# M2. Méthodes en ARITHMETIQUE

Nous avons vu en S7 et S8 que l'arithmétique est l'étude de l'ensemble des entiers naturels et des relations numériques dans cet ensemble. On se place ici dans l'ensemble des nombres entiers naturels $\mathbb{N} = \{0;1;2;3;......\}$.

### ↘ Méthodes pour déterminer si un nombre est premier

Un nombre premier est un nombre entier supérieur ou égal à 2 qui a exactement deux diviseurs, 1 et lui-même. Ainsi 0 n'est pas premier car il a une infinité de diviseurs, 1 n'est pas premier car il a un seul diviseur qui est lui-même, 9 n'est pas premier car il a trois diviseurs 1, 3, 9.

#### 1. Crible d'Eratosthène :

On barre successivement les multiples de 2 (supérieurs à 2), les multiples de3 (supérieurs à 3), les multiples de 5 (supérieurs à 5), les multiples de7 (supérieurs à 7)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~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~~ |
| ~~40~~ | **41** | ~~42~~ | **43** | ~~44~~ | ~~45~~ | ~~46~~ | **47** | ~~48~~ | ~~49~~ |
| ~~50~~ | ~~51~~ | ~~52~~ | **53** | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | **59** |
| ~~60~~ | **61** | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | **67** | ~~68~~ | ~~69~~ |
| ~~70~~ | **71** | ~~72~~ | **73** | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | **79** |
| ~~80~~ | ~~81~~ | ~~82~~ | **83** | ~~84~~ | ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | **89** |
| ~~90~~ | ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ | **97** | ~~98~~ | ~~99~~ |

Les nombres premiers inférieurs à 100 sont :
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.

**2. Méthode au-delà de 100** : pour savoir si un nombre est premier ou non, on regarde s'il est divisible par un des nombres premiers qui lui est inférieur. En pratique, il suffit de tester s'il est divisible par un des nombres premiers inférieurs à sa racine carrée.

Par exemple pour savoir si 221 est premier, on constate avec les critères de divisibilité que 221 n'est pas divisible par 2, par 3, par 5. L'encadrement (ou la valeur approchée de la racine carrée) va permettre de préciser cette recherche :

$14^2 = 196 \qquad 15^2 = 225 \qquad 14^2 < 221 < 15^2 \quad ou \quad \sqrt{221} \approx 14,...$ On va poursuivre la recherche jusqu'à 13.

221 n'est pas divisible par 7 ($221 = 7 \times 31 + 4$), il n'est pas divisible par 11 ($221 = 11 \times 20 + 1$).
La division par 13 nous montre que $221 = 13 \times 17$. Il n'est donc pas premier.

Par contre, $1<\sqrt{113}<11$ et les divisions successives jusqu'à 7 montrent que 113 est premier. Cependant les critères de divisibilité peuvent être dans certains cas, plus rapides. Ainsi 813 n'est pas premier car la somme de ses chiffres est divisible par 3.

### Méthodes pour déterminer les diviseurs d'un nombre entier.

1. La décomposition d'un entier *a* en un produit de deux facteurs $a=b\times c$, permet de dire que *b et c* sont deux diviseurs de *a*. On peut donc trouver les diviseurs d'un nombre en le divisant successivement par les entiers inférieurs 1, 2, 3 … jusqu'à retrouver la même décomposition.

Ainsi $60=1\times 60=2\times 30=3\times 20=4\times 15=5\times 12=6\times 10$ (on retrouve ensuite $10\times 6$).

On en déduit que $D_{60}=\{1,2,3,4,5,6,10,12,15,20,30,60\}$

De meme, $126=1\times 126=2\times 63=3\times 42=6\times 21=7\times 18=9\times 14$

Les diviseurs de 126 sont donc : $\{1, 2, 3, 6, 7, 9, 14, 18, 21, 42, 63, 126\}$.

2. La décomposition d'un nombre en produit de facteurs premiers permet aussi de trouver l'ensemble de tous les diviseurs d'un nombre entier.

Ainsi $60=2^2\times 3\times 5$.

L'ensemble des diviseurs se trouve en listant successivement les facteurs présents dans la décomposition, soit $\{1,2,2^2,3,5,2\times 3,2\times 5,3\times 5,2\times 3\times 5,2^2\times 3,2^2\times 5,2^2\times 3\times 5\}$. Ne pas oublier 1 (qui n'est pas écrit dans la décomposition) et le nombre lui-même.

De même, $72=8\times 9=2^3\times 3^2$.Les diviseurs de 72 sont donc : $2^0,2^1,2^2,2^3,3^1,3^2,2\times 3,2\times 3^2,2^2\times 3,2^2\times 3^2,2^3\times 3,2^3\times 3^2$ soit $D_{72}=\{1,2,3,4,6,8,9,12,18,24,36,72\}$.

### Recherche du PGCD de deux nombres entiers.

Soient *a* et *b* deux entiers naturels non nuls. Ils ont au moins un diviseur commun qui est 1. Le Plus Grand Diviseur Commun à *a* et *b* est appelé le PGCD de *a* et de *b*.

Plusieurs méthodes sont utilisables :

1. On peut chercher l'ensemble de diviseurs de chacun des nombres (ce qui est souvent long), déterminer les diviseurs communs, puis trouver le plus grand.

Ainsi pour trouver le PGCD de 60 et 105, on va lister les diviseurs :

$D_{60}=\{1,2,3,4,5,6,10,12,15,20,30,60\}$

$D_{105}=\{1,3,5,7,15,21,35,105\}$ $\quad D_{(60,105)}=\{1,3,5,15\}$ $\quad PGCD(60,105)=15$

2. Le PGCD de deux entiers non nuls peut aussi s'obtenir en écrivant le *produit de tous les facteurs premiers communs* aux deux décompositions, affectés *du plus petit de leurs exposants* figurant dans les décompositions.

Ainsi, pour trouver le PGCD de 180 et 144, on va d'abord décomposer en facteurs premiers ces deux nombres :

$180=2\times 9\times 2\times 5=2^2\times 3^2\times 5$

$144=12\times 12=2^2\times 3\times 2^2\times 3=2^4\times 3^2$ $\quad PGCD(180,144)=2^2\times 3^2=36$

De meme, $180 = 10 \times 2 \times 9 = 2^2 \times 3^2 \times 5$ et $378 = 9 \times 42 = 3^2 \times 2 \times 3 \times 7 = 2 \times 3^3 \times 7$

On en déduit que le PGCD de180 et 378 est égal à $2^2 \times 3$,soit 18.

**3.** Cette méthode s'appuie sur la définition de la division euclidienne que nous avons vue en S8, et ses propriétés.

Pour tout entier naturel *a* et tout entier naturel *b* non nul, il existe un entier naturel unique *q* et un entier naturel unique *r* tels que $a = b \times q + r$, avec $0 \leq r < b$.

Soient deux entiers naturels *a* et *b*, avec *a*>*b*. Si un nombre *d* est à la fois diviseur de *a* et diviseur de *b*, alors il divise également le reste *r* de la division euclidienne de *a* par *b*.

**Algorithme d'EUCLIDE**

*Un algorithme peut se définir rapidement comme une suite d'actions élémentaires, répétées en nombre fini.*

Pour déterminer le PGCD de deux nombres entiers naturels *a et b*, l'algorithme consiste à effectuer des divisions successives. Le PGCD de *a et b* est alors le dernier reste non nul.

- Diviser *a par b*, on obtient un reste *r*
- Si $r = 0$, alors le PGCD est *b*. Si $r \neq 0$, alors diviser *b par r*
- Recommencer à diviser le diviseur par le reste jusqu'à obtenir un reste nul.

Ainsi pour trouver le PGCD de 255 et 136, on commence par diviser 255 par 136 jusqu'à trouver un reste nul

$255 = 136 \times 1 + 119$ $\quad 136 = 119 \times 1 + 17$ $\quad 17 = 17 \times 1$ Le PGCD de 255 et 13 est 17.

De meme, pour trouver le PGCD de 3596 et 3393

| | | | |
|---|---|---|---|
| $3596 = 3393 \times 1 + 203$ | $r = 203$ | $3393 = 203 \times 16 + 145$ | $r = 145$ |
| $203 = 145 \times 1 + 58$ | $r = 58$ | $145 = 58 \times 2 + 29$ | $r = 29$ |
| $58 = 29 \times 2 + 0$ | $r = 0.$ | Le PGCD de 3596 et 3393 est 29. | |

**Recherche du PPCM de deux nombres entiers.**

Soient *a* et *b* deux entiers naturels non nuls. Ils ont au moins un multiple commun $a \times b$. Le Plus Petit Multiple Commun à *a* et *b* est appelé le PPCM de *a* et de *b*.

Plusieurs méthodes sont utilisables :

**1.** Pour trouver le PPCM de deux nombres, on peut lister les multiples de chaque nombre (ce qui est souvent long) et prendre le plus petit multiple commun.

Par exemple, les multiples de 40 sont 40, 80, 120, 160, 200, 240, 280....Les multiples de 60 sont 60, 120, 180, 240...
*PPCM* $(40,60) = 120$.

**2.** Le PPCM de deux entiers non nuls s'obtient en écrivant le produit de tous les nombres premiers qui figurent *au moins une fois* dans les deux décompositions, affectés du *plus grand de leurs exposants* figurant dans les décompositions.

Ainsi pour trouver le PPCM de 24 et de 18, on va d'abord chercher leur décomposition en facteurs premiers :

$24 = 2^3 \times 3$ $\quad 18 = 2 \times 3^2$ $\quad PPCM(24,18) = 2^3 \times 3^2 = 72$

De meme, $90 = 2 \times 3^2 \times 5$ $\quad 12 = 2^2 \times 3$ $\quad$ PPCM $(12, 90) = 2^2 \times 3^2 \times 5 = 180$