CHAPITRE 3

Arithmétique

Ce chapitre concerne les notions les plus utiles à l'informatique.

COURS

1 Systèmes de numération

A. Base d'un système de numération

L'écriture des nombres suivant l'époque et le lieu fut très diverse : pensez, par exemple, aux chiffres romains I, II, III, IV, V, VI,...

Numération en base 10

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.

Observez que c'est la **position** des deux 5 figurant dans 5 615 qui définit le rôle de chacun.

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

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

Ainsi les nombres entiers positifs sont écrits à l'aide des dix chiffres 0, 1, 2, ..., 9, la position de chaque chiffre indiquant à quelle puissance de 10 il est associé.

Les nombres négatifs sont précédés du signe moins (–).

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

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

Numération en base 2

bit : binary digit.

En informatique, le plus petit élément d'information utilisé, appelé **bit**, 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.**

Le système de numération en base 2 est aussi appelé système **binaire** et celui en base 10 système **décimal.**

Dans la numération en base 2, on dispose de deux chiffres : 0 et 1.

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.

Ainsi $3 = 2 + 1 = 1 \times 2^1 + 1 \times 2^0$ est noté 11 en base 2 et lu « un un ».

$3 = 11_2$ où la base 2 est rappelée en indice pour éviter la confusion avec le nombre onze.

De même $6 = 4 + 2 = 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0$ est noté 110 en base 2.

$6 = 110_2$ lu « un un zéro ».

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

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

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

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

Le programme de mathématiques n'aborde pas l'étude des codes.

Remarques

- Quelle que soit la base utilisée, les nombres négatifs sont précédés du signe moins (–).
- L'écriture 101101 en binaire correspond en décimal à :

$1\times2^5+0\times2^4+1\times2^3+1\times2^2+0\times2^1+1\times2^0=32+8+4+1=45$.

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.

Numération en base 16

L'intérêt essentiel du système binaire en informatique provient du lien entre le calcul binaire (voir le paragraphe C) et le calcul booléen (voir le chapitre 4).

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 élevé de bits pour écrire un nombre entier dès que celui-ci atteint quelques dizaines.

hexa vient du mot grec signifiant 6 et **décimal** du mot latin signifiant 10.

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,… 9 les six lettres majuscules A, B, C, D, E, F.

Nous obtenons ainsi le tableau de correspondance entre les systèmes décimal, hexadécimal et binaire, ce dernier étant ici exprimé à l'aide de quatre bits.

Observez que quatre bits sont nécessaires et suffisants pour représenter en binaire les seize symboles de l'hexadécimal.

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,… 9, A,… F, la position de chacun correspondant à une puissance de 16.

$16^2=256$,
$16^3=4\,096$,…

Ainsi $38=32+6=2\times16^1+6\times16^0$ est 26 en hexadécimal et noté 26_{16}.

De même $164=160+4=10\times16^1+4\times16^0$ est noté A4 en hexadécimal.

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

$16^{-1}=\dfrac{1}{16}=0{,}0625$; donc $0{,}0625=1\times16^{-1}$ est 0,1 en hexadécimal et noté $0{,}1_{16}$.

$16^{-2}=\dfrac{1}{256}=0{,}00390625$; donc $0{,}00390625=0\times16^{-1}+1\times16^{-2}$ est 0,01 en hexadécimal et noté $0{,}01_{16}$.

Inversement A2C en hexadécimal correspond au nombre
$10\times16^2+2\times16^1+12\times16^0=2\,560+32+12=2\,594$.

De même 0,3B en hexadécimal correspond au nombre
$3\times16^{-1}+11\times16^{-2}=3\times0{,}0625+11\times0{,}00390625=0{,}2304715$.

B. Conversions 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.

Nous admettons la portée générale des méthodes ainsi introduites.

Passage du binaire au décimal

Exemple

$101{,}0101_2 = 2^2 + 1 + 2^{-2} + 2^{-4}$

$101{,}0101_2 = 4 + 1 + 0{,}25 + 0{,}0625.$

Donc $101{,}0101_2 = 5{,}3125$.

On n'écrit ici ni les puissances de 2 multipliées par 0, ni les facteurs 1 et on remplace 2^0 par 1.

MÉTHODE

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

Le calcul est effectué dans le système décimal.

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 (au plus près) à 10^{-3} est 5,313 car la première décimale abandonnée est 5,
- l'arrondi (au plus près) à 10^{-2} est 5,31 car la première décimale abandonnée est 2.

Ici la précision de l'arrondi est 10^{-3}.

L'expression « au plus près » est en général sous-entendue.

Ici la précision de l'arrondi est 10^{-2}.

D'une manière générale, l'arrondi (au plus près) 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.**

L'arrondi **par défaut** correspond à une **troncature** : on coupe l'écriture en enlevant des décimales.

L'arrondi **par excès** consiste à **ajouter** 1 à la dernière décimale conservée.

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.

13	2		
1	6	2	
0	3	2	
	1	1	2
		1	0

Sens de la lecture

$13 = 6 \times 2 + 1,$

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

$3 = 2 + 1,$ donc $13 = (2 + 1)2^2 + 1,$

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

Donc $13 = 1101_2$.

La division « posée » avec un calcul « à la main » figure dans les programmes de l'école et du collège.

Les restes successifs sont notés en vert.

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 la façon suivante.

Pour 1,5 nous ne retenons que sa partie décimale 0,5 pour la multiplication suivante.

Sens de la lecture

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

$0{,}75 \times 2 = 1{,}5$ donc $0{,}75 = 2^{-1} \times 1{,}5$ et $0{,}375 = 2^{-1}(2^{-1} \times 1{,}5) = 2^{-2} \times 1{,}5$, $0{,}375 = 2^{-2}(1 + 0{,}5)$

$0{,}5 \times 2 = 1$ donc $0{,}5 = 2^{-1}$ et $0{,}375 = 2^{-2}(1 + 2^{-1})$, $0{,}375 = 2^{-2} + 2^{-3}$.

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 définitive $13{,}375 = 13 + 0{,}375$ a pour écriture en binaire $1101{,}011_2$.

Nous venons de démontrer que $13 = 1101_2$.

Remarque

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

$0{,}4 \times 2 = 0{,}8$ donc $0{,}4 = 2^{-1} \times 0{,}8$

$0{,}8 \times 2 = 1{,}6$ donc $0{,}8 = 2^{-1} \times 1{,}6$ et $0{,}4 = 2^{-2} \times 1{,}6$

$0{,}6 \times 2 = 1{,}2$ donc $0{,}6 = 2^{-1} \times 1{,}2$ et $0{,}4 = 2^{-2}(1 + 2^{-1} \times 1{,}2)$, $0{,}4 = 2^{-2} + 2^{-3} \times 1{,}2$.

$0{,}2 \times 2 = 0{,}4$ donc $0{,}2 = 2^{-1} \times 0{,}4$ et $0{,}4 = 2^{-2} + 2^{-4} \times 0{,}4$,

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

$0{,}4 \times 2$ est le premier membre de la première égalité ci-dessus.

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 alors le problème de l'**arrondi** (au plus près) **en binaire**, qui est géré comme dans la numération en base 10 :
– **si le premier symbole abandonné est 0, on fait une troncature** : on abandonne les symboles suivants (arrondi par défaut) ;
– **si le premier symbole abandonné est 1, on ajoute 1 au dernier symbole conservé** (arrondi par excès).

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.

Nous observons le même phénomène dans le système décimal où $\dfrac{1}{3} = 0{,}333\ldots$ et $\dfrac{1}{7} = 0{,}142\,857\,142\,857\ldots$

L'addition en binaire est présentée au paragraphe C.

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 d'arrondi en binaire.

Voir ci-dessus la démarche détaillée pour 13,375 et 13,4.

1 est le seul entier non nul qui peut ainsi être obtenu.

Voir la remarque ci-dessus.

Passage de l'hexadécimal au binaire

Exemple

Le calcul est effectué dans le système décimal.

$3C,1A_{16} = 3 \times 16 + 12 + 16^{-1} + 10 \times 16^{-2}$ car $C_{16} = 12$ et $A_{16} = 10$.

$3C,1A_{16} = (2 + 1)2^4 + (2^3 + 2^2) + (2^4)^{-1} + (2^3 + 2)(2^4)^{-2}$ en exprimant 3, 12 et 10 à l'aide des puissances de 2 et car $16 = 2^4$.

$(2^4)^{-1} = 2^{-4}$ et $(2^4)^{-2} = 2^{-8}$.

$3C,1A_{16} = 2^5 + 2^4 + 2^3 + 2^2 + 2^{-4} + 2^{-5} + 2^{-7}$,

$3C,1A_{16} = 111100,0001101_2$.

$16 = 2^4$.

Regroupons ces symboles 0 et 1 par paquets de 4 bits autour de la virgule et rajoutons (en vert) des 0 pour compléter les paquets aux deux extrémités :

$3C,\ 1A_{16} = 0011\ 1100,0001\ 1010_2$

Voir le tableau de correspondance à la fin du paragraphe **A** ou en bas de cette page.

Or $0011_2 = 3_{16}$, $1100_2 = C_{16}$, $0001_2 = 1_{16}$ et $1010_2 = A_{16}$.

Nous constatons que l'écriture en binaire d'un nombre écrit en hexadécimal est obtenue par la méthode suivante.

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.

Cette correspondance entre les systèmes de numération de base 2 et 16 et la correspondance inverse ci-dessous reposent sur l'égalité $16 = 2^4$.

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.

Voir le tableau de correspondance à la fin du paragraphe **A** ou ci-dessous.

Exemple

$1101101,111011_2 = 0110\ 1101,1110\ 1100$

$\qquad\qquad\qquad\quad\ 6\ \ D\ \ E\ \ C$

$1101101,111011_2 = 6D,EC_{16}$

Passage de l'hexadécimal au décimal

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,... F.

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

MÉTHODE

Passage de l'hexadécimal au décimal :
Exprimer le nombre à l'aide des puissances de 16.

Le calcul est effectué dans le système décimal.

Exemple

$3C,1A_{16} = 3 \times 16 + 12 + 16^{-1} + 10 \times 16^{-2}$

$3C,1A_{16} = 48 + 12 + 0,0625 + 0,0390625$

$3C,\ 1A_{16} = 60,1015625$.

Passage du décimal à l'hexadécimal

On adapte la méthode de passage du décimal au binaire.

MÉTHODE

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.

La règle d'arrondi en base 16 n'est pas au programme de mathématiques du BTS SIO.

Exemple

Exprimons 2 656,718 75 en hexadécimal.

2 656	16	
0	166	16
6	10	16
10	0	

A60

$0{,}718\,75 \times 16 = 11{,}5$
$0{,}5 \times 16 = 8$ ↓ B8

A	B
10	11

$2\,656{,}718\,75 = A60{,}B8_{16}$.

Remarque

Le **tableur** permet d'effectuer directement les conversions entre systèmes de numération de base 10, 2 et 16, mais **uniquement pour des nombres entiers.**

BIN pour binaire, DEC pour décimal et HEX pour hexadécimal.

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

Formule	Résultat	Égalité
=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	$203 = CB_{16}$

C. Opérations sur les entiers naturels

Nous nous limitons ici aux « capacités attendues » figurant dans le programme de mathématiques du BTS SIO.

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.

Dans le système décimal, en notant la retenue en rouge :

$$\begin{array}{r} {\scriptstyle 1} \\ 85 \\ +\ 39 \\ \hline 124 \end{array}$$

+	**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**.

En pratique, on n'écrit pas les retenues et on donne directement le résultat.

Exemple

$$\begin{array}{r} {\scriptstyle 1} \\ 1\,101 \\ +\;\;110 \\ \hline 10\,011 \end{array}$$

où ^{1} est la retenue avec $1+1$.

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	5	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	^{1}0
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1
3	3	4	5	6	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2
4	4	5	6	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3
5	5	6	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4
6	6	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5
7	7	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6
8	8	9	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7
9	9	A	B	D	C	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8
A	A	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9
B	B	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9	^{1}A
C	C	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9	^{1}A	^{1}B
D	D	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9	^{1}A	^{1}B	^{1}C
E	E	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9	^{1}A	^{1}B	^{1}C	^{1}D
F	F	^{1}0	^{1}1	^{1}2	^{1}3	^{1}4	^{1}5	^{1}6	^{1}7	^{1}8	^{1}9	^{1}A	^{1}B	^{1}C	^{1}D	^{1}E

Exemple

$$\begin{array}{r} {\scriptstyle 1\;\;1} \\ \text{BA3E} \\ +\;\;\text{752} \\ \hline \text{C190} \end{array}$$

Multiplications et divisions par une puissance de deux, en base 2

• 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).

$56 = 5 \times 10 + 6$
$56 \times 10 = 5 \times 10^2 + 6 \times 10 + 0$

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

De façon plus 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 $\frac{56}{10^3} = 0{,}056$ et $\frac{23{,}17}{10} = 2{,}317$.

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 $101_2 = 2^2 + 1$ et $10_2 = 2$,
donc $101_2 \times 10_2 = (2^2 + 1)2 = 2^3 + 2$,
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 $110{,}01_2 \times 1\,000_2 = 110\,010_2$ avec une démonstration analogue : la multiplication par $1\,000_2 = 2^3$ 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 :

$101_2 : 10_2 = \frac{2^2+1}{2} = 2 + 2^{-1}$, 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 de 101_2 d'un rang vers la droite, ce qui entraîne l'apparition d'une virgule.

De même $110{,}01_2 : 1\,000_2 = 0{,}110\,01_2$ avec une démonstration analogue : la division par $1\,000_2 = 2^3$ 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.

Système décimal	*Système binaire*
2	10_2
$2^2 = 4$	100_2
$2^3 = 8$	$1\,000_2$
...	...
2^n	$\underbrace{10\ldots0}_{n \text{ zéros}}{}_2$

MÉTHODE

Pour **multiplier** (respectivement **diviser**) **par** $2^n = \underbrace{10\ldots0}_{n \text{ zéros}}{}_2$, un nombre écrit en base 2, **on décale tous ses chiffres de** n **rangs vers la gauche** (respectivement **vers la droite**).

On peut être ainsi amené à supprimer (resp. introduire) ou déplacer la virgule et à ajouter (resp. supprimer) des 0.

Exemples

$10\,010_2 \times 100_2 = 1\,001\,000_2$

$11{,}001_2 \times 10_2 = 110{,}01_2$

$10\,010_2 : 100_2 = 100{,}1_2$

$11{,}011_2 : 10_2 = 1{,}100\,1_2$.

2 Arithmétique modulaire

La signification de l'adjectif « modulaire » apparaîtra au paragraphe D ci-après.

A. Division euclidienne

Le résultat exact ou approché de la division d'un nombre entier naturel par un nombre entier naturel non nul est généralement obtenu par calcul mental dans les cas élémentaires ou à l'aide d'une calculatrice ou d'un tableur.

Euclide est un mathématicien de la Grèce antique dont les « Éléments » constituent un texte fondateur des mathématiques.

Exemples

$6 : 3 = 2$ ou $\frac{6}{3} = 2$; $\frac{15}{2} = 7{,}5$;

$\frac{13}{3} = 4{,}333\ldots$ avec une infinité de 3 ou $\frac{13}{3} \approx 4{,}3$ en arrondissant à 10^{-1}.

$\frac{136}{17} = 8$; $\frac{153}{17} = 9$ et $\frac{149}{17} \approx 8{,}765$ en arrondissant à 10^{-3}.

Remarque

À l'école, puis au collège, la division « posée » avec un calcul « à la main » a aussi été introduite et utilisée.

$$\begin{array}{r|l} 149 & 17 \\ \hline -136 & 8 \\ \hline 13 & \end{array} \quad \text{ou} \quad \begin{array}{r|l} 149 & 17 \\ \hline 13 & 8 \end{array}$$

Rappelons sur cet exemple le vocabulaire utilisé :
149 est le **dividende**, 17 est le **diviseur**, 8 est le **quotient** et 13 est le **reste**.

Cette division peut être prolongée

$$\begin{array}{r|l} 149 & 17 \\ \hline 130 & 8{,}7 \\ 11 & \end{array}$$

mais dans la suite nous ne considérerons que des nombres entiers naturels.

Les derniers exemples ci-dessus nous permettent de remarquer que la partie entière de $\frac{149}{17} \approx 8{,}765$ est 8 et que $17 \times 8 = 136$.

$149 - 136 = 13$.

Donc $149 = 17 \times 8 + 13$ où $0 \leq 13 < 17$.

Dans chaque cas, 8 est le plus grand entier naturel tel que 17×8 soit inférieur ou égal au nombre figurant dans le membre de gauche de l'égalité.

De même :

$152 = 17 \times 8 + 16$ où $0 \leq 16 < 17$,
$151 = 17 \times 8 + 15$ où $0 \leq 15 < 17$,
$150 = 17 \times 8 + 14$ où $0 \leq 14 < 17$,

$137 = 17 \times 8 + 1$ où $0 \leq 1 < 17$,
$136 = 17 \times 8 + 0$ où $0 \leq 0 < 17$.

En continuant au-delà de 152 et en deçà de 136, nous obtenons :

$153 = 17 \times 9 + 0$ où $0 \leq 0 < 17$,
$154 = 17 \times 9 + 1$ où $0 \leq 1 < 17$,

$135 = 17 \times 7 + 16$ où $0 \leq 16 < 17$,
$134 = 17 \times 7 + 15$ où $0 \leq 15 < 17$.

Tous ces résultats sont du type : $a = bq + r$ où $0 \leq r < b$.

Nous venons de démontrer que, pour tout entier naturel a compris entre 134 et 135 et pour $b = 17$, **il existe deux entiers naturels uniques q et r tels que $a = bq + r$ avec $0 \leq r < b$** :
q est le plus grand nombre entier naturel tel que $bq \leq a$ et $r = a - bq$.

Nous admettons ici que ce résultat est général.

Conformément au programme du BTS SIO, « *on se limite aux entiers naturels* ».

THÉORÈME

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

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

DÉFINITION

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.

B. Nombres premiers

Diviseurs et multiples d'un nombre entier naturel

Ici le mot diviseur a un sens différent de celui figurant dans une division euclidienne.

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 pour diviseurs 2, 6, 1 et 12.

DÉFINITION

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

Remarques

- 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.

Par exemple, les multiples de 2 sont les nombres pairs.

$0b = 0$, pour tout b.

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.

1 712 est divisible par 4 car 12 est divisible par 4.

Définition des nombres premiers

DÉFINITION

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

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 a un seul diviseur : 1.

2 est premier.

3, 5 et 7 sont premiers.

2 est le seul entier pair premier.

Ce résultat est démontré dans les Éléments d'Euclide (III^e siècle avant notre ère ?).

Remarque

L'ensemble des nombres premiers a une infinité d'éléments.
L'étude de cet ensemble fait toujours l'objet de recherches : ainsi le 25 janvier 2013 le plus grand nombre premier connu devenait $2^{57\,885\,161} - 1$ qui comporte 17 425 170 chiffres dont l'écriture nécessite environ 4 000 pages format A4 polices Times New Roman en taille 12.

Recherche de nombres premiers

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

THÉORÈME

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

En conséquence, **si un nombre entier naturel n, avec $n \geq 2$, n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$, alors n est un nombre premier.**

Exemple

Les nombres 221 et 223 sont-ils premiers ?

$\sqrt{221} \approx 14{,}9$ et $\sqrt{223} \approx 14{,}9$.

Les nombres premiers inférieurs à 14,9 sont : 2, 3, 5, 7, 11 et 13.

221 n'est pas divisible par 2, 3, 5, 7, 11 mais $221 = 13 \times 17$.

Donc 221 n'est pas un nombre premier.

223 n'est pas divisible par 2, 3, 5, 7, 11, 13. Donc 223 est un nombre premier.

Ératosthène (276-194 avant J.-C.) est un mathématicien grec, mais aussi un poète, un astronome,...

• On peut obtenir la liste des nombres premiers inférieurs à un nombre n donné à l'aide du **crible d'Ératosthène** :

– on écrit la liste des nombres compris entre 1 et n, par exemple sous la forme d'un tableau où les lignes correspondent aux dizaines ;

– on barre successivement 1, les multiples de 2, les multiples de 3, les multiples de 5,... c'est-à-dire les multiples de tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$;

– les nombres non barrés ainsi obtenus sont les nombres premiers inférieurs à n.

	1	2		8	9
10	11	12		18	19
20	21	22		28	29

Vérifiez le !

Par exemple, pour $n = 100$, les nombres premiers inférieurs à $\sqrt{100} = 10$ sont 2, 3, 5, 7 et on obtient ainsi 25 nombres premiers inférieurs à 100.

Décomposition en produit de facteurs premiers

Le théorème suivant, que nous admettons, montre l'importance des nombres premiers en arithmétique.

THÉORÈME

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

Exemple

Décomposons 150 en produit de facteurs premiers.

La méthode consiste à diviser 150 par son plus petit diviseur premier et à recommencer avec chaque quotient jusqu'à obtenir 1, les calculs étant présentés comme ci-contre.

150	2
75	3
25	5
5	5
1	

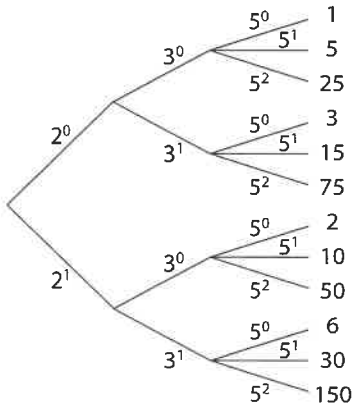
Nous obtenons $150 = 2 \times 3 \times 5^2$.

Cette méthode est à retenir.

Nous admettons ici que **le théorème précédent permet d'obtenir l'ensemble des diviseurs de tout nombre entier naturel supérieur ou égal à 2.**

Ainsi dans l'exemple ci-dessus les diviseurs de 150 sont les nombres $2^i \times 3^j \times 5^k$ avec $0 \leq i \leq 1$, $0 \leq j \leq 1$ et $0 \leq k \leq 2$.

Nous pouvons dresser leur liste à l'aide d'un arbre.



150 a 12 diviseurs : 1, 2, 3, 5, 6, 10, 15, 25, 30, 50, 75, 150.

C. PGCD de deux entiers

Définition et propriétés

Exemple

Cherchons les diviseurs communs à 12 et 30.

La décomposition de 12 et 30 en facteurs premiers donne : $12 = 2^2 \times 3$ et $30 = 2 \times 3 \times 5$.

Les diviseurs de 12 sont : 1, 2, 3, $2^2 = 4$, $2 \times 3 = 6$, $2^2 \times 3 = 12$.

12	2	30	2
6	2	15	3
3	3	5	5
1		1	

Les diviseurs de 30 sont : 1, 2, 3, 5, $2 \times 3 = 6$, $2 \times 5 = 10$, $3 \times 5 = 15$, $2 \times 3 \times 5 = 30$.

Les diviseurs communs à 12 et 30 sont donc : 1, 2, 3, 6.

6 est le plus grand diviseur commun à 12 et 30 : on note 6 = PGCD (12, 30).

Voir le fin du paragraphe B.

Plus Grand Commun Diviseur.

Plus généralement, tout nombre entier naturel non nul n a au moins 1 pour diviseur et tous ses diviseurs sont inférieurs ou égaux à n.

Donc deux nombres entiers naturels non nuls a et b ont au moins 1 pour diviseur commun et tous leurs diviseurs communs sont inférieurs ou égaux à a et b.

Nous admettons qu'il en résulte **qu'il existe un diviseur commun à a et b plus grand que tous les autres : il est noté PGCD (a,b).**

Remarques

- 2 et 3 n'ont aucun diviseur premier commun, leur seul diviseur commun étant 1.
Donc PGCD (2,3) = 1
- $12 = 2^2 \times 3$, $30 = 2 \times 3 \times 5$ et PGCD (12,30) = $6 = 2 \times 3$.
Nous observons que 6 est le produit des facteurs premiers communs à 12 et 36, chacun étant affecté de l'exposant le plus faible.

Nous admettons que ces remarques ont une portée générale.

PROPRIÉTÉ

Soit a et b deux nombres entiers naturels supérieurs ou égaux à 2.

- S'ils n'ont aucun facteur premier commun, alors PGCD $(a,b) = 1$.
- Sinon PGCD (a,b) est le produit des facteurs premiers communs, chacun étant affecté du plus petit exposant avec lequel il figure dans les deux décompositions.

Nous admettons aussi les propriétés suivantes.

PROPRIÉTÉS

Soit a et b deux nombres entiers naturels non nuls tels que $a > b$.

PGCD (a,b) = PGCD $(a - b, b)$.

PGCD (a,b) = PGCD (r,b) où r est le reste de la division euclidienne de a par b.

$a = bq + r$ avec $0 \leq r < b$: voir le paragraphe A.

Ces deux égalités permettent, dans la recherche du PGCD de deux nombres, de remplacer le plus grand (ici a) par un nombre plus petit : $a - b$ ou r.

On peut alors itérer le procédé jusqu'à obtenir une différence ou un reste nul.

Entiers premiers entre eux

Exemple

Les diviseurs de 10 sont 1, 2, 5, 10.

Les diviseurs de 21 sont 1, 3, 7, 21.

Donc 10 et 21 ont 1 pour seul diviseur commun.

DÉFINITION

Deux nombres entiers naturels sont **premiers entre eux** si et seulement si **leur seul diviseur commun est 1**.

10 et 21 sont premiers entre eux.

Remarque

Deux nombres entiers naturels sont premiers entre eux si et seulement si leur PGCD est égal à 1.

D. Congruences

Le programme de mathématiques du BTS SIO limitant l'étude de la division euclidienne aux nombres entiers naturels, nous sommes amenés ici à limiter cette initiation aux congruences aux seuls nombres entiers naturels bien que celles-ci peuvent s'appliquer plus généralement aux nombres entiers relatifs (positifs ou négatifs).

Cette limitation réduit le champ d'intervention des congruences, notamment dans le cas d'un décodage où une différence négative peut apparaître.

Définition

$17 = 7 \times 2 + 3$
$31 = 7 \times 4 + 3$

Nous pouvons observer que les divisions euclidiennes de 17 et 31 par 7 ont le **même reste** : $r = 3$.

DÉFINITION

Soit a et b des nombres entiers naturels et n un nombre entier naturel supérieur ou égal à 2.

a* est congru à *b* modulo *n si et seulement si ***a* et *b* ont le même reste dans la division euclidienne par *n*.**

Les mots congru et modulo viennent du latin *congruus* (convenable) et *modus* (mesure).

Notation : $a \equiv b$ (modulo n).

Cette notation peut être abrégée en : $a \equiv b$ (mod n) ou $a \equiv b$ (n).

Exemples

$17 \equiv 31$ (7)

$31 \equiv 17$ (7)

$17 \equiv 17$ (7) et $31 \equiv 31$ (7)

$17 \equiv 3$(7) et $31 \equiv 3$(7).

3 est le reste des divisions euclidiennes de 13 et 31 par 7.

Plus généralement, pour tout entier naturel a et tout entier naturel n tel que $n \geq 2$, $\boldsymbol{a \equiv a\ (n)}$ et

$a \equiv r(n)$ où r est le reste de la division euclidienne de a par n.

Remarques

- Par définition, **si $a \equiv b(n)$, alors $b \equiv a(n)$.**
On dit que a et b sont congrus modulo n.
- Par définition, **si $a \equiv b(n)$ et si $b \equiv c(n)$, alors $a \equiv c(n)$.**

Propriétés

$31 \equiv 17$ (7) et $31 - 17 = 14 = 2 \times 7$, donc $31 - 17$ est un multiple de 7.

Plus généralement nous admettons la propriété suivante.

PROPRIÉTÉ

Soit a et b des entiers naturels et n un entier naturel supérieur ou égal à 2.

a est congru à b modulo n si et seulement si $|a - b|$ est un multiple de n.

$|a - b|$ est la valeur absolue de $a - b$.

$|31 - 17| = 31 - 17 = 4$.

$|17 - 31| = -(17 - 31) = 4$.

Nous avons introduit ici une valeur absolue car, conformément au programme, nous nous limitons aux nombres entiers naturels.

D'autres propriétés des congruences font intervenir les opérations sur les nombres entiers naturels.

PROPRIÉTÉS

Soit a, a', b et b' des entiers naturels et soit n un entier naturel supérieur ou égal à 2.

Si $a \equiv b$ (n) et $a' \equiv b'$ (n), alors :

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

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

Les propriétés sont exploitées dans les exercices corrigés sur les congruences de ce chapitre.

Une dernière propriété figure au programme.

PROPRIÉTÉ

Modulo n, les multiples de a sont les multiples de PGCD (a, n).

EXERCICES

LES CAPACITÉS ATTENDUES	Exercices corrigés
• Systèmes de numération	
Passer de l'écriture d'un nombre dans une base à une autre.	1, 4, 7, 10, 11, 16, 19, 22, 25
Arrondir un entier ou un réel (par défaut, par excès, au plus près…) et se conformer à un nombre de chiffres significatifs.	11
Calculer à la main : – des additions en base 2 et 16, – des multiplications et des divisions par une puissance de deux, en base 2.	28, 31 34
• Arithmétique modulaire	
Décomposer un entier naturel en produit de facteurs premiers et déterminer tous ses diviseurs.	46
Mettre en œuvre un algorithme : – recherche de nombres premiers, – décomposition en produit de facteurs premiers, – de recherche de PGCD.	38, 41 43, 46, 50 50, 53, 56, 59, 62
Mener un calcul de congruences modulo n.	65, 68, 71, 75

Systèmes de numération

Du binaire au décimal

Écrire dans le système décimal les nombres suivants (exercices 1 à 6).

1. + **Nombres entiers**

a) 110_2 ; b) 1011_2.

CORRIGÉ P. 168

2. + **Nombres entiers**

a) 10011_2 ; b) 11011_2.

3. + **Nombres entiers**

a) 110110_2 ; b) 1010101_2.

4. + **Nombres avec virgule**

a) $10{,}01_2$; b) $100{,}011_2$.

CORRIGÉ P. 168

5. + **Nombres avec virgule**

a) $110{,}11_2$; b) $1010{,}101_2$.

6. + **Nombres avec virgule**

a) $1001{,}110_2$; b) $10110{,}001_2$.

Du décimal au binaire

Écrire dans le système binaire les nombres suivants (exercices 7 à 15).

7. + **Nombres entiers**

a) 21 ; b) 41.

CORRIGÉ P. 168

8. + **Nombres entiers**

a) 29 ; b) 51.

9. + **Nombres entiers**

a) 43 ; b) 85.

10. + **Nombres décimaux**

a) 15,75 ; b) 62,625.

CORRIGÉ P. 168

11. ++ **Arrondis**

0,333 en arrondissant à 2^{-3}

a) par défaut ;

b) par excès ;

c) au plus près.

CORRIGÉ P. 169

12. + **Nombres décimaux**

a) 17,375 ; b) 71,3125.

13. ++ **Nombres décimaux**

a) 17,375 ; b) 71,3125.

14. ++ **Arrondis**

7,4321 en arrondissant à 2^{-4}.

a) par défaut ;

b) au plus près.

15. ++ **Arrondis**

23,23 en arrondissant à 2^{-4}.

a) par excès ;

b) au plus près.

De l'hexadécimal au binaire

Écrire dans le système binaire les nombres suivants (exercices 16 à 18).

16. + **Nombres avec des lettres**

a) $2A7_{16}$; b) $B3C,09_{16}$.

CORRIGÉ P. 169

17. + **Nombres avec des lettres**

a) $C00C_{16}$; b) $A8F,B4_{16}$.

18. + **Nombres avec des lettres**

a) ACE_{16} ; b) ABC,DEF_{16}.

Du binaire à l'hexadécimal

Écrire dans le système hexadécimal les nombres suivants (exercices 19 à 21).

19. + **Écriture condensée**

a) 10011_2 ; b) $110110,101_2$.

CORRIGÉ P. 169

20. + **Écriture condensée**

a) 1100101_2 ; b) $100011010,00111_2$.

21. + **Écriture condensée**

a) 1011011_2 ; b) $1001111100,1010101_2$.

De l'hexadécimal au décimal

Écrire dans le système décimal les nombres suivants (exercices 22 à 24).

22. + **Des lettres aux chiffres**

a) BAC_{16} ; b) $DE,F31_{16}$.

CORRIGÉ P. 169

23. + **Des lettres aux chiffres**

a) $E1C2_{16}$; b) $7D0,3A_{16}$.

24. + **Des lettres aux chiffres**

a) $6BF_{16}$; b) $5C9,4D_{16}$.

Du décimal à l'hexadécimal

Écrire dans le système hexadécimal les nombres suivants (exercices 25 à 27).

25. + **Des chiffres aux lettres**

a) 4 000 ; b) 3 840,289 062 5.

CORRIGÉ P. 169

26. + **Des chiffres aux chiffres**

a) 2 392 ; b) 2 199,437 5.

27. + **Des chiffres aux lettres**

a) 11 525 ; b) 6 926,796 875.

Additions en base 2

Effectuer dans le système binaire les additions suivantes et donner l'équivalent de ces additions dans le système décimal (exercices 28 à 30).

28. ++ **Gérer les retenues**

a) 1100 + 101 ; b) 101,01 + 11,101.

CORRIGÉ P. 169

29. ++ **Gérer les retenues**

a) 10101 + 1100 ; b) 1110,11 + 100,01.

30. ++ **Gérer les retenues**

a) 110011 + 1010 ; b) 10001,011 + 111,001.

Additions en base 16

Effectuer dans le système hexadécimal les additions suivantes et donner l'équivalent de ces additions dans le système décimal (exercices 31 à 33).

31. ++ **Des lettres et des retenues**

a) A2C3 + D58 ; b) 4B,6 + 0,A.

CORRIGÉ P. 169

32. ++ **Des lettres et des retenues**

a) 897 + 798 ; b) AB,C + DE,F.

33. ++ **Des lettres et des retenues**

a) BAC + CAB ; b) 75,B09 + 19,197.

Multiplications et divisions par une puissance de deux, en base 2

Effectuer dans le système binaire les multiplications et les divisions suivantes et donner l'équivalent de ces opérations dans le système décimal (exercices 34 à 36).

34. + **Multiplication et division**

a) 101×100 ; b) 101,1 : 100.

CORRIGÉ P. 169

35. + **Multiplication et division**

a) 1011×1000 ; b) 10,01 : 1000.

36. + **Multiplication et division**

a) $11,11 \times 10$; b) 11,101 : 100.

Arithmétique modulaire

Division euclidienne

37. + Les chocolats

Une boîte contient 41 chocolats identiques à répartir entre 8 enfants.

Le plus âgé propose de les répartir de façon égale entre les 7 autres enfants, lui prenant le reste.

1. Quelle est la part de chacun ?

2. Après vérification, la boîte contient 43 chocolats. L'enfant le plus âgé veut alors changer la règle de répartition. Pourquoi ?

Nombres premiers

38. ++ Nombres premiers ?

Déterminer si les nombres suivants sont premiers :

87 – 89 – 91.

CORRIGÉ P. 169

39. ++ Nombres premiers ?

Déterminer si les nombres suivants sont premiers :

457 – 459 – 461.

40. ++ Nombres premiers ?

Déterminer si les nombres suivants sont premiers :

337 – 447 – 557.

41. ++ Liste de nombres premiers

Déterminer les nombres premiers compris entre 100 et 150 à l'aide du crible d'Ératosthène, en cherchant à alléger la présentation.

CORRIGÉ P. 170

42. ++ Liste de nombres premiers

Même exercice que le précédent pour les nombres premiers entre 150 et 200.

Décomposition en produit de facteurs premiers

Décomposer les nombres entiers suivants en produits de facteurs premiers (exercices **43** à **45**).

43. +

a) 450 ; b) 1 617.

CORRIGÉ P. 170

44. +

a) 605 ; b) 6 552.

45. +

a) 1 296 ; b) 2 431.

Déterminer la liste des diviseurs de chacun des nombres entiers suivants (exercices **46** à **48**).

46. +

a) 24 ; b) 60.

CORRIGÉ P. 170

47. +

a) 50 ; b) 90.

48. +

a) 28 ; b) 120.

49. ++ Longueur et largeur

Un rectangle a pour aire 12 m^2. Sa longueur L et sa largeur l sont des nombres entiers (en mètres).

1. Déterminer toutes les dimensions possibles de ce rectangle.

2. Même question en remplaçant 12 m^2 par :

a) 221 m^2 ; b) 311 m^2.

Recherche de PGCD par décomposition en produit de facteurs premiers

Décomposer les nombres entiers m et n suivants en produits de facteurs premiers et en déduire leur PGCD (exercices **50** à **52**).

50. + Décomposition

a) $m = 15$ et $n = 24$; b) $m = 140$ et $n = 98$.

CORRIGÉ P. 170

51. + Décomposition

a) $m = 198$ et $n = 363$; b) $m = 180$ et $n = 225$.

52. + Décomposition

a) $m = 200$ et $n = 60$; b) $m = 1\,911$ et $n = 2\,366$.

Recherche de PGCD par l'algorithme des différences

Déterminer le PGCD des deux nombres entiers m et n suivants en mettant en œuvre l'algorithme des différences (exercices **53** à **55**).

53. ++ Algorithme des différences

a) $m = 1\,448$ et $n = 1\,086$; b) $m = 1\,788$ et $n = 2\,235$.

CORRIGÉ P. 170

54. ++ Algorithme des différences

a) $m = 580$ et $n = 348$; b) $m = 1\,926$ et $n = 2\,996$.

55. ++ Algorithme des différences

a) $m = 296$ et $n = 703$; b) $m = 1\,065$ et $n = 852$.

Recherche de PGCD par l'algorithme d'Euclide

Déterminer le PGCD des deux nombres entiers m et n suivants en mettant en œuvre l'algorithme des divisions euclidiennes (exercices **56** à **58**).

56. ++ Algorithme d'Euclide

a) $m = 1\,448$ et $n = 1\,086$; b) $m = 1\,788$ et $n = 2\,235$.

CORRIGÉ P. 170

57. ++ Algorithme d'Euclide

a) $m = 580$ et $n = 348$; b) $m = 1\,926$ et $n = 2\,996$.

58. ++ Algorithme d'Euclide

a) $m = 296$ et $n = 703$; b) $m = 1\,065$ et $n = 852$.

Exploitation du PGCD

59. +++ Les dragées

On veut répartir la totalité de 760 dragées au chocolat et de 1 045 dragées aux amandes dans des sachets ayant la même répartition de dragées au chocolat et aux amandes.

1. Peut-on faire 76 sachets ? Justifier la réponse.

2. a) Quel nombre maximum de sachets peut-on réaliser ?

b) Combien de dragées de chaque sorte y a-t-il alors dans chaque sachet ?

CORRIGÉ P. 171

60. +++ Les étudiants sont sportifs

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 210 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 ?

61. +++ Découpe optimisée

Un ouvrier dispose de plaques de métal de 110 cm de longueur et de 88 cm de largeur.

Il a reçu la consigne suivante :

« *Découpe dans ces plaques des carrés tous identiques, dont les longueurs des côtés sont un nombre entier de cm, et de façon à ne pas avoir de perte.* »

1. Peut-il choisir de découper des plaques de 10 cm de côté ? Justifier la réponse.

2. Peut-il choisir de découper des plaques de 11 cm de côté ? Justifier la réponse.

3. On lui impose désormais de découper des carrés les plus grands possibles.

a) Quelle sera la longueur du côté d'un carré ?

b) Combien y aura-t-il de carrés par plaques ?

Nombres entiers premiers entre eux

Déterminer si les deux entiers suivants sont premiers entre eux (exercices **62** à **64**).

62. +

a) $m = 45$ et $n = 93$; b) $m = 63$ et $n = 52$.

CORRIGÉ P. 171

63. +

a) $m = 77$ et $n = 87$; b) $m = 209$ et $n = 114$.

64. +

a) $m = 56$ et $n = 65$; b) $m = 1\,001$ et $n = 42$.

Congruences

Compléter les résultats suivants avec le plus petit entier naturel possible (exercices **65** à **67**).

65. +

a) $11 \equiv \ldots$ (modulo 2) ; b) $135 \equiv \ldots$ (modulo 11).

CORRIGÉ P. 171

66. +

a) $89 \equiv \ldots$ (modulo 7) ; b) $212 \equiv \ldots$ (modulo 5).

67. +

a) $75 \equiv \ldots$ (modulo 6) ; b) $311 \equiv \ldots$ (modulo 4).

68. ++

Démontrer que $47^{900} - 25^{900}$ est un multiple de 11.

CORRIGÉ P. 171

69. ++

Démontrer que $393^{500} \equiv 1$ (mod 7).

70. ++

Déterminer le reste de la division de 142^{142} par 3.

71. +++ Congruences et puissances

1. a) Compléter le résultat suivant :

$2^3 \equiv \ldots$ (modulo 7).

b) En déduire que, pour tout entier naturel n,

$2^{3n} \equiv 1$ (modulo 7).

2. a) Compléter le résultat suivant :

$2\,011 \equiv \ldots$ (modulo 7)

b) En déduire que $2\,011^{2012} \equiv 2^{2012}$ (modulo 7).

3. a) Écrire la division euclidienne de 2 012 par 3.

b) En déduire que $2^{2012} \equiv (2^3)^{670} \times 2^2$.

c) Déduire de ce qui précède que

$2\,011^{2012} \equiv 4$ (mod 7)

et donner le reste de la division euclidienne de $2\,011^{2012}$ par 7.

CORRIGÉ P. 171

72. +++ Congruences et puissances

1. Déterminer le reste dans la division euclidienne par 9 de :

a) 7 ; **b)** $7^2 = 49$; **c)** $7^3 = 343$.

2. Exprimer les trois résultats précédents à l'aide de congruences.

3. En déduire que $7^4 \equiv 7$ (modulo 9), puis compléter et justifier les résultats suivants :

$7^5 \equiv \ldots$ (modulo 9) ; $7^6 \equiv \ldots$ (modulo 9) ;

$7^7 \equiv \ldots$ (modulo 9).

Dans la suite on admet que si $n \equiv 1$ (modulo 3), alors $7^n \equiv 7$ (modulo 9).

4. **a)** Démontrer que $2014 \equiv 7$ (modulo 9) et que $2014 \equiv 1$ (modulo 3).

b) Déduire de ce qui précède que $2014^{2014} \equiv 7$ (modulo 9).

c) Exprimer ce résultat par une phrase concernant le reste d'une division euclidienne à préciser.

73. +++ Congruences et puissances

1. **a)** Calculer 2009^2.

b) Déterminer le reste de la division euclidienne de 2009^2 par 16.

c) Compléter le résultat suivant :

$2009^2 \equiv \ldots$ (modulo 16).

2. On rappelle que $2009^{8001} = (2009^2)^{4000} \times 2009$.

Déduire de ce qui précède que :

$2009^{8001} \equiv 2009$ (modulo 16).

74. +++ 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 :

$3^2 \equiv \ldots$ (modulo 7) et $3^6 \equiv \ldots$ (modulo 7).

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

75. +++ Algorithmes, division et codage ALGO

Partie A

On considère l'algorithme suivant :

Variables :	a est un entier naturel
	b est un entier naturel
	c est un entier naturel
Initialisation :	Affecter à c la valeur 0
	Demander la valeur de a
	Demander la valeur de b
Traitement :	Tant que $a \geq b$
	Affecter à c la valeur $c + 1$
	Affecter à a la valeur $a - b$
	Fin de tant que
Sortie :	Afficher c
	Afficher a

1. Faire fonctionner cet algorithme avec $a = 13$ et $b = 4$ en indiquant les valeurs des variables à chaque étape.

2. **a)** Écrire la division euclidienne de 13 par 4.

b) Qu'a permis de calculer cet algorithme ?

Dans la suite on admet que l'observation effectuée à la question **2.** dans le cas particulier où $a = 13$ et $b = 4$ reste valable pour tous entiers naturels a et b, avec $b \neq 0$.

Partie B

À chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier compris entre 0 et 25.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On définit un procédé de codage de la façon suivante :

Étape 1 : À la lettre que l'on veut coder, on associe le nombre m correspondant dans le tableau.

Étape 2 : On calcule le reste de la division euclidienne de $9m + 5$ par 26 et on le note p.

Étape 3 : Au nombre p, on associe la lettre correspondante dans le tableau.

1. Coder la lettre U.

2. Modifier l'algorithme de la partie A pour qu'à une valeur de m entrée par l'utilisateur, il affiche la valeur de p, calculée à l'aide du procédé de codage précédent.

CORRIGÉ P. 171

76. ++ Chiffrement de Hill

On veut coder un mot de deux lettres selon la procédure suivante :

Étape 1 : Chaque lettre du mot est remplacée par un entier en utilisant le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On obtient un couple d'entiers (x_1, x_2) où x_1 correspond à la première lettre du mot et x_2 correspond à la deuxième lettre du mot.

Étape 2 : (x_1, x_2) est transformé en (y_1, y_2) tel que :

$$(S_1)\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 7x_1 + 4x_2 \pmod{26} \end{cases}$$

avec $0 \leq y_1 \leq 25$ et $0 \leq y_2 \leq 25$.

Étape 3 : (y_1, y_2) est transformé en un mot de deux lettres en utilisant le tableau de correspondance donné dans l'étape 1.

Exemple : $\underbrace{\text{TE}}_{\text{mot en clair}} \overset{\text{étape 1}}{\Rightarrow} (19, 4) \overset{\text{étape 2}}{\Rightarrow} (13, 19) \overset{\text{étape 3}}{\Rightarrow} \underbrace{\text{NT}}_{\text{mot codé}}$

1. Coder le mot ST.

2. On admet que le système (S_1) est équivalent au système

$$(S_2)\begin{cases} x_1 \equiv 16y_1 + y_2 \pmod{26} \\ x_2 \equiv 11y_1 + 5y_2 \pmod{26} \end{cases}$$

Décoder le mot YJ.

77. ++ Codage et décodage

On note E l'ensemble des vingt-sept nombres entiers compris entre 0 et 26.

On note A l'ensemble dont les éléments sont les vingt-six lettres de l'alphabet et un séparateur entre deux mots, noté « ★ », considéré comme un caractère.

Pour coder les éléments de A, on procède de la façon suivante :

• Premièrement : on associe à chacune des lettres de l'alphabet, rangées par ordre alphabétique, un nombre entier naturel compris entre 0 et 25, rangés par ordre croissant. On a donc $a \to 0$, $b \to 1$,... $z \to 25$.
On associe au séparateur « ★ » le nombre 26.

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z	★
14	15	16	17	18	19	20	21	22	23	24	25	26

On dit que a a pour rang 0, b a pour rang 1,..., z a pour rang 25 et le séparateur « ★ » a pour rang 26.

• Deuxièmement : à chaque élément x de E, l'application g associe le reste de la division euclidienne de $4x + 3$ par 27.
On remarquera que pour tout x de E, $g(x)$ appartient à E.

• Troisièmement : le caractère initial est alors remplacé par le caractère de rang $g(x)$.

Exemple :

$s \to 18$, $g(18) = 21$ et $21 \to v$. Donc la lettre s est remplacée lors du codage par la lettre v.

1. Coder :

a) le mot « *tu* »,

b) le mot « *es* »,

c) le début de phrase « *tu es* » constitué des deux mots « *tu* », « *es* » et du séparateur de mots.

2. On admet que pour le décodage, on procède comme pour le codage en remplaçant la fonction g par la fonction f qui, à chaque élément y de E, associe le reste de la division euclidienne de $7y + 6$ par 27.

Décoder le mot « *vfv* ».

78. +++ Parcours d'une liste circulaire par sauts d'amplitude constante

Une puce, initialement placée sur la case 0 du plateau ci-contre, effectue des sauts successifs de p cases.

Dans le cas où $p = 1$, la puce va évidemment se poser successivement sur les 12 cases du plateau.

1. Dans le cas où $p = 2$, compléter le tableau suivant.

Saut n° k	1	2	3	4	5	6
Numéro m de la case atteinte						

Que se passe-t-il après le saut n° 6 ?

2. Dans le cas où $p = 3$, $p = 4$, $p = 5$, $p = 6$, $p = 7$, compléter le tableau suivant en s'arrêtant dès que la puce revient à la case n° 0.

Saut n° k	1	2	...
Numéro m de la case atteinte avec $p = 3$			
Numéro m de la case atteinte avec $p = 4$			
...			

3. a) Pour quelles valeurs de p, avec $1 \leq p \leq 7$, la puce passe par toutes les cases du tableau ?

b) Déterminer PGCD $(12, p)$ pour chaque valeur de p comprise entre 1 et 7.

c) Que peut-on dire des nombres 12 et p, avec $1 \leq p \leq 7$, lorsque la puce passe par toutes les cases du plateau ?

4. On démontre, et on l'admet ici, que la propriété observée ci-dessus dans des cas particuliers est générale.

Compléter l'énoncé de cette propriété :

En parcourant une liste circulaire de n cases par sauts d'amplitude constante p, on passe par toutes les cases si et seulement si n et p sont...

Remarque

Dans le cas où $p = 5$, observer qu'à partir du troisième saut, le numéro m de chaque case occupée est tel que $5k \equiv m$ (modulo 12) : par exemple,
$5 \times 3 \equiv 3$ (modulo 12).
Il en est de même dans le cas où $p = 7$.

EXERCICES pour le BTS

Les exercices pour le BTS sont des exercices qui pourraient figurer dans une épreuve de mathématiques pour le BTS.

79. +++ QCM

Indiquer, pour chaque question, la bonne réponse. Aucune justification n'est demandée.

1. $N = 101101_2$ dans le système binaire.

Dans le système décimal, N est égal à :

Réponse A	Réponse B	Réponse C
29	34	45

2. $N = A7C_{16}$ dans le système hexadécimal.

Dans le système décimal, N est égal à :

Réponse A	Réponse B	Réponse C
1082	2642	2684

3. Dans le système binaire, la somme 110101 + 10011 est égale à :

Réponse A	Réponse B	Réponse C
1000110	1001000	100100

80. +++ Souvenir de Polynésie

Un vendeur possède un stock de 120 flacons de parfum au tiaré et de 144 savonnettes au monoï.

Il veut écouler tout ce stock en confectionnant le plus grand nombre de coffrets « Souvenirs de Polynésie » de sorte que :

- le nombre de flacons de parfum au tiaré soit le même dans chaque coffret ;
- le nombre de savonnettes au monoï soit le même dans chaque coffret ;
- tous les flacons et savonnettes soient utilisés.

1. Déterminer le nombre de coffrets à préparer et la composition de chacun d'eux. Justifier la réponse.

2. Après vérification le vendeur constate qu'il n'a que 119 flacons de parfum au tiaré.

Reprendre la question **1** en remplaçant 120 par 119.

81. +++ Codage et décodage

Le but de cet exercice est l'étude d'un procédé de cryptage des lettres majuscules de l'alphabet français. Chacune des 26 lettres est associée à l'un des entiers de 0 à 25, selon le tableau de correspondance suivant.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Le cryptage se fait à l'aide d'une clé, qui est un nombre entier k fixé, compris entre 0 et 25.

Pour crypter une lettre donnée :

– on repère le nombre x associé à la lettre, dans le tableau de correspondance précédent ;

– on multiplie ce nombre x par la clé k ;

– on détermine le reste r de la division euclidienne de $k \times x$ par 26 ;

– on repère la lettre associée au nombre r dans le tableau de correspondance ; c'est la lettre cryptée.

Par exemple, pour crypter la lettre « R » avec la clé $k = 5$:

– le nombre x associé à la lettre « R » est le nombre 17 ;

– on multiplie 17 par la clé k ce qui donne $5 \times 17 = 85$;

– on détermine le reste de 85 dans la division par 26 : on trouve 7 ;

– on repère enfin la lettre associée à 7 dans le tableau : c'est « H ».

Ainsi, avec la clé $k = 5$, la lettre « R » est cryptée en la lettre « H ».

On crypte un mot en cryptant chacune des lettres de ce mot.

Partie A – *Cryptage d'un mot avec la clé $k = 5$*

Dans cette partie, la clé de cryptage est $k = 5$. Le but de cette partie est de crypter le mot « BTS ».

1. Déterminer en quelle lettre est cryptée la lettre « S ». On détaillera les différentes étapes du processus de cryptage.

2. Crypter le mot « BTS ». On ne demande pas le détail du cryptage.

Partie B – *Décryptage avec la clé $k = 5$*

Dans cette partie, la clé de cryptage est toujours $k = 5$.

Le but de cette partie est de retrouver une lettre initiale connaissant la lettre cryptée.

1. Prouver que $21 \times 5 \equiv 1$ modulo 26.

2. Une lettre associée à un nombre x a été cryptée. Le nombre associé à la lettre cryptée est noté y.

a) Justifier que $5 \times x \equiv y$ modulo 26.

b) Montrer que $21 \times y \equiv x$ modulo 26.

Ces propriétés montrent que pour décrypter une lettre codée y avec la clé $k = 5$, il suffit de crypter cette lettre avec la clé de cryptage $k' = 21$.

Exemple : si une lettre est codée par $y = 12$ on multiplie 12 par 21 et on prend le reste du résultat dans la division euclidienne par 26 ; on obtient $x = 18$. Donc la lettre de départ est S.

3. Utiliser les résultats précédents pour décrypter le mot « WGA ».