Math93.com

Arithmétique

Seconde

I. Division euclidienne (*Euclidean division or division with remainder*)

Propriété 1 (Division euclidienne (*Euclidean division or division with remainder*))

a désigne un entier relatif (*integer*) et b un entier naturel non nul (*natural numbers*).
Il existe un unique couple d'entiers relatifs (q, r) tel que $a = bq + r$ avec $0 \leqslant r < b$.

Remarque

En anglais, les relatifs sont les *integers*, les entiers naturels les *Whole numbers* et les entiers naturels non nul les *Natural numbers*.

Définition 1 (Division Euclidienne (*Euclidean division or division with remainder*))

Soit a un entier relatif et b un entier naturel non nul.
Effectuer une **division euclidienne** d'un entier relatif a par un entier naturel b non nul $(b \neq 0)$, c'est trouver deux nombres entiers relatifs, le quotient q et le reste r , tels que :

$$\boxed{a = b \times q + r} \text{ , avec } \quad 0 \leqslant r < b.$$

Exemple

1. Division euclidienne de $a = 185$ par $b = 7$.

$$\begin{array}{r|l} 185 & 7 \\ \cline{2-2} -14 & 26 \\ \cline{1-1} 45 & \\ -42 & \\ \cline{1-1} 3 & \end{array} \quad \Longrightarrow \quad 185 = 7 \times 26 + 3$$

Dans la division euclidienne de $a = 185$ par $b = 7$, on a :

$$\begin{cases} \text{quotient : } & q = 26 \\ \text{reste : } & 0 \leqslant r = 5 < b = 7 \end{cases}$$

2. Division euclidienne de $a = -17$ par $b = 5$.
La division de -17 par 5 donne

$$-17 = 5 \times (-4) + 3$$

soit un quotient de -4 et un reste de 3.

$$\begin{cases} \text{quotient : } & q = -4 \\ \text{reste : } & 0 \leqslant r = 3 < b = 5 \end{cases}$$

Exercice 1

Effectuer la division euclidienne de -100 par 7..

II. Multiples et diviseurs (*multiples and divisors*)

II.1 Définition

Définition 2 (Multiple et diviseur (*multiples and divisors*))

Soit a et b deux entiers relatifs, ce qui s'écrit $(a\ ;\ b) \in \mathbb{Z} \times \mathbb{Z}$ ou $(a\ ;\ b) \in \mathbb{Z}^2$

- Un nombre entier a **est un multiple** de b non nul lorsque le reste de la division euclidienne de a par b est 0.
- On dit que b **est un diviseur de** a ou que a est divisible par b.
- L'entier relatif b divise l'entier relatif a si et seulement si il existe donc un entier relatif $q \in \mathbb{Z}$ tel que :

$$\boxed{a = b \times q}$$

Exemple

L'entier $a = 15$ est un multiple de $b = 3$ car $15 = 3 \times 5$. Les entiers 3 et 5 sont donc des diviseurs de 15.

II.2 Entiers pairs et impairs (*even and odd integers*)

Remarque

Les restes possibles dans la division euclidienne d'un entier relatif quelconque a par 2 sont 0 et 1.
En effet d'après la définition 1, le reste r de la division par 2 vérifie $0 \leqslant r < 2$.

Définition 3 (Entier pair et impair)

Soit $a \in \mathbb{Z}$. L'entier relatif a est un nombre :

- pair lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = 2 \times k$;
- impair lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = 2 \times k + 1$;

Exemple

- Par exemple (-10) est pair car il existe un relatif $k = -5 \in \mathbb{Z}$ tel que $-10 = 2 \times (-5)$.
- Par exemple 51 est impair car il existe un relatif $k = 25 \in \mathbb{Z}$ tel que $51 = 2 \times 25 + 1$.
- Un entier relatif est soit pair, soit impair.

Propriété 2

Soit $a \in \mathbb{Z}$.

1. L'entier relatif a^2 est impair si, et seulement si, a est impair.
2. L'entier relatif a^2 est pair si, et seulement si, a est pair.

La preuve de cette propriété est au programme et à connaitre !

Preuve

1. On veut montrer que l'entier relatif a^2 est impair si, et seulement si, a est impair. Attention il faut montrer la double implication !

1. a. Supposons que l'entier relatif a soit impair.
Par définition, il existe un relatif k tel que $a = 2k + 1$ et donc :

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\underbrace{(2k^2 + 2k)}_{k'} + 1$$

Donc $a^2 = 2k' + 1$ avec k' entier relatif, ce qui prouve que a^2 est impair.

1. b. Supposons que l'entier a^2 soit impair.
Deux possibilité alors, soit a est impair, soit a est pair.
Supposons que a soit pair.
Par définition, il existe un relatif k tel que $a = 2k$ et donc :

$$a^2 = (2k)^2 = 4k^2 = 2\underbrace{(2k^2)}_{k'}$$

Donc $a^2 = 2k'$ avec k entier relatif, ce qui prouve que a^2 est pair. Ce qui est impossible puisqu'on a supposé a^2 impair.
Donc a est impair, cqfd !

2. On veut montrer que l'entier relatif a^2 est pair si, et seulement si, a est pair.

2. a. Supposons que l'entier relatif a soit pair.
On a déjà montré que dans ce cas a^2 est pair.

2. b. Supposons que l'entier a^2 soit pair.
Deux possibilité alors, soit a est impair, soit a est pair.
Supposons que a soit impair.
On a montré que dans ce cas a^2 est aussi impair donc c'est impossible. a est donc pair.

Propriété 3

Soit $a \in \mathbb{Z}$.
Si b et b' sont deux multiples de a alors $b + b'$ est un multiple de a et $b - b'$ aussi.

On peut aussi dire que si a divise b et b', alors a divise aussi $b + b'$ et $b - b'$.

Preuve

Soit $a \in \mathbb{Z}$ et b et b' sont deux multiples de a . Il existe deux entiers relatifs k et k' tels que

$$\begin{cases} b = k \times a \\ b' = k' \times a \end{cases} \Longrightarrow b + b' = k \times a + k' \times a = a \times \underbrace{(k + k')}_{k''}$$

Donc $b + b' = k'' \times a$ avec $k'' \in \mathbb{Z}$ ce qui prouve que $b + b'$ est un multiple de a.

Et de même :

$$\begin{cases} b = k \times a \\ b' = k' \times a \end{cases} \Longrightarrow b - b' = k \times a - k' \times a = a \times \underbrace{(k - k')}_{n}$$

Donc $b - b' = n \times a$ avec $n \in \mathbb{Z}$ ce qui prouve que $b - b'$ est un multiple de a.

III. Nombres premiers (*prime numbers*)

Définition 4 (Nombres premiers)

Un **nombre premier** est un nombre entier qui a exactement deux diviseurs positifs, 1 et lui-même.
The numbers greater than 1 that are not prime are called composite numbers.

Exemples

Liste des 25 nombres premiers inférieurs à 100.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 et 97.

Remarque historique

La première trace incontestable de la présentation des nombres premiers remonte à l'Antiquité (vers 300 av. J.-C.), et se trouve dans les Éléments d'Euclide (livres VII à IX). Euclide donne une définition des nombres premiers, la preuve de leur infinité, la définition du plus grand commun diviseur (pgcd) et du plus petit commun multiple (ppcm), et les algorithmes pour les déterminer, aujourd'hui appelés algorithmes d'Euclide.

Depuis décembre 2018, le plus grand nombre premier connu est :

$$2^{82\,589\,933} - 1$$

C'est un nombre comportant 24 862 048 chiffres lorsqu'il est écrit en base dix.

Propriété 4 (Test de primalité (*Primality test*))

Soit n un entier naturel supérieur ou égal à 2. Si n n'est divisible par aucun nombre premier p inférieur ou égal à $\sqrt{n}$, alors n est premier.
En effet pour savoir si un nombre est premier, il suffit de tester tous les nombres de 2 à $\sqrt{N}$ seulement, puisque si $N = pq$ alors soit $p \leqslant \sqrt{N}$ soit $q \leqslant \sqrt{N}b$.

Exercice 2

157 est-il premier . . . . . .

I

Théorème 1 (Infinitude of primes)

Il existe une infinité de nombres premiers.
There are infinitely many prime numbers.

Preuve

- Prérequis

  Théorème 2 (Admis, se démontre par récurrence forte)

  Si n est un nombre entier naturel strictement supérieur à 1, alors n admet au moins un diviseur premier.

- Supposons par l'absurde qu'il existe un nombre fini de nombres premiers, que l'on note :

  $$p_1, p_2, p_3, \cdots, p_k, \cdots, p_n \text{ avec } n \in N.$$

  Posons $P = p_1p_2p_3 \cdots p_n + 1$.

  Comme P est strictement supérieur à 1, P admet un diviseur premier d'après le théorème du prérequis.

  Ce nombre premier peut être noté p_k et appartient à liste de nombres premiers donnée en début de démonstration.

  Comme :

  - p_k divise P ;
  - et p_k divise $p_1p_2p_3 \cdots p_n$;
  - alors p_k divise aussi leur différence $(P - p_1p_2p_3 \cdots p_n)$ d'après la propriété 3

  Or, $P - p_1p_2p_3 \cdots p_n = 1$ (par définition de P) donc p_k divise 1, ce qui est absurde !

  On en conclut que l'ensemble des nombres premiers ne peut pas être un ensemble fini : il existe donc une infinité de nombres premiers.

Remarque

Il y a beaucoup de conjectures et de questions ouvertes sur les nombres premiers. Par exemple :

1. Les quatre problèmes de Landau (1912) :
   - **1. a.** conjecture de Goldbach : tout nombre pair strictement supérieur à 2 peut s'écrire comme somme de deux nombres premiers (1742) ;
   - **1. b.** conjecture des nombres premiers jumeaux : il existe une infinité de jumeaux premiers ;
   - **1. c.** conjecture de Legendre : il existe toujours au moins un nombre premier entre n^2 et $(n + 1)^2$;
   - **1. d.** existence d'une infinité de nombres premiers de la forme $n^2 + 1$.
2. L'existence d'une infinité de nombres premiers de Sophie Germain (1776-1831) .
   Un nombre premier G est appelé nombre premier de Sophie Germain si $2G + 1$ est aussi un nombre premier.
3. La conjecture de Polignac (1849) (dont celle des nombres premiers jumeaux est le cas particulier $n = 2$) : tout entier naturel pair n peut s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières.

IV. Décomposition en facteurs premiers (*prime factorization*)

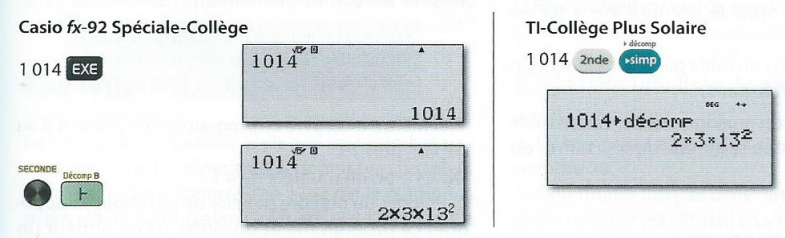
Propriété 5 (Admis)

Un nombre entier supérieur ou égal à 2 se décompose en produit de facteurs premiers. Cette décomposition est unique, à l'ordre des facteurs près.
Writing a number as a product of prime numbers is called a prime factorization of the number.

Exemple

$$1\,014 = 2 \times 507$$
$$1\,014 = 2 \times (3 \times 169)$$
$$1\,014 = 2 \times 3 \times (13 \times 13)$$

$$\boxed{1\,014 = 2 \times 3 \times 13^2}$$



V. Applications de la décomposition

V.1 Calculer le Plus Grand Commun Diviseur de deux entiers (PGCD, gcd en anglais)

Méthode 1 (PGCD)

1. On écrit la décomposition des entiers en facteurs premiers.
2. On recherche les facteurs communs des deux entiers (on les entoure par exemple) .
3. On calcule alors le produit des facteurs communs.

Pour résumer, le PGCD de deux nombres entiers a et b supérieurs ou égaux à 2 a pour décomposition en facteurs premiers le produit des facteurs premiers apparaissant à la fois dans la décomposition de a et de b.

Exemple

Exemple : Calcul du Plus Grand Commun Diviseur de 126 et 180.

$$\begin{cases} 180 &= \boxed{2} \times 2 \times \boxed{3} \times \boxed{3} \times 5 \\ 126 &= \boxed{2} \times \boxed{3} \times \boxed{3} \times 7 \end{cases} \Longrightarrow \begin{cases} 180 &= \underbrace{(2 \times 3 \times 3)}_{18} \times 2 \times 5 \\ 126 &= \underbrace{(2 \times 3 \times 3)}_{18} \times 7 \end{cases} \Longrightarrow \begin{cases} 180 &= \boxed{18} \times 10 \\ 126 &= \boxed{18} \times 7 \end{cases}$$

Le **Plus Grand Diviseur Commun** des entiers 180 et 127 est donc 18.

Exercice 3

Calculer le Plus Grand Commun Diviseur de 150 et 120.

. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .
. . . . . .

VI. Fractions irréductibles

Irreducible fraction, simple fraction (or fraction in lowest terms, simplest form or reduced fraction)

Définition 5 (Fractions irréductibles)

Une fraction est dite **irréductible** lorsque le numérateur et le dénominateur n'ont pas de diviseur commun autre que 1.
An irreducible fraction (or fraction in lowest terms, simplest form or reduced fraction) is a fraction in which the numerator and denominator are integers that have no other common divisors than 1 (and -1, when negative numbers are considered).

Exemple

Pour rendre irréductible une fraction, on peut utiliser la décomposition en facteurs premiers du numérateur et du dénominateur.

$$\begin{aligned}\frac{1\,014}{84} &= \frac{2\times 3\times 13^2}{2^2\times 3\times 7}\\ &= \frac{2\times 3\times 13^2}{2\times 2\times 3\times 7}\\ &= \frac{13^2}{2\times 7}\\ \frac{1\,014}{84} &= \frac{169}{14}\end{aligned}$$

Donc on obtient la fraction sous forme irréductible :

$$\boxed{\frac{1\,014}{84} = \frac{169}{14}}$$

Exercice 4

De la même façon, donner la forme irréductible de la fraction suivante en détaillant tous les calculs :

$$\frac{245}{525} = \frac{\ldots\ldots\ldots\ldots}{\ldots\ldots\ldots\ldots}$$

$$= \frac{\ldots\ldots\ldots\ldots}{\ldots\ldots\ldots\ldots}$$

$$= \frac{\ldots\ldots\ldots\ldots}{\ldots\ldots\ldots\ldots}$$

$$= \frac{\ldots\ldots\ldots\ldots}{\ldots\ldots\ldots\ldots}$$

↤ **Fin du cours** ↦