Divisibilité, division euclidienne, Congruences

Christophe ROSSIGNOL*

Année scolaire 2021/2022

Table des matières

Activité : Activité 1 page 80 [1] [?]

1 Divisibilité dans $\mathbb{Z}$

1.1 Définitions

Rappel : On note :
- $\mathbb{N}$ l'ensemble des entiers naturels : $\mathbb{N} = \{0\,;\,1\,;2\,;\dots\}$
- $\mathbb{Z}$ l'ensemble des entiers relatifs : $\mathbb{Z} = \{\dots\,;\,-2\,;\,-1\,;\,0\,;\,1\,;2\,;\dots\}$

Définition : Soient a et b deux entiers relatifs.
On dit que b divise a s'il existe un entier relatif k tel que $a = kb$.
On note alors $b \mid a$.
Dans ce cas, on dit que b est un diviseur de a, ou que a est un multiple de b.

Exemple : $28 = 7 \times 4$ donc 4 et 7 sont des diviseurs de 28.
Mais on a aussi $28 = (-4) \times (-7)$ donc -4 et -7 sont aussi des diviseurs de 28.
L'ensemble des diviseurs dans $\mathbb{Z}$ de 28 est donc : $D_{28} = \{-28\,;\,-14\,;\,-7\,;\,-4\,;\,-2\,;\,-1\,;\,1\,;\,2\,;\,4\,;\,7\,;\,14\,;\,28\}$.

Remarques : 1. 1 et -1 divisent tout entier relatif n car $n = 1 \times n = (-1) \times (-n)$.
2. 0 est un multiple de n'importe quel entier relatif n car $0 = 0 \times n$.

Exercices : 20, 21, 22 page 91 [2] – 36 page 92 [3] - 50 page 92 [4] [Magnard]

1.2 Deux exemples d'utilisation des diviseurs

Méthode : Comme un entier n'a qu'un petit nombre de diviseurs, on cherchera souvent à factoriser et à énumérer tous les cas possibles pour résoudre un problème de divisibilité.

Exemples :

1. Déterminer les couples d'entiers naturels $(x\,;\,y)$ tels que $x^2 = y^2 + 21$
   On a $x^2 = y^2 + 21 \iff x^2 - y^2 = 21 \iff (x+y)(x-y) = 21$
   $(x+y)$ et $(x-y)$ sont donc un couple de diviseurs de 21.
   On va chercher à réduire le nombre de cas :
   Comme x et y sont des entiers naturels donc $x+y \geq 0$ et comme $(x+y)(x-y) > 0$, on a $x-y > 0$.
   On peut donc se limiter aux diviseurs de 21 dans $\mathbb{N}$: $D_{21} = \{1\,;3\,;\,7\,;21\}$
   De plus, Comme x et y sont des entiers naturels, $x+y \geq x-y$.
   On obtient donc :
   - $21 = 21 \times 1$ d'où $\begin{cases} x+y = 21 \\ x-y = 1 \end{cases} \iff \begin{cases} y+1+y = 21 \\ x = y+1 \end{cases} \iff \begin{cases} 2y = 20 \\ x = y+1 \end{cases} \iff \begin{cases} y = 10 \\ x = 11 \end{cases}$
     Vérification : $11^2 = 121$ et $10^2 + 21 = 100 + 21 = 121$
   - $21 = 7 \times 3$ d'où $\begin{cases} x+y = 7 \\ x-y = 3 \end{cases} \iff \begin{cases} y+3+y = 7 \\ x = y+3 \end{cases} \iff \begin{cases} 2y = 4 \\ x = y+3 \end{cases} \iff \begin{cases} y = 2 \\ x = 5 \end{cases}$
     Vérification : $5^2 = 25$ et $2^2 + 21 = 4 + 21 = 25$
   Les deux couples solutions sont $(5\,;\,2)$ et $(11\,;\,10)$
2. Déterminer les entiers relatifs n tels que $n+3$ divise $n+10$
   Il existe un entier relatif k tel que $n+10 = k(n+3)$
   On a donc :
   $$n+10 = k(n+3) \iff n+3+7 = k(n+3) \iff 7 = k(n+3) + (n+3) \iff 7 = (k+1)(n+3)$$
   Donc $n+3$ est un diviseur de 7.
   Les diviseurs de 7 dans $\mathbb{Z}$ sont $D_7 = \{-7\,;\,-1\,;\,1\,;\,7\}$

1. Trouver et utiliser la liste des diviseurs d'un nombre.
2. Diviseurs d'un nombre.
3. Nombres amiables.
4. Un exemple de disjonction des cas.

— $n+3=-7 \iff n=-10$

Vérification : $n+10=0$ et $n+3=-7$. On a bien $-7 \mid 0$

— $n+3=-1 \iff n=-4$

Vérification : $n+10=6$ et $n+3=-1$. On a bien $-1 \mid 6$

— $n+3=1 \iff n=-2$

Vérification : $n+10=8$ et $n+3=1$. On a bien $1 \mid 8$

— $n+3=7 \iff n=4$

Vérification : $n+10=14$ et $n+3=7$. On a bien $7 \mid 14$

On a donc $S=\{-10\,;\,-4\,;\,-2\,;\,4\}$

Exercices : 1, 2 page 83 ; 38, 39, 46 page 92 et 108 page 99 [5] – 3, 4 page 83 ; 40, 41, 43, 44 page 92 et 107, 109 page 99 [6] – 47, 48, 49 page 92 et 112 page 99 [7] [Magnard]

Module : TP 1 page 102 [8] [Magnard]

1.3 Propriétés

Propriété 1 : Transitivité

Soient a, b et c trois entiers relatifs, avec $a \neq 0$ et $b \neq 0$.
Si a divise b et b divise c alors a divise c.

Démonstration :

Comme a divise b, il existe un entier relatif k tel que $b=ka$.
Comme b divise c, il existe un entier relatif k' tel que $c=k'b$.
On a donc : $c=k'b=k'ka$ donc a divise c.

Propriété 2 : Combinaisons linéaires

Soient a, b et c trois entiers relatifs
Si a divise b et c alors a divise toute combinaison linéaire de b et de c, c'est-à-dire tout entier relatif pouvant s'écrire sous la forme $\alpha b+\beta c$, avec α, $\beta \in \mathbb{Z}$.

Démonstration :

Comme a divise b, il existe un entier relatif k tel que $b=ka$.
Comme a divise c, il existe un entier relatif k' tel que $c=k'a$.
On a donc : $\alpha b+\beta c=\alpha ka+\beta k'a=(\alpha k+\beta k')\,a$ donc a divise $\alpha b+\beta c$.

Exemple : Soit k un entier naturel.
Déterminer les diviseurs communs possibles de $a=9k+2$ et $b=12k+1$ dans $\mathbb{N}$.

Soit d un diviseur commun de a et b.
Comme d divise toute combinaison linéaire de a et de b, on va chercher une combinaison linéaire de a et b dans laquelle il n'y a plus l'inconnu k.
On a $4a-3b=36k+8-36k-3=5$ donc, comme $d \mid 4a-3b$, on a $d \mid 5$.
Les deux seules valeurs possibles sont donc $d=1$ et $d=5$.

Exercices : 25 page 91 ; 45, 52 page 92 et 110, 111 page 99 [9] [Magnard]

5. Résoudre une équation.
6. Utiliser la divisibilité.
7. Parité, disjonction des cas.
8. Diviseurs d'un entier.
9. Utilisation des propriétés de la divisibilité.

2 Division euclidienne dans $\mathbb{Z}$

Activité : Activité 2 page 80 [10] [Magnard]

Propriété : Division euclidienne

Soient a un entier relatif et b un entier naturel, avec $b \neq 0$.

Il existe un unique couple d'entiers relatifs $(q\,;\,r)$ tel que :

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

a est appelé dividende, b est appelé diviseur, q est appelé quotient et r est appelé reste.

Remarque : Pour la démonstration de ce résultat, on admettra le résultat suivant :

« *Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.* »

Démonstration (partielle) :

On se limitera au cas $a > 0$ pour l'existence.

- *Existence* : On note $\mathcal{M}$ l'ensemble des multiples de b, inférieurs ou égaux à a dans $\mathbb{N}$ voir figure 1)

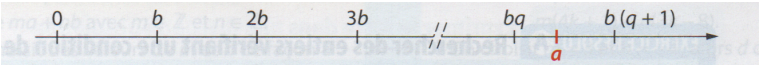

FIGURE 1 – Multiples de b plus petits que a

$\mathcal{M}$ est une partie non vide de $\mathbb{N}$ (car $0 \in \mathcal{M}$), majorée par a. Elle admet donc un plus grand élément noté q.

Puisque $q \in \mathcal{M}$, on a $bq \leq a$ et comme $q+1 \notin \mathcal{M}$, on a $b\,(q+1) > a$.

On note $r = a - bq$. On a alors $a = bq + r$ et :

$$bq \leq a < b\,(q+1) \iff bq - bq \leq a - bq < b\,(q+1) - bq \iff 0 \leq r < bq + b - bq \iff 0 \leq r < b$$

- *Unicité* : Soit $(q'\,;\,r')$ un autre couple d'entiers naturels tels que $a = bq' + r'$ et $0 \leq r' < b$.

On a $r = a - bq$ et $r' = a - bq'$. Par suite :

$$r - r' = a - bq - (a - bq') = a - bq - a + bq' = bq' - bq = b\,(q' - q)$$

donc $r - r'$ est un multiple de b.

De plus $0 \leq r < b$ et $-b < -r' \leq 0$ donc, par addition de ces deux encadrements : $-b < r - r' < b$.

Or, le seul multiple de b strictement compris entre $-b$ et b est zéro. On a donc $r - r' = 0$, c'est-à-dire $r' = r$.

De plus, comme $r - r' = b\,(q' - q)$, on a $b\,(q' - q) = 0$ et comme $b \neq 0$, on a $q' - q = 0$, c'est-à-dire $q' = q$.

Remarque : Attention ! Le reste d'une division euclidienne est toujours un nombre entier positif.

Exemples :

1. On a $60 = 8 \times 7 + 4$ donc le reste de la division euclidienne de 60 par 7 est 4.
   Pour déterminer le reste de la division euclidienne de -60 par 7, on procède de la manière suivante : $-60 = (-8)\times 7 - 4$, mais cela ne donne pas un reste positif... donc $-60 = (-9)\times 7 + 7 - 4 = (-9)\times 7 + 3$.
   Le reste de la division euclidienne de -60 par 7 est donc 3.
2. Si on divise un nombre a par 4, les seuls restes possibles sont 0, 1, 2 et 3.
   Tout nombre a s'écrit donc nécessairement d'une des façons suivantes : $a = 4q$, $a = 4q+1$, $a = 4q+2$ ou $a = 4q+3$ avec $q \in \mathbb{Z}$.

10. Définir la division euclidienne.

Exercices : 26 page 91 et 53, 54 page 92 [11] – 5, 6 page 85 ; 27, 28, 29, 30 page 91 ; 55, 56 page 92 et 113, 155, 116 page 99 [12] – 7, 8 page 85 ; 57, 60, 61 page 93 et 114 page 98 [13] [Magnard]

Module : TP 2 page 102 [14] [Magnard]

3 Congruences dans $\mathbb{Z}$

Activités : Activité 3 page 81 [15] [Magnard]

3.1 Entiers congrus modulo n

Définition : Soit n un entier naturel ($n \geq 2$) et a et b deux entiers relatifs.
On dit que les deux entiers a et b sont congrus modulo n si a et b ont le même reste dans la division euclidienne par n.
On note alors :

$$a \equiv b \ (n)$$

Remarques : 1. On peut aussi noter $a \equiv b \,(\text{mod } n)$ ou $a \equiv b \,[n]$.

2. Tout entier est donc congru au reste de sa division euclidienne par n. En particulier, x pair $\iff x \equiv 0 \ (2)$ et x impair $\iff x \equiv 1 \ (2)$.

3. a multiple de $n \iff a \equiv 0 \,(n)$.

Exemple : $42 \equiv -3 \,(9)$ car $42 = 9\times 3+6$ et $-3 = 9 \times (-1) +6$.

Propriété : Soit n un entier naturel, $n \geq 2$ et a, b et c trois entiers relatifs.

$$a \equiv b \ (\text{mod } n) \iff a - b \text{ multiple de } n$$

Démonstration :
($\Rightarrow$) : Si $a \equiv b \,(\text{mod } n)$ alors a et b ont le même reste par la division euclidienne par n.
On a donc : $a = nq + r$ et $b = nq' + r$.
Par suite : $a - b = nq + r - nq' - r = nq - nq' = n\,(q - q')$ donc $a - b$ est un multiple de n.
($\Leftarrow$) : Si $a - b$ est un multiple de n, il existe k tel que $a - b = kn$, c'est-à-dire $a = b + kn$.
On note r le reste de la division euclidienne de a par n. On a donc : $a = nq + r$ avec $0 \leq r < n$.

$$\begin{aligned} a &= nq + r \\ b + kn &= nq + r \\ b &= nq - nk + r \\ b &= n\,(q - k) + r \end{aligned}$$

Comme $0 \leq r < n$, par unicité de la division euclidienne, r est aussi le reste de la division euclidienne de b par n.
On a donc $a \equiv b \,(\text{mod } n)$.

Exercice : 32 page 91 [16] [Magnard]

11. Effectuer des divisions euclidiennes.
12. Utilisation du vocabulaire.
13. Exercices divers sur les divisions euclidiennes.
14. Division à l'école élémentaire
15. Travailler avec l'arithmétique modulaire.
16. Congruences.

3.2 Propriétés des congruences

Propriété 1 : Relation d'équivalence

Soit n un entier naturel, $n \geq 2$ et a, b et c trois entiers relatifs.
La congruence modulo n est une relation d'équivalence, c'est-à-dire qu'elle a les trois propriétés suivantes :

1. *Réflexivité* : $a \equiv a \pmod{n}$
2. *Symétrie* : Si $a \equiv b \pmod{n}$ alors $b \equiv a \pmod{n}$
3. *Transitivité* : Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ alors $a \equiv c \pmod{n}$

Remarque : Le démonstration de cette propriété découle directement de la définition des congruences.

Propriété 2 : Compatibilité avec les opérations

Soit n un entier naturel, $n \geq 2$ et a, b, c et d quatre entiers relatifs tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$.
On a alors :
— *Compatibilité avec l'addition* : $a + c \equiv b + d \pmod{n}$
— *Compatibilité avec la multiplication* : $ac \equiv bd \pmod{n}$
— *Compatibilité avec les puissances* : Pour tout entier naturel p, $a^p \equiv b^p \pmod{n}$

Démonstration :
Comme $a \equiv b \,(\text{mod } n)$, on a $a - b = kn$ et comme $c \equiv d \,(\text{mod } n)$, on a $c - d = k'n$.
(*addition*) : On a $(a + c) - (b + d) = a + c - b - d = (a - b) + (c - d) = kn + k'n = (k + k')\,n$.
$(a + c) - (b + d)$ est donc un multiple de n. On a donc $a + c \equiv b + d \,(\text{mod } n)$
(*multiplication*) : On a $a = b + kn$ et $c = d + k'n$ donc :

$$\begin{aligned} ac &= (b + kn)(d + k'n) \\ ac &= bd + bk'n + dkn + kk'n^2 \\ ac - bd &= n(bk' + dk + kk'n) \end{aligned}$$

$ac - bd$ est donc un multiple de n. On a donc $ac \equiv bd \,(\text{mod } n)$.
(*puissance*) : Le résultat se montre par récurrence sur p et est laissé en exercice.

Exemple : Comme $22 \equiv 1\,(7)$ et que $37 \equiv 2\,(7)$, on a :
— $22 + 37 \equiv 1 + 2\,(7) \iff 59 \equiv 3\,(7)$
— $22 \times 37 \equiv 1 \times 2\,(7) \iff 814 \equiv 2\,(7)$
— $22^{50} \equiv 1^{50}\,(7) \iff 22^{50} \equiv 1\,(7)$ et $39^3 \equiv 2^3\,(7) \iff 39^3 \equiv 8\,(7) \equiv 1\,(7)$

Exercices : 10 page 87 ; 33, 34, 35 page 91 ; 62, 67, 68 page 93[17] – 18, 19 page 89 ; 80, 81 page 94[18] [Magnard]

3.3 Deux exemples d'utilisation des congruences

Méthode : Pour étudier une divisibilité, on va utiliser un tableau de congruence en utilisant la compatibilité avec les opérations.

Exemple : Déterminer les valeurs de l'entier relatif n tel que $n^3 + 2n^2 - 1$ soit divisible par 5.
On étudie les congruences modulo 5 dans un tableau :

$n \equiv$	0	1	2	3	4
$n^2 \equiv$	0	1	4	$9 \equiv 4$	$16 \equiv 1$
$2n^2 \equiv$	0	2	$8 \equiv 3$	$16 \equiv 1$	1
$n^3 \equiv$	0	1	$8 \equiv 3$	$27 \equiv 2$	$64 \equiv 4$
$n^3 + 2n^2 - 1 \equiv$	$-1 \equiv 4$	2	$5 \equiv 0$	2	4

17. Congruences et puissances.
18. Critères de divisibilité

Donc n^3+2n^2-1 est divisible par 5 si et seulement si $n \equiv 2\,(\text{mod } 5)$.
Les entiers cherchés sont donc ceux de la forme $n = 2+5k$, avec $k \in \mathbb{Z}$.

Exercices : 12, 13 page 87 ; 69, 70, 72,73, 74 page 93 et 120, 121 page 99 [19] [Magnard]

Méthode : Pour déterminer une série de restes pour un nombre puissance n, on va chercher un cycle.

Exemple : Déterminer les entiers n tels que $7^n - 1$ soit divisible par 10.

On commence par étudier les congruences de 7^n modulo 10 :
- $7^0 \equiv 1\,(10)$
- $7^1 \equiv 7\,(10)$
- $7^2 \equiv 9\,(10)$
- $7^3 \equiv 3\,(10)$
- $7^4 \equiv 1\,(10)$
- $7^5 \equiv 7\,(10)$

La série de restes est 1, 7, 9, 3, soit une période de 4.
On peut donc en déduire le résultat suivant :

$n \equiv ....\,(4)$	0	1	2	3
$7^n \equiv ...\,(10)$	1	7	9	3

Par suite : $7^n - 1$ divisible par $10 \iff 7^n \equiv 1\,(10) \iff n \equiv 0\,(4) \iff n$ divisible par 4.

Exercices : 14, 16, 17 page 88 ; 63, 64 page 93 ; 75, 77, 78, 79 page 94 et 122 page 99 [20] [Magnard]

Exercices de synthèse : 87, 88 page 95 [21] – 92 page 95 [22] – 93 page 96 [23] – 123 page 100 [24] [Magnard]

Module : TP 3 page 103 [25] [Magnard]

Références

[Magnard] Maths Tle Expertes, Magnard, 2020

2, 3, 4, 5, 6, 7

19. Utiliser un tableau de congruences
20. Série de restes
21. Suite et congruence
22. Puissances de 2, 3 ou 5
23. Rep-units
24. numéro INSEE.
25. Algorithme de Luhn