Chapitre 5 : Divisibilité dans $\mathbb{Z}$ et congruences

I. Division euclidienne

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

Définition: La **partie entière** d'un réel x est l'entier relatif n tel que $n \leqslant x < n+1$ noté $\boldsymbol{n = E(x)}$.

Remarque : si $x \geqslant 0$ *alors* $E(x) \geqslant 0$

Théorème: Soient a et b deux entiers naturels avec $b \neq 0$.
Il existe un **unique couple** d'entiers naturels $(q;r)$ tel que $\boldsymbol{a = bq + r}$ et $\boldsymbol{0 \leqslant r < b}$.

Définitions: Cette relation s'appelle la division euclidienne de a par b .
q et r s'appellent respectivement le **quotient** et le **reste** de la division euclidienne de a par b .
a et b s'appellent respectivement le **dividende** et le **diviseur** de la division euclidienne de a par b .

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

Existence

Posons $q = E(\frac{a}{b})$. *On a* $\frac{a}{b} > 0$ *donc* $q = E(\frac{a}{b}) > 0$.

Par définition, $q \leqslant \frac{a}{b} < q+1$ *donc* $bq \leqslant a < b(q+1)$ *car* $b > 0$ *donc* $bq \leqslant a < bq + b$ *donc* $0 \leqslant a - bq < b$.

Posons $r = a - bq$. *On a d'une part* $a = bq + r$ *et d'autre part* $0 \leqslant r < b$.
On a donc prouvé l'existence d'un couple $(q;r)$ *vérifiant les conditions demandées.*

Unicité
Supposons qu'il existe deux couples $(q;r)$ *et* $(q';r')$ *tels que :*

- $a = bq + r$ *avec* $0 \leqslant r < b$
- $a = bq' + r'$ *avec* $0 \leqslant r' < b$

On a alors $bq + r = bq' + r'$ *donc* $b(q' - q) = r - r'$ *donc* $b \mid (r - r')$.
On a $0 \leqslant r' < b$ *donc* $-b < -r' \leqslant 0$
Or $0 \leqslant r < b$
donc $-b < r - r' < b$

Ainsi $b \mid (r - r')$ *et* $-b < r - r' < b$ *donc* $r - r' = 0$ *c'est à dire* $r = r'$.
On déduit que $b(q' - q) = r - r' = 0$ *avec* $b \neq 0$ *donc* $q' - q = 0$ *donc* $q = q'$ *d'où l'unicité* #

Remarque : Soient a et b *deux entiers naturels avec* $b \neq 0$.
$a \mid b$ *si et seulement si le reste de la division euclidienne de* a par b *est nul.*

Exemples :
$58=17\times3+7$ avec $0\leqslant7<17$ donc 3 et 7 sont respectivement le quotient et le reste de la division euclidienne de 58 par 17

$-36=11\times(-4)+8$ avec $0\leqslant8<11$ donc -4 et 8 sont respectivement le quotient et le reste de la division euclidienne de -36 par 11.

Exercice 1: Déterminer le quotient et le reste de la division de -5000 par 17.

Exercice 2 : La division euclidienne de 256 par un entier naturel non nul *b* a un reste égal à 25.
Déterminer les valeurs possibles de *b* et du quotient *q*.

Exercice 3 : Soit n un entier naturel. Posons $A=n(n-2)(n+2)$.
Démontrer que A est un multiple de 3.

2. Division euclidienne d'un entier relatif par un entier naturel

Théorème (admis) : Pour tout entier relatif a et tout entier naturel $b\neq0$, il existe un unique couple d'entiers $(q;r)$ tel que $\boldsymbol{a=bq+r}$ et $\boldsymbol{0\leqslant r<b}$.
q est un **entier relatif** et r est un **entier naturel**.

Exemple : Sachant que $524=30\times17+14$, on a $-524=-30\times17-14$.
Le reste ne peut pas être négatif donc il ne peut pas avoir -14 comme reste.
On écrit $-524=-30\times17-17+17-14=(-30-1)\times17+(17-14)=-31\times17+3$
Ainsi, le reste de la division euclidienne de -524 par 17 est 3 et le quotient est -31.

Remarque : on définit de même la division euclidienne d'un entier relatif a par un entier relatif $b\neq0$: il existe un unique couple $(q;r)$ tel que $a=bq+r$ et $0\leqslant r<|b|$.

Exercice 4 : Dans la division euclidienne de -37 par l'entier naturel non nul b , le reste est 14.
Quelles sont les valeurs possibles du diviseur et du quotient ?

II. Congruences

1. Définition

Définition: Soit m un entier naturel non nul et a et b deux entiers relatifs.
On dit que a et b sont **congrus modulo m** lorsqu'ils ont le même reste dans la division euclidienne par m. On dit aussi que **a est congru à b modulo m**. On note $\boldsymbol{a\equiv b[m]}$ **ou** $\boldsymbol{a\equiv b(m)}$ **ou** $\boldsymbol{a\equiv b \bmod m}$

Exemple : $15=2\times7+1$ et $21=2\times10+1$ donc $15\equiv21[2]$

Théorème: Soit m un entier naturel non nul et a et b deux entiers relatifs.

$$a \equiv b[m] \Leftrightarrow m \mid (a-b)$$

Remarque : En particulier, si $a \equiv 0[m]$ *alors* $m \mid a$.

Preuve : exercice
Soit m *un entier naturel non nul. Démontrons que* $\forall (a;b) \in \mathbb{Z}^2, a \equiv b[m] \Leftrightarrow m \mid (a-b)$.

1. *On souhaite démontrer que* $a \equiv b[m] \Rightarrow m \mid (a-b)$
   (a) Sachant que $a \equiv b[m]$ *, écrire les divisions euclidiennes de* a et b par m .
   (b) En déduire que $a-b$ *est un multiple de* m .

2. *On souhaite démontrer que* $m \mid (a-b) \Rightarrow a \equiv b[m]$.
   (a) Écrire la division euclidienne de a par m *. On note écrire* r *le reste de cette division euclidienne.*
   (b) Traduire la relation $m \mid (a-b)$.
   (c) En déduire que a et b *ont le même reste dans la division euclidienne par* m . #

2. Opérations sur les congruences

Propriété de transitivité : Soit a, b et c trois entiers relatifs et m un naturel non nul.

Si $a \equiv b[m]$ et $b \equiv c[m]$ alors $a \equiv c[m]$

Preuve : D'après les hypothèses, a et b *ont le même reste dans la division euclidienne par* m *et* b et c *ont le même reste dans la division euclidienne par* m *donc* a et c *ont le même reste dans la division euclidienne par* m *donc* $a \equiv c[m]$. #

Exemple : $251 \equiv 8[3]$ et $8 \equiv 2[3]$ donc $251 \equiv 2[3]$.

Propriétés : Soit a, b, c et d quatre entiers relatifs et m un naturel non nul.

1. **Compatibilité de la relation de congruence avec l'addition.**

   Si $a \equiv b[m]$ et $c \equiv d[m]$ alors $a+c \equiv b+d[m]$

2. **Compatibilité de la relation de congruence avec la multiplication.**

   Si $a \equiv b[m]$ et $c \equiv d[m]$ alors $a \times c \equiv b \times d[m]$

3. **Compatibilité de la relation de congruence avec les puissances.**

   Si $a \equiv b[m]$ alors $\forall p \in \mathbb{N}^*, a^p \equiv b^p[m]$

Preuve : exercice
On note m un entier naturel non nul et a, b, c et d quatre entiers relatifs.

1. *Compatibilité de la relation de congruence avec l'addition.*
   On suppose que $a \equiv b[m]$ et $c \equiv d[m]$. Démontrer que $a+c \equiv b+d[m]$

2. *Compatibilité de la relation de congruence avec la multiplication.*
   On suppose que $a \equiv b[m]$ et $c \equiv d[m]$. Démontrer que $a \times c \equiv b \times d[m]$

3. *Compatibilité de la relation de congruence avec les puissances.*
   On suppose que $a \equiv b[m]$. Démontrer que $\forall p \in \mathbb{N}^*, a^p \equiv b^p[m]$ #

Cas particuliers : $c \equiv c[m]$ donc, si $a \equiv b[m]$ alors $a+c \equiv b+c[m]$ et $a \times c \equiv b \times c[m]$

Attention : il n'y a pas de compatibilité avec la division !
Contre-exemple : $62 \equiv 26[4]$ mais 31 et 13 ne sont pas congrus modulo 4.

Point méthode
A l'aide d'un tableau de congruence, démontrer que pour tout entier relatif n , le produit $n(n+1)(2n+1)$ est divisible par 3.

- On recherche les restes possibles de n dans la division par 3.

$n \equiv ...[3]$	0	1	2

- On complète le tableau de congruence par les restes possibles de $(n+1)$ et $(2n+1)$ dans la division par 3.

$n \equiv ...[3]$	0	1	2
$(n+1) \equiv ...[3]$	1	2	$3 \equiv 0[3]$
$(2n+1) \equiv ...[3]$	1	$3 \equiv 0[3]$	$5 \equiv 2[3]$

- On complète le tableau de congruence pour obtenir, dans la dernière ligne, les restes possibles de la division de $n(n+1)(2n+1)$ par 3.

$n \equiv ...[3]$	0	1	2
$(n+1) \equiv ...[3]$	1	2	$3 \equiv 0[3]$
$(2n+1) \equiv ...[3]$	1	$3 \equiv 0[3]$	$5 \equiv 2[3]$
$n(n+1)(2n+1) \equiv ...[3]$	$0 \times 1 \times 1 \equiv 0[3]$	$1 \times 2 \times 0 \equiv 0[3]$	$2 \times 0 \times 2 \equiv 0[3]$

- Ces restes étant toujours nuls, on en déduit que, pour tout entier relatif n , le produit $n(n+1)(2n+1)$ est divisible par 3.

3. Inverse modulo m

Définition: Soit m un entier naturel non nul et a un entier relatif.
On dit que a est **inversible modulo m** lorsqu'il existe un entier b tel que $\boldsymbol{a\times b\equiv 1[m]}$.

Exemple : 8 est inversible modulo 3 car $8\times 2\equiv 1[3]$. 2 est donc un inverse de 8 modulo 3.

Point méthode
A l'aide d'un tableau de congruence, démontrer que 3 est inversible modulo 5.

- On recherche les restes possibles de b et $3b$ dans la division par 5 avec $b\in\mathbb{Z}$.

$\boldsymbol{b\equiv ...[5]}$	0	1	2	3	4
$\boldsymbol{3b\equiv ...[5]}$	0	3	1	4	2

- Dans le tableau, on recherche un entier b tel que $3b\equiv 1[5]$. On observe que $3\times 2\equiv 1[5]$ donc 2 est un inverse de 3 modulo 5.

- Attention : Cet inverse n'est pas unique !
  Tout entier relatif de la forme $5k+2$ avec $k\in\mathbb{Z}$ est un inverse de 3 modulo 5.

Exercice 5 : A l'aide de cette méthode, démontrer que 4 n'admet pas d'inverse modulo 6.