DIVISIBILITÉ ET CONGRUENCES

I. Divisibilité dans $\mathbb{Z}$

Définition : Soit a et b deux entiers relatifs.
a divise b s'il existe un entier relatif k tel que $b = ka$.
On dit également :
- a est un diviseur de b,
- b est divisible par a,
- b est un multiple de a.

Exemples :
- 56 est un multiple de -8 car 56 = -7 x (-8)
- L'ensemble des multiples de 5 sont {… ; -15 ; -10 ; -5 ; 0 ; 5 ; 10 ; …}. On note cet ensemble $5\mathbb{Z}$.
- 0 est divisible par tout entier relatif.

Propriété (transitivité) : Soit a, b et c trois entiers relatifs.
Si a divise b et b divise c alors a divise c.

Démonstration :
Si a divise b et b divise c alors il existe deux entiers relatifs k et k' tels que $b = ka$ et $c = k'b$.
Donc il existe un entier relatif $l = kk'$ tel que $c = la$.
Donc a divise c.

Exemple :
- 3 divise 12 et 12 divise 36 donc 3 divise 36.
- On peut appliquer également la contraposée de la propriété de transitivité :
  Comme 2 ne divise pas 1001, aucun nombre pair ne divise 1001.
  En effet, si par exemple 10 divisait 1001 alors 2 diviserait 1001.

Propriété (combinaisons linéaires) : Soit a, b et c trois entiers relatifs.
Si c divise a et b alors c divise $ma + nb$ où m et n sont deux entiers relatifs.

Démonstration :
Si c divise a et b alors il existe deux entiers relatifs k et k' tels que $a = kc$ et $b = k'c$.
Donc il existe un entier relatif $l = mk + nk'$ tel que $ma + nb = lc$.

Exemple :
Soit un entier relatif N qui divise les entiers relatifs n et $n + 1$.
Alors N divise $n + 1 - n = 1$. Donc $N = -1$ ou $N = 1$.

II. Division euclidienne

Propriété : Soit a un entier naturel et b entier naturel non nul.
Il existe un unique couple d'entiers (q ; r) tel que $a = bq + r$ avec $0 \leq r < b$.

Définitions :
- q est appelé le quotient de la division euclidienne de a par b,
- r est appelé le reste.

Exemple :
Dans la division euclidienne de 412 par 15, on a : 412 = 15 x 27 + 7

Démonstration :

Existence :
1er cas : $0 \leq a < b$: Le couple (q ; r) = (0 ; a) convient.

2e cas : $b \leq a$: Soit *E* l'ensemble des multiples de b strictement supérieurs à a.

Alors *E* est non vide car l'entier $2b \times a$ appartient à *E*.
En effet $b \geq 1$ donc $2b \times a \geq 2a > a$.
E possède donc un plus petit élément c'est à dire un multiple de b strictement supérieur à a tel que le multiple précédent soit inférieur ou égal à a.
Il existe donc un entier q tel que $qb \leq a < (q+1)b$.
Comme, $b \leq a$ on a $b \leq a < (q+1)b$.
Et comme b > 0, on a $0 < q$.
q est donc un entier naturel.
On peut poser $r = a - bq$.
Or a, b et q sont des entiers, donc r est entier.
Comme $qb \leq a$, on a $r \geq 0$ donc r est donc un entier naturel.
Et comme $a < (q+1)b$ on en déduit que $r < b$.

Unicité :
On suppose qu'il existe deux couples (q ; r) et (q' ; r').
Donc $a = bq + r = bq' + r'$.
Et donc : $b(q - q') = r' - r$.
Comme $q - q'$ est entier, $r' - r$ est un multiple de b.

On sait que $0 \leq r < b$ et $0 \leq r' < b$ donc $-b < -r \leq 0$ et $0 \leq r' < b$,
donc $-b < r' - r < b$.
Le seul multiple de b compris entre $-b$ et b est 0, donc $r' - r = 0$ et donc $r' = r$.
D'où $q = q'$.

Propriété :
On peut étendre la propriété précédente au cas où a est un entier relatif.

- Admis -

Méthode : Déterminer le quotient et le reste d'une division euclidienne

Vidéo https://youtu.be/bwS45UeOZrg

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

A l'aide de la calculatrice, on obtient :

```
5000/17
          294.1176471
5000-17*294
                    2
```

Ainsi : 5000 = 17 x 294 + 2
Donc : -5000 = 17 x (-294) – 2
Le reste est un entier positif inférieur à 17.

Donc : -5000 = 17 x (-294) – 17 – 2 + 17
Soit : -5000 = 17 x (-295) + 15

D'où, le quotient est -295 et le reste est 15.

III. Congruences dans $\mathbb{Z}$

Exemple :
On considère la suite de nombres : 1, 6, 11, 16, 21, 26, 31, 36.
Si on prend deux quelconques de ces nombres, alors leur différence est divisible par 5.
Par exemple : 21 – 6 = 15 qui est divisible par 5.
On dit que 21 et 6 sont congrus modulo 5.

Définition : Soit n un entier naturel non nul.
Deux entiers a et b sont congrus modulo n lorsque $a - b$ est divisible par n.
On note $a \equiv b\left[n\right]$.

Propriété : Soit n un entier naturel non nul.
Deux entiers a et b sont congrus modulo n, si et seulement si, la division euclidienne de a par n a le même reste que la division euclidienne de b par n.

Démonstration :

- Si $r = r'$:

$a - b = nq + r - nq' - r' = n(q - q')$ donc $a - b$ est divisible par n et donc $a \equiv b\left[n\right]$.

- Si a et b sont congrus modulo n :
$a - b = nq + r - nq' - r' = n(q - q') + r - r'$
Donc $r - r' = a - b - n(q - q')$
Comme $a \equiv b[n]$, $a - b$ est divisible par n et donc $r - r'$ est divisible par n.
Par ailleurs, $0 \le r < n$ et $0 \le r' < n$
Donc $-n < -r \le 0$ et $0 \le r' < n$
Et donc $-n < r' - r \le n$.
$r - r'$ est un multiple de n compris entre $-n$ et n donc $r - r' = 0$, soit $r = r'$.

Exemple :
On a vu que $21 \equiv 6[5]$.
Les égalités euclidiennes 21 = 4 x 5 + 1 et 6 = 1 x 5 + 1 montrent que le reste de la division de 21 par 5 est égal au reste de la division de 6 par 5.

Propriétés : Soit n un entier naturel non nul.
a) $a \equiv a[n]$ pour tout entier relatif a.
b) Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (Relation de transitivité)

Démonstration :
a) $a - a = 0$ est divisible par n.
b) $a \equiv b[n]$ et $b \equiv c[n]$ donc n divise $a - b$ et $b - c$ donc n divise $a - b + b - c = a - c$.

Propriété (Opérations) : Soit n un entier naturel non nul.
Soit a, b, a' et b' des nombres relatifs tels que $a \equiv b[n]$ et $a' \equiv b'[n]$ alors on a :
- $a + a' \equiv b + b'[n]$
- $a - a' \equiv b - b'[n]$
- $a \times a' \equiv b \times b'[n]$
- $a^p \equiv b^p[n]$ avec $p \in \mathbb{N}$

Démonstration de la dernière relation :

- Initialisation : La démonstration est triviale pour $p = 0$ ou $p = 1$
- Hérédité :
  - Hypothèse de récurrence :
  Supposons qu'il existe un entier k tel que la propriété soit vraie : $a^k \equiv b^k[n]$
  - Démontrons que : La propriété est vraie au rang $k + 1$: $a^{k+1} \equiv b^{k+1}[n]$.
  $a^{k+1} \equiv a \times a^k \equiv b \times b^k \equiv b^{k+1}[n]$
- Conclusion :

La propriété est vraie pour $p = 0$ et héréditaire à partir de ce rang. D'après le principe de récurrence, elle est vraie pour tout entier naturel p.

Exemples :
On a $7 \equiv 4[3]$ et $11 \equiv 20[3]$ donc :
- $7+11 \equiv 4+20 \equiv 24[3]$ et on a alors $7+11 \equiv 0[3]$
- $7 \times 11 \equiv 4 \times 20 \equiv 80[3]$ et on a alors $7 \times 11 \equiv 2[3]$.

Démontrer une congruence :

Vidéo https://youtu.be/wdFNCnSflgE

Méthode : Déterminer le reste d'une division euclidienne à l'aide de congruences

Vidéo https://youtu.be/uVS-oeibDJ4

a) Déterminer le reste de la division de 2^{456} par 5.
b) Déterminer le reste de la division de 2^{437} par 7.

a) Toute puissance de 1 est égale à 1. On cherche donc une puissance de 2 qui est égale à 1 modulo 5.
On choisit alors de décomposer 456 à l'aide du facteur 4 car $2^4 \equiv 16 \equiv 1[5]$.

$$\begin{aligned} 2^{456} &\equiv 2^{4\times 114}[5], \\ &\equiv \left(2^4\right)^{114}[5] \text{, on applique la formule de congruences des puissances.} \\ &\equiv 1^{114}[5] \\ &\equiv 1[5] \end{aligned}$$

Le reste est égal à 1.

b) On cherche donc une puissance de 2 qui est égale à 1 modulo 7.
On choisit alors de décomposer 437 à l'aide du facteur 3 car $2^3 \equiv 8 \equiv 1[7]$.

$$\begin{aligned} 2^{437} &\equiv 2^{3\times 145+2}[7] \\ &\equiv \left(2^3\right)^{145} \times 2^2[7] \\ &\equiv 1^{145} \times 4[7] \\ &\equiv 4[7] \end{aligned}$$

Le reste est égal à 4.

Méthode : Résoudre une équation avec des congruences

Vidéo https://youtu.be/Hb39SqG6nbg
Vidéo https://youtu.be/aTn05hp_b7I

a) Déterminer les entiers x tels que $6+x \equiv 5[3]$

b) Déterminer les entiers x tels que $3x \equiv 5[4]$

a) $6+x \equiv 5[3]$

$6+x-6 \equiv 5-6[3]$

$x \equiv -1[3]$

$x \equiv 2[3]$

Les entiers x solutions sont tous les entiers de la forme 2 + 3k avec $k \in \mathbb{Z}$

b) $3x \equiv 5[4]$ donc $3x \equiv 1[4]$

Or x est nécessairement congru à l'un des entiers 0, 1, 2 ou 3 modulo 4.
Par disjonction des cas, on a :

x modulo 4	0	1	2	3
$3x$ modulo 4	0	3	2	1

On en déduit que $x \equiv 3[4]$.
Les entiers x solutions sont tous les entiers de la forme 3 + 4k avec $k \in \mathbb{Z}$

Appliquer un codage (Cryptographie) :

Vidéo https://youtu.be/GC7IFz4WGsc