Chapitre 4

Arithmétique

Arithmétique modulaire

I Entiers naturels et division euclidienne

Définition (rappel) : ensemble des entiers naturels

On note $\mathbb{N}$ l'ensemble des *entiers naturels*.

$$\mathbb{N} = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12 \ldots\}$$

Définition (rappel) : division euclidienne dans $\mathbb{N}$

Soient A et B deux entiers naturels, et $B \neq 0$. Il existe deux nombres uniques Q et R (vérifiant $0 \geqslant R < B$) tels que l'on puisse écrire

$$A = Q \times B + R$$

C'est exactement la division que l'on a apprise en sixième (celle où l'on s'arrête aux nombres entiers) :

A	B
R	Q

- A est appelé le *dividende* ;
- B est le *diviseur* ;
- Q est le *quotient* ;
- R est le *reste*, il est *impérativement* plus petit que B.

Exemples

Effectuons la division euclidienne de 27 par 7 :

27	7
6	3

Ainsi on a $\underbrace{27}_{A} = \underbrace{3}_{Q} \times \underbrace{7}_{B} + \underbrace{6}_{R}$.

Effectuons la division euclidienne de 297 par 11 :

297	11
0	27

Ainsi on a $\underbrace{286}_{A} = \underbrace{26}_{Q} \times \underbrace{11}_{B} + \underbrace{0}_{R}$.

Exercice 1

Effectuer les divisions euclidiennes suivantes :

a. 28 par 8 **b.** 100 par 9 **c.** 379 par 11 **d.** 427 par 13

Définition : diviseurs et multiples

Quand la division euclidienne de A par B donne un reste nul (lorsqu'elle tombe juste) on dit que *B est un diviseur de A* ou bien (ce qui revient au même) que *A est un multiple de B*.

Exemples

- $27 = 3 \times 7 + 4$ donc 7 ne divise pas 27 (7 n'est pas *un diviseur* de 27).
  On peut dire aussi que 27 n'est pas multiple de 7.
- $286 = 26 \times 11 + 0$ donc 1 est donc un diviseur de 286.

Remarques

a. $28 = 4 \times 5 + 8$ mais ce n'est pas la division euclidienne de 28 par 5 car le « reste » 8 n'est pas plus petit que 5.

$28 = 4 \times 5 + 8$
$= 4 \times 5 + 5 + 3$
$= 5 \times 5 + 3$ voilà la division euclidienne.

b. *« une division euclidienne n'en donne pas toujours 2 »* :
$27 = 3 \times 7 + 4$ est la division euclidienne de 27 par 7.
On peut réarranger : $27 = 7 \times 3 + 4$ mais ce n'est pas la division euclidienne de 27 par 3 car le reste est trop grand.

Ceci dit quand le reste est suffisamment petit, on obtient « 2 divisions pour le prix d'une » : $162 = 12 \times 13 + 1$ est la division euclidienne de 162 par 12, et de 162 par 13 aussi.

c. *« une division euclidienne qui tombe juste en donne deux en général »* :
$297 = 27 \times 11$ nous donne 2 diviseurs de 297 : 27 et 11.
$16 = 4 \times 4$ aussi… mais c'est deux fois le même !

d. avec la calculatrice, pour savoir si B divise A il suffit d'entrer $A \div B$ et de regarder si le résultat est entier.

Exercice 2

Les égalités suivantes, peuvent-elles être des divisions euclidiennes ?
Si oui, préciser A, B, Q et R.

a. $65 = 32 \times 2 + 1$ b. $80 = 5 \times 10 + 30$ c. $100 = 9 \times 11 + 1$ d. $17 = 3 \times 4 + 5$

Exercice 3

Les égalités suivantes ne sont pas des divisions euclidiennes.
Transformez-les pour qu'elles le deviennent (il peut y avoir plusieurs possibilités).

a. $19 = 3 \times 4 + 7$ b. $30 = 2 \times 10 + 10$ c. $29 = 4 \times 5 + 9$ d. $23 = 4 \times 7 - 5$

Code Python

```
>>> a = 17   # déclare une variable a de type int (entier)
>>> b = 5    # idem avec b
>>> q = a // b # // donne le quotient par b
>>> r = a % b  # %  donne le reste modulo b
>>> print(q)
5
>>> print(r)
2
```

II Diviseurs et nombres premiers

Propriété

Soient a et b deux entiers naturels. Dire que b est un diviseur de a veut dire que la division euclidienne de a par b donne un reste nul.
Cela signifie donc qu'il existe un entier naturel k tel que

$$a = k \times b$$

On peut également dire que a est multiple de b

Remarque

Si b divise a il existe un entier naturel k tel que

$$a = k \times b$$

et donc k divise a également.

Exemple

$20 = 5 \times 4$ donc 5 et 4 sont deux diviseurs de 20.

Exercice 4

À l'aide de la calculatrice (ou non), déterminer si b divise a.

a. $a = 251$ et $b = 13$

b. $a = 8$ et $b = 80$

c. $a = 111$ et $b = 37$

d. $a = 131072$ et $b = 8192$

Propriétés

a. Si a est divisible par b alors tout multiple de a est également divisible par b.

b. Si a est divisible par b et que b est divisible par c alors a est divisible par c.

c. Si a et b sont divisibles par c alors a+b aussi et (si a>b) a-b aussi.

Exemples

a. 12 est divisible par 3 donc tout multiple de 12 aussi : 12 000 est donc divisible par 3.

b. 120 est divisible par 12 et 12 est divisible par 3 donc 120 est divisible par 3.

c. Puisque 12 000 et 12 sont divisibles par 3, 12 000-12, soit 11 988, l'est aussi.

Définition : entier naturel premier

Un entier naturel est dit *premier* lorsqu'il admet 2 diviseurs *distincts* : 1 et lui-même.

- 0 n'est pas premier : $0 = 1 \times 0 = 2 \times 0 = 3 \times 0 = \ldots$
- 1 n'a qu'un diviseur : lui-même. Il n'est pas premier.
- 2 est premier.
- 3 aussi.
- 4 ne l'est pas car 1, 2 et 4 divisent 1.

Il est assez simple de montrer qu'il y a une infinité de nombres premiers. Les nombres premiers jouent un rôle très important en mathématiques et interviennent dans les systèmes de cryptographie (basiques ou sophistiqués).

Exercice 5 : crible d'Ératosthène

Dans la grille suivante :

- Entourer 2 et barrer 2 et tous ses multiples.
- Une fois cela fait, 3 est le premier nombre non barré après 2 donc on l'entoure et on barre tous ses multiples.
- Continuer jusqu'à ce que tous les nombres de la grilles soient traités (soit barrés soit entourés).
- Les nombres entourés sont *des nombres premiers*.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Recopier ici la liste des nombres premiers trouvés :

Propriété

Soit n un entier supérieur ou égal à 2 :

- ou bien n possède un diviseur inférieur ou égal à $\sqrt{n}$ et, à ce moment là, n *n'est pas premier.*
- ou bien *aucun nombre premier* inférieur à $\sqrt{n}$ ne divise n et *il est premier.*

Méthode : déterminer si un nombre est premier ou non

Voici le début de la liste des nombres premiers :

$$\{2;\ 3;\ 5;\ 7;\ 11;\ 13;\ 17;\ 19\}$$

- 133 est-il premier ?

  $\sqrt{133} \approx 11,5$ donc on regarde si 133 est divisible par 2, 3, 5, 7 ou 11.
  On trouve que $133 = 19 \times 7$ donc 133 n'est pas premier.

- 251 est-il- premier ?
  $\sqrt{251} \approx 15,8$ donc on regarde si 251 est divisible par 2, 3, 5, 7, 11, ou 13.
  Ce n'est pas le cas : 251 est donc premier.

Exercice 6

Les nombres suivants sont ils premiers ?

a. 143 **c.** 141 **e.** 247

b. 145 **d.** 147 **f.** 257

Propriété : décomposition en produit de facteurs premiers

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

Méthode

Pour décomposer un nombre en produit de facteurs premiers, on cherche n'abord ses petits diviseurs premiers et on recommence jusqu'à trouver 1 :

234	2	on voit que 234 est pair
117	3	car 3 est le plus petit nombre premier qui divise 117
39	3	et ainsi de suite
13	13	...
1		on arrête

On a donc

$234 = 2 \times 3 \times 3 \times 13$
$= 2 \times 3^2 \times 13$ et c'est la décomposition en produit de facteurs premiers de 234.

Exercice 7

Décomposer les nombres suivants en produit de facteurs premiers.

a. 30 **b.** 60 **c.** 96 **d.** 684

Méthode : liste des diviseurs d'un entier

Pour trouver *tous* les divieurs d'un entier supérieur ou égal à 2 :

a. on le décompose en produit de facteurs premiers.

b. on écrit tous les nombres que l'on peut former en prenant « moins de facteurs » dans cette décomposition.

Exemple

Trouvons tous les diviseurs de 60 :
$60 = 2 \times 30 = 2^2 \times 15 = 2^2 \times 3 \times 5$. Ses diviseurs sont donc

1	$2^0 \times 3^0 \times 5^0$
5	$2^0 \times 3^0 \times 5^1$
3	$2^0 \times 3^1 \times 5^0$
15	$2^0 \times 3^1 \times 5^1$
2	$2^1 \times 3^0 \times 5^0$
10	$2^1 \times 3^0 \times 5^1$
6	$2^1 \times 3^1 \times 5^0$
30	$2^1 \times 3^1 \times 5^1$
4	$2^2 \times 3^0 \times 5^0$
20	$2^2 \times 3^0 \times 5^1$
12	$2^2 \times 3^1 \times 5^0$
60	$2^2 \times 3^1 \times 5^1$

Il est très facile d'oublier des diviseurs. Pour que cela n'arrive pas il faut utiliser une méthode logique pour les énumérer.
Voici un exemple d'algorithme qui les donne tous, en reprenant l'exemple de 60.

```
Variables
i, j, k : entiers
Début
    Pour i allant de 0 à 2
        Pour j allant de 0 à 1
            Pour k allant de 0 à 1
                Afficher 2^i * 3^j * 5^k
            FinPour
        FinPour
    FinPour
Fin
```

Exercice 8

Donner la liste des diviseurs des nombres suivants.

a. 30 **b.** 25 **c.** 96 **d.** 684

III pgcd de deux entiers naturels non nuls

Deux entiers naturels non nuls ont au moins un diviseur commun : 1. Parmi tous les nombres qui les divisent tous les deux il y en a un plus grand : leur pgcd.

Définition

Soient a et b deux entiers naturels non nuls.
On note $pgcd(a;b)$ et on lit « pgcd de a et de b » le plus grand entier qui divise à la fois a et b.

Exemples

Le plus grand nombre qui divise à la fois 12 et 16, c'est 4. Ainsi $pgcd(12;16) = 4$.
25 et 27 n'ont aucun diviseur commun plus grand que 1 : $pgcd(25;27) = 1$.

Définition

Lorsque $pgcd(a;b) = 1$ on dit que a et b sont *premiers entre eux*.

Exemples

25 et 27 sont premiers entre eux. 8 et 15 aussi.

Remarque

Il ne faut pas confondre *nombre premier* (tout court) et *nombres premiers entre eux* :

- 25 et 27 sont premiers entre eux mais aucun de ces deux nombres n'est premier.
- 3 et 30 ne sont pas premiers entre eux : leur pgcd vaut 3. Pourtant 3 est premier.

Méthode

Soient a et b deux entiers naturels que l'on a décomposés en produit de facteur premiers :

- S'ils n'ont aucun facteur commun alors ils sont premiers entres eux.
- Sinon, on fait le produit des facteurs communs avec la plus petite puissance qui apparaît dans chacune des décompositions.

Exemple

On veut $pgcd(240; 72)$.

- On commence par décomposer 240 : $240 = 2^4 \times 3^1 \times 5^1$.
- On fait de même pour 72 : $72 = 2^3 \times 3^2$
- Il y a deux facteurs premiers en commun dans cette décomposition : 2 et 3. On garde à chaque fois l'exposant le plus petit et on en fait le produit :

$$pgcd(a; b) = 2^3 \times 3^1 = 24$$

Exercice 9

En utilisant les décompositions en produit de facteurs premiers, donner le PGCD de

a. 15 et 27 **b.** 63 et 99 **c.** 222 et 148 **d.** 192 et 69

Propriété

Soient a et b 2 entiers non nuls. Si $b < a$ et qu'on effectue la division euclidienne de a par b, on obtient

$$a = q \times b + r$$

et à ce moment là

$$pgcd(a; b) = pgcd(b; r)$$

Méthode : Algorithme d'Euclide

Cette méthode se base sur la propriété précédente. On veut trouver le pgcd de 420 et 182.

$420 = 2 \times 182 + 56$ donc $pgcd(420; 182) = pgcd(182, 56)$ et on recommence.
$182 = 3 \times 56 + 14$ donc $pgcd(182, 56) = pgcd(56, 14)$ et on poursuit.
$56 = 3 \times 14 + \boxed{0}$ et on s'arrête.

La dernière ligne nous indique que $pgcd(56; 14) = 14$, ainsi $pgcd(420; 182) = 14$.

Exercice 10

En utilisant la méthode de votre choix, donner le PGCD de

a. 198 et 256 **b.** 546 et 230 **c.** 180 et 105 **d.** 357 et 399

Exercice 11

En utilisant l'algorithme d'Euclide, donner le PGCD de

a. 130 et 85 **b.** 4114 et 1530 **c.** 882 et 540 **d.** 1725 et 1309

Exercice 12

On dispose de 280 roses rouges et 490 roses blanches, avec lesquelles on veut faire le plus grand nombre possible de bouquets identiques.
Combien peut-on faire de tels bouquets et quelle est la composition de chacun d'eux ?

Exercice 13

Une feuille A4 a pour dimensions 21 cm et 29,7 cm. Alice cherche à savoir comment elle peut quadriller sa feuille à l'aide de carrés de mêmes dimensions, qui soient les plus gros possibles.
Quelle sera la taille des carrés ? Combien en fera-t-elle ?

IV Congruences

Définition

Soit n un entier naturel non nul et a et b deux entiers naturels.
On dit que a et b sont *congrus modulo* n si les divisions euclidiennes de a et b par n donnent le même reste.
On écrit cela

$$a \equiv b \quad [n]$$

Exemple

a. Prenons deux multiples de 5, ils sont tous congrus modulo 5 puisque lorsqu'on les divise par 5 le reste est nul.

$$15 \equiv 20 \quad [5]$$

b. Ajoutons leur 2 à tous les deux, ils sont encore congrus modulo 5 puisque lorsqu'on les divise par 5 le reste est 2.

$$17 \equiv 22 \quad [5]$$

c. Dans la vie courante, on raisonne parfois *modulo* 12 :

$16 = 1 \times 12 + 4$
$16 \equiv 4 \quad [12]$

Et de même $17 \equiv 5 \quad [12]$ et $18 \equiv 6 \quad [12]$: « 5 heures de l'après-midi, c'est 17 :00 » et cætera.

Propriété

Soient a et b deux entiers naturels tels que $a > b$.
Dire que $a \equiv b \quad [n]$ revient à dire que $a - b$ est un multiple de n.

Exemples

a. On a vu que $17 \equiv 22 \quad [5]$, et en effet $22 - 17 = 5$.

b. Partons de 11 et ajoutons lui un multiple de 3 : $11 + 7 \times 3 = 32$.
11 et 32 sont congrus modulo 3 : la différence est $32 - 11 = 7 \times 3$, et en faisant les divisions euclidiennes on trouve : $11 = 3 \times 3 + 2$ et $32 = 10 \times 3 + 2$ donc 11 et 32 on le même reste dans la division euclidienne par 3.

Exercice 14

Ci dessous, il y a 4 congruences. Dire si elles sont vraies ou non :

1. En faisant les « divisions euclidiennes par le modulo ».
2. En regardant si la différence des deux nombres est un « multiple du modulo ».

Quelle est-la méthode la plus rapide ?

a. $19 \equiv 13 \quad [6]$ b. $53 \equiv 29 \quad [5]$ c. $28 \equiv 0 \quad [7]$ d. $257 \equiv 353 \quad [32]$

Propriété : compatibilité avec les opérations

Soient a, b, c, d, n et p 5 entiers naturels, et n non nul.

Supposons que $a \equiv b \quad [n]$ et $c \equiv d \quad [n]$. Alors

$$a + p \equiv b + p \quad [n]$$

$$a + c \equiv b + d \quad [n]$$

$$a - c \equiv b - d \quad [n]$$

$$a \times p \equiv b \times p \quad [n]$$

$$a \times c \equiv b \times d \quad [n]$$

$$a^p \equiv b^p \quad [n]$$

Exemples

a. Par quel nombre se termine $123456789 \times 981234567$?
$123456789 = 12345678 \times 10 + 9$ donc le premier nombre est congru à 9 modulo 10.
De même le deuxième est congru à 7 modulo 10.
Donc leur produit est congru à $9 \times 7 = 63$ modulo 10, donc 3 modulo 10.
Ainsi $123456789 \times 981234567$ se termine par 3.

b. Que vaut 1314 modulo 13 ?

$$\begin{aligned} 1314 &= 13 \times 100 + 14 \\ &\equiv 0 \times 100 + 1 \quad [13] \\ &\equiv 1 \quad [13] \end{aligned}$$

Exercice 15

1. Vérifier que $90 \equiv 6 \quad [7]$ et que $66 \equiv 3 \quad [7]$.

2. En utilisant les propriétés des congruences, compléter les résultats suivants en mettant l'entier naturel le plus petit possible :

a. $90 + 66 \equiv$ ..... [7]
b. $90 \times 66 \equiv$ ..... [7]
c. $902 \equiv$ ..... [7]
d. $663 \equiv$ ..... [7]

Exercice 16

1. Faire les divisions euclidiennes de 200 et de 900 par 13 et traduire les résultats en congruences.

2. En utilisant les propriétés des congruences, compléter les résultats suivants en mettant l'entier naturel le plus petit possible :

a. $200 + 900 \equiv$ ..... [13]
b. $200 \times 900 \equiv$ ..... [13]
c. $2002 \equiv$ ..... [13]
d. $9003 \equiv$ ..... [13]
e. $2900 \equiv$ ..... [13]
f. $9413 \equiv$ ..... [13]

Propriété

Modulo n, les multiples de a sont les multiples de $pgcd(a, n)$.

Méthode

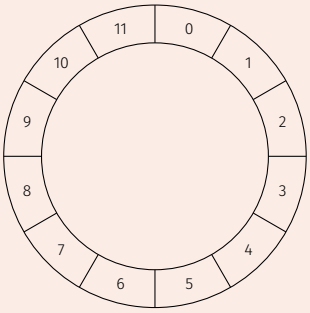
Soit une liste `L` de longueur 90, dont les éléments sont `L[0]`, `L[1]` ...`L[89]`.
On la parcourt en commençant par `L[0]` et en ajoutant 50 à chaque fois, modulo 90, indéfiniment.
Alors, puisque $pgcd(50, 90) = 10$, les multiples de 50 modulo 90 sont les multiples de 10 modulo 90 : cela veut dire qu'on ne parcourra pas tous les éléments de la liste, mais seulement :
`L[0]`, `L[10]`, `L[20]`, `L[30]`, `L[40]`, `L[50]`, `L[60]`, `L[70]` `L[80]`, `L[90]`.

Remarque

Si on parcourt une liste de longueur n en faisant des « sauts de p indices modulo n » alors on ne parcourra l'ensemble de la liste que si n et p sont premiers entre eux.

Exercice 17 : parcours d'une liste circulaire à pas constant

On considère le motif suivant : les cases sont numérotés de 0 à 11 (il y en a donc 12).

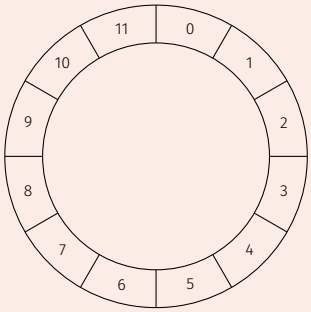


1. On choisit de parcourir les cases en partant de zéro et en se déplaçant à chaque fois de 3 cases, indéfiniment.
   Colorier toutes les case parcourues.
2. Recopier leurs indices (leur numéro) :

   Case parcourues : .....

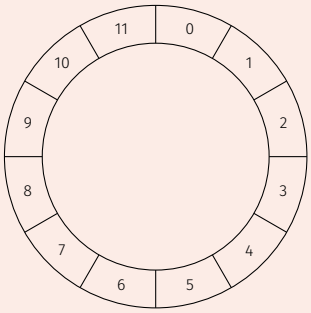
3.

Refaire **1.** et **2.** mais en sautant 4 cases.
Case parcourues : .....



4.

Refaire **1.** et **2.** mais en sautant 5 cases.
Case parcourues : .....



5. Comment expliquer la différence entre la dernière liste et les deux premières ?

Exercice 18

On parcourt une liste circulaire de longueur 84 comme à l'exercice précédent, en partant de la case d'indice zéro et en sautant 735 cases (et oui cela fait beaucoup) à chaque fois, indéfiniment.
La liste sera-t-elle parcourue entièrement ? Si ce n'est pas le cas, donner la liste des cases parcourues.
Justifier les réponses.