Chapitre

Arithmétique 4

4.1 Facteurs, multiples et division euclidienne

Définition 4.1 — Multiples. Soit n et $m \in \mathbb{N}$.

m est un multiple de n **si et seulement si** il existe $k \in \mathbb{N}$ tel que $m = k \times n$.

Les multiples de n tous les nombres de la forme kn, où $k \in \mathbb{N}$.

■ **Exemple 4.1**

a) 45 est un multiple de 9 et de 5 car $45 = 5 \times 9$.

b) Enumérer tous les diviseurs de 45.

R Pour tout $m \in \mathbb{N}$, $0 = 0 \times m$. Donc 0 **est un multiple de tout entier, et tout entier divise** 0. Néanmoins, l'usage est souvent d'ignorer 0 comme multiple.

Définition 4.2 — Division entière. Soit $n \in \mathbb{N}$ et $d \in \mathbb{N}^*$.

On appelle quotient de n par d l'entier q tel que :

$$qd \leqslant n < qd + d$$

Le reste de la division de n par d est l'entier définit par :

$$n = qd + r \qquad 0 \leqslant r < d$$

n est un multiple de d s.s.i. le reste de la division de n par d est nul.

■ **Exemple 4.2**

a) $3 \times 5 \leqslant 17 < 4 \times 5$ et $17 = 3 \times 5 + 2$.

b) $4 \times 5 \leqslant 20 < 5 \times 5$ et $20 = 4 \times 5 + 0$.

$$\begin{array}{r|l} 1\,7 & 5 \\ \cline{2-2} -\underline{1\,5} & 3 \\ 2 & \end{array} \qquad\qquad \begin{array}{r|l} 2\,0 & 5 \\ \cline{2-2} -\underline{2\,0} & 4 \\ 0 & \end{array}$$

Figure 4.1 – $17 = 3 \times 5 + 2$ et $20 = 4 \times 5$

4.1.1 Exercices

Exercice 1

1) Pour $n \in \mathbb{N}$, on pose $A(n) = n^2 + (n+1)^2$.
   a) Vérfiez que si $n = 5$, alors $A(n)$ est impair.
   b) Montrer que pour tout $n \in \mathbb{N}$, $A(n)$ est impair
2) Montrer que pour tout $n \in \mathbb{N}$, $B(n) = (3n+1)^2 - (3n-1)^2$ est un multiple de 4.
3) Montrer que pour tout $n \in \mathbb{N}$, $C(n) = (2n+3)^2 - (2n-3)^2$ est un multiple de 8.

■ **Exemple 4.3** Pour $n \in \mathbb{N}$.
Exprimer à l'aide de n, le quotient et le reste de la division de a par b dans les cas suivants :

1) $a = 15n + 2$ et $b = 3$.
2) $a = 15n + 13$ et $b = 5$.
3) $a = 15n - 4$ et $b = 5$.

Exercice 2 — À vous. Pour $n \in \mathbb{N}$. Exprimer à l'aide de n, le quotient et le reste de la division de a par b dans les cas suivants :

1) $a = 6n + 2$ et $b = 2$
2) $a = 12n + 2$ et $b = 3$
3) $a = 12n + 7$ et $b = 3$
4) $a = 6n - 5$ et $b = 6$
5) $a = 12n - 7$ et $b = 6$
6) $a = 6n - 5$ et $b = 3$

Exercice 3 Mêmes consignes.

1) $a = (2n+1)^2$ et $b = 4$
2) $a = (2n-1)^2$ et $b = 2$
3) $a = (3n+2)^2$ et $b = 3$

Exercice 4 Associe pour les énoncés le mieux adapté.

Pour tout $p, q \in \mathbb{N}$, $2p+1$ et $2p+3$ sont ... •	• deux nombres consécutifs
Pour tout $p, q \in \mathbb{N}$, $2p+1$ et $2p+2$ sont ... •	• deux nombres pairs consécutifs
Pour tout $p, q \in \mathbb{N}$, $2p$ et $2q$ sont ... •	• deux nombres impairs consécutifs
Pour tout $p, q \in \mathbb{N}$, $2p$ et $2p+2$ sont ... •	• un nombre pair et le nombre impair suivant
Pour tout $p, q \in \mathbb{N}$, p et $p+1$ sont ... •	• un nombre impair et le nombre pair suivant
Pour tout $p, q \in \mathbb{N}$, $2p$ et $2p+1$ sont ... •	• deux nombres impairs quelconques
Pour tout $p, q \in \mathbb{N}$, $2p+1$ et $2q+1$ sont ... •	• deux nombres pairs quelconques

Exercice 5

1) Montrer que la somme de 3 nombres consecutifs est toujours un multiple de 3.
2) Montrer que la somme de 3 nombres pairs consécutifs est toujours un multiple de 6.
3) Montrer que la somme de 4 nombres impairs consécutifs est toujours un multiple de 8.

Exercice 6

$a, b \in \mathbb{N}$ deux entiers non nuls. On considère la division euclidienne $a = qb + r$.

a) Montrer que si un entier d divise b et r alors d divise aussi a.

b) Montrer que si un entier d divise a et b alors d divise aussi r.

Les deux questions précédentes impliquent que le PGCD de a et b est aussi le PGCD de b et r.

Algorithme d'Euclide

Le PGCD de deux nombres n'est pas changé si on remplace le plus grand d'entre eux par le reste de la division du plus grand par le plus petit.

Calculons le PGCD de 8136 et 492 à l'aide de l'algorithme d'Euclide :

$8136 = 492 \times 16 + 264$; $\qquad$ $\text{PGCD}(8136; 492) = \text{PGCD}(492; 264)$.

L'algorithme d'Euclide peut s'écrire à l'aide d'une boucle infinie :

```python
def pgcd(a,b) :                 # deux arguments en entrée
    while b != 0 :
        a , b = b , a%b         # double affectation
    return a
```

Faire tourner à la main le script avec les instructions :

`pgcd(39,15)`

	a	b	sortie de boucle ?
fin 1re boucle			

`pgcd(32,13)`

	a	b	sortie de boucle ?
fin 1re boucle			

`pgcd(13,32)`

	a	b	sortie de boucle ?
fin 1re boucle			

R Illustration géométrique de l'algorithme d'Euclide https://www.geogebra.org/m/qjd4ngam et souvenirs de 3e.

4.2 Nombres premiers

Définition 4.3 Un nombre entier est **premiers** s'il admet **exactement** 2 diviseurs **différents** : 1 et lui même.

On classe les nombres entiers $\mathbb{N}^*$ en 3 catégories :
l'unité 1
les nombres premiers 2, 3, 5...
les nombres composés tout le reste.

Théorème 4.4 — Nombres premiers < 100. sont :
- 2, 3, 5 et 7.
- tous les nombres non divisibles par 2, 3, 5 et 7.

■ **Exemple 4.5** 11 , 31 et 97 sont des nombres premiers.

Théorème 4.6 — Test de primalité (admis). Si $n \in \mathbb{N}^*$ n'admet pour diviseur aucun des nombres (premiers) compris entre 2 et $\sqrt{n}$, alors n est premier.

■ **Exemple 4.7** Vérifier que les nombres 149 et 173 sont premiers.

Théorème 4.8 — théorème fondamental de l'arithmétique. Tout nombre entier $n \in \mathbb{N}^*$ se décompose de manière unique (à l'ordre près) en produit de facteurs premiers.

■ **Exemple 4.9** 31 est un nombre premier, sa décomposition en facteurs premiers est lui-même.
$1008 = 2^4 \times 3^2 \times 7^1$. Le facteur 2 a pour multiplicité 4.
$25777 = 149 \times 173$.

4.2.1 TP Algorithmes de test de primalité

- l'instruction `a//b` retourne le quotient de la division entière de a par b.
- l'instruction `a%b` retourne le reste de la division entière de a par b.

L'objectif est de comprendre le fonctionnement des différents scripts par une lecture attentive. Les programmer sur une calculatrice peut servir de vérification, mais n'est ni nécessaire ni suffisant.

Exercice 1

```
1 def fonction(n) :
2     x = 0
3     for i in range(1,n):
4         if n%i == 0 :
5             x = x+1
6     return x
```

```
7 def estpremier(n) :
8     p = fonction(n)
9     if ....
10        return True
11    else :
12        return False
```

1) On utilise l'instruction `fonction(12)`. Faire tourner le script à la main, et vérifier que la valeur retournée est 5. Préciser :
   a) le nombre de répétitions de la boucle `for`.
   b) pour chaque répétition `i`, la valeur de `x` à la fin.
2) Lancer à la main l'instruction `fonction(5)` et `fonction(6)`, et préciser la valeur retournée.
3) On suppose que `fonction(n)` est un entier $\geqslant 2$. Corriger la ligne 3 afin que l'instruction `fonction(n)` retourne le nombre de diviseurs de `n`.
4) Comment utiliser l'instruction `fonction(n)` pour déterminer si `n` est premier ?
5) Compléter la ligne 9 afin que l'instruction `estpremier(n)` retourne `True` si `n` est premier, et `False` dans le cas contraire.

Exercice 2

```
1 def fonction(n) :
2     i = 2
3     while n%i !=0 :
4         i = i + 1
5     return i
6
```

```
7 def estpremier(n) :
8     p = fonction(n)
9     if ......
10        return True
11    else :
12        return False
```

1) Faire tourner le script à la main, et vérifier que l'instruction `fonction(7)` retourne `7`.
2) Que retourne l'instruction `fonction(12)` ? `fonction(35)` ?
3) Que retourne l'instruction `fonction(n)` lorsque `n` est un nombre entier supérieur ou égal à 2 ?
4) Comment utiliser l'instruction `fonction(n)` pour déterminer si `n` est premier ?
5) Compléter la ligne 9 afin que l'instruction `estpremier(n)` retourne `True` si `n` est premier, et `False` dans le cas contraire.

Exercice 3

1) Expliquer pourquoi 10101 n'est pas premier.
2) Comparer le nombre de boucles nécessaire à chacun des algorithmes des exercices 1 et 2 pour identifier que 10101 n'est pas premier. Quel algorithme est le plus rapide ?
3) Le script ci dessous `estpremier()` ci-dessous est supposé retourner `True` si la variable en entrée `n` est un nombre premier et `False` sinon.

```
1 def estpremier(n) :
2     x = 2
3     while x < n**0.5 :        # rappel : n^{0,5} = √n, alternative x**2<n
4         if n%x== 0 :
5             return ...
6         else :
7             x = x + 1
8     return ...
```

On rappelle que l'exécution de la fonction s'arrête à l'exécution d'une instruction `return`.

a) Faire tourner le script avec l'instruction `estpremier(15)`.
Combien de fois la boucle `while` est exécutée ?
Que vaut la variable `x` à l'arrêt de la fonction ?

b) Mêmes questions, cette fois on utilise l'instruction `estpremier(15)`.

c) Compléter les lignes 5 et 8 par `True` ou `False`.

4) Expliquer pourquoi il n'est pas nécessaire de chercher des diviseurs au delà de $\sqrt{n}$.
5) Faire tourner (à la main) le scipt avec l'instruction `estpremier(9)` puis `estpremier(16)`. Que constatez vous ?
6) Corriger la ligne 3, afin de remédier à l'erreur de la question précédente.

Exercice 4 — Réfuter une conjecture à l'aide d'un algorithme.

Pierre de Fermat (* 1605, † 1665) pensait que tous les entiers $F_n = 2^{(2^n)} + 1$ étaient des nombres premiers. Effectivement $F_0 = 3$, $F_1 = 5$ et $F_2 = 2^{(2^2)} + 1 = 17$ sont des nombres premiers.

À l'aide de l'algorithme final de l'exercice 3 , et en complétant le script ci-dessous, trouve le plus petit entier F_n qui n'est pas premier.

```
n , F = 0 , 3
while ....
    n = n + 1
    F =
print(n)
```

4.3 TD Implications et raisonnement par contraposée

P et Q sont des affirmations dont les valeurs de vérité sont soit VRAI soit FAUX. Une implication est un énoncé de la forme « Si P alors Q » ou « P implique Q » (en abrégé $P \Rightarrow Q$).

> « P implique Q » est un énoncé FAUX quand « P VRAI et Q FAUX ».
> L'implication est VRAI dans les autres cas.

■ **Exemple 4.10** Donner les valeurs de vérité des implications suivantes :

	Vrai	Faux
1/ Si 12 est un multiple de 9, alors 12 est un multiple de 3.	☐	☐
2/ Si 10 est un multiple de 9, alors 10 est un multiple de 3.	☐	☐
3/ Si x est un multiple de 9, alors x est un multiple de 3.	☐	☐
4/ Si 18 est un multiple de 3, alors 18 est un multiple de 9.	☐	☐
5/ Si 12 est un multiple de 3, alors 12 est un multiple de 9.	☐	☐
6/ Si 10 est un multiple de 3, alors 10 est un multiple de 9.	☐	☐
7/ Si x est un multiple de 3, alors x est un multiple de 9.	☐	☐

> **À retenir**
>
> | Sa contraposée | L'implication | Sa réciproque |
> |---|---|---|
> | Si non Q alors non P | Si P alors Q | Si Q alors P |

■ **Exemple 4.11** Pour chacune des implications suivantes rédiger la réciproque et la contraposée et préciser si elles sont vraies ou fausses.

	Vrai	Faux
1/ Implication Si c'est un ours polaire, alors l'animal sait nager.	☐	☐
2/ Contraposée	☐	☐
3/ Réciproque	☐	☐

	Vrai	Faux
1/ Implication Si le triangle ABC est rectangle en A, alors $AB^2 + AC^2 = BC^2$.	☐	☐
2/ Contraposée	☐	☐
3/ Réciproque	☐	☐

Exercice 1 — À vous. Mêmes consignes

	Vrai	Faux
1/ Implication Si l'animal est une poule, alors l'animal pond des oeufs.	☐	☐
2/ Contraposée	☐	☐
3/ Réciproque	☐	☐

	Vrai	Faux
1/ Implication Si c'est un carré alors le quadrilatère a 4 angles droits.	☐	☐
2/ Contraposée	☐	☐
3/ Réciproque	☐	☐

	Vrai	Faux
1/ Implication Si deux droites du plan se coupent alors elles sont perpendiculaires.	☐	☐
2/ Contraposée	☐	☐
3/ Réciproque	☐	☐

Une implication et sa contraposée ont toujours même valeur de vérité (soit toutes les deux vraies, soit toutes les deux fausses).

Définition 4.4 Un nombre $p \in \mathbb{N}$ est pair (multiple de 2) s'il peut s'écrire sous la forme $p = 2k$, avec $k \in \mathbb{N}$.

Un nombre $q \in \mathbb{N}$ est impair, si le reste de la division de q par 2 est 1. c.à.d. il peut s'écrire sous la forme $2k + 1$ avec $k \in \mathbb{N}$.

Théorème 4.12 Pour tout entier $n \in \mathbb{N}$:

Si n est pair alors n^2 est pair.

Si n est impair alors n^2 est impair.

Exercice 2 — au programme. Démontrer les implications.

n est pair. Il existe $k \in \mathbb{N}$ tel que

$$n = 2k$$

n est impair. Il existe $k \in \mathbb{N}$ tel que

$$n = 2k + 1$$

Théorème 4.13 Pour tout entier $n \in \mathbb{N}$:

Si n^2 est pair alors n est pair.

Si n^2 est impair alors n est impair.

Contraposée Si

Contraposée Si

4.4 Le raisonnement par l'absurde

Démontrer par l'absurde

Démontrer par l'absurde[1] que P est VRAI revient à démontrer l'implication :

« (non P) implique FAUX »

[1] Raisonnement par l'absurde de Galilée sur la chute des corps. Vidéo d'Etiuenne Klein, France-Culture.

Par la suite nous utiliserons plusieurs fois le résultat suivant.

Proposition 4.14 Pour tout entier $n \in \mathbb{N}$. n et n^2 sont de même parité.

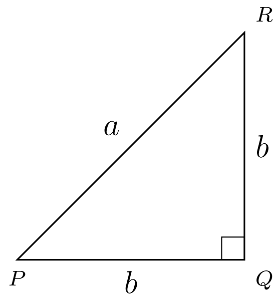

Figure 4.2 – Il n'existe pas de triangle rectangle isocèle dont les côtés sont tous entiers.

Théorème 4.15 $\sqrt{2}$ est un irrationnel.
Il n'exite pas d'entiers $a, b \in \mathbb{N}$ tel que $2b^2 = a^2$.

Démonstration. au programme.

Nous allons montrer « $\sqrt{2} \in \mathbb{Q}$ implique FAUX » en 3 étapes.

Supposons $\sqrt{2} \in \mathbb{Q}$. Il existe $a, b \in \mathbb{N}$:

$$\sqrt{2} = \frac{a}{b} \qquad \frac{a}{b} \text{ irréductible}$$
$$2 = \frac{a^2}{b^2}$$
$$2b^2 = a^2$$

Établir la parité de a et de b a^2 est pair.
a est de même parité que a^2, a est aussi pair.
b ne peut pas être pair, la fraction $\frac{a}{b}$ serait réductible.
b est forcément impair.

Établir la contradiction à partir des parités de a et b a est pair : il existe $p \in \mathbb{N}$ tel que $a = 2p$.
b est impair : il existe $q \in \mathbb{N}$ tel que $b = 2q + 1$.

$$\begin{aligned} 2(2q+1)^2 &= (2p)^2 && \text{\textit{On développe}} \\ 4q^2 + 4q + 2 &= 4p^2 && \times\frac{1}{2} \\ 2q^2 + 2q + 1 &= 2p^2 \\ \underbrace{2(q^2+q)+1}_{\text{impair}} &= \underbrace{2p^2}_{\text{pair}} \end{aligned}$$

D'ou la contradiction. FAUX. ∎

4.4.1 Exercices : raisonnement par l'absurde

Exercice 1 — $\sqrt{6} \notin \mathbb{Q}$. [1]

Supposons le contraire : $\sqrt{6}$ est un rationnel et $\sqrt{6} = \dfrac{a}{b}$ irréductible avec $a, b \in \mathbb{N}$.

1) Établir que $6b^2 = a^2$
2) a) Justifier soigneusement que a est un nombre pair.
   b) En déduire que b est un nombre impair.
3) Soit p et q deux entiers tels que $a = 2p$, et $b = 2q + 1$.
   a) Montrer que $6q^2 + 6q + 3 = 2p^2$
   b) Expliquer pourquoi la dernière égalité amène une contradiction qui permet de conclure.

Exercice 2 — $\sqrt{3} \notin \mathbb{Q}$. [2]

Supposons le contraire : $\sqrt{3}$ est un rationnel et $\sqrt{3} = \dfrac{a}{b}$ irréductible avec $a, b \in \mathbb{N}$.

1) Établir que $3b^2 = a^2$
2) a) Justifier soigneusement que si b est pair, alors a est aussi pair.
   b) Justifier soigneusement que si b est impair, alors a est aussi impair.
   c) Expliquer pourquoi la possibilité que a et b soient tous les deux pairs est à rejeter.
   d) Que peut-on en déduire ?
3) Soit p et q deux entiers tels que $a = 2p + 1$, et $b = 2q + 1$.
   a) Montrer que $6q^2 + 6q + 1 = 2p^2 + 2p$
   b) Expliquer pourquoi la dernière égalité amène une contradiction qui permet de conclure.

Exercice 3 — $\sqrt{5} \notin \mathbb{Q}$. [3]

Supposons le contraire : $\sqrt{5}$ est un rationnel et $\sqrt{5} = \dfrac{a}{b}$ irréductible avec $a, b \in \mathbb{N}$.

1) Établir que $5b^2 = a^2$
2) En suivant la même démarche que la question 2 de l'exercice précédent, montrer que a et b sont tous les deux impairs.
3) Soit p et q deux entiers tels que $a = 2p + 1$, et $b = 2q + 1$.
   a) Montrer que $5q^2 + q + 1 = p^2 + p$, puis que $5q(q + 1) + 1 = p(p + 1)$.
   b) Justifier que $p(p + 1)$ et $q(q + 1)$ sont des nombres pairs.
   c) Expliquer pourquoi cela amène une contradiction qui permet de conclure.

Exercice 4 — $\sqrt{12} \notin \mathbb{Q}$. [4]

Supposons le contraire : $\sqrt{12}$ est un rationnel et $\sqrt{12} = \dfrac{a}{b}$ irréductible avec $a, b \in \mathbb{N}$.

a) Justifier que $\frac{\sqrt{12}}{2}$ est aussi un rationnel.
b) En simplifiant la racine carré, montrer que $\frac{\sqrt{12}}{2} = \sqrt{3}$.
c) Expliquer pourquoi cela amène une contradiction qui permet de conclure.

1. La même méthode s'applique pour $\sqrt{10}$, $\sqrt{14}$ et $\sqrt{18}$.
2. La même méthode s'applique pour $\sqrt{7}$, $\sqrt{11}$, $\sqrt{15}$ et $\sqrt{19}$.
3. La même méthode s'applique pour $\sqrt{13}$, mais ne marchera pas pour $\sqrt{17}$!
4. La même méthode s'applique pour $\sqrt{8} = 2\sqrt{2}$, $\sqrt{18} = 3\sqrt{2}$ et $\sqrt{20} = 2\sqrt{5}$.

Exercice 5

1) Expliquer pourquoi l'implication « Si x et y sont rationnels alors $x + y$ est un rationnel » est vraie.
2) Nous voulons démontrer par l'absurde que $1 + \sqrt{6}$ est un irrationnel. Supposons le contraire : $\alpha = 5 + 2\sqrt{6} \in \mathbb{Q}$.
   a) Montrer que $\sqrt{6} = \frac{1}{2}(\alpha - 5)$. En déduire que $\sqrt{6} \in \mathbb{Q}$.
   b) Expliquer pourquoi cela amène une contradiction qui permet de conclure.

Exercice 6

1) Que pensez vous de l'argument « $\sqrt{2}$ et $\sqrt{3}$ sont irrationnels, donc $\sqrt{2} + \sqrt{3}$ l'est aussi » ?
2) Démontrer par l'absurde que $\sqrt{2} + \sqrt{3}$ est irrationnel. *Indication :* développer $(\sqrt{2} + \sqrt{3})^2$.

Exercice 7

$n \in \mathbb{N}$ est un entier différent de 1. x est le plus petit diviseur de n autre que 1. Nous voulons démontrer par l'absurde que x est toujours un nombre premier.

Recopier les encadrés en les mettant dans le bon ordre pour avoir une démonstration valide.

Supposons au contraire que x n'est pas premier	p et q sont inferieur à x.	$n = pqy$.
Contradiction car x est le plus petit diviseur différent de 1 de n.	il existe $y \in \mathbb{N}$ tel que $n = xy$
p et q sont des diviseurs de n	il existe p et $q \in \mathbb{N}$ différents de 1 tel que $d = pq$.

■ **Exemple 4.16 — Application.** En trouvant le plus petit facteur autre que 1 d'un nombre, on trouve aussi le plus petit facteur premier. Ce théorème est à la base des algorithmes de décomposition en facteurs premiers d'un entier.

Analysons le fonctionnement des instructions `decomposition(24)` et `decomposition(150)` :

```python
def decomposition(n) :       # n est un entier
    x = 2
    while n != 1 :           #
        if n%x==0 :          #
            print(x)         #
            n = n // x       #
        else :
            x = x + 1        #
    return "FIN"
```

24	.....	150	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....		.....	

Déterminer le plus grand facteur premier de 600 851 475 143 ....