# Arithmetique

## 1. PGDC de deux entiers

### 1) Définition et propriétés

Exemple :

Tous les diviseurs de 60 sont : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60
Tous les diviseurs de 100 sont : 1, 2, 4, 5, 10, 20, 25, 50, 100
Les diviseurs communs à 60 et 100 sont : 1, 2, 4, 5, 10, 20
Le plus grand diviseur commun à 60 et 100 est 20. On le nomme le PGCD de 60 et 100.

Définition : Soit $a$ et $b$ deux entiers naturels non nuls.
On appelle PGDC de $a$ et $b$ le plus grand commun diviseur de $a$ et $b$ et note PGDC($a$;$b$)= a∧b

Remarque :
On peut étendre cette définition à des entiers relatifs. Ainsi dans le cas d'entiers négatifs, la recherche du PGDC se ramène au cas positif.
Par exemple, PGDC(-60;100) = PGDC(60,100).
On a ainsi de façon général : $PGDC\left(|a|;|b|\right) = PGDC\left(a;b\right)$ .=a∧b

Propriétés : Soit $a$ et $b$ deux entiers naturels non nuls.
a) PGDC($a$ ; 0) = $a$
b) PGDC($a$ ; 1) = 1
c) Si $b$ divise $a$ alors PGDC($a$ ; $b$) = $b$

### 2) Algorithme d'Euclide

C'est avec *Euclide d'Alexandrie* (-3200 ; -2600), que les théories sur les nombres premiers se mettent en place.
Dans « *Les éléments* » (livres VII, VIII, IX), il donne des définitions, des propriétés et démontre certaines affirmations du passé, comme l'existence d'une infinité de nombres premiers.
« Les nombres premiers sont en quantité plus grande que toute quantité proposée de nombres premiers ».
Il présente aussi la décomposition en facteurs premiers liée à la notion de PGDC.

Propriété : Soit $a$ et $b$ deux entiers naturels non nuls.
Soit $r$ est le reste de la division euclidienne de $a$ par $b$.
On a : PGDC($a$ ; $b$) = PGDC($b$ ; $r$)

Démonstration :
On note respectivement $q$ et $r$ le quotient et le reste de la division euclidienne de $a$ par $b$.
Si d un diviseur de $b$ et $r$ alors d divise $a = bq + r$ et donc d est un diviseur de $a$ et $b$.
Réciproquement, si d un diviseur de $a$ et $b$ alors d divise $r = a - bq$ et donc d est un diviseur de $b$ et $r$.
On en déduit que l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs communs de $b$ et $r$. Et donc en particulier, PGDC($a$ ; $b$) = PGDC($b$ ; $r$).

Méthode : Recherche de PGDC par l'algorithme d'Euclide

Déterminer le PGDC de 252 et 360.

On applique l'algorithme d'Euclide :
360 = 252 x 1 + 108
252 = 108 x 2 + 36
108 = 36 x 3 + 0
Le dernier reste non nul est 36 donc PGDC(252 ; 360) = 36.
En effet, d'après la propriété précédente :
PGDC(252 ; 360) = PGDC(252 ; 108) = PGDC(108 ; 36) = PGDC(36 ; 0) = 36

Propriété : Soit $a$ et $b$ deux entiers naturels non nuls.
L'ensemble des diviseurs communs de $a$ et $b$ est l'ensemble des diviseurs de leur PGDC.

Démonstration :
On a démontré précédemment que l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs communs de $b$ et $r$.
En poursuivant par divisions euclidiennes successives, on obtient une liste strictement décroissante de restes $r, r_1, r_2, r_3, ...$ En effet, on a successivement :
$0 \leq r < b$, $0 \leq r_1 < r$, $0 \leq r_2 < r_1$, $0 \leq r_3 < r_2$, …
Il n'existe qu'un nombre fini d'entiers compris entre 0 et $r$.
Il existe donc un rang $k$ tel que $r_k \neq 0$ et $r_{k+1} = 0$.
Ainsi l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs communs de $r_k$ et 0.

A noter qu'à ce niveau ce résultat démontre le fait que dans l'algorithme d'Euclide, le dernier reste non nul est égal au PGDC de $a$ et $b$. En effet, PGDC($r_k$ ; 0) = $r_k$.

On en déduit que l'ensemble des diviseurs communs de $a$ et $b$ est égal à l'ensemble des diviseurs de $r_k$.

Exemple :

Chercher les diviseurs communs de 2730 et 5610 revient à chercher les diviseurs de leur PGDC.
A l'aide de la calculatrice, on obtient : PGDC(2730 ; 5610) = 30.
Les diviseurs de 30 sont 1, 2, 3, 5, 6, 10, 15 et 30.
Donc les diviseurs communs à 2730 et 5610 sont 1, 2, 3, 5, 6, 10, 15 et 30.

Propriété : Soit $a$, $b$ et $k$ des entiers naturels non nuls.
$PGDC(ka;kb) = k \times PGDC(a;b)$

Démonstration :
En appliquant l'algorithme d'Euclide, on obtient successivement :
$PGCD(ka;kb) = PGDC(kb;kr) = PGDC(kr;kr_1) = PGDC(kr_1;kr_2) = ... = PGDC(kr_k;0) = kr_k$

Exemple :

Chercher le PGDC de 420 et 540 revient à chercher le PGDC de 21 et 27.
En effet, 420 = 2 x 10 x 21 et 540 = 2 x 10 x 27.
Or PGDC(21 ; 27) = 3 donc PGDC(420 ; 540) = 2 x 10 x 3 = 60.

## 2. Théorème de Bézout et théorème de Gauss

### 1) Nombres premiers entre eux

**Définition :** Soit $a$ et $b$ deux entiers naturels non nuls.
On dit que $a$ et $b$ sont premiers entre eux lorsque leur PGDC est égal à 1.

Exemple :

42 et 55 sont premiers entre eux en effet PGDC(42 ; 55) = 1.

### 2) Théorème de Bézout

**Propriété (Identité de Bézout) :** Soit $a$ et $b$ deux entiers naturels non nuls et $d$ leur PGDC.
Il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = d$.

Démonstration :
On appelle $E$ l'ensemble des entiers strictement positifs de la forme $am + bn$ avec $m$ et $n$ entiers relatifs.
$a$ et $-a$ appartiennent à $E$ donc $E$ est non vide et $E$ contient un plus petit élément strictement positif noté $d$.

- Démontrons que $PGDC(a;b) \leq d$ :
$PGDC(a;b)$ divise $a$ et $b$ donc divise $d$ et donc $PGDC(a;b) \leq d$ .

- Démontrons que $d \leq PGDC(a;b)$ :
On effectue la division euclidienne de $a$ par $d$ :
Il existe un unique couple d'entiers $(q ; r)$ tel que $a = dq + r$ avec $0 \leq r < d$
On a alors :
$r = a - dq = a - (au + bv)q = a - auq - bvq = (1 - uq)a - vqb$
Donc $r$ est un élément de $E$ plus petit que $d$ ce qui est contradictoire et donc $r = 0$.
On en déduit que $d$ divise $a$. On montre de même que $d$ divise $b$ et donc $d \leq PGCD(a;b)$.

On conclut que $d = PGCD(a;b)$ et finalement, il existe deux entiers $u$ et $v$ tels que :
$au + bv = PGCD(a;b)$.

Exemple :
On a par exemple : PGDC(54 ; 42) = 6.
Il existe donc deux entiers $u$ et $v$ tels que : $54u + 42v = 6$.
Le couple (-3 ; 4) convient. En effet : 54 x (-3) + 42 x 4 = 6.

**Théorème de Bézout :** Soit $a$ et $b$ deux entiers naturels non nuls.
$a$ et $b$ sont premiers entre eux si, et seulement si, il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = 1$.

Démonstration :

- Si $a$ et $b$ sont premiers entre eux alors le résultat est immédiat d'après l'identité de Bézout.
- Supposons qu'il existe deux entiers relatifs $u$ et $v$ tels que $au + bv = 1$.
$PGDC(a;b)$ divise $a$ et $b$ donc divise $au + bv = 1$.

Donc $PGCD(a;b)=1$. La réciproque est prouvée.

Exemple :
22 et 15 sont premiers entre eux.
On est alors assuré que l'équation $22x+15y=1$ admet un couple solution d'entiers.

Méthode : Démontrer que deux entiers sont premiers entre eux

Démontrer que pour tout entier naturel $n$, $2n + 3$ et $5n + 7$ sont premiers entre eux.

$5(2n+3)-2(5n+7)=10n+15-10n-14=1$
D'après le théorème de Bézout, avec les coefficients 5 et -2, on peut affirmer que
$2n + 3$ et $5n + 7$ sont premiers entre eux.

## 3) Théorème de Gauss

Théorème de Gauss : Soit $a$, $b$ et $c$ trois entiers naturels non nuls.
Si $a$ divise $bc$ et si $a$ et $b$ sont premiers entre eux alors $a$ divise $c$.

Démonstration :
$a$ divise $bc$ donc il existe un entier $k$ tel que $bc = ka$.
$a$ et $b$ sont premiers entre eux donc il existe deux entiers relatifs $u$ et $v$ tels que :
$au + bv = 1$.
Soit : $acu + bcv = c$ soit encore $acu + kav = c$
Et donc $a(cu + kv) = c$
On en déduit que $a$ divise $c$.

Corollaire : Soit $a$, $b$ et $c$ trois entiers naturels non nuls.
Si $a$ et $b$ divise $c$ et si $a$ et $b$ sont premiers entre eux alors $ab$ divise $c$.

Démonstration :
$a$ et $b$ divise $c$ donc il existe deux entiers $k$ et $k'$ tel que $c = ka = k'b$.
Et donc $a$ divise $k'b$.
$a$ et $b$ sont premiers entre eux donc d'après le théorème de Gauss, $a$ divise $k'$.
Il existe donc un entier $k''$ tel que $k' = ak''$.
Comme $c = k'b$, on a $c = ak''b = k''ab$
Et donc $ab$ divise $c$.

Exemple :
6 et 11 divisent 660,
6 et 11 sont premiers entre eux,
donc 66 divise 660.

Remarque :
Intuitivement, on pourrait croire que la condition "$a$ et $b$ sont premiers entre eux" est inutile.
Prenons un contre-exemple :
6 et 9 divisent 18,
6 et 9 ne sont pas premiers entre eux,
et 6 x 9 = 54 ne divise pas 18.

Méthode : Résoudre une équation du type $ax + by = c$

a) Déterminer les entiers $x$ et $y$ tels que $5x+7y=1$
b) Déterminer les entiers $x$ et $y$ tels que $5x+7y=12$
reponse

a) On a $y=\frac{1-5x}{7}$. En choisissant $x=-4$, $y$ est entier.

Ainsi, le couple (-4 ; 3) est une solution particulière de l'équation.
Donc $5x+7y=5\times(-4)+7\times 3$

Soit $5(x+4)=7(3-y)$.

5 divise $7(3-y)$ et 5 et 7 sont premiers entre eux.

D'après le théorème de Gauss, 5 divise $3-y$.

On prouve de même que 7 divise $x+4$.
Il existe donc deux entiers $k$ et $k'$ tels que $x+4=7k$ et $3-y=5k'$.

Réciproquement, on remplace dans l'équation $5(x+4)=7(3-y)$ soit :

$5\times 7k=7\times 5k'$ et donc $k=k'$.
Ainsi, les solutions sont de la forme $x=7k-4$ et $y=3-5k$, avec $k$ entier quelconque.

b) On a vu que : $5\times(-4)+7\times 3=1$ donc $5\times(-4)\times 12+7\times 3\times 12=12$
Soit encore : $5\times(-48)+7\times 36=12$ et donc le couple (-48 ; 36) est une solution particulière de l'équation.
En appliquant la même méthode qu'à la question a, on prouve que les solutions sont de la forme $x=7k-48$ et $y=36-5k$, avec $k$ entier quelconque.

## 3. Nombres premiers

Les plus anciennes traces des nombres premiers ont été trouvées près du lac *Edouard* au *Zaïre* sur un os (de plus de 20000 ans), l'os d'*Ishango*, recouvert d'entailles marquant les nombres premiers 11, 13, 17 et 19. Est-ce ici l'ébauche d'une table de nombres premiers ou cette correspondance est-elle due au hasard ?

### 1) Définition et propriétés

Définition : Un nombre entier naturel est premier s'il possède exactement deux diviseurs positifs distincts 1 et lui-même.

Exemples et contre-exemples :
- 2, 3, 5, 7 sont des nombres premiers.
- 6 n'est pas un nombre premier car divisible par 2 et 3.
- 1 n'est pas un nombre premier car il ne possède qu'un seul diviseur positif.

Liste des nombres premiers inférieurs à 100 :
**2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97**

Propriété : Tout entier naturel $n$ strictement supérieur à 1 et non premier admet un diviseur premier $p$ tel que $p\leq\sqrt{n}$.

Démonstration :

Soit $E$ l'ensemble des diviseurs de $n$ autre que 1 et $n$. Cet ensemble est non vide car $n$ n'est pas premier donc $E$ admet un plus petit élément noté $p$.
$p$ est premier car dans le cas contraire, $p$ admettrait un diviseur autre que 1 et $p$. Ce diviseur serait plus petit que $p$ et diviserait également $n$ ce qui contredit le fait que $p$ est le plus petit élément de $E$.

On peut écrire que $n = pq$ avec $p \leq q$ car $p$ est le plus petit élément de $E$.
Donc $p \times p \leq pq = n$ et donc $p \leq \sqrt{n}$.

Remarque :
Pour savoir si un nombre $n$ est premier ou non, la recherche de diviseurs peut s'arrêter au dernier entier premier inférieur à $\sqrt{n}$.

Méthode : Déterminer si un nombre est premier ou non

391 est-il premier ?

Pour le vérifier, on teste la divisibilité par tous les nombres premiers inférieurs à $\sqrt{391} \approx 19{,}8$.
Soit : 2, 3, 5, 7, 11, 13, 17 et 19.
Les critères de divisibilités connus en classe du collège permettent de vérifier facilement que 391 n'est pas divisible par 2, 3 et 5.
En vérifiant par calcul pour 7, 11, 13 et 17, on constate que 391 : 17 = 23.
On en déduit que 391 n'est pas premier.

*Pierre de Fermat* (1601 ; 1665) est l'auteur de la plus célèbre conjecture des mathématiques :
« L'équation $x^n + y^n = z^n$ n'a pas de solution avec $x, y, z > 0$ et $n > 2$ ».

*Fermat* prétendait en détenir une preuve étonnante, mais il inscrivit dans la marge d'un ouvrage de *Diophante d'Alexandrie* ne pas avoir assez de place pour la rédiger !!!
Il fallu attendre trois siècles et demi pour qu'en 1995, un anglais, *Andrew Wiles*, en vienne à bout et empoche récompenses et célébrité.

## 2) Décomposition en facteurs premiers

Exemple :
On veut décomposer 600 en produit de facteurs premiers.
$600 = 6 \times 100 = 6 \times 10^2 = 2 \times 3 \times 2^2 \times 5^2 = 2^3 \times 3 \times 5^2$
En effet, 2, 3 et 5 sont des nombres premiers.

Propriété : Tout entier naturel $n$ strictement supérieur à 1 se décompose en produit de facteurs premiers.
Cette décomposition est unique à l'ordre près des facteurs.
On note $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ avec $p_1, p_2, \ldots, p_r$ nombres premiers distincts et $\alpha_1, \alpha_2, ..., \alpha_r$ entiers naturels non nuls.

Propriété : Soit $p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ la décomposition en produit de facteurs premiers d'un entier naturel $n$ non nul.
Tout diviseur de $n$ admet une décomposition en produit de facteurs premiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq r$.

Démonstration :

- $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ divise $p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$

- Réciproquement, soit $d$ un diviseur de $n = p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$.
Donc tout facteur premier de $d$ divise $n$ et est donc égal à $p_1$, $p_2$, … ou $p_r$.
Par extension, on en déduit que $d$ peut s'écrire $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$.

Exemple :

$600 = 2^3 \times 3 \times 5^2$
Donc $2^2 \times 3^0 \times 5^1 = 20$ est un diviseur de 600.

Méthode : Déterminer un PGCD ou un PPCM( le plus petit multiple commun)

a) Décomposer 17 640 et 411 600 en produits de facteurs premiers.
b) En déduire le PGCD et le PPCM (plus petit multiple commun) de ces deux nombres.

a) $17\,640 = 2 \times 8820$
$= 2^2 \times 4410$
$= 2^3 \times 2205$
$= 2^3 \times 3 \times 735$
$= 2^3 \times 3^2 \times 245$
$= 2^3 \times 3^2 \times 5 \times 49$
$= 2^3 \times 3^2 \times 5 \times 7^2$

$411\,600 = 2 \times 205\,800$
$= 2^2 \times 102\,900$
$= 2^3 \times 51\,450$
$= 2^4 \times 25\,725$
$= 2^4 \times 3 \times 8575$
$= 2^4 \times 3 \times 5 \times 1715$
$= 2^4 \times 3 \times 5^2 \times 343$
$= 2^4 \times 3 \times 5^2 \times 7 \times 49$
$= 2^4 \times 3 \times 5^2 \times 7^3$

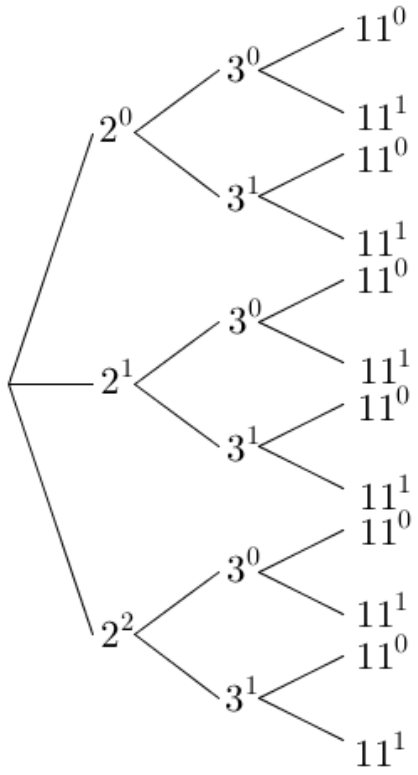
b) Le PGCD de 17 640 et 411 600 est donc $2^3 \times 3 \times 5 \times 7^2 = 5880$
Le PPCM de 17 640 et 411 600 est donc $2^4 \times 3^2 \times 5^2 \times 7^3 = 1\,234\,800$

Méthode : Déterminer tous les diviseurs d'un entier

Déterminer tous les diviseurs de 132.

On décompose 132 en produit de facteurs premiers :
$132 = 2 \times 66 = 2 \times 2 \times 33 = 2^2 \times 3 \times 11$

On construit un arbre donnant tous les cas possibles :




En parcourant tous les chemins possibles de l'arbre, on obtient tous les diviseurs de 132.
Ainsi par exemple, $2^1 \times 3^0 \times 11^1 = 22$ est un diviseur de 132.
L'ensemble des diviseur de 132 est : 1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132.

Remarque : La décomposition permet également de déterminer le nombre de diviseurs d'un entier. Il s'agit du produit des exposants augmentés de 1 des facteurs premiers. Cela correspond au produit des branches de chaque niveau de l'arbre.
Ainsi 132 possède (2 + 1) x (1 + 1) x (1 + 1) = 12 diviseurs.

# 4-DIVISIBILITÉ ET CONGRUENCES

## 1- 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 $N = 1$.

## 2- 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.

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

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

On a : 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.

## 3- 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 $a \equiv b \left[ n \right]$, $a - b$ est divisible par $n$ et donc $r - r'$ est divisible par $n$.

Par ailleurs, $0 \leq r < n$ et $0 \leq r' < n$

Donc $-n < -r \leq 0$ et $0 \leq r' < n$

Et donc $-n < r' - r \leq n$.

$r - r'$ est un multiple de $n$ compris entre $-n$ et $n$ donc $r - r' = 0$, soit $r = r'$.

Exemple :

On a vu que $21 \equiv 6 \left[ 5 \right]$.

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) $a \equiv a \left[ n \right]$ pour tout entier relatif $a$.

b) Si $a \equiv b \left[ n \right]$ et $b \equiv c \left[ n \right]$ alors $a \equiv c \left[ n \right]$ (Relation de transitivité)

Démonstration :

a) $a - a = 0$ est divisible par $n$.

b) $a \equiv b \left[ n \right]$ et $b \equiv c \left[ n \right]$ 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 $a \equiv b \left[ n \right]$ et $a' \equiv b' \left[ n \right]$ alors on a :

- $a + a' \equiv b + b' \left[ n \right]$
- $a - a' \equiv b - b' \left[ n \right]$
- $a \times a' \equiv b \times b' \left[ n \right]$
- $a^p \equiv b^p \left[ n \right]$ avec $p \in IN$

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 : $a^k \equiv b^k \left[ n \right]$

  - Démontrons que : La propriété est vraie au rang $k + 1$ : $a^{k+1} \equiv b^{k+1} \left[ n \right]$.

$a^{k+1} \equiv a \times a^k \equiv b \times b^k \equiv b^{k+1} \left[ n \right]$

- Conclusion :

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 :**

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

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

reponse
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 $2^4 \equiv 16 \equiv 1[5]$.

$2^{456} \equiv 2^{4\times 114}[5]$,

$\equiv (2^4)^{114}[5]$, on applique la formule de congruences des puissances.

$\equiv 1^{114}[5]$

$\equiv 1[5]$

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 $2^3 \equiv 8 \equiv 1[7]$.

$2^{437} \equiv 2^{3\times 145+2}[7]$

$\equiv (2^3)^{145} \times 2^2[7]$

$\equiv 1^{145} \times 4[7]$

$\equiv 4[7]$

Le reste est égal à 4.

Résoudre une équation avec des congruences

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 + 3$k$ 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 $k \in \mathbb{Z}$.

## 5)l'ensemble $\mathbb{Z}/n\mathbb{Z}$ et operation

### Definition

Soit $n$ un entier naturel non nul.
*Et a un* entier relative ; r est le reste de la division de a par n ;
On note $\bar{a}$ l'ensemble des entier relatives ayant le même reste r dans la division par n

Donc $x \in \bar{a} \Leftrightarrow x \equiv a[n]$
$\Leftrightarrow x \equiv r[n]$

$\bar{a}$ est appeler la classe d'équivalence de a

Et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence

### Exemple

*si n=2 alors $\bar{0} = \{2k, k \in \mathbb{Z}\}$ *et* $\bar{1} = \{2k+1, k \in \mathbb{Z}\}$

On remarque que

$\bar{0} \cup \bar{1} = \mathbb{Z}$ et dans ce cas $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}\}$

Application

Pour n=4 déterminer les ensembles $\bar{0}; \bar{1}; \bar{2}$ *et* $\bar{3}$

Propriété

Soit $n$ un entier naturel non nul.

On a : $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \quad \cup \overline{n-1}$

Et $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \quad ; \overline{n-1}\}$

### Operations dans $\mathbb{Z}/n\mathbb{Z}$

Soit $n$ un entier naturel non nul.

Dans $\mathbb{Z}/n\mathbb{Z}$ on a $\forall (\bar{a}, \bar{b}) \in (\mathbb{Z}/n\mathbb{Z})^2$ $\begin{cases} \bar{a} + \bar{b} = \overline{a+b} \\ \bar{a} \times \bar{b} = \overline{a \times b} \end{cases}$

Exemple

1-dans$\mathbb{Z}/2\mathbb{Z}$

On a $\bar{1} + \bar{1} = \bar{2} = \bar{0}$ *et* $\bar{2} \times \bar{1} = \bar{2} = \bar{0}$

| + | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| × | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ |

2- dans$\mathbb{Z}/3\mathbb{Z}$

On a :

| × | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{1}$ |

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

3-dans$\mathbb{Z}/4\mathbb{Z}$

…….

## 6)les systèmes de numération

### 1) Base d'un système de numération

La base d'un système de numération est le nombre de chiffres différents qu'utilise ce système de numération. En électronique numérique, les systèmes les plus couramment utilisés sont : le système binaire, le système octal, le système décimal et le système hexadécimal.

**Se rappeler que : $a^0 = 1$.**

a) Système décimal

C'est le système de numération décimal que nous utilisons tous les jours. C'est le système de **base 10** qui utilise donc 10 symboles différents : 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9.

Un nombre N (entier positif) exprimé dans le système de numération décimale est défini par la relation ci-dessous :

$N = a_n \times 10^n + a_{n-1} \times 10^{n-1}$ ..... $+ a_0 \times 10^0$ (où $a_n$ est un chiffre de rang n)

*Exemple :* $N = (1975)_{10}$

$N = 1 \times 10^3 + 9 \times 10^2 + 7 \times 10^1 + 5 \times 10^0$

**Exercice :**

$N = (6281)_{10} =$

$N = (1967)_{10} =$

$N = 2 \times 10^4 + 8 \times 10^3 + 4 \times 10^2 + 2 \times 10^1 + 9 \times 10^0 =$

b) système binaire

Le système binaire est le système de **base 2**, c'est à dire qui utilise deux symboles différents : le 0 et le 1. Chacun d'eux est appelé **bit** (contraction de binary digit) ou élément binaire.

*Exemple :* $N = (10110)_2$
$N = 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$
$N = (22)_{10}$

Puissance de 2 :

| n | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^n$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 | 16384 | 32768 |

***c) système octal***

Le système de numération octal est de **base 8**, ainsi il utilise 8 symboles différents : 0, 1, 2, 3, 4, 5, 6 et 7.

*Exemple :* $N = (6543)_8$
$N = 6 \times 8^3 + 5 \times 8^2 + 4 \times 8^1 + 3 \times 8^0$
$N = (3427)_{10}$

**2) Changement de base**

a) tableau de correspondance entre nombre de différentes bases

| Décimal (base 10) | Binaire (base 2) | Octal (base 8) |
|---|---|---|
| 0 | 0000 | 0 |
| 1 | 0001 | 1 |
| 2 | 0010 | 2 |
| 3 | 0011 | 3 |
| 4 | 0100 | 4 |
| 5 | 0101 | 5 |
| 6 | 0110 | 6 |
| 7 | 0111 | 7 |
| 8 | 1000 | 10 |
| 9 | 1001 | 11 |
| 10 | 1010 | 12 |
| 11 | 1011 | 13 |
| 12 | 1100 | 14 |
| 13 | 1101 | 15 |
| 14 | 1110 | 16 |
| 15 | 1111 | 17 |

| | | |
|---|---|---|
| 16 | 10000 | 20 |
| 17 | 10001 | 21 |