Divisibilité
Congruences

Christophe ROSSIGNOL*

Année scolaire 2018/2019

Table des matières

Liste des algorithmes

Table des figures

Activité : Problème 1 page 8 [1] et problème 3 page 11 [2] [TransMath]

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 $a = kb$.
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 : -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 $0 = 0 \times n$.

Exercice résolu 1 : Exercice 4 page 14 [TransMath]

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

On veut que $(x+2)(y-5) = 15$, avec $x, y \in \mathbb{N}$.
Les diviseurs de 15 dans $\mathbb{Z}$ sont : -15 ; -5 ; -3 ; -1 ; 1 ; 3 ; 5 ; 15.
Les seules décompositions possibles sont donc :
- $15 = 15 \times 1$ donne deux cas possibles :
  - $\begin{cases} x+2 = 15 \\ y-3 = 1 \end{cases} \iff \begin{cases} x = 13 \\ y = 4 \end{cases}$
  - $\begin{cases} x+2 = 1 \\ y-3 = 15 \end{cases} \iff \begin{cases} x = -1 \\ y = 18 \end{cases}$ Impossible car x doit être un entier naturel.
- $15 = (-15) \times (-1)$ donne deux cas possibles :
  - $\begin{cases} x+2 = -15 \\ y-3 = -1 \end{cases} \iff \begin{cases} x = -17 \\ y = 2 \end{cases}$ Impossible car x doit être un entier naturel.
  - $\begin{cases} x+2 = -1 \\ y-3 = -15 \end{cases} \iff \begin{cases} x = -3 \\ y = -12 \end{cases}$ Impossible car x doit être un entier naturel.
- $15 = 3 \times 5$ donne deux cas possibles :
  - $\begin{cases} x+2 = 3 \\ y-3 = 5 \end{cases} \iff \begin{cases} x = 1 \\ y = 8 \end{cases}$
  - $\begin{cases} x+2 = 5 \\ y-3 = 3 \end{cases} \iff \begin{cases} x = 3 \\ y = 6 \end{cases}$
- $15 = (-3) \times (-5)$ donne deux cas possibles :
  - $\begin{cases} x+2 = -3 \\ y-3 = -5 \end{cases} \iff \begin{cases} x = -1 \\ y = -2 \end{cases}$ Impossible car x doit être un entier naturel.
  - $\begin{cases} x+2 = -5 \\ y-3 = -3 \end{cases} \iff \begin{cases} x = -3 \\ y = 0 \end{cases}$ Impossible car x doit être un entier naturel.

Les couples solutions sont donc : $(13\,;\,4)\,;\,(1\,;\,8)\,;(3\,;\,6)$.

1. Questions de calendriers.
2. Numéro ISBN.

Exercices : 42, 43, 50 page 29 [3] ; 2, 5 page 14 et 48, 51, 52 page 29 [4] [TransMath]

1.2 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, $\beta \in \mathbb{Z}$.

Remarque : En particulier, a divise $b + c$ et $b - c$.

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 $\alpha b + \beta c$.

Exercice résolu 2 : Exercice 1 page 14 [TransMath]

Méthode : Comme un entier n'a qu'un nombre restreint de diviseurs, on cherchera souvent éliminer l'inconnu par une combinaison linéaire et à énumérer tous les cas possibles pour résoudre un problème de divisibilité.

1. $-2n\,(n+2) + 6 = -2n^2 - 4n + 6$
2. On a donc $a = -2nb + 6$.
   Si b divise a alors b divise $a + 2nb$, c'est-à-dire que b divise 6.
   Les seules valeurs possibles pour b sont donc -6, -3, -1, 1, 3 et 6. Reste à voir si ces valeurs sont bien valables.
   - Si $b = -6$, alors $n = b - 2 = -8$ et $a = -2 \times (-8)^2 - 4 \times (-8) + 6 = -90$.
     Cette valeur convient car $-90 = 15 \times (-6)$.
   - Si $b = -3$, alors $n = b - 2 = -5$ et $a = -2 \times (-5)^2 - 4 \times (-5) + 6 = -24$.
     Cette valeur convient car $-24 = 8 \times (-3)$.
   - Si $b = -1$, alors b divise n'importe quel entier donc la valeur $n = b - 2 = -3$ convient.
   - Si $b = 1$, alors b divise n'importe quel entier donc la valeur $n = b - 2 = -1$ convient.
   - Si $b = 3$, alors $n = b - 2 = 1$ et $a = -2 \times 1^2 - 4 \times 1 + 6 = 0$.
     Cette valeur convient car $0 = 0 \times 3$.
   - Si $b = 6$, alors $n = b - 2 = 4$ et $a = -2 \times 4^2 - 4 \times 4 + 6 = -42$.
     Cette valeur convient car $-42 = -7 \times 6$.

   Les valeurs de n sont : -8, -5, -3, -1, 1 et 4.

Exercices : 3, 6 page 14 et 53, 54, 56 page 29 [5] ; 7, 8, 10, 11 page 15 [6] [TransMath]

3. Listes de diviseurs.
4. Équations.
5. Rechercher des entiers vérifiant une condition de divisibilité.
6. Diviseurs communs.

2 Division euclidienne

2.1 Division euclidienne dans $\mathbb{N}$, dans $\mathbb{Z}$

Propriété 1 : Division euclidienne dans $\mathbb{N}$

Soient a et b deux entiers naturels, avec $b \neq 0$.

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

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

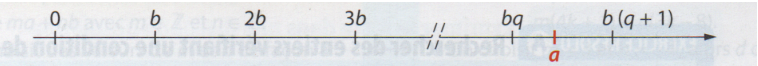

FIGURE 1 – Multiples de b plus petits que a

$\mathcal{M}$ 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 : On admettra que ce résultat est aussi valable sur l'ensemble des entiers relatifs. On a alors la propriété suivante :

Propriété 1 : Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers relatifs, avec $b \neq 0$.

Il existe un unique couple $(q\,;\,r)$ avec q entier relatif et r entier naturel tel que :

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

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 $q \in \mathbb{Z}$.

Exercice résolu 3 : Exercice 18 page 17 [TransMath]

Méthode : Comme le nombre de restes possibles dans une division euclidienne est fini, on va souvent énumérer tous les cas possibles. On dit qu'on procède par disjonction des cas.

Un nombre n est soit pair, soit impair. Il s'écrit donc sous la forme $n = 2k$ ou $n = 2k+1$,avec $k \in \mathbb{N}$.
— Si $n = 2k$:

$$A = 3n^4 + 5n + 1 = 3 \times (2k)^4 + 5 \times 2k + 1 = 3 \times 16k^4 + 10k + 1 = 48k^4 + 10k + 1 = 2\left(24k^4 + 5k\right) + 1$$

Comme $0 \leq 1 < 2$, il s'agit du reste de la division euclidienne de A par 2. Donc A est impair.
— Si $n = 2k + 1$:

$$\begin{aligned} A &= 3n^4 + 5n + 1 \\ &= 3(2k+1)^4 + 5(2k+1) + 1 \\ &= 3(2k+1)^2(2k+1)^2 + 10k + 5 + 1 \\ &= 3\left(4k^2 + 4k + 1\right)\left(4k^2 + 4k + 1\right) + 10k + 6 \\ &= 3\left(16k^4 + 16k^3 + 4k^2 + 16k^3 + 16k^2 + 4k + 4k^2 + 4k + 1\right) + 10k + 6 \\ &= 48k^4 + 96k^3 + 72k^2 + 8k + 3 + 10k + 6 \\ &= 48k^4 + 96k^3 + 72k^2 + 18k + 9 \\ &= 2\left(24k^4 + 48k^3 + 26k + 9k + 4\right) + 1 \end{aligned}$$

Comme $0 \leq 1 < 2$, il s'agit du reste de la division euclidienne de A par 2. Donc A est impair.
Donc, dans tous les cas, on obtient un nombre A impair.
De plus, soit n, soit $n+1$ est pair, donc le produit $n(n+1)$ est pair.
Si $n(n+1)$ divise A, comme 2 divise $n(n+1)$ alors, par transitivité, 2 divise A. Ce qui est impossible car A est impair.
Donc A n'est jamais divisible par $n(n+1)$.

Exercices : 44, 45, 46, 57 page 29 [7] ; 13, 15, 16 page 16 ; 59 page 29 et 61, 63 page 30 [8] ; 17, 19, 20 page 17 et 66, 67, 69, 70, 71 page 30 [9] – 73, 74 page 30 [10] [TransMath]

2.2 Algorithmes de divisions euclidiennes dans $\mathbb{N}$

2.2.1 Position du problème

Soient a et b deux entiers naturels, avec $b \neq 0$. On veut écrire un algorithme qui demande les deux nombres a et b et qui affiche le quotient q et le reste r de la division euclidienne de $a$par b. Suivant la calculatrice ou le logiciel utilisé, il est possible d'avoir ou de ne pas avoir d'instruction donnant directement le reste de cette division euclidienne.
D'où la nécessité de voir deux algorithmes différents.

7. Divisions euclidienne.
8. Déterminer un entier.
9. Disjonction des cas.
10. Calendriers.

2.2.2 Algorithme à partir du reste

Dans l'algorithme 1, le reste de la division euclidienne de a par b est noté `reste(a,b)`.
Le quotient est alors trouvé grâce à la relation :

$$a = bq + r \iff a - r = bq \iff \frac{a-r}{b} = q$$

Algorithme 1 Division euclidienne dans $\mathbb{N}$, à partir du reste

```
Variables
    a, b, q, r : nombres entiers
Algorithme
    Saisir a
    Saisir b
    r prend la valeur reste(a,b)
    q prend la valeur (a-r)/b
    Afficher q
    Afficher r
```

Remarques : 1. Sous AlgoBox, cette instruction est `a%b`.

2. Sur les calculatrices Casio Graph 35+, cette instruction est `MOD(A,B)`.
3. Sur les calculatrices TI-83 Premium, cette instruction est notée `reste(A,B)`.
4. Les TI-82 et TI-83+ n'ont pas cette instruction.
5. Le programme correspondant sous AlgoBox est `diveuclidienne1.alg`. On pourra trouver une copie d'écran des programmes sur les calculatrices à la figure 2.

2.2.3 Algorithme à partir du quotient

S'il n'existe pas d'instruction pour le reste disponible, on peut calculer facilement le quotient : c'est la partie entière de la fraction $\frac{a}{b}$. Dans l'algorithme 2, la partie entière d'un nombre x est noté `Ent(x)`.
Le reste est alors trouvé grâce à la relation :

$$a = bq + r \iff a - bq = r$$

Algorithme 2 Division euclidienne dans $\mathbb{N}$, à partir du quotient

```
Variables
    a, b, q, r : nombres entiers
Algorithme
    Saisir a
    Saisir b
    q prend la valeur Ent(a/b)
    r prend la valeur a-b*q
    Afficher q
    Afficher r
```

Remarques : 1. Sous AlgoBox, l'instruction partie entière est `floor(x)`.

2. Sur les calculatrices Casio Graph 35+, cette instruction est `INT(X)`.
3. Sur les calculatrices TI-83 Premium, cette instruction est notée `ent(X)`.
4. Sur les calculatricesTI-82 et TI-83+, cette instruction est notée `partEnt(X)`.
5. Le programme correspondant sous AlgoBox est `diveuclidienne2.alg`. On pourra trouver une copie d'écran des programmes sur les calculatrices à la figure 2.

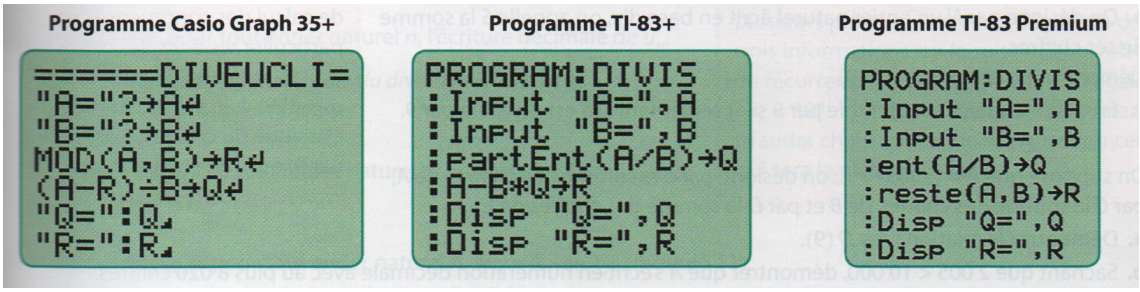

FIGURE 2 – Algorithmes de division euclidienne dans $\mathbb{N}$

3 Congruences dans $\mathbb{Z}$

Activités : Activités 1 et 2 de la feuille « Un peu de cryptographie ».

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 :

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

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

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

Exemple : $42 \equiv -3 \pmod 9$ 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.

$$a \equiv b \pmod{n} \iff a - b \text{ multiple de } n$$

Démonstration :
($\Rightarrow$) : Si $a \equiv b \pmod n$ 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 : 47 page 29 et 76 page 30 [11] [TransMath]

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* : $a \equiv a \ (\text{mod } n)$
2. *Symétrie* : Si $a \equiv b \ (\text{mod } n)$ alors $b \equiv a \ (\text{mod } n)$
3. *Transitivité* : Si $a \equiv b \ (\text{mod } n)$ et $b \equiv c \ (\text{mod } n)$ alors $a \equiv c \ (\text{mod } n)$

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 $a \equiv b \ (\text{mod } n)$ et $c \equiv d \ (\text{mod } n)$.
On a alors :
— *Compatibilité avec l'addition* : $a + c \equiv b + d \ (\text{mod } n)$
— *Compatibilité avec la multiplication* : $ac \equiv bd \ (\text{mod } n)$
— *Compatibilité avec les puissances* : Pour tout entier naturel p, $a^p \equiv b^p \ (\text{mod } n)$

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.

Exercice résolu 4 : Exercice 23 page 23 [TransMath]

Méthode : On va utiliser un tableau de congruence pour étudier une divisibilité.

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

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 $k \in \mathbb{Z}$.

11. Premières congruences.

Exercices : 22, 25 page 23 ; 32 page 24 ; 79, 80, 82, 84, 86 page 31 [12] – 26, 27 page 24 ; 75, 77, 88 page 31 [13] – 29, 30, 31 page 24 ; 87, 89 page 31 [14] – 38 page 27, 97 page 33 et 103 page 34 [15] – 91, 95 page 32 et 96 page 33 [16] – 102, 104 page 35 [17] [TransMath]

Exercices de synthèse : Problème 5 page 20 et exercice 92 page 32 [18] – TD 41 page 28 [19] – 106, 107 page 36 [20] [TransMath]

Références

[TransMath] TransMATH Term S Spécialité, programme 2012 (Nathan)

2, 3, 5, 8, 9

12. Tableau de congruences.
13. Restes de divisions euclidiennes.
14. Avec des puissances.
15. Suites et congruences.
16. Problèmes concrets.
17. Type BAC.
18. Clés de contrôles.
19. Critères de divisibilité.
20. Plus difficiles.