Division Euclidienne et Congruences

Terminale S spécialité - Lycée Saint-Charles

Patrice Jacquet - www.mathxy.fr - 2015-2016

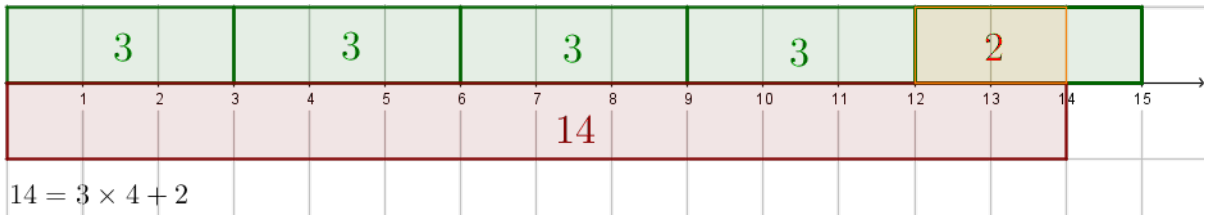
1 Division euclidienne

Propriété 1 – Théorème fondamental

Soit a un entier relatif et b un entier naturel non nul.
Il existe un couple unique $(q;r)$ d'entiers vérifiant à la fois :

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

Preuve. (*en 2 étapes*)
***étape 1*) Existence de q et r**
On peut encadrer a par deux multiples consécutifs de b.
Il existe donc un entier q tel que $bq \leqslant a < b(q+1)$,
d'où : $0 \leqslant a - bq < b$. En posant $r = a - bq$, on a bien $a = bq + r$ et $0 \leqslant r < b$.



***étape 2*) Unicité**
On raisonne par l'absurde. Supposons qu'il existe deux couples $(b;q)$ et $(b';q')$ vérifiant :
$a = bq + r$ et $a = bq' + r'$ et $0 \leqslant r < b$ et $0 \leqslant r' < b$.
Alors $b(q - q') = r - r'$ et $-b < r - r' < b$, donc $r - r'$ est un multiple de b.
Or le seul multiple de b dans $]-b;b[$ est 0, donc $r - r' = 0$ et $q - q' = 0$.
On en déduit que le couple $(q;r)$ est unique.

Définition 1 – Division euclidienne

Effectuer la division euclidienne de l'entier relatif a par l'entier relatif non nul b, c'est trouver le couple $(q;r)$ appartenant à $\mathbb{Z} \times \mathbb{N}$, tel que :

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

a est le **dividende**, b est le **diviseur**, q est le **quotient**, r est le **reste**.

Exemple. attention aux signes du dividende et du diviseur ...

- Division euclidienne de 50 par 3 : $50 = 16 \times 3 + 2$ (comme appris à l'école primaire).
- Division euclidienne de -50 par 3 : $-50 = -17 \times 3 + 1$ (le reste est toujours positif ou nul).
- Division euclidienne de 50 par -3 : $50 = -16 \times -3 + 2$.
- Division euclidienne de -50 par -3 : $-50 = 17 \times -3 + 1$.

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

2 Le langage des congruences

2.1 Une autre façon de visualiser les nombres

Nous avons habituellement une vision linéaire des nombres placés sur une règle ou sur l'axe des abscisses. Il est parfois utile de briser cette vision linéaire en plaçant les nombres dans des colonnes, dont le nombre peut varier.

- **Les entiers naturels vus linéairement** :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

- **Les entiers naturels sur 4 colonnes :**

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23

- **Les entiers naturels sur 10 colonnes :**

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39

Remarque. Observons dans ces tableaux les nombres d'une même colonne ...

- **Dans le tableau à 4 colonnes** : dans la première colonne on trouve les multiples de 4.
  Dans la deuxième colonne tous les nombres ont pour reste 1 dans la division euclidienne par 4.
  Dans la troisième colonne tous les nombres ont pour reste 2 dans la division euclidienne par 4.
  Dans la quatrième colonne tous les nombres ont pour reste 3 dans la division euclidienne par 4.
  On peut aussi remarquer que la différence de deux nombres d'une même colonne est toujours un multiple de 4.

- **Dans le tableau à 10 colonnes** : dans la première colonne on trouve les multiples de 10.
  Dans la deuxième colonne tous les nombres ont pour reste 1 dans la division euclidienne par 10.
  Dans la troisième colonne tous les nombres ont pour reste 2 dans la division euclidienne par 10.
  etc...

2.2 Entiers congrus modulo m

Définition 2 – entiers congrus modulo m

m est un entier naturel non nul.
Dire que deux entiers a et b **sont congrus modulo m** signifie qu'ils ont le **même reste** dans la division euclidienne par m.
On note $a \equiv b \pmod{m}$.
On lit : « a est congru à b modulo m ».

Exemple. $6 \equiv 18 \pmod{4}$

Exemple. $17 \equiv 37 \pmod{10}$

Propriété 2

m est un entier naturel non nul.
Pour tous entiers a et b,

$$a \equiv b \pmod{m} \quad \text{si et seulement si} \quad m \text{ divise } a-b.$$

Preuve. $a \equiv b \pmod{m}$ donc a et b ont le même reste dans la division euclidienne par m. On a donc : $a = mq + r$ et $b = mq' + r$, d'où $a - b = m(q - q')$. $a - b$ est donc bien un multiple de m.
Réciproquement, supposons que $a-b$ soit un multiple de m. Il existe un entier k tel que $a-b = km$ et donc $b = a - km$.
De plus, on a $a = mq + r$ avec $0 \leqslant r < m$, d'où $b = (q - k)m + r$.
a et b ont donc bien le même reste par la division euclidienne par m : $a \equiv b \pmod{m}$.

Exemple. $18 \equiv 6 \pmod{4}$, $18 - 6 = 12$ et 4 divise 12.

2.3 Propriétés des congruences

Propriété 3

m est un entier naturel non nul.
Pour tous entiers a et b,

$$\text{Si} \quad a \equiv b \pmod{m} \quad \text{alors} \quad b \equiv a \pmod{m}$$

Preuve. Si $a - b$ est un multiple de m alors $b - a$ est aussi un multiple de m.

Propriété 4

m est un entier naturel non nul.
Pour tous entiers a, b et c,

$$\text{Si} \quad a \equiv b \pmod{m} \quad \text{et} \quad b \equiv c \pmod{m} \quad \text{alors} \quad a \equiv c \pmod{m}$$

Preuve. Dans la division euclidienne par m, a et b ont le même reste, ainsi que b et c.

Propriété 5

m est un entier naturel non nul.
Pour tous entiers a, b, a' et b', si $a \equiv b \pmod{m}$ et $a' \equiv b' \pmod{m}$ alors :

- $a + a' \equiv b + b' \pmod{m}$
- $a - a' \equiv b - b' \pmod{m}$
- $aa' \equiv bb' \pmod{m}$

Preuve. $a - b = km$ et $a' - b' = k'm$, donc :

- $(a + a') - (b + b') = (k + k')m$
- $(a - a') - (b - b') = (k - k')m$
- $aa' - bb' = a(a' - b') + b'(a - b) = ak'm + b'km = (ak' + b'k)m$

Remarque. En partant de la dernière propriété, on peut facilement prouver par récurrence que si $a \equiv b \pmod{m}$ alors $a^p \equiv b^p \pmod{m}$ (p entier naturel).

Exemple. $18 \equiv 6 \pmod{4}$, $18 - 6 = 12$ et 4 divise 12.