

Chapitre 2

Divisibilité dans $\mathbb{Z}$

Table des matières

1	Diviseurs et multiples	2
1.1	Définitions	2
1.2	Propriétés de la divisibilité	3
2	Division euclidienne	3
3	Congruences	5
3.1	Définition et propriétés	5
3.2	Inverse modulo n	7

1 Diviseurs et multiples

1.1 Définitions

Définition 1 :

Soient a et b deux entiers relatifs.

On dit que a divise b si il existe un entier relatif k tel que $b = a \times k$.

On dit aussi que a est un diviseur de b ou que b est un multiple de a . On note $a|b$.

Exemple 1 :

• $-124 = -31 \times 4$. Donc $31| -124$, $4| -124$, $-31| -124$ et $-4| -124$.

• 0 est un multiple de n'importe quel entier relatif b (en effet : $0 = b \times 0$). En revanche, 0 n'est un diviseur d'aucun entier relatif.

• Pour tout entier relatif a , $1|a$ et $a|a$.

Propriété 1 :

• Soit n un entier relatif non nul.

Tout diviseur de n est compris entre $-|n|$ et $|n|$.

Tout entier relatif non nul a donc un nombre fini de diviseurs mais a un nombre infini de multiples.

• Soient a et b deux entiers relatifs tel que a divise b . Alors,

- Les multiples de b sont DES multiples de a .

- Les diviseurs de a sont DES diviseurs de b .

Remarque :

L'ensemble des multiples d'un entier relatif b dans $\mathbb{Z}$ est noté $b\mathbb{Z}$.

L'ensemble des diviseurs d'un entier relatif b dans $\mathbb{Z}$ est noté $\mathcal{D}(b)$.

Si a divise b alors $b\mathbb{Z} \subset a\mathbb{Z}$ et $\mathcal{D}(a) \subset \mathcal{D}(b)$.

Exemple 2 :

Les multiples de 24 sont aussi des multiples de 3, de 4, de 2, de 6 et de 12.

Les diviseurs de 12 sont : $\mathcal{D}(12) = \{-12; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 12\}$

Les diviseurs de 24 sont : $\mathcal{D}(24) = \{-24; -12; -8; -6; -4; -3; -2; -1; 1; 2; 3; 4; 6; 8; 12; 24\}$.

On a bien : $\mathcal{D}(12) \subset \mathcal{D}(24)$.

Exercice 1 : 1) Déterminer les entiers naturels n tels que 4 divise $n + 13$.

2) Déterminer dans $\mathbb{Z}$, les entiers relatifs n tels que $4n + 1$ divise 7.

Propriété 2 :

Soient a et b deux entiers relatifs.

$$a|b \Leftrightarrow (-a)|b \Leftrightarrow a|(-b) \Leftrightarrow (-a)|(-b)$$

Conséquence :

a et $-a$ ont les mêmes diviseurs de $\mathbb{Z}$.

Exercice 2 : Déterminer les entiers naturels a et b vérifiant $a^2 - b^2 = 35$.

Méthode :

- On factorise pour obtenir un produit d'entiers. On obtient une équation du type $A \times B = 35$ où A et B sont des diviseurs positifs de 35.
- On recherche les conditions que l'on a sur A et B .
- Après avoir déterminé les diviseurs de 35, on écrit les systèmes vérifiés par A et B selon les conditions trouvées ci-dessus.

La résolution de ces systèmes nous donne les solutions cherchées.

1.2 Propriétés de la divisibilité

:

Propriété 3 :

Soient a , b et c trois entiers relatifs.
Si $a|b$ et $b|c$ alors $a|c$.

Exemple 3 :

On a $19|38$ et $38|114$ donc $19|114$.

Propriété 4 :

Soient a , b et c trois entiers relatifs.

- Si $a|b$ et $a|c$ alors, pour tous les entiers relatifs m et n , $a|mb + nc$.
- En particulier, si $a|b$ alors $a|(a + b)$ et $a|(a - b)$.

Exercice 3 : Déterminer tous les entiers relatifs n tels que $(2n + 7)|(n - 3)$.

Méthode :

- On recherche une combinaison linéaire de $(n - 3)$ et $(2n + 7)$ de manière à éliminer l'inconnue n . On obtient alors que $(2n + 7)$ divise l'entier 13 qui est indépendant de n .
- On raisonne alors par disjonction de cas en cherchant les diviseurs de 13.
- Les solutions POSSIBLES sont alors les résultats trouvés. Mais comme on ne raisonne pas par équivalence, il faut ensuite vérifier par le calcul que les résultats correspondent bien à des entiers solutions.

2 Division euclidienne

Théorème 1 :

Soient a un entier relatif et b un entier naturel non nul.
Il existe un unique couple d'entiers $(q; r)$ tel que :

$$a = q \times b + r \quad \text{et} \quad 0 \leq r < b$$

Définition 2 :

Faire la division euclidienne de a par b , c'est déterminer le couple d'entiers (q, r) tel que :
 $a = q \times b + r$ et $0 \leq r < b$.

q est un entier relatif et est appelé quotient de la division euclidienne de a par b . r est un entier naturel et est appelé reste de la division euclidienne de a par b .

Interprétation graphique :

On encadre a par deux multiples consécutifs de b : $q \times b$ et $(q + 1) \times b$. (faire un schéma)

Exemple 4 :

- Déterminer la division euclidienne de 59 par 3.

On divise 59 par 3 à la calculatrice : $59/3 = 19,6$ donc il y a au moins 19 fois 3 dans 59. De plus, $3 \times 19 = 57$. Donc $59 = 3 \times 19 + 2$. On a bien $0 \leq 2 < 3$ donc on a bien la division euclidienne de 59 par 3.

- De même, $5000 = 17 \times 294 + 2$. Et la division euclidienne de -5000 par 17. On a donc $-5000 = 17 \times (-294) - 2$ mais -2 est négatif donc il ne peut pas être le reste!! Il faut récupérer 17 dans le premier terme et le rendre au reste pour avoir un nombre positif donc $-5000 = 17 \times (-295) - 2 + 17 = 17 \times (-295) + 15$ et $0 \leq 15 < 17$ donc on a bien la division euclidienne de -5000 par 17.

Remarques :

- Dans la division euclidienne de a par b , il y a b restes possibles : $0, 1, 2, 3, \dots, b - 1$.
- Il existe plusieurs écritures de la forme $a = q \times b + r$: $59 = 3 \times 19 + 2 = 3 \times 18 + 5 = 3 \times 17 + 8$. Mais une seule de ces écritures vérifie : $0 \leq r < b$ ce qui explique l'unicité du couple (q, r) .
- On définit de même la division euclidienne d'un entier relatif a par un entier relatif non nul b : il existe un unique couple d'entiers relatifs $(q; r)$ tel que : $a = q \times b + r$ et $0 \leq r < |b|$.

Exercice 4 : Dans la division euclidienne de -37 par l'entier naturel non nul n , le reste est 14.

Déterminer les valeurs possibles du diviseur et du quotient.

Méthode :

On écrit la division euclidienne de -37 par b : $-37 = q \times b + 14$ ce qui donne une équation de la forme $q \times b = n$.

On cherche les diviseurs de n et comme la division euclidienne impose $0 \leq r < b$, on trouve les entiers solutions.

Propriété 5 :

Soient a un entier relatif et b un entier naturel non nul.

b divise a si et seulement si le reste de la division euclidienne de a par b est nul.

Exemple 5 :

Montrer que $214 \equiv 25 [9]$.

On calcule : $214 - 25 = 189$ et $189/9 = 21$ donc $9|(214 - 25)$ donc $214 \equiv 25 [9]$.

Propriété 6 :

Soit b un entier naturel supérieur ou égal à 2.

Tout entier relatif s'écrit de manière unique sous l'une des formes suivantes : $q \times b$, $q \times b + 1$, $q \times b + 2, \dots, q \times b + (b - 1)$ où q est un entier relatif.

Exercice 5 : Soit n un entier naturel. Posons : $A = n \times (n + 1) \times (n + 2)$.

Démontrer que A est multiple de 3. (autrement dit, montrer que le produit de trois entiers naturels consécutifs est divisible par 3.

Méthode :

Tout entier n s'écrit de manière unique sous l'une des trois formes : $3k$, $3k + 1$, $3k + 2$.

On raisonne par disjonction de cas, en distinguant les trois cas possibles et en montrant le résultat dans les trois cas.

3 Congruences

3.1 Définition et propriétés

Définition 3 :

Soit n un entier naturel non nul et soient a et b deux entiers relatifs.

On dit que a et b sont congrus modulo n lorsqu'ils ont le même reste dans la division euclidienne par n .

On dit aussi que a est congru à b modulo n ou que b est congru à a modulo n . On note : $a \equiv b [n]$ ou $a \equiv b (n)$ ou $a \equiv b (\text{mod } n)$.

Exemple 6 :

On a : $15 = 2 \times 7 + 1$ et $21 = 2 \times 10 + 1$ donc $21 \equiv 15 [2]$.

Comme 1 est le reste de la division euclidienne de 15 par 2, on a aussi : $15 \equiv 1 [2]$ et de même $21 \equiv 1 [2]$.

Les congruences permettent entre autre de faire des calculs sur des nombres plus simples.

Propriété 7 :

Soient n un entier naturel non nul, a et b des entiers relatifs.

$$a \equiv b [n] \Leftrightarrow a - b \text{ est divisible par } n \Leftrightarrow n | (a - b)$$

Exemple 7 :

$21 - 15 = 6$ et $2 | 6$ donc $21 \equiv 15 [2]$.

Propriété 8 :

Soient n un entier naturel non nul et soient a , b et c des entiers relatifs.

1. $a \equiv 0 [n]$ si et seulement si a est divisible par n .
2. $a \equiv a [n]$.
3. r est le reste de la division euclidienne de a par n si et seulement si $a \equiv r [n]$ et $0 \leq r < n$.
4. Si $a \equiv b [n]$ et $b \equiv c [n]$ alors $a \equiv c [n]$ (on dit que la relation de congruence est transitive).

Exemple 8 :

- $12 \equiv 0 [2]$ mais aussi $12 \equiv 0 [3]$ et $12 \equiv 0 [6]$.
- $31 \equiv 13 [2]$ et $13 \equiv 1 [2]$ donc $31 \equiv 1 [2]$.

Propriété 9 :

Règles de calcul sur les congruences : Soient n un entier naturel non nul et a , b , c et d des entiers relatifs.

1. Compatibilité avec l'addition :
 - a) Si $a \equiv b [n]$ alors $a + c \equiv b + c [n]$
 - b) Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a + c \equiv b + d [n]$
2. Compatibilité avec la multiplication :
 - a) Si $a \equiv b [n]$ alors $a \times c \equiv b \times c [n]$.
 - b) Si $a \equiv b [n]$ et $c \equiv d [n]$ alors $a \times c \equiv b \times d [n]$.
3. Compatibilité avec les puissances :
Si $a \equiv b [n]$ alors pour tout entier naturel non nul p , $a^p \equiv b^p [n]$.

Remarques :

- Attention, on n'a pas le droit de diviser les congruences : on a que : $6 \equiv 2 [4]$ mais (en divisant tout par 2), 3 ne congru pas à 1 modulo 4.
- Attention, si $a \times b \equiv 0 [n]$ alors $a \equiv 0 [n]$ ou $b \equiv 0 [n]$ est FAUX. Par exemple : $2 \times 3 \equiv 0 [6]$ mais 2 ne congru pas à 0 modulo 6 et 3 ne congru pas à 0 modulo 6.

Exemple 9 :

- Calculer : $2 \times 3 \times 5 \times 3 \equiv [7]$ (-1 ou 6 modulo 7).
- Calculer $6^{43} [7]$ (on va essayer de se ramener à 1 ou -1. $6 \equiv -1 [7]$ donc $6^{43} \equiv -1 [7]$)
- Calculer $4^{50} [7]$. ($4^2 \equiv 2 [7]$ et $4^3 \equiv 2 \times 4 \equiv 1 [7]$ et $50 = 3 \times 16 + 2...$ donc $4^{50} \equiv 2 [7]$. On peut remplacer 4 par un nombre qui lui est égal modulo 7 MAIS on ne peut pas remplacer 50 par un nombre qui lui est égal modulo 7!!!.
- On résout : $x + 2 \equiv 3 [4]$. On sait que $-2 \equiv -2 [4]$ donc $x + 2 - 2 \equiv 3 - 2 [4]$ donc

$x \equiv 1 [4]$ donc $\mathcal{S} = \{1 + 4k, k \in \mathbb{Z}\}$

- $10 \equiv 1 [9]$ donc $10^p \equiv 1^p [9]$ donc $10^p \equiv 1 [9]$ avec p un entier naturel non nul.
- Soit x un entier relatif.

Démontrer que si x n'est pas multiple de 3 alors $x^2 \equiv 1 [3]$.

x n'est pas multiple de 3 donc $x \equiv 1 [3]$ ou $x \equiv 2 [3]$. On raisonne par disjonction de cas :

★ si $x \equiv 1 [3]$ alors $x^2 \equiv 1^2 [3]$ donc $x^2 \equiv 1 [3]$.

★ si $x \equiv 2 [3]$ alors $x^2 \equiv 2^2 [3]$ donc $x^2 \equiv 4 [3]$ donc $x^2 \equiv 1 [3]$.

On a donc montré que si x n'est pas multiple de 3 alors $x^2 \equiv 1 [3]$.

Exercice 6 : tableau de congruences

Déterminer les restes possibles de la division de n^2 par 7 suivant les valeurs de l'entier relatif n .
En déduire les solutions de $n^2 \equiv 2 [7]$.

3.2 Inverse modulo n

Définition 4 :

Soient a un entier relatif et n un entier naturel non nul.

On dit que a est inversible modulo n lorsqu'il existe un entier b tel que $a \times b \equiv 1 [n]$.

Exemple 10 :

1) Montrer que $4 \times 7 \equiv 1 [9]$. Que peut-on en déduire? ($4 \times 7 = 28 = 3 \times 9 + 1$ donc $4 \times 7 \equiv 1 [9]$ donc 4 ou 7 sont inversibles modulo 9.)

2) 7 admet-il un inverse modulo 22? ($7 \times 2 = 14$, $7 \times 3 = 21 \equiv -1 [22]$ donc $7 \times -3 = -21 \equiv 1 [22]$ donc -3 est l'inverse de 7 modulo 22).

Exercice 7 :

1. Construire le tableau de congruences de $4x$ modulo 9.
2. Résoudre alors $4x \equiv 5 [9]$.
3. En remarquant que $4 \times 7 \equiv 1 [9]$, résoudre sans utiliser le tableau de congruences, l'équation : $7x \equiv 8 [9]$.
4. Résoudre $3x \equiv 6 [9]$