Date :

DOSSIER N°1

ARITHMÉTIQUE

Objectifs ⇨

- Présenter les grandes notions arithmétiques utiles à l'informatique.
- Maîtriser les principes de numération indispensables aux langages de bas niveau.
- Maîtriser les outils d'arithmétique modulaire utiles à l'algorithmique.

1ère partie : Systèmes de numération.

I. Base d'un système de numération :

1°) Numération en base 10 (système décimal) :

Dans la vie courante, nous utilisons des nombres écrits en **base 10**.

Rappelons sur quelques exemples comment ils sont constitués à partir des puissances de 10 :

$5\ 615 = 5\ 000 + 600 + 10 + 5$
$5\ 615 = 5 \times 1\ 000 + 6 \times 100 + 1 \times 10 + 5 \times 1$
$5\ 615 = 5 \times 10^3 + 6 \times 10^2 + 1 \times 10^1 + 5 \times 10^0$

De même $304 = 300 + 4$
$304 = 3 \times 100 + 0 \times 10 + 4 \times 1$
$304 = 3 \times 10^2 + 0 \times 10^1 + 4 \times 10^0$

Ainsi les nombres entiers positifs sont écrits à l'aide des dix chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9 (d'où l'appellation « **système décimal** »), la position de chaque chiffre indiquant à quelle puissance de 10 il est associé.

Ce procédé est étendu aux nombres réels positifs en écriture décimale en utilisant les exposants négatifs des puissances de 10.

Exemple : $3{,}14 = 3 \times 1 + 1 \times 0{,}1 + 4 \times 0{,}01$
$3{,}14 = 3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2}$

2°) Numération en base 2 (système binaire) :

En informatique, le plus petit élément d'information utilisé, appelé **bit** (la contraction de binary digit), est obtenu en associant soit 0, soit 1 à un signal par exemple une tension électrique, suivant la valeur de ce signal.

On est alors amené à représenter les nombres en **base 2**.

Dans la numération en base 2, on dispose de deux chiffres : 0 et 1 (d'où l'appellation « **système binaire** »).

Les nombres entiers positifs sont écrits suivant la même méthode positionnelle que dans la numération en base 10, en remplaçant les puissances de 10 par les puissances de 2.

Exemples :

- $3 = 2 + 1$
  $3 = 1 \times 2^1 + 1 \times 2^0$
  Ainsi 3 est noté 11 en base 2 et lu « un un ».
  On écrit $3 = (11)_2$ où la base 2 est rappelée en indice pour éviter la confusion avec le nombre onze.

- $6 = 4 + 2$
  $6 = 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$
  Ainsi 6 est noté 110 en base 2 et lu « un un zéro ».

Comme dans la numération en base 10, les puissances de 2 d'exposant négatif permettent d'écrire des nombres avec virgule en base 2 :

$2^{-1} = \frac{1}{2^1} = \frac{1}{2} = 0{,}5$ donc $0{,}5 = 0 \times 2^0 + 1 \times 2^{-1}$
donc 0,5 est noté 0,1 en binaire et lu « zéro virgule un ».

$2^{-2} = \frac{1}{2^2} = \frac{1}{4} = 0{,}25$ donc $0{,}25 = 0 \times 2^0 + 0 \times 2^{-1} + 1 \times 2^{-2}$
donc 0,25 est noté 0,01 en binaire et lu « zéro virgule zéro un ».

$2^{-1} + 2^{-2} = 0{,}5 + 0{,}25 = 0{,}75$ donc $0{,}75 = 0 \times 2^0 + 1 \times 2^{-1} + 1 \times 2^{-2}$
donc 0,75 est noté 0,11 en binaire et lu « zéro virgule un un ».

Remarques :

- Quelle que soit la base utilisée, les nombres négatifs sont précédés du signe moins (-).

- L'écriture 101101 en binaire correspond en décimal à :
  $1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 32 + 8 + 4 + 1 = 45.$
  Nous observons ainsi que l'écriture d'un nombre entier, réalisée avec deux chiffres dans le système décimal, peut nécessiter six bits en système binaire.

3°) Numération en base 16 (système hexadécimal) :

Nous venons de voir que le système de numération binaire présente, à côté de ses nombreux avantages pour l'informatique, un inconvénient important : il nécessite l'utilisation d'un nombre relativement levé de bits pour écrire un nombre entier dès que celui-ci atteint quelques dizaines.

Pour remédier à cela, tout en conservant la bonne adaptation du binaire aux signaux intervenant en informatique, on utilise un système de numération dont la base est une puissance de 2 : le **système hexadécimal** qui est le système de numération positionnelle en **base 16** = 2^4.

Pour obtenir les 16 symboles nécessaires, on ajoute aux dix chiffres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 les six lettres majuscules A, B, C, D, E et F.

Nous obtenons ainsi le tableau de correspondance entre le système décimal, hexadécimal et binaire, ce dernier étant exprimé à l'aide de quatre bits :

Décimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadécimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Binaire à quatre bits	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Dans le système hexadécimal, les nombres entiers positifs sont écrits à l'aide des seize symboles 0, 1, 2, … , 9, A, B, C, … , F, la position de chacun correspondant à une puissance de 16.

Exemples :
- $38 = 32 + 6$
  $38 = 2 \times 16^1 + 6 \times 16^0$
  Ainsi 38 est 26 en hexadécimal. On note $38 = (26)_{16}$.
- $164 = 160 + 4$
  $164 = 10 \times 16^1 + 4 \times 16^0$
  Ainsi 164 est A4 en hexadécimal. On note $164 = (A4)_{16}$.

Ici encore, les puissances de 16 d'exposant négatif permettent d'écrire des nombres avec virgule en hexadécimal :

$16^{-1} = \frac{1}{16^1} = \frac{1}{16} = 0{,}0625$ donc $0{,}0625 = 0 \times 16^0 + 1 \times 16^{-1}$
donc 0,0625 est 0,1 en hexadécimal. On note et $0{,}0625 = (0{,}1)_{16}$.

$16^{-2} = \frac{1}{16^2} = \frac{1}{256} = 0{,}0039065$ donc $0{,}00390625 = 0 \times 16^0 + 0 \times 16^{-1} + 1 \times 16^{-2}$
donc 0,00390625 est 0,01 en hexadécimal. On note $(0{,}01)_{16}$.

Inversement :
- A2C en hexadécimal correspond au nombre :
  $10 \times 16^2 + 2 \times 16^1 + 12 \times 16^0 = 2\,560 + 32 + 12 = 2\,604$.
- 0,3B en hexadécimal correspond au nombre :
  $0 \times 16^0 + 3 \times 16^{-1} + 11 \times 16^{-2} = 3 \times 0{,}0625 + 11 \times 0{,}00390625 = 0{,}23046875$.

II. Conversion entre bases :

Nous venons de voir, sur quelques exemples particuliers, des correspondances entre les écritures d'un même nombre dans les systèmes de numération en base 10,2 et 16. Il s'agit maintenant d'introduire des méthodes générales de conversion entre bases à partir de l'étude détaillée d'un exemple.

1°) Passage du binaire au décimal :

Exemple : $(101{,}0101)_2 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 + 0 \times 2^{-1} + 1 \times 2^{-2} + 0 \times 2^{-3} + 1 \times 2^{-4}$
$(101{,}0101)_2 = 2^2 + 2^0 + 2^{-2} + 2^{-4}$ si on n'écrit ni les puissances de 2 multipliées par 0, ni les facteurs 1.
Donc $(101{,}0101)_2 = 5{,}3125$.

Méthode : Passage du binaire au décimal :
- Exprimer le nombre à l'aide des puissances de 2.

Remarque : Rappelons que pour 5,3125 :
- l'arrondi **par défaut** à 10^{-3} est 5,312,
- l'arrondi **par excès** à 10^{-3} est 5,313,
- l'arrondi à 10^{-3} est 5,313 car la première décimale abandonnée est 5,
- l'arrondi à 10^{-2} est 5,31 car la première décimale abandonnée est 2.

D'une manière générale, l'arrondi est effectué :
- par défaut si la première décimale abandonnée est 0, 1, 2, 3 ou 4 ;
- par excès si la première décimale abandonnée est 5, 6, 7, 8 ou 9.

Applications immédiates : Écrire dans le système décimal les nombres suivants.

▪ $(101010)_2 =$

▪ $(1011101)_2 =$

▪ $(100,011)_2 =$

▪ $(1001,110)_2 =$

2°) Passage du décimal au binaire :

Exemple : Le nombre 13,375 a pour partie entière (avant la virgule) 13 et pour partie décimale (après la virgule) 0,375.

▪ Pour la partie entière 13, nous allons effectuer des divisions successives par 2 jusqu'à obtenir 0 pour quotient, en les présentant de la façon suivante :

$$\begin{array}{l|l|l|l|l}
13 & 2 & & & \\
1 & 6 & 2 & & \\
 & 0 & 3 & 2 & \\
 & & 1 & 1 & 2 \\
 & & & 1 & 0
\end{array}$$

Sens de la lecture

$13 = 6 \times 2 + 1$

$6 = 3 \times 2$ donc $13 = 6 \times 2 + 1 = 3 \times 2 \times 2 + 1 = 3 \times 2^2 + 1$

$3 = 2 + 1$ donc $13 = 3 \times 2^2 + 1 = (2 + 1) \times 2^2 + 1$

$13 = 2^3 + 2^2 + 1$

Donc $13 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$

Donc $13 = (1101)_2$

Nous observons que la liste des restes successifs lus dans le sens de la flèche donne l'écriture en binaire de 13.

▪ Pour la partie décimale 0,375, nous allons effectuer des multiplications successives par 2 ne portant que sur les parties décimales jusqu'à obtenir 1, en les présentant de façon suivante :

Sens de la lecture

$0{,}375 \times 2 = 0{,}75$ donc $0{,}375 = \frac{0{,}75}{2} = 2^{-1} \times 0{,}75$

$0{,}75 \times 2 = 1{,}5$ donc $0{,}75 = \frac{1{,}5}{2} = 2^{-1} \times 1{,}5$

donc $0{,}375 = 2^{-1} \times 0{,}75$

$0{,}375 = 2^{-1} \times 2^{-1} \times 1{,}5$

$0{,}375 = 2^{-2} \times 1{,}5 = 2^{-2} \times (1 + 0{,}5) = 2^{-2} + 2^{-2} \times 0{,}5$

$0{,}5 \times 2 = 1$ donc $0{,}5 = \frac{1}{2} = 2^{-1}$

donc $0{,}375 = 2^{-2} + 2^{-2} \times 0{,}5$

$0{,}375 = 2^{-2} + 2^{-2} \times 2^{-1} = 2^{-2} + 2^{-3}$

$0{,}375 = 0 \times 2^{-1} + 1 \times 2^{-2} + 1 \times 2^{-3}$ donc $0{,}375 = (0{,}011)_2$

Nous observons que la liste des parties entières des produits successifs lus dans le sens de la flèche donne l'écriture en binaire de 0,375.

- En définitif 13,375 = 13 + 0,375 a pour écriture en binaire $(1101{,}011)_2$.

Remarque : Reprenons ces calculs avec 13,4 à la place de 13,375. Seule la partie décimale a changé.

Nous venons de démontré que 13 = $(1101)_2$.

$0{,}4 \times 2 = 0{,}8$
$0{,}8 \times 2 = 1{,}6$
$0{,}6 \times 2 = 1{,}2$
$0{,}2 \times 2 = 0{,}4$
$0{,}4 \times 2 = 0{,}8$ À partir de cette ligne, nous retrouvons la succession des quatre égalités précédentes sans jamais obtenir 1 comme produit.

Il y a donc une infinité de symboles 0 et 1 après la virgule, la séquence 0110 se reproduisant indéfiniment.

Dans ce cas, c'est le nombre de bits disponibles après la virgule qui va fixer le nombre de symboles à retenir, c'est-à-dire la précision.
Se pose lors le problème de **l'arrondi en binaire** qui est géré comme dans la numération en base 10 :
- **si le premier symbole abandonné est 0, on fait une troncature** (on coupe l'écriture) : on abandonne les symboles suivants ;
- **si le premier symbole abandonné est 1, on ajoute 1 au dernier symbole conservé.**

Ainsi 13,4 a pour écriture arrondie en binaire avec quatre bits après la virgule 1101,0110 qui est aussi l'écriture en binaire de 13,375.

Méthode : Passage du décimal au binaire :

- Pour **la partie entière** du nombre :

- effectuer des **divisions successives par 2**, la dernière ayant pour quotient 0 ;
- écrire la liste **des restes** dans le sens inverse de leur obtention.

- Pour la partie décimale du nombre :

- effectuer des **multiplications successives par 2 ne portant que sur les parties décimales** jusqu'à obtenir soit 1 soit la précision demandée ;
- écrire la liste des **parties entières** des produits dans l'ordre où ils sont apparus ;
- appliquer éventuellement la règle de l'arrondie en binaire.

Applications immédiates : Écrire dans le système binaire les nombres suivants.

71 =

238 =

25,25 =

62,625 =

3°) <u>Passage de l'hexadécimal au décimal</u> :

C'est la même méthode que pour passer du binaire au décimal, en remplaçant 2 par 16 et en utilisant éventuellement le tableau de correspondance par A, B, C, … , F.

10	11	12	13	14	15
A	B	C	D	E	F

<u>Méthode</u> : Passage de l'hexadécimal au décimal :
- Exprimer le nombre à l'aide des puissances de 16.

<u>Exemple</u> : $(3C,1A)_{16} = 3 \times 16^1 + 12 \times 16^0 + 1 \times 16^{-1} + 10 \times 16^{-2}$
$(3C,1A)_{16} = 48 + 12 + 0,0625 + 0,0390625$
Donc $(3C,1A)_{16} = 60,1015625$.

<u>Applications immédiates</u> : Écrire dans le système décimal les nombres suivants.

▪ $(BAC)_{16} =$

▪ $(6BF)_{16} =$

▪ $(DE,F31)_{16} =$

▪ $(7D0,3A)_{16} =$

4°) <u>Passage du décimal à l'hexadécimal</u> :

On adapte la méthode de passage du décimal au binaire.

<u>Méthode</u> : Passage du décimal à l'hexadécimal :
- Pour **la partie entière** du nombre :

- effectuer des **divisions successives par 16**, la dernière ayant pour quotient 0 ;
- écrire la liste **des restes** dans le sens inverse de leur obtention.

- Pour la partie décimale du nombre :

- effectuer des **multiplications successives par 16 ne portant que sur les parties décimales** jusqu'à obtenir soit un entier (non nul) soit la précision demandée ;
- écrire la liste des **parties entières** des produits dans l'ordre où ils sont apparus ;

<u>Exemple</u> : Exprimons 2 656,71875 en hexadécimal.

2 656 | 16
0 | 166 | 16
6 | 10 | 16
10 | 0

A60

$0,71875 \times 16 = 11,5$
$0,5 \times 16 = 8$

B8

Donc $2\,656,71875 = (A60,B8)_{16}$

Applications immédiates : Écrire dans le système hexadécimal les nombres suivants.

2 392 =

11 525 =

3 840,2890625 =

2 199,4375 =

5°) Passage de l'hexadécimal au binaire :

Exemple : $(3C,1A)_{16} = 3 \times 16^{1} + 12 \times 16^{0} + 1 \times 16^{-1} + 10 \times 16^{-2}$ Le calcul est effectué dans le système décimal.

$(3C,1A)_{16} = 3 \times (2^{4})^{1} + 12 \times (2^{4})^{0} + 1 \times (2^{4})^{-1} + 10 \times (2^{4})^{-2}$ puisque $16 = 2^{4}$.

$(3C,1A)_{16} = 3 \times 2^{4} + 12 \times 2^{0} + 1 \times 2^{-4} + 10 \times 2^{-8}$

$(3C,1A)_{16} = (2 + 1) \times 2^{4} + (8 + 4) \times 2^{0} + 1 \times 2^{-4} + (8 + 2) \times 2^{-8}$

$(3C,1A)_{16} = (2^{1} + 1) \times 2^{4} + (2^{3} + 2^{2}) \times 2^{0} + 1 \times 2^{-4} + (2^{3} + 2^{1}) \times 2^{-8}$ en exprimant 2,8 et 4 à l'aide de puissances de 2.

$(3C,1A)_{16} = 2^{5} + 2^{4} + 2^{3} + 2^{2} + 2^{-4} + 2^{-5} + 2^{-7}$

$(3C,1A)_{16} = 1 \times 2^{5} + 1 \times 2^{4} + 1 \times 2^{3} + 1 \times 2^{2} + 0 \times 2^{1} + 0 \times 2^{0} + 0 \times 2^{-1} + 0 \times 2^{-2} + 0 \times 2^{-3} + 1 \times 2^{-4} + 1 \times 2^{-5} + 0 \times 2^{-6} + 1 \times 2^{-7}$

$(3C,1A)_{16} = (111100,0001101)_{2}$

Regroupons ces symboles et 1 par paquets de 4 bits autour de la virgule et ajoutons des 0 pour compléter les paquets aux deux extrémités :

$(3C,1A)_{16} = (\underbrace{0011}\underbrace{1100},\underbrace{0001}\underbrace{1010})_{2}$

Or $(0011)_{2} = (3)_{16}$, $(1100)_{2} = (C)_{16}$, $(0001)_{2} = (1)_{16}$ et $(1010)_{2} = (A)_{16}$.

Décimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadécimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Binaire à quatre bits	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Méthode : Passage de l'hexadécimal au binaire :

- Exprimer en **binaire à 4 bits** chaque symbole du nombre en hexadécimal.
- Supprimer les éventuels 0 (inutiles) à gauche de la partie entière et à l'extrémité droite après la virgule.

Remarque : Cette correspondance entre les systèmes de numération de base 2 et 16 repose sur l'égalité $16 = 2^{4}$.

Applications immédiates : Écrire dans le système binaire les nombres suivants.

$(2A7)_{16} =$

$(B3C,09)_{16} =$

6°) **Passage du binaire à l'hexadécimal :**

C'est le passage inverse du précédent d'où la méthode.

Méthode : Passage du binaire à l'hexadécimal :
- Regrouper les symboles du nombre binaire en paquets de 4 bits à partir de la virgule en complétant avec des 0 si nécessaire.
- Remplacer alors chaque regroupement par sa valeur en hexadécimal.

Exemple : $(1101101,111011)_2 = \underbrace{0110}_{6}\underbrace{1101}_{D},\underbrace{1110}_{E}\underbrace{1100}_{C}$

$(1101101,111011)_2 = (6D,EC)_{16}$

Applications immédiates : Écrire dans le système hexadécimal les nombres suivants.

$(10011)_2 =$

$(110110,101)_2 =$

7°) **Conversions à l'aide des TICE :**

Le **tableur** et la **calculatrice CASIO** Graph 85 permettent d'effectuer directement les conversions entre systèmes de numération de base 10, 2 et 16 mais **uniquement pour des nombres entiers**.

Sur EXCEL :

Formule	Résultat	Egalité
=BINDEC (11011)	27	$(11011)_2 = 27$
=DECBIN (17)	1001	$17 = (10001)_2$
=HEXBIN ("3C")	111100	$(3C)_{16} = (111100)_2$
=BINHEX (110011)	33	$(110011)_2 = (33)_{16}$
=HEXDEC (23)	35	$(23)_{16} = 35$
=DECHEX (203)	CB	$203 = (CB)_{16}$

Remarque : La présence d'une lettre dans 3C oblige à mettre " " dans la parenthèse.

Sur CASIO :

- Appuyer sur **MENU** afin d'afficher le menu principal.
- Le mode **RUN** est en surbrillance, appuyer sur **EXE**
- Appuyer sur **SHIFT** **MENU** pour faire apparaitre l'écran de configuration.
- À l'aide du curseur, mettre la surbrillance sur **Mode** et sélectionner le mode d'affichage des résultats : **F2** pour DECimal, **F3** pour HEXadécimal, **F4** pour BINaire. Appuyer sur **EXE**
- Appuyer sur **F1** pour afficher un menu de symboles représentant les systèmes de numération.
- Saisir une valeur dans une autre base en la précédent de "d" (**F1**:décimal), "h" (**F2**:hexadécimal) ou "b" (**F3**:binaire) suivant la base dans laquelle est exprimée cette valeur.
- Appuyer sur **EXE**

III. Opérations sur les entiers naturels :

1°) Additions en base 2 :

Méthode : Les **additions en base 2** s'effectuent de la même façon que dans le système décimal, avec notamment la notion de **retenue** (ici en rouge), en utilisant la table d'addition suivante.

+	**0**	**1**
0	0	1
1	1	^{1}0

L'égalité 1 + 1 = 2 en système décimal se traduit en système binaire par :

1 + 1 = 10 noté $^{1}0$ où 1 est la **retenue**.

Exemple :

	1			
	1	1	0	1
+		1	1	0
1	0	0	1	1

où ^{1} est la retenue avec 1 + 1.

Applications immédiates :

	1	1	0	0
+		1	0	1

	1	0	1 ,		0	1	
+		1	1 ,		1	0	1

	1	0	1	0	1
+		1	1	0	0

	1	1	1	0 ,		1	1
+		1	0	0 ,		0	1

	1	1	0	0	1	1
+			1	0	1	0

	1	0	0	0	1 ,		0	1	1
+			1	1	1 ,		0	0	1

2°) Additions en base 16 :

Méthode : Les **additions en base 16** s'effectuent de la même façon que dans le système décimal, avec notamment la notion de **retenue** (ici en rouge), en utilisant la table d'addition suivante.

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11
3	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12
4	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13
5	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14
6	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15
7	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16
8	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17
9	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18
A	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19
B	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A
C	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B
D	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C
E	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D
F	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E

Exemple :

	1		1	
	B	A	3	E
+		7	5	2
	C	1	9	0

Applications immédiates :

	A	2	C	3
+		D	5	8

	8	9	7
+	7	9	8

	B	A	C
+	C	A	B

	4	B	,	6
+		0	,	A

	A	B	,	C
+	D	E	,	F

	7	5	,	B	0	9
+	1	9	,	1	9	7

3°) <u>Multiplications et divisions par une puissance de deux en base 2</u> :

Rappelons que dans le **système décimal**, c'est-à-dire **en base 10**, multiplier un nombre par 10 revient à décaler tous ses chiffres d'un rang vers la gauche (en ajoutant un zéro ou en déplaçant la virgule).

Ainsi $56 \times 10 = 560$ et $23{,}17 \times 10 = 231{,}7$.

De façon générale, multiplier un nombre par 10^n, où n est un entier naturel, revient à décaler tous ses chiffres de n rangs vers la gauche (en ajoutant des 0 ou en déplaçant la virgule).

Ainsi $56 \times 10^3 = 56\,000$ et $23{,}17 \times 10^4 = 231\,700$.

Inversement, diviser un nombre par 10^n, où n est un entier naturel, revient à décaler tous ses chiffres de n rangs vers la droite (en supprimant des 0 ou en déplaçant la virgule).

Ainsi $\dfrac{56}{10^3} = 0{,}056$ et $\dfrac{23{,}17}{10} = 2{,}317$.

Nous pouvons observer un phénomène analogue dans le **système binaire**, c'est-à-dire **en base 2**, pour la multiplication et la division par une puissance de deux.

Ainsi pour $(101)_2 \times (10)_2$:
nous avons $(101)_2 = 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 2^2 + 1$ et $(10)_2 = 1 \times 2^1 + 0 \times 2^0 = 2$
donc $(101)_2 \times (10)_2 = (2^2 + 1) \times 2 = 2^3 + 2$
donc $(101)_2 \times (10)_2 = (1010)_2$

Nous constatons que pour multiplier $(101)_2$ par $(10)_2 = 2$, il suffit de décaler tous les chiffres de $(101)_2$ d'un rang vers la gauche et d'ajouter un zéro.

De même $(110{,}01)_2 \times (1000)_2 = (110010)_2$ avec une démonstration analogue.
La multiplication par $(1000)_2 = 2^3$ revient à décaler tous les chiffres de 3 rangs vers la gauche en déplaçant la virgule et en ajoutant un zéro.

Dans le cas inverse d'une division, nous obtenons :
$(101)_2 : (10)_2 = \dfrac{2^2 + 1}{2} = \dfrac{2^2}{2} + \dfrac{1}{2} = 2 + 2^{-1}$ donc $(101)_2 : (10)_2 = (10{,}1)_2$

Nous constatons que pour diviser $(101)_2$ par $(10)_2 = 2$, il suffit de décaler tous les chiffres $(101)_2$ d'un rang vers la droite, ce qui entraîne l'apparition d'une virgule.

De même $(110{,}01)_2 : (1000)_2 = (0{,}11001)_2$ avec une démonstration analogue.
La division par $(1000)_2 = 2^3$ revient à décaler tous les chiffres de 3 rangs vers la droite en déplaçant la virgule.

Les démonstrations détaillées ci-dessus sur des exemples ont une portée générale et permettent d'énoncer la méthode suivante.

<u>Méthode</u> : ▪ Pour **multiplier par 2^n = $(\underbrace{100\ldots0}_{n\ \text{zéros}})_2$** un nombre écrit en base 2, **on décale tous ses chiffres de n rangs vers la gauche.**
On peut être ainsi amené à supprimer ou déplacer la virgule et à ajouter des 0.

▪ Pour **diviser par 2^n = $(\underbrace{100\ldots0}_{n\ \text{zéros}})_2$** un nombre écrit en base 2, **on décale tous ses chiffres de n rangs vers la droite.**
On peut être ainsi amené à introduire ou déplacer la virgule et à supprimer des 0.

Système décimal	Système binaire
2	$(10)_2$
2^2	$(100)_2$
2^3	$(1000)_2$
…	…
2^n	$(\underbrace{100\ldots0}_{n\ \text{zéros}})_2$

Exemples : $(10010)_2 \times (100)_2 = (1001000)_2$
$(11{,}001)_2 \times (10)_2 = (110{,}01)_2$
$(10010)_2 : (100)_2 = (100{,}1)_2$
$(11{,}011)_2 : (10)_2 = (1{,}1001)_2$

Applications immédiates :

$(101)_2 \times (100)_2 =$

$(1011)_2 \times (1000)_2 =$

$(11{,}11)_2 \times (10)_2 =$

$(101{,}1)_2 : (100)_2 =$

$(10{,}01)_2 : (1000)_2 =$

$(11{,}101)_2 : (100)_2 =$

IV. Exercice d'application :

Sur un ordinateur 16 bits, un entier N est représenté de la manière suivante : le premier bit à gauche donne le signe (0 correspond à + et 1 à –), et lorsque l'entier est positif, les 15 suivants sont les chiffres de l'écriture binaire de N.

Par exemple : **0**000000000011101 représente + $(11101)_2$ c'est-à-dire + 29.

1°) a) Que devrait logiquement représenter le nombre **1**000000000011101 ?

b) À quoi devrait être égal **0**000000000011101 + **1**000000000011101 ? Est-ce le cas ?

À cause du problème précédent, on opère différemment pour coder les entiers négatifs : le premier bit représente bien – s'il est égal à 1. Cependant, la somme d'un nombre N et de son opposé – N devra toujours être nulle. Pour cela, on adopte la méthode dite des **compléments**.

Par exemple, pour – 29, on part de la représentation de 29, c'est-à-dire **0**000000000011101 et on détermine les 16 bits **X**XXXXXXXXXXXXXXX tels que :
0000000000011101 + **X**XXXXXXXXXXXXXXX = **0**000000000000000.

Il s'agit alors de changer les 0 par des 1 et les 1 par des 0 dans la représentation de 29, puis d'ajouter 1 : cela donne **1**111111111100010 + 1 donc **1**111111111100011.

La représentation de 29 + (– 29) donne alors **1**0000000000000000, donc **0**000000000000000 (par dépassement des capacités de l'ordinateur).

2°) a) Déterminer la représentation de l'entier – 123 dans un ordinateur de 16 bits.

b) Déterminer la représentation de l'entier – 43 dans un ordinateur de 16 bits.

2

$2^{\text{ème}}$ partie : Arithmétique modulaire.

I. Division euclidienne :

Vous vous souvenez sans doute d'avoir fait des divisions à l'école primaire, dans lesquelles n'intervenaient que des nombres entiers positifs.

Par exemple : $\begin{array}{r|l} 43 & 5 \\ \hline 3 & 8 \end{array}$

Dans cette écriture : 43 s'appelle le **dividende** ; 5 est le **diviseur** ; 8 est le **quotient** et 3 est le **reste**.

Dans cette division très simple, vous pouvez établir sans difficulté les deux propriétés suivantes :

$43 = 5 \times 8 + 3$ et $0 \leq 3 < 5$

Dividende = Diviseur × Quotient + Reste et $0 \leq$ Reste $<$ Diviseur

Nous appelons désormais ce type de division : une **division euclidienne**.

Euclide est un mathématicien grec de l'Antiquité.

Notez bien que dans ce genre de division :
- n'interviennent que des nombres entiers (et jamais des décimaux) ;
- il est indispensable de bien avoir la relation : $0 \leq$ Reste $<$ Diviseur.

Nous pouvons désormais généraliser cette notion :

Pour tout entier naturel a et pour tout entier naturel non nul b, il existe des entiers naturels uniques q et r tels que :

$$\mathbf{a = bq + r \text{ avec } 0 \leq r < b}$$

L'entier naturel q est **le quotient** de **la division euclidienne** de a par b et l'entier naturel r est **le reste** de cette division.

<u>Exemple</u> : Le quotient est le reste de la division euclidienne de a = 53 par b = 6 sont respectivement q = 8 et r = 5.
En effet : $53 = 6 \times 8 + 5$ et $0 \leq 5 < 6$.

Sur EXCEL : La fonction MOD (a ; b) renvoie le reste de la division euclidienne de a par b.

<u>Application immédiate</u> :

1°) Déterminer un entier x positif, qui, divisé par 23 donne pour reste 1 et qui, divisé par 17 donne le même quotient et 13 pour reste.

2°) On note q et r le quotient et le reste de la division euclidienne de a par b ($a > 0$). Déterminer q sachant que q et r ne change pas lorsqu'on augmente a de 52 et b de 4.
Donner un exemple d'une telle division satisfaisant cette condition.

II. <u>Nombres premiers</u> :

1°) <u>Diviseurs et multiples d'un nombre entier naturel</u> :

Rappelons sur un exemple le vocabulaire concernant les diviseurs et les multiples d'un nombre entier naturel.

$12 = 3 \times 4$ donc 3 et 4 sont des **diviseurs** de 12 et 12 est un **multiple** de 3 et de 4.

$12 = 2 \times 6$ et $12 = 1 \times 12$
Donc 12 a aussi comme diviseurs 2, 6, 1 et 12.

Soit a et b des nombres entiers naturels.
a est un **multiple** de b s'il existe un entier naturel q tel que $a = bq$.
Alors, si $b \neq 0$, b est un **diviseur** de a (ou a **est divisible par** b).

Le reste de la division euclidienne de a par b est égal à 0.

<u>Remarques</u> :
- 1 a pour seul diviseur 1.
- Tout nombre entier naturel n tel que $n \geq 2$ a au moins deux diviseurs : 1 et n.
- Tout nombre entier naturel non nul a une infinité de multiples.
- 0 a pour seul multiple 0.
- 0 est un multiple de tout nombre entier naturel.

Rappelons quelques critères de divisibilité pour un nombre entier naturel n :
- n est **divisible par 2** s'il est pair (son chiffre des unités est 0, 2, 4, 6 ou 8) ;
- n est **divisible par 3** si la somme de ses chiffres est divisible par 3 ;
- n est **divisible par 4** si le nombre formé par ses deux chiffres de droite est divisible par 4 ;
- n est **divisible par 5** si son chiffre des unités est 0 ou 5 ;
- n est **divisible par 9** si la somme de ses chiffres est divisible par 9.

2°) Définition des nombres premiers :

Un nombre entier naturel est **premier** s'il a **exactement deux diviseurs** : 1 et lui-même.

Exemples : ▪ 0 n'est pas premier car il a une infinité de diviseurs : tous les entiers naturels non nuls.
▪ 1 n'est pas premier car il n'a qu'un seul diviseur : 1.
▪ 2 est premier car il a exactement deux diviseurs : 1 et 2.
▪ 3 est premier car il a exactement deux diviseurs : 1 et 3.
▪ 4 n'est pas premier car il a trois diviseurs : 1, 2 et 4.
▪ 5 est premier car il a exactement deux diviseurs : 1 et 5.
▪ 6 n'est pas premier car il a quatre diviseurs : 1, 2, 3 et 6.
▪ 7 est premier car il a exactement deux diviseurs : 1 et 7.
…

Remarque : L'ensemble des nombres premiers a une infinité d'éléments. L'étude de cet ensemble fait toujours l'objet de recherches.

3°) Reconnaissance des nombres premiers :

Le théorème suivant, que nous admettons, permet de tester si un nombre entier naturel donné est premier.

Théorème : Soit n un entier naturel supérieur ou égal à 2.
Si n n'est pas premier, alors il possède au moins un diviseur premier inférieur ou égal à $\sqrt{n}$.

Exemples : ▪ 221 est-il un nombre premier ?
$\sqrt{221}$ = 14,8660…
Les nombres premiers inférieurs à 14,9 sont : 2, 3, 5, 7, 11 et 13.
221 n'est pas divisibles par 2, 3, 5, 7 et 11 mais il est divisible par 13 ($221 = 13 \times 17$).
Donc 221 n'est pas un nombre premier.

▪ 223 est-il un nombre premier ?
$\sqrt{223}$ = 14,93318…
Les nombres premiers inférieurs à 14,9 sont : 2, 3, 5, 7, 11 et 13.
223 n'est pas divisibles par 2, 3, 5, 7, 11 et 13.
Donc 223 est un nombre premier.

Remarque : Mémoriser les nombres premiers inférieurs à 20, ils vous seront utiles par la suite : 2, 3, 5, 7, 11, 13, 17 et 19.

4°) Décomposition d'un nombre en produit de facteurs premiers :

Un nombre qui n'est pas premier peut être divisible par un nombre premier et même s'écrire uniquement avec des nombres premiers sous forme d'un produit.

Théorème : Tout entier naturel supérieur ou égal à 2 se décompose de façon unique (à l'ordre des facteurs près) en un produit de facteurs premiers.

Exemples :

- 84 n'est pas premier, il se décompose en un produit de facteurs premiers :
  $84 = 2 \times 42 = 2 \times 6 \times 7 = 2 \times 2 \times 3 \times 7 = 2^2 \times 3 \times 7$
  Cette décomposition est unique à l'ordre des facteurs près.
- 975 n'est pas premier, il se décompose en un produit de facteurs premiers :
  $975 = 5 \times 95 = 5 \times 5 \times 39 = 5 \times 5 \times 3 \times 13 = 3 \times 5^2 \times 13$.

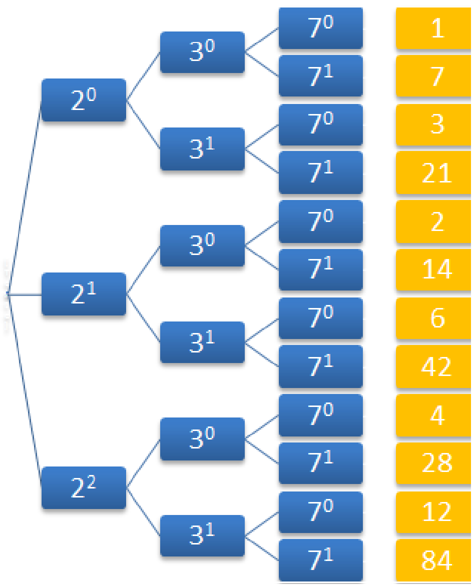
En pratique, on divise le nombre par son **plus petit diviseur premier** et on recommence jusqu'à ce que le quotient soit 1. Les calculs étant présentés comme ci-dessous :

84	2
42	2
21	3
7	7
1	

975	3
325	5
65	5
13	13
1	

La décomposition d'un nombre en produit de facteurs premiers permet d'obtenir tous ses diviseurs.

Exemple : $84 = 2^2 \times 3 \times 7$
Un diviseur de 84 s'écrit donc : $2^i \times 3^j \times 7^k$ avec $0 \leq i \leq 2$, $0 \leq j \leq 1$, $0 \leq k \leq 1$.
Nous pouvons dresser leur liste à l'aide d'un arbre :



84 a 12 diviseurs : 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 et 84.

5°) Applications immédiates :

Exercice 1 : Sans les déterminer tous, calculer le nombre de diviseurs de 3 600 ? De 21 168 ?

Exercice 2 : En employant la méthode l'arbre vue précédemment, déterminer la liste des diviseurs de 5 096. Combien y en a-t-il ?

Exercice 3 : On pose : $x = 2^4 \times 3^5 \times 5 \times 7^2 \times 11$ et $y = 2^3 \times 3^2 \times 7 \times 11$.

1°) Montrer que x est divisible par y.

2°) Quel est le quotient de la division de x par y ?

3°) Quel est le plus petit entier naturel par lequel il faut multiplier x pour obtenir le carré d'un entier naturel ?

III. PGCD de deux entiers :

Étant donnée deux entiers naturels non nuls a et b, il existe un diviseur commun à a et à b qui est plus grand que tous les autres. Ce diviseur est appelé **Plus Grand Commun Diviseur** et se note PGCD(a ; b).

Remarque : Deux entiers naturels non nuls sont **premiers entre eux** si et seulement si leur PGCD est égal à 1.

Exemple : ▪ Les diviseurs de 45 sont : 1, 3, 5, 9, 15 et 45 (puisque $45 = 3^2 \times 5$).
Ceux de 105 sont : 1, 3, 5, 7, 15, 21, 35 et 105 (puisque $105 = 3 \times 5 \times 7$).
Les diviseurs communs à 45 et 105 sont : 1, 3, 5 et 15.
Le plus grand d'entre eux est 15 donc 15 est le PGCD de 45 et 105.
On écrit PGCD(45 ; 105) = 15.

$$\begin{array}{r|l} 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r|l} 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

▪ Les diviseurs de 15 sont : 1, 3, 5 et 15 (puisque $15 = 3 \times 5$).
Ceux de 44 sont : 1, 2, 4, 11, 22 et 44 (puisque $44 = 2^2 \times 11$).
Le seul diviseur commun à 15 et à 44 est 1 donc 1 est le PGCD de 15 et 44.
On écrit PGCD(15 ; 44) = 1.
15 et 44 sont donc premiers entre eux.

$$\begin{array}{r|l} 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r|l} 44 & 2 \\ 22 & 2 \\ 11 & 11 \\ 1 & \end{array}$$

Remarque : $45 = 3^2 \times 5$ et $105 = 3 \times 5 \times 7$.
PGCD (45 ; 105) $= 15 = 3 \times 5$.
Nous observons que 15 est le produit des facteurs premiers communs à 45 et 105, chacun étant affecté de l'exposant le plus faible.

Propriété 1 : Soit a et b deux entiers naturels supérieurs ou égaux à 2 dont on connaît les décompositions en produits de facteurs premiers :
▪ s'ils n'ont pas de facteur commun, alors leur PGCD est 1 ;
▪ sinon, leur PGCD est le produit des facteurs communs aux deux décompositions, chaque facteur étant affecté du plus petit exposant avec lequel il figure dans les deux décompositions.

Exemples : ▪ Soient $a = 4\,950 = 2 \times 3^2 \times 5^2 \times 11$ et $b = 4\,875 = 3 \times 5^3 \times 13$.
Les facteurs communs aux deux décompositions sont 3 et 5.
3 figure avec les exposants 2 et 1, on garde le plus petit, c'est-à-dire 1.
5 figure avec les exposants 2 et 3, on garde le plus petit, c'est-à-dire 2.
Donc PGCD(4 950 ; 4 875) $= 3 \times 5^2 = 75$.

$$\begin{array}{r|l} 4\,950 & 2 \\ 2\,475 & 3 \\ 825 & 3 \\ 275 & 5 \\ 55 & 5 \\ 11 & 11 \\ 1 & \end{array} \qquad \begin{array}{r|l} 4\,875 & 3 \\ 1\,625 & 5 \\ 325 & 5 \\ 65 & 5 \\ 13 & 13 \\ 1 & \end{array}$$

▪ Soient $a = 2^4 \times 3 \times 5^2 \times 7 \times 19$ et $b = 2^3 \times 3^2 \times 7^2 \times 17$.
Les facteurs communs aux deux décompositions sont 2, 3 et 7.
Les plus petits exposants sont 3 pour le facteur 2, 1 pour le facteur 3 et 1 pour le facteur 7.
Donc PGCD $= 2^3 \times 3 \times 7 = 168$.

Propriété 2 : Soit a et b deux entiers naturels non nuls tels que $a > b$.
Soit r le reste de la division euclidienne de a par b.
Alors PGCD(a ; b) = PGCD(b ; r).

Cette deuxième propriété permet d'avoir une autre méthode pour chercher un PGCD. On applique plusieurs fois la propriété jusqu'à obtenir un reste nul. Le PGCD est alors le dernier diviseur essayé.
Son avantage est qu'elle est algorithmique, donc programmable. Elle est connue sous le nom d'**algorithme d'Euclide**.

Exemple : Cherchons le PGCD de 420 et 182.

a	b	Reste de a : b
420	182	56
182	56	14
56	14	0

Le dernier diviseur essayé est 14.
Donc PGCD(420 ; 182) = 14.

Application immédiate : Un lycée organise un tournoi sportif par équipe pour tous ses étudiants en BTS. Chaque équipe doit comporter le même nombre de filles et le même nombre de garçons. Les professeurs souhaitent constituer le plus grand nombre possible d'équipes. Il y a 201 filles et 294 garçons.

1°) Quel est le plus grand nombre d'équipes que l'on peut constituer ?

2°) Combien y a-t-il alors de filles et de garçons dans chaque équipe ?

IV. Congruences :

Soit n un entier naturel non nul. On dit que deux entiers naturels **a et b sont congrus modulo n** si et seulement si a et b ont le même reste dans la division euclidienne par n.

On écrit alors a ≡ b (n) ou b ≡ a (n).

Quel que soit a entier, **a ≡ a (n)** et **a ≡ r (n)**, r étant le reste de la division euclidienne de a par n.

Exemples : ▪ $\begin{array}{r|l} 101 & \underline{\ 7\ } \\ 3 & 14 \end{array}$ et $\begin{array}{r|l} 66 & \underline{\ 7\ } \\ 3 & 9 \end{array}$

$101 = 7 \times 14 + 3$ et $66 = 7 \times 9 + 3$

Donc 101 et 66 sont congrus modulo 7 car ils ont le même reste dans les divisions euclidiennes par 7.

On peut donc écrire $101 \equiv 66\ (7)$.

▪ $\begin{array}{r|l} 67 & \underline{\ 12\ } \\ 7 & 5 \end{array}$ et $\begin{array}{r|l} 139 & \underline{\ 12\ } \\ 7 & 11 \end{array}$

$67 = 12 \times 5 + 7$ et $139 = 12 \times 11 + 7$

Donc $67 \equiv 139\ (12)$ car le reste est le même dans les divisions euclidiennes par 12.

▪ $\begin{array}{r|l} 29 & \underline{\ 8\ } \\ 5 & 3 \end{array}$ donc $29 \equiv 5\ (8)$ puisque $\begin{array}{r|l} 5 & \underline{\ 8\ } \\ 5 & 0 \end{array}$

▪ $\begin{array}{r|l} 90 & \underline{\ 11\ } \\ 2 & 8 \end{array}$ et $\begin{array}{r|l} 80 & \underline{\ 11\ } \\ 3 & 7 \end{array}$

90 et 80 ne sont pas congrus modulo 11 car les restes dans les divisions euclidiennes par 11 sont 2 et 3.

Propriété 1 : Soit a et b deux entiers naturels tels que $a > b$ et soit n un entier naturel non nul.
a est congru à b modulo n si et seulement si $a - b$ est multiple de n.

Exemples : ▪ On vient de montrer que $101 \equiv 66\ (7)$.

Et $101 - 66 = 35 = 5 \times 7$.

Donc $101 - 66$ est un multiple de 7.

▪ On vient de montrer que $67 \equiv 139\ (12)$.

Et $139 - 67 = 72 = 6 \times 12$.

Donc $139 - 67$ est un multiple de 12.

Propriété 2 : Soit a, a', b et b' des entiers naturels et soit n un entier naturel non nul.
Si $a \equiv b\ (n)$ et $a' \equiv b'\ (n)$ alors :

- $a + a' \equiv b + b'\ (n)$;
- $aa' \equiv bb'\ (n)$;
- $ma \equiv mb\ (n)$ pour tout entier naturel non nul m.
- $a^m \equiv b^m\ (n)$ pour tout entier naturel non nul m.

Si, de plus, $a \geq a'$ et $b \geq b'$, alors $a - a' \equiv b - b'\ (n)$.

Exemples : À partir des congruences $2\,014 \equiv 1\ (3)$ et $1\,000 \equiv 1\ (3)$, les propriétés précédentes permettent d'obtenir facilement d'autres congruences :

$\begin{array}{r|l} 2\,014 & \underline{\ 3\ } \\ 1 & 671 \end{array}$ $\begin{array}{r|l} 1\,000 & \underline{\ 3\ } \\ 1 & 333 \end{array}$

$2\,014 + 1\,000 \equiv 1 + 1\ (3)$ c'est-à-dire $3\,014 \equiv 2\ (3)$

$2\,014 \times 1\,000 \equiv 1 \times 1\ (3)$ c'est-à-dire $2\,014\,000 \equiv 1\ (3)$

$2\,014^{70} \equiv 1^{70}\ (3)$ c'est-à-dire $2\,014^{70} \equiv 1\ (3)$

$\begin{array}{r|l} 2\,014\,000 & \underline{\ 3\ } \\ 1 & 671\,333 \end{array}$ $\begin{array}{r|l} 3\,014 & \underline{\ 3\ } \\ 2 & 1\,004 \end{array}$

Application immédiate : Congruences et puissances.

1°) a) Donner le quotient et le reste de la division euclidienne de 2012 par 6.

b) En déduire que $3^{2012} = (3^6)^{335} \times 3^2$.

2°) a) Compléter les résultats suivants : $3^2 \equiv$ ………. (7) et $3^6 \equiv$ ………. (7).

b) Déduire de ce qui précède que $3^{2012} \equiv 2$ (7) et déterminer le reste de la division euclidienne de 3^{2012} par 7.