Leçon : Congruences dans $\mathbb{Z}$

Préparation à l'oral du CAPES de mathématiques

Table des matières

1 Prérequis et objectifs **1**

2 Définition et premières propriétés **1**
2.1 Définition 1
2.2 Lien avec la division euclidienne 2
2.3 Propriétés de la relation de congruence 2

3 Règles de calcul **2**
3.1 Compatibilité avec les opérations 2
3.2 Attention à la simplification 3

4 Résolution des congruences linéaires **4**
4.1 Équation de la forme $ax \equiv b \pmod{n}$ 4
4.2 Inverse modulo n et identité de Bézout 5

5 Applications arithmétiques **5**
5.1 Critères de divisibilité 5
5.2 Étude d'une parité 5
5.3 Résolution de systèmes : théorème chinois 6
5.4 Petit théorème de Fermat 6

6 Interprétation algébrique **6**
6.1 Classes d'équivalence 6
6.2 Structure de $\mathbb{Z}/n\mathbb{Z}$ 7

7 Liste d'exercices **7**

8 Éléments de correction de quelques exercices **8**

9 Conclusion **9**

10 Références bibliographiques **9**

1 Prérequis et objectifs

Prérequis

Cette leçon mobilise les connaissances suivantes :

— la division euclidienne dans $\mathbb{Z}$;

— les notions de multiple et de diviseur ;

— le calcul algébrique dans $\mathbb{Z}$;

— le PGCD et les propriétés de divisibilité ;

— les opérations élémentaires sur les entiers ;

— les notions de relation d'équivalence et de classe d'équivalence, dans une perspective plus théorique.

Objectifs

L'objectif principal est d'introduire les congruences comme un outil permettant de raisonner sur les restes de divisions euclidiennes. On cherchera à :

— définir la congruence modulo un entier non nul ;

— établir ses propriétés fondamentales ;

— justifier les règles de calcul sur les congruences ;

— résoudre des congruences linéaires ;

— utiliser les congruences pour étudier la divisibilité, les chiffres d'un entier et les problèmes arithmétiques ;

— présenter le lien entre congruences, classes d'équivalence et anneaux quotients.

Les congruences constituent à la fois un outil de calcul élémentaire et une première rencontre avec les structures algébriques quotient.

2 Définition et premières propriétés

2.1 Définition

Définition 2.1. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est congru à b modulo n, et l'on écrit

$$a \equiv b \pmod{n},$$

si et seulement si

$$n \mid (a - b).$$

Autrement dit, il existe $k \in \mathbb{Z}$ tel que

$$a - b = kn.$$

Exemple 2.2. On a

$$23 \equiv 5 \pmod{9},$$

car $23 - 5 = 18$ est divisible par 9.

De même,

$$-7 \equiv 3 \pmod{10},$$

car $-7 - 3 = -10$ est un multiple de 10.

2.2 Lien avec la division euclidienne

Théorème 2.3. *Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Les deux propriétés suivantes sont équivalentes :*

1. *$a \equiv b \pmod{n}$;*
2. *a et b ont le même reste dans la division euclidienne par n.*

Démonstration. Supposons $a \equiv b \pmod{n}$. Écrivons les divisions euclidiennes

$$a = q_1 n + r_1, \qquad b = q_2 n + r_2,$$

avec $0 \leq r_1, r_2 < n$.

Alors

$$a - b = (q_1 - q_2)n + (r_1 - r_2).$$

Puisque n divise $a - b$, il divise $r_1 - r_2$. Or $-(n-1) \leq r_1 - r_2 \leq n - 1$. Le seul multiple de n dans cet intervalle est 0. Ainsi $r_1 = r_2$.

Réciproquement, si $r_1 = r_2$, alors

$$a - b = (q_1 - q_2)n,$$

donc $n \mid (a - b)$ et $a \equiv b \pmod{n}$. □

Corollaire 2.4. Tout entier a est congru modulo n à un unique entier $r \in \{0, 1, \ldots, n-1\}$. Cet entier est le reste de la division euclidienne de a par n.

2.3 Propriétés de la relation de congruence

Propriété 2.5. *Pour tout $n \in \mathbb{N}^*$, la congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Démonstration.
- Réflexivité : $a - a = 0$ est divisible par n, donc $a \equiv a \pmod{n}$.
- Symétrie : si $n \mid (a - b)$, alors $n \mid (b - a)$; ainsi $b \equiv a \pmod{n}$.
- Transitivité : si $n \mid (a - b)$ et $n \mid (b - c)$, alors $n \mid [(a - b) + (b - c)] = a - c$. Donc $a \equiv c \pmod{n}$.

□

Remarque 2.6. La congruence modulo 1 est toujours vérifiée : tous les entiers sont congrus modulo 1.

3 Règles de calcul

3.1 Compatibilité avec les opérations

Théorème 3.1. *Soient $a, b, c, d \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si*

$$a \equiv b \pmod{n} \quad \text{et} \quad c \equiv d \pmod{n},$$

alors :

1. $a + c \equiv b + d \pmod{n}$;
2. $a - c \equiv b - d \pmod{n}$;
3. $ac \equiv bd \pmod{n}$;
4. *pour tout $k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$.*

Démonstration. Il existe $u, v \in \mathbb{Z}$ tels que

$$a - b = un, \qquad c - d = vn.$$

Alors

$$(a + c) - (b + d) = (u + v)n$$

et

$$(a - c) - (b - d) = (u - v)n.$$

Les deux premières propriétés en découlent.

Pour le produit,

$$ac - bd = a(c - d) + d(a - b) = (av + du)n.$$

Donc $ac \equiv bd \pmod{n}$.

Enfin, la congruence des puissances résulte d'une application répétée de la compatibilité avec le produit. □

Exemple 3.2. Calculons le reste de la division de 7^{100} par 5. Puisque

$$7 \equiv 2 \pmod 5,$$

on obtient

$$7^{100} \equiv 2^{100} \pmod 5.$$

Or $2^4 \equiv 1 \pmod 5$, donc

$$2^{100} = (2^4)^{25} \equiv 1 \pmod 5.$$

Le reste recherché est donc 1.

3.2 Attention à la simplification

Remarque 3.3. On ne peut pas simplifier systématiquement un facteur dans une congruence. Par exemple,

$$2 \cdot 1 \equiv 2 \cdot 4 \pmod 6,$$

car $2 \equiv 8 \pmod 6$, mais

$$1 \not\equiv 4 \pmod 6.$$

Théorème 3.4 (Règle de simplification)**.** *Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Si*

$$ac \equiv bc \pmod n$$

et si $\operatorname{pgcd}(c, n) = 1$*, alors*

$$a \equiv b \pmod n.$$

Démonstration. L'hypothèse donne $n \mid c(a-b)$. Comme $\operatorname{pgcd}(c, n) = 1$, le lemme de Gauss implique $n \mid (a-b)$. Ainsi $a \equiv b \pmod n$. □

Plus généralement, si $d = \operatorname{pgcd}(c, n)$, la congruence

$$ac \equiv bc \pmod n$$

implique

$$a \equiv b \pmod{n/d}.$$

4 Résolution des congruences linéaires

4.1 Équation de la forme $ax \equiv b \pmod n$

Théorème 4.1. *Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. L'équation*

$$ax \equiv b \pmod n$$

admet une solution entière si et seulement si

$$\operatorname{pgcd}(a, n) \mid b.$$

Si $d = \operatorname{pgcd}(a, n)$ divise b, cette équation possède exactement d solutions distinctes modulo n.

Démonstration. L'équation équivaut à l'existence de $k \in \mathbb{Z}$ tel que

$$ax - b = kn,$$

soit

$$ax - kn = b.$$

Tout diviseur commun de a et de n divise donc b : la condition est nécessaire.

Réciproquement, si $d = \text{pgcd}(a, n)$ divise b, écrivons

$$a = da', \quad n = dn', \quad b = db',$$

avec $\text{pgcd}(a', n') = 1$. L'équation devient

$$a'x \equiv b' \pmod{n'}.$$

Puisque a' est premier avec n', il est inversible modulo n', donc cette dernière équation possède une unique solution modulo n'.

Cette classe modulo n' correspond à exactement d classes modulo n, ce qui établit le résultat. □

Exemple 4.2. Résolvons

$$6x \equiv 8 \pmod{14}.$$

Comme $\text{pgcd}(6, 14) = 2$ divise 8, il existe des solutions. En divisant par 2, on obtient

$$3x \equiv 4 \pmod{7}.$$

Or $3^{-1} \equiv 5 \pmod{7}$, car $3 \cdot 5 \equiv 1 \pmod{7}$. Par conséquent,

$$x \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod{7}.$$

Les solutions modulo 14 sont donc

$$\boxed{x \equiv 6 \pmod{7}},$$

c'est-à-dire $x \equiv 6$ ou $x \equiv 13 \pmod{14}$.

4.2 Inverse modulo n et identité de Bézout

Théorème 4.3. *Un entier a possède un inverse multiplicatif modulo n, c'est-à-dire un entier u tel que*

$$au \equiv 1 \pmod{n},$$

si et seulement si $\text{pgcd}(a, n) = 1$.

Démonstration. Si $au \equiv 1 \pmod{n}$, il existe $k \in \mathbb{Z}$ tel que $au - kn = 1$. Tout diviseur commun de a et de n divise donc 1 : le PGCD vaut 1.

Réciproquement, si $\text{pgcd}(a, n) = 1$, le théorème de Bézout donne des entiers u, v tels que

$$au + nv = 1.$$

Ainsi $au \equiv 1 \pmod{n}$. □

Exemple 4.4. Résolvons

$$5x \equiv 3 \pmod{11}.$$

Comme $5 \cdot 9 = 45 \equiv 1 \pmod{11}$, l'inverse de 5 modulo 11 est 9. Il vient

$$x \equiv 9 \cdot 3 \equiv 27 \equiv 5 \pmod{11}.$$

5 Applications arithmétiques

5.1 Critères de divisibilité

Les congruences permettent de retrouver les critères de divisibilité usuels.

Propriété 5.1. *Soit*

$$N = \sum_{i=0}^{r} a_i 10^i$$

l'écriture décimale d'un entier naturel, où $a_i \in \{0, \dots, 9\}$.

1. *Comme* $10 \equiv 1 \pmod 9$*, on a*

$$N \equiv \sum_{i=0}^{r} a_i \pmod 9.$$

   Un entier est donc divisible par 9 *si et seulement si la somme de ses chiffres l'est.*

2. *De même,* $10 \equiv 1 \pmod 3$*, donc le même critère vaut modulo* 3*.*

3. *Comme* $10 \equiv -1 \pmod{11}$*, on a*

$$N \equiv \sum_{i=0}^{r} (-1)^i a_i \pmod{11}.$$

   La divisibilité par 11 *se teste à l'aide de la somme alternée des chiffres.*

5.2 Étude d'une parité

Exemple 5.2. Tout carré entier est congru à 0 ou 1 modulo 4.

En effet, si n est pair, il existe $k \in \mathbb{Z}$ tel que $n = 2k$, donc $n^2 = 4k^2 \equiv 0 \pmod 4$.

Si n est impair, on peut écrire $n = 2k + 1$, d'où

$$n^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4.$$

En particulier, un entier congru à 2 modulo 4 ne peut pas être un carré parfait.

5.3 Résolution de systèmes : théorème chinois

Théorème 5.3 (Théorème chinois des restes)**.** *Soient* $m, n \in \mathbb{N}^*$ *tels que* $\text{pgcd}(m, n) = 1$*. Pour tous* $a, b \in \mathbb{Z}$*, le système*

$$\begin{cases} x \equiv a \pmod m, \\ x \equiv b \pmod n \end{cases}$$

admet une solution unique modulo mn*.*

Exemple 5.4. Résolvons

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 3 \pmod 5. \end{cases}$$

Écrivons $x = 2 + 3k$. La seconde congruence donne

$$2 + 3k \equiv 3 \pmod 5,$$

donc $3k \equiv 1 \pmod 5$. Comme $3^{-1} \equiv 2 \pmod 5$, on obtient

$$k \equiv 2 \pmod 5.$$

Ainsi

$$\boxed{x \equiv 8 \pmod{15}}.$$

5.4 Petit théorème de Fermat

Théorème 5.5 (Petit théorème de Fermat)**.** *Si p est un nombre premier et $a \in \mathbb{Z}$, alors*

$$a^p \equiv a \pmod{p}.$$

En particulier, si $p \nmid a$, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Remarque 5.6. Ce résultat permet notamment de réduire certaines puissances modulo un nombre premier. Sa démonstration peut s'appuyer sur le fait que, pour $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k}$ est divisible par p, ou sur la permutation des classes non nulles modulo p par multiplication par a.

6 Interprétation algébrique

6.1 Classes d'équivalence

Pour $a \in \mathbb{Z}$, la classe de a modulo n est

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = a + n\mathbb{Z}.$$

L'ensemble des classes d'équivalence est noté

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

Il possède exactement n éléments :

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}.$$

6.2 Structure de $\mathbb{Z}/n\mathbb{Z}$

Les opérations sont définies par

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a}\,\overline{b} = \overline{ab}.$$

La compatibilité des congruences avec l'addition et la multiplication garantit que ces opérations ne dépendent pas du choix des représentants.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire. Il est un corps si et seulement si n est premier.

En effet, si n est premier, tout entier non nul modulo n est premier avec n et possède donc un inverse. Si n est composé, on peut écrire $n = ab$ avec $1 < a < n$ et $1 < b < n$; les classes de a et de b sont non nulles mais leur produit est nul. L'anneau possède alors des diviseurs de zéro et n'est pas un corps.

7 Liste d'exercices

Les exercices suivants permettent de travailler les calculs, les démonstrations et les applications des congruences.

Exercice 1 – Calculs élémentaires

Déterminer le reste de la division euclidienne de chacun des entiers suivants par le module indiqué :

$$2026 \pmod{7}, \qquad 3^{20} \pmod{7}, \qquad 2^{100} \pmod{13}.$$

Justifier chaque résultat à l'aide de congruences.

Exercice 2 – Critères de divisibilité

a) Démontrer le critère de divisibilité par 9.

b) Établir le critère de divisibilité par 11.

c) Utiliser ces critères pour tester la divisibilité de 123456789 par 9 et par 11.

Exercice 3 – Carrés modulo un entier

a) Déterminer les carrés possibles modulo 8.

b) Montrer que l'équation $x^2 \equiv 3 \pmod 8$ n'a pas de solution.

c) En déduire qu'il n'existe pas d'entier x tel que $x^2 = 8k + 3$, avec $k \in \mathbb{Z}$.

Exercice 4 – Congruence linéaire

Résoudre dans $\mathbb{Z}$ les congruences suivantes :

$$7x \equiv 4 \pmod{15}, \qquad 12x \equiv 8 \pmod{20}, \qquad 6x \equiv 5 \pmod{15}.$$

Pour chacune, préciser si une solution existe et donner l'ensemble des solutions.

Exercice 5 – Inverses modulo n

Déterminer les inverses multiplicatifs, lorsqu'ils existent, des entiers suivants :

$$7 \pmod{12}, \qquad 8 \pmod{15}, \qquad 9 \pmod{21}.$$

Justifier l'existence ou l'absence de chaque inverse.

Exercice 6 – Théorème chinois des restes

Résoudre les systèmes :

$$\begin{cases} x \equiv 1 \pmod 4, \\ x \equiv 2 \pmod 5, \end{cases} \qquad \begin{cases} x \equiv 3 \pmod 7, \\ x \equiv 4 \pmod 9. \end{cases}$$

Dans chaque cas, donner la solution modulo le produit des deux modules.

Exercice 7 – Une impossibilité arithmétique

Montrer que l'équation

$$x^2 + y^2 = 4z + 3$$

n'admet aucune solution dans $\mathbb{Z}^3$.

Exercice 8 – Puissances et périodicité

Déterminer le reste de la division de 2026^{2026} par 13. On cherchera d'abord une puissance de 2026 congrue à 1 modulo 13.

Exercice 9 – Petit théorème de Fermat

a) Calculer le reste de 2^{100} modulo 17.

b) Démontrer que si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod p$.

Exercice 10 – Structure de $\mathbb{Z}/n\mathbb{Z}$

a) Déterminer les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$.

b) Déterminer les diviseurs de zéro de $\mathbb{Z}/12\mathbb{Z}$.

c) Expliquer pourquoi $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps.

8 Éléments de correction de quelques exercices

Correction de l'exercice 1

On a $2026 = 7 \cdot 289 + 3$, donc le reste est 3.
Comme $3^6 \equiv 1 \pmod 7$, on obtient

$$3^{20} = 3^{18} \cdot 3^2 \equiv (3^6)^3 \cdot 9 \equiv 2 \pmod 7.$$

Modulo 13, on a $2^{12} \equiv 1 \pmod{13}$. Ainsi

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 16 \equiv 3 \pmod{13}.$$

Correction de l'exercice 3

Les carrés des classes modulo 8 sont :

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 1 \pmod 8.$$

En poursuivant pour les classes $4, 5, 6, 7$, on retrouve uniquement les restes $0, 1, 4$. La congruence $x^2 \equiv 3 \pmod 8$ est donc impossible.

Correction de l'exercice 4

Pour $7x \equiv 4 \pmod{15}$, l'inverse de 7 modulo 15 est 13, car $7 \cdot 13 = 91 \equiv 1 \pmod{15}$. Ainsi

$$x \equiv 13 \cdot 4 \equiv 7 \pmod{15}.$$

Pour $12x \equiv 8 \pmod{20}$, le PGCD vaut 4 et divise 8. En divisant par 4, on obtient

$$3x \equiv 2 \pmod 5.$$

L'inverse de 3 modulo 5 est 2, donc $x \equiv 4 \pmod 5$. Les solutions modulo 20 sont $x \equiv 4, 9, 14, 19 \pmod{20}$.

Enfin, $6x \equiv 5 \pmod{15}$ n'a aucune solution, car $\text{pgcd}(6, 15) = 3$ ne divise pas 5.

Correction de l'exercice 7

Tout carré entier est congru à 0 ou 1 modulo 4. La somme de deux carrés est donc congrue à 0, 1 ou 2 modulo 4, jamais à 3. L'équation est impossible.

9 Conclusion

La congruence modulo n formalise l'idée de travailler sur les restes de divisions euclidiennes. Elle permet de simplifier des calculs arithmétiques, de démontrer des critères de divisibilité, d'étudier des équations diophantiennes et de résoudre des systèmes de congruences.

Sur le plan algébrique, elle conduit à la construction de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$. Ce point de vue unifie les règles de calcul et met en évidence le rôle du PGCD dans l'existence des inverses et la résolution des congruences linéaires.

À l'oral du CAPES, il est important de distinguer les résultats élémentaires directement accessibles à partir de la division euclidienne des résultats plus avancés, comme le théorème chinois des restes et le petit théorème de Fermat, dont les hypothèses doivent être clairement énoncées.

10 Références bibliographiques

Références

[1] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers*, 6^{e} édition, Oxford University Press, 2008. Référence classique pour l'arithmétique des entiers, les congruences et les théorèmes de Fermat.

[2] M. Demazure, *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, Paris. Ouvrage de référence pour les aspects algébriques et arithmétiques des entiers.

[3] X. Gourdon, *Les maths en tête : Algèbre*, Ellipses, Paris. Pour les outils d'algèbre et les méthodes de démonstration.

[4] Euclide, *Les Éléments*, livre VII. Source historique pour les notions de divisibilité et d'arithmétique des entiers.

[5] Ministère de l'Éducation nationale, *Programmes de mathématiques du lycée général et technologique*. Ressource institutionnelle pour situer les congruences dans les apprentissages du secondaire. Disponible sur : https://eduscol.education.fr/.

[6] J.-M. Arnaudiès et H. Fraysse, *Cours de mathématiques, tome 1 : Algèbre*, Dunod. Pour les structures algébriques, les anneaux quotients et les propriétés des classes de congruence.