# Divisibilité et nombres premiers

Y. Moncheaux


Avril 2022

# Table des matières

# Ne pas noter

**Rappels :**

# Ne pas noter

**Rappels :**

$\mathbb{Z}$ est l'ensemble des entiers relatifs (positifs ou négatifs)

# Ne pas noter

**Rappels :**

$\mathbb{Z}$ est l'ensemble des entiers relatifs (positifs ou négatifs)

$\mathbb{N}$ est l'ensemble des entiers naturels (positifs)

# Ne pas noter

**Rappels :**

$\mathbb{Z}$ est l'ensemble des entiers relatifs (positifs ou négatifs)

$\mathbb{N}$ est l'ensemble des entiers naturels (positifs)

Écrire « $n \in \mathbb{Z}$ » est une façon rapide de dire que $n$ est un entier.

# Ne pas noter

La branche des mathématiques qui s'occupe des nombres entiers est appelée **arithmétique**.

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

**Exemple 1**

12 est un multiple de 3 car $12 = 3 \times 4$ ;

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

**Exemple 1**

12 est un multiple de 3 car $12 = 3 \times 4$ ;
851 est un multiple de 37 car $851 = 37 \times 23$.

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

**Exemple 1**

12 est un multiple de 3 car $12 = 3 \times 4$ ;
851 est un multiple de 37 car $851 = 37 \times 23$.

Ⓓ Si $b = a \times c$ avec $a$, $b$, $c$ entiers alors le nombre $a$ est un diviseur de $b$ (et $b$ est *divisible* par $a$).

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

**Exemple 1**

12 est un multiple de 3 car $12 = 3 \times 4$ ;
851 est un multiple de 37 car $851 = 37 \times 23$.

Ⓓ Si $b = a \times c$ avec $a$, $b$, $c$ entiers alors le nombre $a$ est un diviseur de $b$ (et $b$ est *divisible* par $a$).

**Exemple 2**

7 est un diviseur de 21 ;

# I – Diviseurs et multiples

Ⓓ Un nombre $b \in \mathbb{Z}$ est un multiple de $a \in \mathbb{Z}$ s'il existe $c \in \mathbb{Z}$ tel que $b = a \times c$.

**Exemple 1**

12 est un multiple de 3 car $12 = 3 \times 4$ ;
851 est un multiple de 37 car $851 = 37 \times 23$.

Ⓓ Si $b = a \times c$ avec $a$, $b$, $c$ entiers alors le nombre $a$ est un diviseur de $b$ (et $b$ est *divisible* par $a$).

**Exemple 2**

7 est un diviseur de 21 ;
37 est un diviseur de 851.

# Ne pas noter

**Remarque**

0 est un multiple de n'importe quel nombre (car $0 = a \times 0$) mais n'est le diviseur d'aucun nombre.

# Ne pas noter

**Remarque**

0 est un multiple de n'importe quel nombre (car $0 = a \times 0$) mais n'est le diviseur d'aucun nombre.

**Remarque**

Quand nous disons que $b$ est divisible par $a$, il s'agit de divisibilité dans $\mathbb{Z}$.

# Ne pas noter

**Remarque**

0 est un multiple de n'importe quel nombre (car $0 = a \times 0$) mais n'est le diviseur d'aucun nombre.

**Remarque**

Quand nous disons que $b$ est divisible par $a$, il s'agit de divisibilité dans $\mathbb{Z}$.
Ainsi $9 = 5 \times 1,8$ mais 9 n'est pas divisible par 5 (dans $\mathbb{Z}$).

**Propriété**

La somme de deux multiples d'un nombre $a$ est un multiple de $a$.

## Propriété

La somme de deux multiples d'un nombre $a$ est un multiple de $a$.

## Démonstration

Soient $b = a \times c$ et $b' = a \times c'$ deux multiples de $a$ (où $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$).

## Propriété

La somme de deux multiples d'un nombre $a$ est un multiple de $a$.

## Démonstration

Soient $b = a \times c$ et $b' = a \times c'$ deux multiples de $a$ (où $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$).
Alors $b + b' = a \times c + a \times c' = a \times (c + c')$.

## Propriété

La somme de deux multiples d'un nombre $a$ est un multiple de $a$.

## Démonstration

Soient $b = a \times c$ et $b' = a \times c'$ deux multiples de $a$ (où $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$).
Alors $b + b' = a \times c + a \times c' = a \times (c + c')$.
Or $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$ donc $c + c' \in \mathbb{Z}$
donc $b + b'$ est un multiple de $a$.

## Propriété

La somme de deux multiples d'un nombre $a$ est un multiple de $a$.

## Démonstration

Soient $b = a \times c$ et $b' = a \times c'$ deux multiples de $a$ (où $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$).
Alors $b + b' = a \times c + a \times c' = a \times (c + c')$.
Or $c \in \mathbb{Z}$ et $c' \in \mathbb{Z}$ donc $c + c' \in \mathbb{Z}$
donc $b + b'$ est un multiple de $a$.

## Exemple 3

63 et 49 sont des multiples de 7 donc $63 + 49 = 112$ aussi.

# Partie exercices

Exercices 1 page 70 (résolu), 5 page 70, 15, 19, 22 page 72

# Ne pas noter

Un nombre est parfait s'il est égal à la somme de ses diviseurs.
Par exemple : $6 = 1 + 2 + 3$ est parfait.

# Ne pas noter

Un nombre est parfait s'il est égal à la somme de ses diviseurs.
Par exemple : $6 = 1 + 2 + 3$ est parfait.

Après 2000 ans de recherche, nous ne connaissons que 47 nombres parfaits et nous ne savons pas s'il existe des nombres parfaits impairs !

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

**Propriété**

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

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.
$n^2 = (2\,n' + 1)^2$

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.
$n^2 = (2\,n' + 1)^2 = (2\,n')^2 + 2 \times (2\,n') \times 1 + 1^2$

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.
$n^2 = (2\,n' + 1)^2 = (2\,n')^2 + 2 \times (2\,n') \times 1 + 1^2 =$
$4\,n'^2 + 4\,n' + 1$

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.
$n^2 = (2\,n' + 1)^2 = (2\,n')^2 + 2 \times (2\,n') \times 1 + 1^2 =$
$4\,n'^2 + 4\,n' + 1 = 2(2\,n'^2 + 2\,n') + 1.$

Ⓓ $n \in \mathbb{Z}$ est pair s'il s'écrit $n = 2\,n'$ avec $n' \in \mathbb{Z}$.
$n \in \mathbb{Z}$ est impair s'il s'écrit $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.

## Propriété

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

## Démonstration

Soit $n$ un nombre impair, alors $n = 2\,n' + 1$ avec $n' \in \mathbb{Z}$.
$n^2 = (2\,n' + 1)^2 = (2\,n')^2 + 2 \times (2\,n') \times 1 + 1^2 =$
$4\,n'^2 + 4\,n' + 1 = 2(2\,n'^2 + 2\,n') + 1$.
Comme $N = 2\,n'^2 + 2\,n'$ est un entier, $n^2 = 2\,N + 1$ est donc impair.

# Ne pas noter

**Rappels : critères de divisibilité**

Un nombre entier est divisible par :

- 2 si son chiffre des unités est 0 ; 2 ; 4 ; 6 ou 8
- 5 si son chiffre des unités est 0 ou 5
- 3 si la somme de ses chiffres est divisible par 3
- 9 si la somme de ses chiffres est divisible par 9

# Ne pas noter

**Rappels : critères de divisibilité**

Un nombre entier est divisible par :

- 2 si son chiffre des unités est 0 ; 2 ; 4 ; 6 ou 8
- 5 si son chiffre des unités est 0 ou 5
- 3 si la somme de ses chiffres est divisible par 3
- 9 si la somme de ses chiffres est divisible par 9

**Exemple 4**

570 est divisible par 2, par 5 et aussi par 3 car $5+7+0=12$ qui est divisible par 3.

# Partie exercices

Exercices 29, 30, 31, 32, 35, 38, 40 page 73

# Ne pas noter

Il est souvent utile de décomposer un nombre entier en produit de nombres entiers, par exemple $12 = 3 \times 4$.

# Ne pas noter

Il est souvent utile de décomposer un nombre entier en produit de nombres entiers, par exemple $12 = 3 \times 4$.
Certains nombres « résistent » à cette décomposition, par exemple 17 ne peut se décomposer qu'en $17 \times 1$.

# Ne pas noter

Il est souvent utile de décomposer un nombre entier en produit de nombres entiers, par exemple $12 = 3 \times 4$.
Certains nombres « résistent » à cette décomposition, par exemple 17 ne peut se décomposer qu'en $17 \times 1$.
De tels nombres sont dits premiers.

# II – Nombres premiers

## 1) Définition

Ⓓ Un nombre premier est un nombre entier positif qui a exactement deux diviseurs entiers : 1 et lui-même.

# II – Nombres premiers

## 1) Définition

Ⓓ Un nombre premier est un nombre entier positif qui a exactement deux diviseurs entiers : 1 et lui-même.

**Exemple 5**

6 n'est pas premier car $6 = 2 \times 3$ mais 7 est premier.

# II – Nombres premiers

## 1) Définition

Ⓓ Un nombre premier est un nombre entier positif qui a exactement deux diviseurs entiers : 1 et lui-même.

**Exemple 5**

6 n'est pas premier car $6 = 2 \times 3$ mais 7 est premier.
1 n'est pas premier car il a un seul diviseur : 1.

# Ne pas noter

Nous savons depuis Euclide (il y a plus de 2300 ans) qu'il existe une infinité de nombres premiers mais il existe plusieurs conjectures encore non résolues sur les nombres premiers :

# Ne pas noter

Nous savons depuis Euclide (il y a plus de 2300 ans) qu'il existe une infinité de nombres premiers mais il existe plusieurs conjectures encore non résolues sur les nombres premiers :
– existe-t-il un infinité de nombres premiers jumeaux (tels que 3 et 5 ou 11 et 13) ?

# Ne pas noter

Nous savons depuis Euclide (il y a plus de 2300 ans) qu'il existe une infinité de nombres premiers mais il existe plusieurs conjectures encore non résolues sur les nombres premiers :

– existe-t-il un infinité de nombres premiers jumeaux (tels que 3 et 5 ou 11 et 13) ?

– y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$ ?

# Ne pas noter

Nous savons depuis Euclide (il y a plus de 2300 ans) qu'il existe une infinité de nombres premiers mais il existe plusieurs conjectures encore non résolues sur les nombres premiers :

– existe-t-il un infinité de nombres premiers jumeaux (tels que 3 et 5 ou 11 et 13) ?

– y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$ ?

– la conjecture de Riemann qui porte sur la répartition des nombres premiers est un des problèmes les plus célèbres ; sa résolution rapporterait à son découvreur 1 million de dollars !

# Partie exercices

Exercices 45, 42, 44 page 73 ; 47, 49, 50 page 74

# 2) Décomposition d'un nombre entier en un produit

**Propriété**

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

# 2) Décomposition d'un nombre entier en un produit

**Propriété**

Tout entier strictement positif peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

**Exemple 6**

$7632 = 2^4 \times 3^2 \times 53$

# Ne pas noter

**Remarque**

Nous admettrons cette propriété. Les éléments de preuve se trouvent encore dans les textes d'Euclide.

# Ne pas noter

**Remarque**

Nous admettrons cette propriété. Les éléments de preuve se trouvent encore dans les textes d'Euclide.

**Remarque**

Cette propriété est appelée le théorème fondamental de l'arithmétique.

# Ne pas noter

**Remarque**

Les techniques de cryptographies les plus utilisées sur Internet reposent sur cette factorisation en produit de nombres premiers.

# Ne pas noter

## Remarque

Un entier peut donc se décomposer comme produit de nombres premiers mais peut-il se décomposer comme somme de nombres premiers ?
Goldbach (1742) proposa cette conjecture : tout nombre pair supérieur à 4 s'écrit comme somme de deux nombres premiers.

# Ne pas noter

**Remarque**

Un entier peut donc se décomposer comme produit de nombres premiers mais peut-il se décomposer comme somme de nombres premiers ?
Goldbach (1742) proposa cette conjecture : tout nombre pair supérieur à 4 s'écrit comme somme de deux nombres premiers.
Nous sommes encore très loin de la démonstration (à 1 million de dollars) de cette conjecture... (Terence Tao (2012) : tout nombre pair supérieur à 4 s'écrit comme somme d'au maximum 5 nombres premiers).

# Partie exercices

Exercices 55, 56, 57, 61 page 74 ; 63, 68 page 75

# 3) Fractions irréductibles

Ⓓ Une fraction d'entiers $\frac{a}{b}$ est irréductible si $a$ et $b$ n'ont pas de diviseur commun autre que 1.

# 3) Fractions irréductibles

Ⓓ Une fraction d'entiers $\frac{a}{b}$ est irréductible si $a$ et $b$ n'ont pas de diviseur commun autre que 1.

**Exemples 7**

$\frac{21}{10}$ est irréductible car $21 = 3 \times 7$ et $10 = 2 \times 5$.

# 3) Fractions irréductibles

Ⓓ Une fraction d'entiers $\frac{a}{b}$ est irréductible si $a$ et $b$ n'ont pas de diviseur commun autre que 1.

## Exemples 7

$\frac{21}{10}$ est irréductible car $21 = 3 \times 7$ et $10 = 2 \times 5$.

mais $\frac{252}{70} = \frac{2^2 \times 3^2 \times 7}{2 \times 5 \times 7} = \frac{2 \times 3^2}{5} = \frac{18}{5}$.

# Ne pas noter

**Remarque**

Deux nombres entiers $a$ et $b$ qui n'ont pas de diviseur commun sont dits premiers entre eux.

# Ne pas noter

**Remarque**

Deux nombres entiers $a$ et $b$ qui n'ont pas de diviseur commun sont dits premiers entre eux.
La probabilité qu'une fraction choisie au hasard soit irréductible (que deux nombres entiers choisis au hasard soient premiers entre eux) est $\frac{6}{\pi^2}$ !!

# Partie exercices

Exercices 72, 73, 75, 78 page 75
Activité : écriture d'un algorithme puis d'une fonction disant un nombre est premier.