Division euclidienne, congruence

Objectifs :

- Connaître et savoir utiliser la division euclidienne dans $\mathbb{N}$ et dans $\mathbb{Z}$
- Découvrir la notion de congruence, et savoir l'utiliser pour traiter des problèmes liés à la divisibilité
- Savoir combiner les outils issus des notions précédentes pour modéliser puis résoudre des problèmes

Aperçu historique :

La congruence sur les entiers est une relation pouvant unir deux entiers. Elle fut pour la première fois étudiée en tant que structure par le mathématicien allemand ***Carl Friedrich Gauss*** à la fin du XVIIIe siècle et présentée au public dans ses *Disquisitiones arithmeticae* en 1801. Elle est aujourd'hui couramment utilisée en théorie des nombres, en algèbre générale et en cryptographie (étude des codes secrets). Elle représente le fondement d'une branche mathématique appelée arithmétique modulaire.
C'est une arithmétique où l'on ne raisonne pas directement sur les nombres mais sur leurs restes respectifs par la division euclidienne par un certain entier : le module. On parle alors de congruence.
Cette arithmétique est parfois appelée "arithmétique de l'horloge". Par exemple, si nous partons à 9 heures et voyageons pendant 4 heures, alors au lieu de dire que l'on arrive à 13 heures ($9+4=14$), On pourra dire que l'on arrive à 1 heure. Les heures "13 heures" et "1 heure" sont considérées comme équivalentes.
De la même manière, si nous partons à 10h et voyageons pendant 19h, nous ne dirons pas que nous arrivons à 29 heures ($10+19=29$), mais à 5h le lendemain matin ($29=5+2\times 12$: 29 est "égal à 5, à un certain nombre de fois 12 près").
En résumé, chaque fois que l'on atteint 12, tout se passe comme si l'on recommençait à zéro ; on dira que l'on travaille modulo 12. Pour reprendre l'exemple précédent, on dit que 5 et 29 sont congrus modulo 12. Les nombres 5, 17, 29, 41, etc. sont considérés comme égaux lorsqu'on travaille modulo 12.

Carl Friedrich Gauss

1. Division euclidienne

A. Division euclidienne dans $\mathbb{N}$

Propriété 5.1 : *Propriété d'Archimède.*
Pour tout $a \in \mathbb{N}$ et tout $b \in \mathbb{N}^*$, il existe un entier naturel n tel que $a < nb$ (il suffit de prendre $n = a+1$).
On dit que $\mathbb{N}$ est ***Archimédien*** : en faisant suffisamment de "pas" de longueur $b \neq 0$, on pourra toujours dépasser a.

Théorème 5.1 Pour tout $a \in \mathbb{N}$ et tout $b \in \mathbb{N}^*$, il existe un unique couple $(q;r)$ d'entiers naturels tels que :

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

q est le quotient et r le reste de la division euclidienne de a par b.

Démonstration Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

- Existence du couple $(q;r)$ (construisons-le) :
  D'après la propriété d'Archimède, l'ensemble A des $n \in \mathbb{N}$ t.q. $a < nb$ n'est pas vide ; il admet donc un plus petit élément k.
  Si $k = 0$, alors $a < kb$ signifie $a < 0$, impossible car $a \in \mathbb{N}$. Donc $k \neq 0$.
  Comme k est le plus petit élément de A, $(k-1)$ ne fait pas partie de A et l'on a : $a \geqslant (k-1)b$, i.e. $(k-1)b \leqslant a$.
  Posons $q = k - 1$. Il vient $qb \leqslant a < (q+1)b$.
  En retranchant qb à chaque membre, il vient : $0 \leqslant a - qb < b$.
  En posant $r = a - qb$, on a bien $a = bq + r \qquad$ et $\qquad 0 \leqslant r < b$.
- Unicité du couple $(q;r)$ (par l'absurde) :
  Supposons qu'il existe deux couples distincts $(q_1;r_1)$ et $(q_2;r_2)$ qui conviennent.
  On a $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$, donc $-b < r_1 - r_2 < b$.
  On a $a = bq_1 + r_1 = bq_2 + r_2$, donc $r_1 - r_2 = bq_2 - bq_1 = b(q_2 - q_1)$.
  Finalement, $(r_1 - r_2)$ est un multiple de b strictement compris entre $-b$ et b, donc $r_1 - r_2 = 0$.
  Donc $r_2 = r_1$, donc $a = bq_1 + r_1 = bq_2 + r_1$, d'où $bq_1 = bq_2$, i.e. $q_1 = q_2$.
  Cela contredit que les deux couples soient distincts, et prouve donc l'unicité.

Exemple 5.1 :

2 5	7
4	3

Vérification : $25 = 7 \times 3 + 4$

Propriété 5.2 Pour tous $a \in \mathbb{N}$, $b \in \mathbb{N}^*$:
a est divisible par b ssi le reste de la division euclidienne de a par b est nul.

B. Division euclidienne dans $\mathbb{Z}$

Théorème 5.2 Pour tout $a \in \mathbb{Z}$ et tout $b \in \mathbb{Z}^*$, il existe un unique couple $(q;r)$ d'entiers relatifs tels que :

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

q est le quotient et r le reste de la division euclidienne de a par b.

Le reste de la division euclidienne doit donc être **positif**.

Démonstration L'existence sera démontrée en exercice.
L'unicité se montre par l'absurde comme dans $\mathbb{N}$.

Exemple 5.2 :
Division euclidienne de -65 par -7 : on a $-65 = -7 \times 10 + 5$; $q = 10$, $r = 5$, et $0 \leqslant 5 < 7$.
Attention : l'écriture $-65 = -7 \times 9 + (-2)$ n'est pas une division euclidienne car l'on n'a pas $0 \leqslant -2 < |-7|$.

2. Congruence

A. Définition et premières propriétés

Définition 5.1 Soient $n \in \mathbb{N}^*$, et a et b deux entiers relatifs.
On dit que a est congru à b modulo n, et on note

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

ssi a et b ont ***le même reste*** dans la ***division euclidienne*** par n.
On dit aussi que a et b sont ***congrus*** modulo n.

Exemple 5.3 Les nombres 17 et 32 sont congrus modulo 5.
En effet, on a :

$$\begin{array}{r|l} 17 & 5 \\ \hline 2 & 3 \end{array} \qquad\qquad \begin{array}{r|l} 32 & 5 \\ \hline 2 & 6 \end{array}$$

Donc 32 et 17 sont tous les deux congrus à 2 modulo 5 : le reste de leur division euclidienne par 5 est 2.
On dit que 32 et 17 sont congrus modulo 5 .

Intuitivement, "a et b sont congrus modulo n" signifie que a et b sont "égaux à un certain nombre de fois n près".

Exemple 5.4 Les angles $\frac{7\pi}{3}$ et $\frac{13\pi}{3}$ sont congrus à $\frac{\pi}{3}$ modulo 2π.
Ils sont "égaux à $\frac{\pi}{3}$, à un certain nombre de fois 2π près". En effet :

- $\frac{13\pi}{3} = \frac{\pi}{3} + \frac{12\pi}{3} = \frac{\pi}{3} + 4\pi = \frac{\pi}{3} + 2 \times 2\pi$: $\frac{13\pi}{3}$ est "égal à $\frac{\pi}{3}$, à 2 fois 2π près".
- $\frac{7\pi}{3} = \frac{\pi}{3} + \frac{6\pi}{3} = \frac{\pi}{3} + 2\pi = \frac{\pi}{3} + 1 \times 2\pi$: $\frac{7\pi}{3}$ est "égal à $\frac{\pi}{3}$, à 1 fois 2π près".

Exemple 5.5 Les heures $14h$ et $2h$ sont congrues modulo 12 : elles sont égales à "un certain nombre de fois $12h$ près". En effet, $14 = 2 + 1 \times 12$.
De même pour $8h$ et $20h$, ou $5h$ et $17h$.

Propriété 5.3 Premières conséquences :

- $a \equiv b\,[n] \Leftrightarrow (a - b)$ est divisible par n
- $a \equiv 0\,[n] \Leftrightarrow a$ est divisible par n
- Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$

Démonstration :

- ($\Rightarrow$) $a \equiv b\,[n]$ signifie que a et b ont le même reste r dans leur division euclidienne par n. Si l'on note q et q' leurs quotients respectifs dans cette division, cela signifie que :
  $a = qn + r$ et $b = q'n + r$. D'où $(a - b) = (q - q')n + r - r = (q - q')n$, donc $n|(a - b)$.
  ($\Leftarrow$) Réciproquement, si $n|(a - b)$, il existe $k \in \mathbb{Z}$ t.q. $a - b = kn$, i.e. $a = b + kn$.
  Soient q, r le quotient et le reste de la division euclidienne de b par n.
  On a : $b = qn + r$ avec $0 \leqslant r < n$, donc $a = qn + r + kn = (q + k)n + r$ avec $0 \leqslant r < n$.
  D'après l'unicité du quotient et du reste d'une division euclidienne, r est le reste de la division euclidienne de a par n, c'est le même que celui de b, donc $a \equiv b\,[n]$
- Il suffit de prendre $b = 0$ dans l'équivalence précédente.
- D'après le premier point, $a \equiv b\,[n] \Leftrightarrow n|(a - b)$, et $b \equiv c\,[n] \Leftrightarrow n|(b - c)$.
  Donc n divise leur somme $(a - b) + (b - c)$, i.e. $n|(a - c)$. D'après le premier point, cela signifie que $a \equiv c\,[n]$

B. Congruence et opérations

Théorème 5.3 Soient a, b, c et d quatre entiers relatifs, et soit $n \in \mathbb{N}^*$.
Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors :
$a + c \equiv b + d\,[n]$, et $ac \equiv bd\,[n]$
La relation de congruence est ***compatible*** avec l'addition et la multiplication.

Démonstration Démonstration faite en exercice.

Propriété 5.4 Soient $n \in \mathbb{N}^*$, et a, $b \in \mathbb{Z}$.

- $\forall k \in \mathbb{Z}$, si $a \equiv b\,[n]$, alors $a + k \equiv b + k\,[n]$
- $\forall k \in \mathbb{Z}$, si $a \equiv b\,[n]$, alors $ka \equiv kb\,[n]$
- $\forall p \in \mathbb{N}^*$, si $a \equiv b\,[n]$, alors $a^p \equiv b^p\,[n]$

Démonstration Les deux premiers points découlent du théorème ci-dessus, avec $c = d = k$.
Le troisième point sera démontré en exercice.

Attention, la réciproque des deuxième et troisième points est fausse :
$6 \times 5 \equiv 6 \times 2\,[2]$, mais 5 et 2 ne sont pas congrus modulo 2.
$5^2 \equiv 2^2\,[7]$, mais 5 et 2 ne sont pas congrus modulo 7.
En revanche, la réciproque du premier point est vraie :
$a + k \equiv b + k\,[n]$

$$\begin{cases} a + k = qn + r \\ b + k = q'n + r \end{cases} \Rightarrow \begin{cases} a + k = qn + r \\ -b - k = -q'n - r \end{cases} \Rightarrow a - b = qn - q'n \Rightarrow a - b = (q - q')n \Rightarrow n|(a - b) \Rightarrow a \equiv b\,[n]$$