1

Les ensembles d'entiers $\mathbb{N}$ et $\mathbb{Z}$

Au programme

- √ Approfondir la notion de nombre.
- √ Approfondir l'étude des multiples et diviseurs d'un entier.
- √ Modéliser et résoudre des problèmes avec multiples et diviseurs.
- √ Modéliser et résoudre des problèmes avec des nombres pairs ou impairs.
- √ Décomposer un entier en produit de facteurs premiers.
- √ Présenter les résultats fractionnaires sous forme de fractions irréductibles.
- √ Découvrir certains symboles mathématiques.
- √ Découvrir certains types de raisonnements mathématiques.

Table des matières

I Les ensembles $\mathbb{N}$ et $\mathbb{Z}$

Les **entiers naturels** sont les nombres qui servent à compter. Ce sont les nombres 0, 1, 2, 3, 4, $\ldots$ L'ensemble des entiers naturels est noté $\mathbb{N}$. Cette notation est due à Richard DEDEKIND en 1888 (ce n'est pas si vieux que ça). On a donc

$$\mathbb{N} = \{0,1,2,3,4,\ldots\}.$$

L'ensemble des entiers naturels non nuls se note $\mathbb{N}^*$. Donc,

$$\mathbb{N}^* = \{1,2,3,4,\ldots\}.$$

Quand un nombre n est un entier naturel, on écrit $n \in \mathbb{N}$ ce qui se lit « n appartient à $\mathbb{N}$ ».

Les **entiers relatifs** sont les nombres $\ldots -4$, -3, -2, -1, 0, 1, 2, 3, 4, $\ldots$ Un entier relatif peut être pensé comme un entier naturel muni d'un signe ($1 = +1$, $2 = +2$, $\ldots$). On note $\mathbb{Z}$ l'ensemble des entiers relatifs. On a donc

$$\mathbb{Z} = \{\ldots,-4,-3,-2,-1,0,1,2,3,4,\ldots\}.$$

Cet ensemble de nombres a d'abord été noté K par Richard DEDEKIND. Il a ensuite été noté $\mathbb{Z}$ par Nicolas BOURBAKI dans la première moitié du XX ème siècle. Le nom Nicolas BOURBAKI n'est pas le nom d'une personne physique mais le pseudonyme d'un groupe de mathématiciens crée en 1935. La lettre $\mathbb{Z}$ est l'initiale du mot allemand « zahl » qui signifie numéro ou nombre, le verbe « zahlen » signifiant compter.

L'ensemble des entiers relatifs positifs peut être noté $\mathbb{Z}^+$. On a donc

$$\mathbb{Z}^+ = \{0,1,2,3,4,\ldots\} = \mathbb{N}.$$

L'ensemble des entiers relatifs négatifs peut être noté $\mathbb{Z}^-$: $\mathbb{Z}^- = \{\ldots,-4,-3,-2,-1,0\}$. On dispose aussi de l'ensemble des entiers relatifs non nuls $\mathbb{Z}^* = \{\ldots,-4,-3,-2,-1,1,2,3,4,\ldots\}$, de l'ensemble des entiers relatifs strictement positifs $\mathbb{Z}^{+*} = \{1,2,3,4,\ldots\}$ (ou aussi $\mathbb{Z}_+^*$ ou aussi $\mathbb{N}^*$) et de l'ensemble des entiers relatifs strictement négatifs $\mathbb{Z}^{-*} = \{\ldots,-4,-3,-2,-1\}$ (ou aussi $\mathbb{Z}_-^*$).

Enfin, un entier naturel est un entier relatif d'un type particulier : c'est un entier relatif positif. L'ensemble des entiers naturels est donc une **partie** (on dit aussi un **sous-ensemble**) de l'ensemble des entiers relatifs. Ceci se note

$$\mathbb{N} \subset \mathbb{Z}$$

ce qui se lit « $\mathbb{N}$ est contenu dans $\mathbb{Z}$ » ou aussi « $\mathbb{N}$ est **inclus** dans $\mathbb{Z}$ ».

Un entier relatif strictement négatif n'appartient pas à $\mathbb{N}$. Par exemple, $-7 \notin \mathbb{N}$ ce qui se lit « -7 n'appartient pas à $\mathbb{N}$ ».

Enfin, l'ensemble $\mathbb{N}$ est inclus dans l'ensemble $\mathbb{Z}$ mais l'ensemble $\mathbb{Z}$ n'est pas inclus dans l'ensemble $\mathbb{N}$. Ceci s'écrit

$$\mathbb{Z} \not\subset \mathbb{N}.$$

II Arithmétique dans $\mathbb{Z}$

A Divisibilité dans $\mathbb{Z}$

Définition 1

Soient a et b deux entiers relatifs.

b est un **multiple** de a équivaut à : il existe un entier relatif q tel que $b = a \times q$.

ce qui signifie

Si b est un multiple de a, **alors** il existe un entier relatif q tel que $b = a \times q$ et
Si il existe un entier relatif q tel que $b = a \times q$, **alors** b est un multiple de a.

Ces deux phrases peuvent aussi se résumer en une seule :

b est un multiple de a **si et seulement si** il existe un entier relatif q tel que $b = a \times q$.

☞ *Donc, dans la définition précédente, l'expression « si et seulement si » peut se détailler en deux phrases : « si b*

est un multiple de a, alors il existe un entier relatif q tel que $b = qa$ » et aussi « si il existe un entier relatif q tel que $b = qa$, alors b est un multiple de a ». Une phrase comportant l'expression « si et seulement si » doit se lire aussi bien de gauche à droite (la partie de gauche entraine la partie de droite) que de droite à gauche (la partie de droite entraine la partie de gauche).

• L'entier 6 est un multiple de 3 car $6 = 3 \times 2$ où 2 est un entier relatif.
• L'entier -6 est aussi un multiple de 3 car $-6 = 3 \times (-2)$ où -2 est un entier relatif.
• De manière générale, les multiples de 3 sont les nombres de la forme $3q$ où q est dans $\mathbb{Z}$ (ce qui s'écrit $q \in \mathbb{Z}$ et se lit « q appartient à $\mathbb{Z}$ ») c'est-à-dire les nombres $\ldots, -21, -18, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, 21, \ldots$.

• Tout nombre entier relatif n est multiple de 1. En effet, $n = 1 \times n$ avec n entier relatif.
• 0 est un multiple de tout entier relatif n. En effet, $0 = n \times 0$ avec n entier relatif.

Dire qu'un entier naturel b est multiple d'un entier a signifie aussi que la division de b par a « tombe juste ». On rappelle ce qu'est la **division euclidienne** d'un entier naturel b par un entier naturel non nul a : il existe un entier naturel q et un entier naturel r tels que $b = a \times q + r$ et $0 \leqslant r < b$. q est le **quotient** de la division euclidienne de b par a et r est le **reste** de la division euclidienne de b par a. La division euclidienne se présente sour la forme :

a	b
r	q

Par exemple, la division euclidienne de 37 par 4 s'écrit $37 = 4 \times 9 + 1$:

37	4
1	9

Dire qu'un entier naturel b est un multiple d'un entier naturel non nul équivaut à dire que le reste de la division euclidienne de b par a est nul :

a	b
0	q

On peut renverser la phrase « b est un multiple de a » en écrivant que a est un diviseur de b ou que a divise b. Mais **attention, on ne divise pas par** 0. D'où la définition précise :

Définition 2

Soient a un entier relatif non nul et b un entier relatif.

L'entier a **divise** l'entier b (on dit aussi que l'entier a est un **diviseur** de l'entier b) si et seulement si il existe un entier relatif q tel que $b = a \times q$.

☞ *1 - Si a n'est pas nul, il revient au même de dire que b est un multiple de a ou que a est un diviseur de b ou que a divise b.*

2 - De nouveau, la phrase de gauche entraine la phrase de droite et la phrase de droite entraine la phrase de gauche.

Par exemple, l'entier 17 est un diviseur de l'entier 51 ou encore 17 divise 51 car $51 = 17 \times 3$ avec 3 entier relatif. De même, l'entier relatif -6 divise l'entier relatif 24 car $24 = (-6) \times (-4)$ avec -4 entier relatif.

Theoreme 1

Soient a, b et c trois entiers relatifs.

Si b et c sont multiples de a, **alors** $b + c$ est un multiple de a et $b - c$ est un multiple de a.

Démonstration : (au programme pour une valeur numérique de a donnée).

Montrons que la somme et la différence de deux multiples de 6 est un multiple de 6 (donc, dans cette démonstration, $a = 6$).

Soient b et c deux entiers relatifs tels que b et c soient des multiples de 6.

Il existe deux entiers relatifs q et q' tels que $b=6q$ et $c=6q'$. Mais alors, $b+c=6q+6q'=6(q+q')$ et $b-c=6(q-q')$ où de plus $q+q'$ et $q-q'$ sont des entiers relatifs. Ceci montre que $b+c$ et $b-c$ sont des multiples de 6.

■

Démonstration : (pas au programme pour une valeur de a quelconque).

Soient a, b et c trois entiers relatifs tels que b et c soient des multiples de a.

Puisque b et c sont des multiples de a, il existe deux entiers relatifs q et q' tels que $b=qa$ et $c=q'a$. Mais alors, $b+c=qa+q'a=(q+q')a$ et $b-c=qa-q'a=(q-q')a$ où de plus $q+q'$ et $q-q'$ sont des entiers relatifs. Ceci montre que $b+c$ et $b-c$ sont des multiples de a.

■

Dans la démonstration précédente, il y a un piège. On a bien écrit $b=qa$ et $c=q'a$ et on n'a pas écrit $b=qa$ et $c=qa$. Si on avait écrit $b=qa$ et $c=qa$, on aurait démontré le résultat du théorème uniquement dans le cas où b et c sont égaux. Dans le cas général, les quotients $\frac{b}{a}$ et $\frac{c}{a}$ peuvent être différents et on ne les note pas de la même façon : $\frac{b}{a}=q$ et $\frac{c}{a}=q'$ ou encore $b=qa$ et $c=q'a$. Maintenant, quand on écrit $b=qa$ et $c=q'a$, on ne suppose pas non plus que b et c sont différents ou encore, on ne suppose pas que q et q' sont différents. Les nombres q et q' peuvent être égaux ou différents.

Exercice 1

Montrer que la somme de trois entiers relatifs consécutifs est toujours divisible par 3.

Solution 1 : Trois entiers relatifs consécutifs s'écrivent sous la forme n, $n+1$ et $n+2$ où n est un entier relatif. Or

$$n+(n+1)+(n+2)=3n+3=3(n+1)$$

où de plus $n+1$ est un entier relatif. Donc, $n+(n+1)+(n+2)$ est un multiple de 3 ou encore $n+(n+1)+(n+2)$ est un entier divisible par 3.

■

☞ *Il aurait été encore plus élégant de dire que trois entiers consécutifs sont trois entiers de la forme $n-1$, n, et $n+1$, auquel cas leur somme est $(n-1)+n+(n+1)=3n$.*

Pour finir ce paragraphe, rappelons quelques critères de divisibilité. Soit n un entier naturel.

• n est divisible par 2 si et seulement si n est pair, ce qui équivaut à dire que le chiffre des unités de n est 0, 2, 4, 6 ou 8.

• n est divisible par 4 si et seulement le nombre formé par ses deux derniers chiffres est divisible par 4. Par exemple, 1524 est divisible par 4 alors que 2018 ne l'est pas.

• n est divisible par 5 si et seulement si le chiffre des unités de n est 0 ou 5.

• n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

• n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.

Exercice 2

1) Montrer que pour tous nombres entiers naturels a, b et c,

$$10^2a+10b+c=a+b+c+9(11a+b).$$

2) Montrer le critère de divisibilité par 9 pour les nombres entiers naturels ayant un nombre de chiffres inférieurs ou égal à 3.

Solution 2 :

1) Soient a, b et c trois entiers naturels.

$$10^2a+10b+c=100a+10b+c=99a+a+9b+b+c=a+b+c+9(11a+b).$$

On a montré que pour tous nombres entiers naturels a, b et c, $10^2a+10b+c=a+b+c+9(11a+b)$.

2) Soit n un entier naturel ayant au plus trois chiffres. Notons a, le chiffre des centaines, b le chiffre des dizaines et c le chiffre des unités de l'entier n. Donc, a, b et c sont trois nombres entiers compris au sens large entre 0 et 9 tels que $n=10^2a+10b+c$.

Supposons que la somme des chiffres de n est divisible par 9. Donc, il existe un entier naturel k tel que $a+b+c=9k$. D'après la question 1),

$$n=a+b+c+9(11a+b)=9k+9(11a+b)=9(k+11a+b)$$

où de plus $k+11a+b$ est un entier relatif. Donc, n est divisible par 9.

Inversement, supposons que n est divisible par 9. Donc, il existe un entier naturel k tel que $n=9k$. Alors,

$$a+b+c=10^2a+10b+c-9(11a+b)=n-9(11a+b)=9k-9(11a+b)=9(k-(11a+b))=9(k-11a-b)$$

où de plus $k-11a-b$ est un entier relatif. Donc, $a+b+c$ est divisible par 9.

On a montré que n est divisible par 9 si et seulement si la somme de ses chiffres $a+b+c$ est divisible par 9.

■

☞ *Dans la solution précédente, on emploie les mots « chiffres » et « nombres ». Les nombres servent à compter et les chiffres servent à représenter les nombres. C'est la même chose dans le langage : il y a des mots qui servent à s'exprimer et des lettres qui servent à écrire ces mots. Il y a des mots à trois lettres (par exemple « mot »), des mots à deux lettres (par exemple, « un ») et des mots à une lettre (par exemple, « à »). De même, il y a des nombres à trois chiffres, deux chiffres, un chiffre comme* 407, 21 *ou* 5.

B Nombres pairs, nombres impairs

Définition 3

Les **entiers pairs** sont les multiples de 2 c'est-à-dire les entiers de la forme $2k$ où k est un entier relatif.
Les **entiers impairs** sont les entiers de la forme $2k+1$ où k est un entier relatif.

Les entiers relatifs pairs sont les entiers $\ldots -6, -4, -2, 0, 2, 4, 6, \ldots$ et les entiers relatifs impairs sont les entiers $\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots$

Les entiers pairs sont les multiples de 2 et les entiers impairs sont les entiers pairs augmentés de 1.

Tout entier est ou bien pair, ou bien impair. Le mot « pair » doit être relié au mot « paire » : quand on a un nombre pair d'objets (par exemple, 6 lettres a, b, c, d, e, f), on peut regrouper ces objets par paires (par exemple, $\{a,b\}$, $\{c,d\}$, $\{e,f\}$). Le mot « impair » est alors le contraire du mot « pair » comme le mot « impossible » est le contraire du mot « possible ».

Theoreme 2

La somme de deux entiers pairs est un entier pair.
La somme de deux entiers impairs est un entier pair.
La somme d'un entier pair et d'un entier impair est un entier impair.

Démonstration :

La somme de deux entiers pairs est un entier pair car la somme de deux multiples de 2 est un multiple de 2 d'après le théorème 1.

Soient n et m deux entiers relatifs impairs. Il existe deux entiers relatifs k et k' tels que $n=2k+1$ et $m=2k'+1$ puis

$$n+m=(2k+1)+(2k'+1)=2k+2k'+2=2(k+k'+1)$$

où de plus $k+k'+1$ est un entier relatif. Donc, $n+m$ est un entier relatif pair.

Soient n un entier relatif pair et m un entier relatif impair. Il existe deux entiers relatifs k et k' tels que $n=2k$ et $m=2k'+1$ puis

$$n+m=(2k)+(2k'+1)=2k+2k'+1=2(k+k')+1$$

où de plus $k+k'$ est un entier relatif. Donc, $n+m$ est un entier relatif impair.

■

Theoreme 3

Le carré d'un nombre pair est un nombre pair.
Le carré d'un nombre impair est un nombre impair.

Démonstration : (au programme)

Soit n un entier relatif pair. Il existe un entier relatif k tel que $n=2k$. Mais alors

$$n^2=(2k)^2=(2k)\times(2k)=2\times\left(2k^2\right)$$

où de plus $2k^2$ est un entier relatif. Donc, n^2 est un entier relatif pair.

Soit n un entier relatif impair. Il existe un entier relatif k tel que $n=2k+1$. Mais alors

$$n^2=(2k+1)^2=(2k+1)\times(2k+1)=(2k)^2+2k+2k+1^2=4k^2+4k+1=2\times\left(2k^2+2k\right)+1$$

où de plus $2k^2+2k$ est un entier relatif. Donc, n^2 est un entier relatif impair.

■

☞ *On déduit du théorème 3 le fait que si le carré d'un entier n est pair, n ne peut être que pair et si le carré d'un entier n est impair, celui-ci ne peut être que impair.*

Exercice 3

Montrer que le produit de deux entiers consécutifs est un nombre pair.

Solution 3 : Deux entiers consécutifs s'écrivent n et $n+1$ où n est un entier relatif. n est ou bien pair, ou bien impair.

1er cas. Supposons n pair. Il existe un entier relatif k tel que $n=2k$. On a alors

$$n(n+1)=(2k)(2k+1)=2\times k(2k+1)$$

où de plus $k(2k+1)$ est un entier relatif. Donc, $n(n+1)$ est un entier pair.

2ème cas. Supposons n impair. Il existe un entier relatif k tel que $n=2k+1$. On a alors

$$n(n+1)=(2k+1)(2k+2)=(2k+1)\times 2(k+1)=2\times(2k+1)(k+1)$$

où de plus $(2k+1)(k+1)$ est un entier relatif. Donc, $n(n+1)$ est un entier pair.

On a montré dans tous les cas que $n(n+1)$ est un entier pair ou encore on a montré que le produit de deux entiers consécutifs est un entier pair.

■

La solution précédente aurait pu être plus brève : l'un des deux entiers n ou $n+1$ est pair et le produit d'un entier pair par un entier quelconque est un entier pair. Donc, $n(n+1)$ est un entier pair.

☞ *Dans la solution précédente, nous avons utilisé un certain type de raisonnement, le* ***raisonnement par disjonction des cas****. Un entier est soit pair, soit impair. Nous avons alors analysé ce qui se passait dans chacune des deux situations ou encore dans chacun des deux cas.*

C Nombres premiers

Définition 4

Un nombre premier est un entier naturel n supérieur ou égal à 2 qui admet exactement deux diviseurs dans $\mathbb{N}$.

Les dix premiers nombres premiers sont

$$2 \quad 3 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29$$

Il est possible de démontrer qu'il y en a une infinité mais la démonstration est d'un niveau trop élevé pour une classe de seconde.

Le nombre 1 ne fait pas partie de la liste des nombres premiers.

Theoreme 4

Soit n un entier supérieur ou égal à 2.

n est premier si et seulement si les seuls diviseurs de n dans $\mathbb{N}^*$ sont 1 et n.
n est non premier si et seulement si n admet au moins un diviseur autre que 1 et n.

Un entier n supérieur ou égal à 2 et non premier peut donc s'écrire sous la forme $n = a \times b$ où a est un entier **strictement** compris entre 1 et n.

Définition 5

Un entier supérieur ou égal à 2 et non premier est dit **composé**.

Par exemple, l'entier 7 est premier car les seuls diviseurs de 7 dans $\mathbb{N}^*$ sont 1 et 7 alors que l'entier 15 est composé car l'entier 15 admet pour diviseur 1 et 15 mais aussi 3 ou 5.

Les nombres premiers sont d'abord utilisés pour décomposer n'importe quel entier (supérieur ou égal à 2) en produit de nombres qui eux ne sont plus décomposables (les nombres premiers).
Par exemple, $6 = 2 \times 3$ ou $45 = 3 \times 3 \times 5 = 3^2 \times 5$. Cette décomposition peut ensuite être utilisée de multiples façons. En seconde, on utilise la décomposition en produit de facteurs premiers pour simplifier le plus possible des fractions ou des racines carrées. On admet le théorème suivant, appelé « **théorème fondamental de l'arithmétique** » :

Theoreme 5

Tout nombre entier supérieur ou égal à 2, est soit un nombre premier, soit un produit de nombres premiers. De plus, cette décomposition est unique à l'ordre près des facteurs.

Dire que cette décomposition est unique permet d'affirmer sans calcul que $2^{47} \times 3^{51} \times 7^{12} \neq 2^{63} \times 3^{50} \times 7^{10}$ car 2, 3 et 7 sont des nombres premiers et par exemple, le nombre premier 7 apparaît 12 fois dans le nombre $2^{47} \times 3^{51} \times 7^{12}$ et seulement 10 fois dans le nombre $2^{63} \times 3^{50} \times 7^{10}$. De manière générale, si on est dans la situation $2^a 3^b 7^c = 2^{a'} 3^{b'} 7^{c'}$, alors on peut affirmer que nécessairement $a = a'$, $b = b'$ et $c = c'$.

Pour décomposer un entier supérieur ou égal à 2 donné en produit de facteurs premiers, on utilise une méthode **algorithmique**. Voyons cela sur un exemple.

Exemple. On veut décomposer le nombre $222\,264$ en produit de facteurs premiers.

• On prend le premier nombre premier, à savoir 2, puis on « extrait » le plus possible ce nombre 2 du nombre $222\,264$:

$$222\,264 = 2 \times 111\,132 = 2^2 \times 55\,556 = 2^3 \times 27\,783.$$

• $27\,783$ n'est plus divisible par 2. On passe au nombre premier suivant, à savoir 3 :

$$222\,264 = 2^3 \times 27\,783 = 2^3 \times 3 \times 9\,261 = 2^3 \times 3^2 \times 3\,087 = 2^3 \times 3^3 \times 1\,029 = 2^3 \times 3^4 \times 343.$$

• 343 n'est plus divisible par 3 (car la somme de ses chiffres $3 + 4 + 3 = 10$ n'est pas divisible par 3). On passe au nombre premier suivant, à savoir 5.

• 343 n'est pas divisible par 5. On passe au nombre premier suivant, à savoir 7.

$$222\,264 = 2^3 \times 3^4 \times 343 = 2^3 \times 3^4 \times 7 \times 49 = 2^3 \times 3^4 \times 7^3.$$

Les nombres 2, 3 et 7 sont des nombres premiers. La décomposition de $222\,264$ en produit de facteurs premiers est donc

$$222\,264 = 2^3 \times 3^4 \times 7^3.$$

■

On donne d'ores et déjà deux applications de la décomposition en produit de facteurs premiers. La première est la simplification des fractions. Par exemple, on veut simplifier la fraction $\frac{1575}{2205}$:

$$\frac{1575}{2205}=\frac{3^2\times5^2\times7}{3^2\times5\times7^2}=\frac{3\times3\times5\times5\times7}{3\times3\times5\times7\times7}=\frac{5}{7}.$$

La décomposition en produit de facteurs premiers permet de simplifier au maximum sans rien oublier. On peut aussi simplifier des racines carrées « en sortant un maximum de choses de la racine carrée ». Par exemple,

$$\sqrt{72}=\sqrt{36\times2}=\sqrt{6^2\times2}=\sqrt{6^2}\times\sqrt{2}=6\sqrt{2}.$$

L'intérêt d'une telle transformation est par exemple le calcul mental. Il n'est pas évident d'avoir une idée précise de la valeur de $\sqrt{72}$ alors que si l'on sait que $\sqrt{2}=1,414\ldots$, on obtient sans trop d'effort $\sqrt{72}=6\sqrt{2}=8,48\ldots$ Nous reviendrons sur ces deux situations dans le chapitre suivant.

Dès que les nombres sont un peu grands, il n'est pas évident de savoir si un nombre est premier. Par exemple, 323 est-il un nombre premier ? La première technique qui vient à l'esprit est de diviser 323 par tous les nombres qui lui sont strictement inférieurs de 2 à 322. Si une division tombe juste, le nombre n'est pas premier. Mais si aucune des 321 divisions ne tombe juste, ce nombre est premier. Le théorème qui suit a pour but de diminuer énormément le nombre de ces divisions.

Theoreme 6

Soit n un nombre entier supérieur ou égal à 4.

n n'est pas premier si et seulement si n est divisible par au moins un nombre premier inférieur ou égal à sa racine carrée.
n est premier si et seulement si n n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée.

Démonstration : Soit n un entier supérieur ou égal à 4. Vérifions d'abord que $\sqrt{n}<n$.
On a $n-\sqrt{n}=\sqrt{n}\times\sqrt{n}-\sqrt{n}=\sqrt{n}\left(\sqrt{n}-1\right)$. Puisque $n\geqslant4$, on a $\sqrt{n}>1$ puis $\sqrt{n}-1>0$ et donc $\sqrt{n}\left(\sqrt{n}-1\right)>0$. On en déduit que $n-\sqrt{n}>0$ et donc que $\sqrt{n}<n$.

Supposons que n est divisible par au moins un nombre premier p inférieur ou égal à sa racine carrée. D'abord $p\geqslant2$ et d'autre part, $p\leqslant\sqrt{n}$ et donc $p<n$ (d'après la remarque initiale). Ainsi, n admet un diviseur p strictement compris entre 1 et n et donc n n'est pas premier.

Supposons que n n'est pas premier. il existe donc deux entiers a et b compris entre 2 et $n-1$ au sens large tels que $n=a\times b$ et $a\leqslant b$ (a est donc le plus petit des deux nombres a et b). Mais alors, après multiplication par le nombre positif a,

$$a\times a\leqslant a\times b$$

ou encore $a^2\leqslant n$ puis $a\leqslant\sqrt{n}$. Donc, a est un diviseur de n vérifiant $2\leqslant a\leqslant\sqrt{n}$. Soit alors p un nombre premier apparaissant dans la décomposition de a en produit de facteurs premiers. En particulier, $p\leqslant a$ puis $p\leqslant\sqrt{n}$.

Ensuite, il existe un entier k tel que $a=pk$ et il existe un entier k' tel que $n=ak'$. On en déduit que $n=ak'=pkk'$ où de plus kk' est un entier relatif. L'entier p divise donc l'entier n. On a montré qu'il existe un nombre premier p tel que $2\leqslant p\leqslant\sqrt{n}$ et n est divisible par p.

Finalement, l'entier n n'est pas premier si et seulement si il existe un nombre premier p tel $2\leqslant p\leqslant\sqrt{n}$ et n est divisible par p.

■

☞ *1 - Dans la démonstration précédente, nous sommes passés de l'inégalité $a^2\leqslant n$ à l'inégalité $a\leqslant\sqrt{n}$ en considérant ce raisonnement comme intuitif. La racine carrée sera étudiée avec soin dans les chapitres suivants et le raisonnement précédent deviendra tout à fait rigoureux.*

*2 - L'implication « **si** n est premier, **alors** n n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée » est équivalente à l'implication « **si** n est divisible par au moins nombre premier inférieur ou égal à sa racine carrée , **alors** n n'est pas premier » et l'implication « **si** n n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée, **alors** n est premier » est équivalente à l'implication « **si** n n'est pas premier, **alors** n est divisible par au moins nombre premier inférieur ou égal à sa racine carrée ».*

*De manière générale, l'implication « si A est vraie, alors B est vraie » est équivalente à l'implication « si B est faux, alors A est faux ». L'implication « si B est faux, alors A est faux » est la **contraposée** de l'implication « si A est vraie,*

alors B *est vraie ». La contraposée d'une implication est équivalente à cette implication. On dit alors que l'on a raisonné* ***par contraposition.***

Exercice 4

Les entiers 323 et 151 sont-ils des nombres premiers ?

Solution 4 :

• $144 < 151 < 169$ ou encore $12^2 < 151 < 13^2$. Donc, $\sqrt{151} = 12,\ldots$ Les nombres premiers inférieurs ou égaux à $\sqrt{151}$ sont 2, 3, 5, 7 et 11.

151 est impair et n'est donc pas divisible par 2.
151 n'est pas divisible par 3 car la somme de ses chiffres $1+5+1=7$ n'est pas divisible par 3.
151 n'est pas divisible par 5 car son chiffre des unités n'est ni 0, ni 5.
$\dfrac{151}{7} = 21,5\ldots$ La division de 151 par 7 ne tombe pas juste et donc 151 n'est pas divisible par 7.
$\dfrac{151}{11} = 13,7\ldots$ et donc 151 n'est pas divisible par 11.

Finalement, 151 n'est divisible par aucun nombre premier inférieur ou égal à sa racine carrée et donc 151 est un nombre premier.

• $289 < 323 < 324$ ou encore $17^2 < 323 < 18^2$. Donc, $\sqrt{323} = 17,\ldots$ Les nombres premiers inférieurs ou égaux à $\sqrt{323}$ sont 2, 3, 5, 7, 11, 13 et 17.

323 est impair et n'est donc pas divisible par 2.
323 n'est pas divisible par 3 car la somme de ses chiffres $3+2+3=8$ n'est pas divisible par 3.
323 n'est pas divisible par 5 car son chiffre des unités n'est ni 0, ni 5.
$\dfrac{323}{7} = 46,1\ldots$ et donc 323 n'est pas divisible par 7.
$\dfrac{323}{11} = 29,3\ldots$ et donc 323 n'est pas divisible par 11.
$\dfrac{323}{13} = 24,8\ldots$ et donc 323 n'est pas divisible par 13.
$323 = 17 \times 19$ et donc 323 n'est pas un nombre premier.

■