Divisibilité et congruences dans Z

Introduction :

Ce premier cours d'arithmétique concerne les congruences dans $\mathbb{Z}$: en partant de la notion de divisibilité dans $\mathbb{Z}$ et en utilisant la division euclidienne – qui ont toutes les deux été vues au collège –, nous allons définir la notion de congruences dans $\mathbb{Z}$ et en donner les principales propriétés.

Dans un premier temps, nous allons revoir la notion de divisibilité dans $\mathbb{Z}$ et la division euclidienne qui sera étendue aux nombres entiers relatifs. Nous verrons la notion de congruences dans $\mathbb{Z}$, qui est une nouveauté, et ses principales propriétés.

1 Divisibilité dans $\mathbb{Z}$

a. Définitions

Commençons par quelques rappels simples, étendus à l'ensemble des entiers relatifs.

Définition

Divisibilité dans $\mathbb{Z}$:

Soit a et b des entiers relatifs, b étant non nul. On dit que b est un diviseur de a, et on note $b|a$, lorsqu'il existe un entier relatif k tel que $a = k \times b$.

→ On peut dire aussi que :

- a est divisible par b ;

- a est un multiple de b ;
- b divise a.

À retenir

- Les diviseurs de 1 ou -1 sont -1 et 1.
- 1 et -1 sont des diviseurs de n'importe quel entier relatif.
- 0 est multiple de n'importe quel entier relatif, et ne divise aucun entier relatif.
- Les entiers relatifs pairs sont les multiples de 2, c'est-à-dire ceux qui s'écrivent sous la forme $2k$ avec $k \in \mathbb{Z}$.
- Les entiers relatifs impairs sont les entiers qui ne sont pas multiples de 2, c'est-à-dire ceux qui s'écrivent sous la forme $2k+1$ avec $k \in \mathbb{Z}$.

Rappelons aussi les règles de divisibilité.

À retenir

- Un entier relatif est **divisible par** 2 si et seulement si son chiffre des unités est 0, 2, 4, 6 ou 8.
- Un entier relatif est **divisible par** 3 si et seulement si la somme de ses chiffres est divisible par 3.
- Un entier relatif est **divisible par** 4 si et seulement si le nombre formé par son chiffre des dizaines et celui des unités est divisible par 4.
- Un entier relatif est **divisible par** 5 si et seulement si son chiffre des unités est 0 ou 5.
- Un entier relatif est **divisible par** 9 si et seulement si la somme de ses chiffres est divisible par 9.
- Un entier relatif est **divisible par** 10 si et seulement si son chiffre des unités est 0.

b. Propriétés

Revoyons maintenant les principales propriétés de la divisibilité dans l'ensemble $\mathbb{Z}$.

Propriété

Transitivité :

Soit a, b et c des entiers relatifs.
Si b divise a et si c divise b, alors c divise a.

Démonstration

Comme b divise a, il existe un entier relatif k tel que $a = bk$.
Comme c divise b, il existe un entier relatif k' tel que $b = ck'$.

Ainsi, nous avons :

$$\begin{aligned} a &= bk \\ &= (ck')k \\ &= c(k'k) \\ &= cK \ (\text{avec } K = kk') \end{aligned}$$

K étant le produit deux entiers relatifs, c'est un entier relatif.

→ c divise a.

Propriété

Combinaisons linéaires entières :

Soit a, b et c des entiers relatifs.
Si c divise a et b, alors pour tous les entiers relatifs n et n', c divise $na + n'b$.

À retenir

Autrement dit, si c divise a et b, alors il divise toutes les combinaisons linéaires entières de a et b.

Démonstration

Comme c divise a et b, il existe deux entiers relatifs k et k' tels que $a = kc$ et $b = k'c$.

Alors, avec n et n' deux entiers relatifs :

$$\begin{aligned} na + n'b &= n(kc) + n'(k'c) \\ &= (nk + n'k')c \\ &= Kc \text{ (avec } K = nk + n'k') \end{aligned}$$

K étant la somme de deux produits d'entiers relatifs, c'est un entier relatif.

→ Ainsi, c divise $na + n'b$.

2 Division euclidienne

Après avoir revu la notion de divisibilité dans $\mathbb{Z}$, revoyons la division euclidienne, que nous allons étendre aux nombres entiers relatifs.

a. Définitions

Définition

Division euclidienne :

Soit a et b deux entiers naturels avec b non nul.
Il existe un unique couple (q, r) d'entiers naturels tels que :

$$a = bq + r \text{ et } 0 \leq r < b$$

→ L'entier naturel a est le dividende et b est le diviseur.

→ L'entier naturel q s'appelle le quotient et r s'appelle le reste de la division euclidienne de a par b.

Exemple

- La division euclidienne de 343 par 12 donne :

$$343 = 12 \times 28 + 7 \text{ (avec } 0 \leq 7 < 12)$$

- La division euclidienne de $1\,526$ par 11 donne :

$$1\,526 = 11 \times 138 + 8 \text{ (avec } 0 \leq 8 < 11)$$

Nous pouvons étendre la division euclidienne sur les entiers naturels à celle d'un entier relatif par un entier naturel non nul.

Propriété

Soit a un entier relatif et $b \neq 0$ un entier naturel.
Il existe un unique couple (q, r), avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$, tels que :

$$a = bq + r \text{ et } 0 \leq r < b$$

Une différence entre la division euclidienne d'un élément de $\mathbb{Z}$ et la division euclidienne d'un élément de $\mathbb{N}$ est que le quotient peut être négatif.

Exemple

- La division euclidienne de -431 par 17 donne :

$$-431 = \underbrace{17}_{b} \times \underbrace{(-26)}_{q<0} + \underbrace{11}_{r} \text{ (avec } 0 \leq 11 < 17)$$

- La division euclidienne de -121 par 9 :

$$-121 = 9 \times (-14) + 5 \text{ (avec } 0 \leq 5 < 9)$$

b. Une application dans la vie quotidienne

On se sert par exemple de la division euclidienne lorsque qu'on nous attribue notre numéro de Sécurité sociale.
Ce numéro est constitué de 15 chiffres :

1. le premier chiffre est 1 s'il s'agit d'un homme, 2 s'il s'agit d'une femme ;
2. les deux chiffres suivants sont les deux derniers chiffres de l'année de naissance ;
3. viennent ensuite les deux chiffres du mois de naissance ;
4. les cinq chiffres suivants désignent le lieu de naissance (numéro du département et code de la commune de naissance, ou 99 si la naissance est à l'étranger, suivi du code du pays) ;
5. les trois chiffres d'après désignent le numéro d'ordre de la naissance dans le mois et la commune ;
6. les deux derniers chiffres enfin résultent d'un calcul.

→ Voici comment faire ce calcul.

Il faut effectuer la division euclidienne des 13 premiers chiffres par 97. Ensuite, on calcule la différence entre 97 et le reste obtenu. On a ainsi les deux derniers chiffres, qui constituent une clé de contrôle.

→ Le calcul du numéro de Sécurité sociale fait donc appel à la division euclidienne.

Astuce

La clé est comprise entre 01 et 97 (ne pas prendre le reste lui-même permet d'éviter d'avoir une clé nulle).

→ Il s'agit d'un code correcteur d'erreur, très utilisé en informatique, qui permet de localiser une erreur et même de la corriger.

> Pour avoir un exemple, très simplifié, d'un code correcteur, vous pouvez regarder ce petit cours sur le code de Hamming $(7,\ 4,\ 3)$.

La divisibilité dans $\mathbb{Z}$ et la division euclidienne de deux entiers relatifs vont nous permettre de travailler sur une nouvelle notion, qui est la **congruence** dans $\mathbb{Z}$.

3 Congruences dans $\mathbb{Z}$

Commençons par donner la définition de cette nouvelle notion.

a. Définition

Regardons la suite de nombres suivante :

$$-11 \xrightarrow{+3} -8 \xrightarrow{+3} -5 \xrightarrow{+3} -2 \xrightarrow{+3} 1 \xrightarrow{+3} 4 \xrightarrow{+3} 7 \xrightarrow{+3} 10$$

Si l'on prend 2 nombres, n'importe lesquels, parmi cette suite, nous voyons facilement que leur différence sera toujours un multiple de 3.

1. Par exemple, nous voyons que, pour « passer » de -8 à 7, nous ajoutons 5 fois 3 :

$$-8 + 5 \times 3 = 7 \Leftrightarrow 7 - (-8) = 5 \times 3$$

2. Pour autre exemple, nous voyons que, pour « passer » de 1 à -5, nous soustrayons 2 fois 3 :

$$1 - 2 \times 3 = -5 \Leftrightarrow -5 - 1 = -2 \times 3$$

Comme ils sont égaux à un multiple de 3 près, on dit que :

1. 7 et -8 sont congrus modulo 3 ;
2. -5 et 1 sont congrus modulo 3.

Définition

> **Congruence :**

n désigne un entier naturel non nul, a et b sont des entiers relatifs.
On dit que a et b sont congrus modulo n lorsque la différence $a - b$ est un multiple de n, ou bien que n divise $a - b$, ce qui est équivalent.

→ On dit aussi que a et b sont égaux modulo n.

Les notations possibles sont les suivantes :

- $a \equiv b \bmod n$,
- ou $a \equiv b\,(n)$,
- ou encore $a \equiv b\,[n]$.

→ Dans ce cours, nous choisissons d'utiliser cette dernière notation.

À retenir

- Si $a \equiv b\,[n]$, avec a et b des entiers relatifs, et n un entier naturel non nul, alors, pour tout $k \in \mathbb{Z}$:

$$k + a \equiv k + b\,[n]$$

$$ka \equiv kb\,[n]$$
$$-a \equiv -b\,[n] \text{ (avec } k = -1)$$

- La relation de congruence est **symétrique**, c'est-à-dire que, si $a \equiv b\,[n]$, on a aussi $b \equiv a\,[n]$.

→ En effet, si $a - b$ est un multiple de n, $b - a$ est aussi un multiple de n.

- Dernier point, la relation de congruence est **réflexive**, c'est-à-dire qu'on a toujours $a \equiv a\,[n]$.

Prenons quelques exemples pour comprendre cette notion.

Exemple

1 $-19 - (-4) = -15$.

Le nombre -15 est un multiple de 5, donc -19 et -4 sont congrus modulo 5 :

$$-19 \equiv -4\,[5]$$

2 $-16-(-1)=-15$.

Donc -16 et -1 sont congrus modulo 5 :

$$-16 \equiv -1\,[5]$$

Pour utiliser les propriétés vues plus haut, nous pouvons aussi le déduire de la relation 1 :

$$\begin{aligned} -19 \equiv -4\,[5] &\Leftrightarrow -19+3 \equiv -4+3\,[5] \\ &\Leftrightarrow -16 \equiv -1\,[5] \\ &\quad (\text{car, si } a \equiv b\,[n], \text{ alors } a+k \equiv b+k\,[n]) \\ &\Leftrightarrow 16 \equiv 1\,[5] \\ &\quad (\text{car, si } a \equiv b\,[n], \text{ alors } -a \equiv -b\,[n]) \\ &\Leftrightarrow 1 \equiv 16\,[5] \ (\text{par symétrie}) \end{aligned}$$

3 $8-16=-8$.

Le nombre -8 n'est pas un multiple de 5, donc 8 et 16 ne sont pas congrus modulo 5 :

$$8 \not\equiv 16\,[5]$$

En revanche, -8 est un multiple de 4, donc 8 et 16 sont congrus modulo 4.

Les « raccourcis » suivants sont à connaître.

À retenir

- Un entier relatif est congru à 0 modulo n si et seulement si ce nombre est un multiple de n.

→ Par exemple 25 est congru à 0 modulo 5 : $25 \equiv 0\,[5]$.

- Tout nombre pair est congru à 0 modulo 2, et tout nombre impair est congru à 1 modulo 2. On a donc :

→ $1\,235$ est congru à 1 modulo 2 : $1\,235 \equiv 1\,[2]$;

→ $1\,236$ est congru à 0 modulo 2 : $1\,236 \equiv 0\,[2]$.

- Tout entier relatif est congru à son chiffre des unités modulo 10.

→ $35\,794$ est congru à 4 modulo 10 : $35\,794 \equiv 4\,[10]$.

b. Lien entre congruences et division euclidienne

Maintenant que nous savons ce qu'est la congruence, voyons son lien avec la division euclidienne revue en début de cours.

Propriété

Pour un entier naturel non nul n, tout entier relatif est congru modulo n au reste de sa division euclidienne par n.

Démonstration

Si on effectue la division euclidienne d'un entier relatif a par un entier naturel non nul n, on sait qu'il existe q appartenant à l'ensemble des entiers relatifs $\mathbb{Z}$ et r appartenant à l'ensemble des entiers naturels $\mathbb{N}$ tels que $a = qn + r$, avec $0 \leq r < n$.
On a alors $a - r = qn$.

→ Donc $a - r$ est un multiple de n et ainsi a est congru à r modulo n.

Par conséquent, il advient la propriété suivante pour deux entiers relatifs a et b.

Propriété

- a et b sont congrus modulo n si et seulement si a et b ont le même reste dans la division euclidienne par n.

- Si $a \equiv r\,[n]$ avec r tel que $0 \leq r < n$, alors r est le reste de la division euclidienne de a par n.

Prenons deux exemples pour illustrer ces propriétés.

Exemple

Avec la division euclidienne de 551 par 26, on obtient : $551 = 21 \times 26 + 5$.

→ Donc 551 est congru à 5 modulo 26 :

$$551 \equiv 5\,[26]$$

Avec la division euclidienne de 189 par 35, on obtient : $189 = 5 \times 35 + 14$.

→ Donc 189 est congru à 14 modulo 35 :

$$189 \equiv 14\,[35]$$

Voyons maintenant les principales propriétés de la congruence dans $\mathbb{Z}$.

c. Propriétés

Soit un entier naturel non nul n et cinq entiers relatifs a, b, c, a' et b'.

Propriété

- Si on a $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors :

$$a \equiv c\,[n]$$

→ C'est la **transitivité**.

- Si on a $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$, alors :

$$a + a' \equiv b + b' \,[n]$$
$$a - a' \equiv b - b' \,[n]$$

→ On dit que la congruence est compatible avec l'addition (et la soustraction).

 Exemple

$-13 \equiv -8 \,[5]$ et $46 \equiv 21 \,[5]$, donc :

$$33 \equiv 13 \,[5]$$
$$-59 \equiv -29 \,[5]$$

Les réponses données dans l'exemple ci-dessus sont justes.
Il est tout de même préférable, et fortement recommandé, de se ramener à une congruence $b \,[n]$ où $0 \leq b < n$.

→ Cela se justifie par le lien entre congruence et division euclidienne.

Pour cela, nous utilisons la propriété – évidente mais à ne jamais oublier – suivante.

 Propriété

Avec k un entier relatif :

$$a + kn \equiv a \,[n]$$

 Exemple

Ainsi, en reprenant les résultats de l'exemple précédent, nous obtenons :

$$\begin{aligned} 33 &\equiv 13\,[5] \\ &\equiv 3 + 2 \times 5\,[5] \\ &\equiv 3\,[5] \end{aligned}$$

$$\begin{aligned} -59 &\equiv -29\,[5] \\ &\equiv 1 - 6 \times 5\,[5] \\ &\equiv 1\,[5] \end{aligned}$$

Nous aurions aussi pu transformer les expressions dès le début, pour arriver au même résultat :

$$\begin{aligned} -13 &\equiv -8\,[5] \\ &\equiv 2 - 2 \times 5\,[5] \\ &\equiv 2\,[5] \end{aligned}$$

$$\begin{aligned} 46 &\equiv 21\,[5] \\ &\equiv 1 + 4 \times 5\,[5] \\ &\equiv 1\,[5] \end{aligned}$$

Continuons à étudier les propriétés des congruences.

Propriété

La congruence est compatible avec la multiplication.
C'est-à-dire que, si on a $a \equiv b\,[n]$ et $a' \equiv b'[n]$, alors :

$$aa' \equiv bb'\,[n]$$

Attention

Ce n'est pas valable avec la division ! Par exemple :

$$25 \equiv 5\,[10] \text{ mais } 5 \not\equiv 1\,[10]$$

De la dernière propriété, nous pouvons tirer une conséquence.

Propriété

Si on a $a \equiv b\,[n]$, alors, pour tout $p \in \mathbb{N}$:

$$a^p \equiv b^p\,[n]$$

Exemple

$7 \equiv 2\,[5]$, donc $7^2 \equiv 2^2\,[5]$, c'est-à-dire :

$$49 \equiv 4\,[5]$$

Astuce

Si on a $a \equiv -1\,[n]$, alors, pour tout $p \in \mathbb{N}$:

$$a^p \equiv (-1)^p\,[n]$$

Nous allons maintenant prendre l'exemple simple d'un raisonnement à mener dans un exercice faisant intervenir les congruences.

Exemple

Il s'agit de montrer que $6^{10} \equiv 1\,[11]$.

→ Autrement dit, pour nous figurer plus « concrètement » le raisonnement théorique, il s'agit de montrer que le reste de la division euclidienne de 6^{10} par 11 est égal à 1.

1. Nous pouvons commencer par remarquer que $6^2 = 36$, qui est proche de $3 \times 11 = 33$.

Nous avons donc :

$$\begin{aligned} 6^2 &= 36 \\ &= 3 \times 11 + 3 \\ &\equiv 3\,[11] \end{aligned}$$

$$\begin{aligned} \text{D'où : } 6^{10} &= \left(6^2\right)^5 \\ &\equiv 3^5\,[11] \ (\text{car, si } a \equiv b\,[n], \text{ alors } a^p \equiv b^p\,[n]) \end{aligned}$$

2 $3^2 = 9$ est proche de 11, nous allons donc faire apparaître 3^2 en utilisant le fait que $5 = 2 \times 2 + 1$:

$$\begin{aligned} 6^{10} &\equiv 3^5\,[11] \\ &\equiv 3^{2\times 2+1}\,[11] \\ &\equiv \left(3^2\right)^2 \times 3\,[11] \\ &\equiv 9^2 \times 3\,[11] \end{aligned}$$

3 Nous remarquons enfin que $9 - (-2) = 11$ et donc que $9 \equiv -2\,[11]$.

Nous obtenons ainsi :

$$\begin{aligned} 6^{10} &\equiv 9^2 \times 3\,[11] \\ &\equiv (-2)^2 \times 3\,[11] \ (\text{car } 9^2 \equiv (-2)^2\ [11]) \\ &\equiv 4 \times 3\,[11] \\ &\equiv 12\,[11] \\ &\equiv 1\,[11] \end{aligned}$$

C Le reste de la division euclidienne de 6^{10} par 11 est égal à 1.

d. Résolution d'une équation avec des congruences

Nous allons maintenant, à travers un exemple, voir comment nous pouvons résoudre une équation du type $ax \equiv b\,[n]$.

Exemple

Nous souhaitons résoudre l'équation $3x \equiv 4\,[5]$ où x est un entier relatif.

→ Il s'agit de trouver l'ensemble des x tels que le division euclidienne de $3x$ par 5 ait pour reste 4.

Pour résoudre cette équation, nous allons remplir un tableau, afin d'étudier les différents cas possibles.

1. Modulo 5, l'entier relatif x est congru à 0, 1, 2, 3 ou 4 (qui est l'ensemble des restes possibles de la division euclidienne par 5).

→ Nous pouvons donc remplir la première ligne du tableau :

x modulo 5	0	1	2	3	4
$3x$ modulo 5					

Astuce

En règle générale, pour résoudre une équation du type $ax \equiv b\,[n]$, nous nous assurons que $b < n$, puis nous nous intéressons aux valeurs de x comprises entre 0 et $n-1$.

2. Nous allons maintenant étudier, pour chaque cas, $3x$ modulo 5.

- Si $x \equiv 0\,[5]$, nous avons :

$$\begin{aligned} 3x &\equiv 3 \times 0\,[5] \\ &\equiv 0\,[5] \end{aligned}$$

- Si $x \equiv 1\,[5]$, nous avons :

$$\begin{aligned} 3x &\equiv 3 \times 1\,[5] \\ &\equiv 3\,[5] \end{aligned}$$

- Si $x \equiv 2\,[5]$, nous avons :

$$\begin{aligned} 3x &\equiv 3 \times 2\,[5] \\ &\equiv 6\,[5] \\ &\equiv 1 + 5\,[5] \\ &\equiv 1\,[5] \end{aligned}$$

- Si $x \equiv 3\,[5]$, nous avons :

$$\begin{aligned} 3x &\equiv 3 \times 3\,[5] \\ &\equiv 9\,[5] \\ &\equiv 4\,[5] \end{aligned}$$

- Si $x \equiv 4\,[5]$, nous avons :

$$\begin{aligned} 3x &\equiv 3 \times 4\,[5] \\ &\equiv 12\,[5] \\ &\equiv 2 + 2 \times 5\,[5] \\ &\equiv 2\,[5] \end{aligned}$$

→ Nous pouvons donc compléter le tableau, en identifiant la valeur (en rouge) et la colonne (en vert) qui nous intéressent :

x modulo 5	0	1	2	3	4
$3x$ modulo 5	0	3	1	4	2

C En lisant le tableau, nous pouvons conclure que les seules solutions de l'équation $3x \equiv 4\,[5]$ sont donc les nombres entiers relatifs x congrus à 3 modulo 5.

→ Nous avons donc :

$$S = \{3 + 5k\ ;\ k \in \mathbb{Z}\}$$

Conclusion :

Dans ce cours, après avoir rappelé la division euclidienne et l'avoir étendue à l'ensemble des entiers relatifs, nous avons découvert la notion

de congruences, où, pour que deux entiers relatifs a et b soient congrus modulo n (un entier naturel non nul), il faut et il suffit que la différence $a - b$ soit un multiple de n, ou bien que n divise $a - b$.