérifier que leur nombre est

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).

$\varphi(12)$.

c) Résoudre dans $\mathbb{Z}/12\mathbb{Z}$: $x^2 = \overline{1}$. Combien de solutions ? Comparer avec un corps.

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

Exercice 14 – Cubes modulo 9

a) Montrer que tout cube est congru à 0, 1 ou -1 modulo 9.

b) En déduire les restes possibles de $x^3 + y^3 + z^3$ modulo 9.

c) Montrer que $x^3 + y^3 + z^3 = 2\,030$ n'a pas de solution entière. Qu'en est-il pour $2\,026$?

d) Montrer que $n^3 + (n+1)^3 + (n+2)^3$ est toujours divisible par 9.

Exercice 15 – Synthèse : clé de contrôle ISBN

Un ISBN-13 est une suite de 13 chiffres $a_1 a_2 \cdots a_{13}$ telle que

$$S = a_1 + 3a_2 + a_3 + 3a_4 + \ldots + 3a_{12} + a_{13} \equiv 0 \pmod{10}$$

(poids 1 et 3 alternés ; a_{13} est la **clé de contrôle**).

a) Calculer la clé du livre dont les douze premiers chiffres sont 978 2 7011 9361.

b) Montrer qu'une **erreur sur un seul chiffre** est toujours détectée.

c) Montrer que l'échange de deux chiffres **voisins** $a_i \neq a_{i+1}$ est détecté si et seulement si $|a_i - a_{i+1}| \neq 5$.

d) Pourquoi un poids 2 à la place de 3 serait-il un mauvais choix ?

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).