1 Divisibilité

Définition

Un nombre relatif a est *divisible* par un entier naturel n non nul s'il existe un entier k tel que $a = kn$.

$$a \in \mathbb{Z},\ n \in \mathbb{N}^*,\ a \text{ divisible par } n \Leftrightarrow \exists k \in \mathbb{N}^*,\ a = kn.$$

n est alors appelé un *diviseur* de a.

Exemples :

- 786 est divisible par 2 et par 3, car $786 = 2 \times 393$ et $786 = 3 \times 262$.
- 0 est divisible par tout entier naturel n non nul car $0 = k \times 0$.

Définition

L'ensemble des entiers naturels compris entre deux entiers naturels a et b est noté :

$$[\![a\ ;\ b]\!].$$

Exemple : $[\![0\ ;\ 5]\!] = \{0; 1; 2; 3; 4; 5\}$.

Propriété

Soit n un entier relatif non nul. L'ensemble des diviseurs positifs de n est un ensemble fini.

Démonstration

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

Propriété

Soient a, b et c trois entiers relatifs, $a \neq 0$ et $b \neq 0$.

1. Si a divise b et b divise c alors a divise c.
2. Si a divise b et c alors a divise toute combinaison linéaire de b et c.

Démonstration

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

2 Division euclidienne

Théorème

Soient a et b deux entiers naturels. Il existe un unique couple $(q;r)$ d'entiers naturels tels que :

$$a = bq + r, \qquad 0 \leqslant r < b.$$

Cette dernière écriture est appelée la *division euclidienne de a par b*.
q est alors le *quotient* et r le *reste* de cette division.

Démonstration

Exemple :

La division euclidienne de 37 par 11 est : $37 = 3 \times 11 + 4$.
Le quotient de cette division est 3, et le reste 4.

Propriété

Soit b un entier naturel tel que $b \geqslant 2$. Tout entier a s'écrit sous une, et une seule, des formes bq, $bq+1$, $bq+2$, $\cdots$, $bq+(b-1)$, où q est un entier.

Démonstration

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

Exemple : Raisonnement par disjonction de cas

Soit n un entier naturel. Posons $A = n(n-2)(n+2)$. Démontrer que A est un multiple de 3.

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

3 Congruences

Définition

Soient m un entier naturel non nul, et a et b deux entiers relatifs.
On dit que a et b sont congrus modulo m lorsqu'ils ont le même reste dans division euclidienne par m.
On dit aussi que a est congru à b modulo m.
On note alors :

$$a \equiv b \quad [m] \qquad \text{ou} \qquad a \equiv b \quad (m) \qquad \text{ou} \qquad a \equiv b \mod m.$$

Exemples :

— $21 = 2 \times 10 + 1$ et $15 = 2 \times 7 + 1$, donc

$$21 \equiv 15 \quad [2] \qquad \text{ou} \qquad 21 \equiv 15 \quad (2) \qquad \text{ou} \qquad 21 \equiv 15 \mod 2.$$

— $21 = 4 \times 5 + 1$ et $17 = 4 \times 4 + 1$, donc

$$21 \equiv 17 \quad [4] \qquad \text{ou} \qquad 21 \equiv 17 \quad (4) \qquad \text{ou} \qquad 21 \equiv 17 \mod 4.$$

— $21 = 3 \times 6 + 3$ et $33 = 5 \times 6 + 3$, donc

$$21 \equiv 33 \quad [3] \qquad \text{ou} \qquad 21 \equiv 33 \quad (3) \qquad \text{ou} \qquad 21 \equiv 33 \mod 3.$$

Propriétés

Soient a et b deux entiers relatifs, et n un entier naturel.

1. **Divisibilité :** $a \equiv b \quad (n) \Leftrightarrow n|(a-b)$.
2. **Transitivité :** Si $a \equiv c \quad (n)$ et $c \equiv b \quad (n)$ alors $a \equiv b \quad (n)$, pour $c \in \mathbb{Z}$.
3. **Somme :**
   a. $a \equiv b \quad (n) \Leftrightarrow a + k \equiv b + k \quad (n)$ pour $k \in \mathbb{Z}$.
   b. $\begin{cases} a \equiv b \quad (n) \\ a' \equiv b' \quad (n) \end{cases} \Longrightarrow a + a' \equiv b + b' \quad (n)$.
4. **Produit :**
   a. $a \equiv b \quad (n) \Leftrightarrow ka \equiv kb \quad (n)$ pour $k \in \mathbb{Z}$.
   b. $\begin{cases} a \equiv b \quad (n) \\ a' \equiv b' \quad (n) \end{cases} \Longrightarrow aa' \equiv bb' \quad (n)$.
5. **Puissance :** $a \equiv b \quad (n) \Longrightarrow a^k \equiv b^k \quad (n)$ pour $k \in \mathbb{N}^*$.

Démonstration

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

4 PGCD de deux entiers

Définition

Soient a et b deux entiers naturels non tous les deux nuls.
Le *plus grand commun diviseur* de a et b, noté $a \wedge b$ ou $PGCD(a;b)$, est le plus grand diviseur de a et de b.

Exemples :

Les diviseurs de 12 sont : 1, 2, 3, 4, 6, 12.
Les diviseurs de 15 sont : 1, 3, 5.
Ainsi, $12 \wedge 15 = 3$ car 3 divise 12 et 15, et c'est le plus grand des diviseurs communs qui apparaît dans les deux listes.

Propriété

Soient a et b deux entiers naturels non nuls tels que : $\exists q \in \mathbb{N}^*,\ a = bq + r, \quad 0 \leqslant r < b$. Alors, $a \wedge b = b \wedge r$.

Démonstration

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

Théorème

On définit par récurrence la suite des entiers $r_0, r_1, \cdots, r_n$ tels que :
r_0 est le reste de la division euclidienne de a par b.
Si $r_0 \neq 0$, r_1 est le reste de la division euclidienne de b par r_0.
Pour tout $k \in \{1; \cdots ; n-1\}$, si $r_k \neq 0$, alors r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k.
Alors, cette suite d'entiers est nulle à partir d'un certain rang et la dernière valeur non nul prise par cette suite est $a \wedge b$.

Démonstration

Soit r_0 le reste de la division euclidienne de a par b. Par définition du reste d'une division euclidienne, $0 \leqslant r_0 < b$ et on sait que $a \wedge b = b \wedge r_0$.
Soit $m \in \mathbb{N}$. Supposons qu'on ait construit $r_0, r_1, \cdots, r_{m-1}$ non nuls et r_m tels que pour tout $k \in \{1; \cdots ; m-1\}$, r_{k+1} soit le reste de la division euclidienne de r_{k-1} par r_k.
Alors, $0 \leqslant r_m < r_{m-1} < \cdots < b$ et $a \wedge b = b \wedge r_0 = \cdots = r_{m-1} \wedge r_m$.
Si $r_m = 0$ alors $r_{m-1} \wedge r_m = r_{m-1}$.
La suite d'entiers naturels (r_m) est strictement décroissante et minorée par 0. Elle est donc nulle à partir d'un certain rang.
Soit alors n_0 tel que $r_{n_0} = 0$ et $r_{n_0-1} > 0$.

Ainsi, par construction, $a \wedge b = b \wedge r_0 = \cdots = r_{n_0-1} \wedge r_{n_0} = r_{n_0-1}$.

Exemple :
Prenons $a = 1\,386$ et $b = 1\,092$. Déterminer $a \wedge b$ en utilisant l'algorithme d'Euclide.

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

Propriété

Pour tous entiers naturels non nuls a, b et k, on a $ka \wedge kb = k \times a \wedge b$.

Démonstration

La division euclidienne de a par b est donnée par l'écriture unique : $a = bq + r$ avec $0 \leqslant r < b$.
Notons r_n le dernier reste non nul des divisions euclidiennes effectuées selon l'algorithme d'Euclide.
Par ailleurs, on peut écrire, $ka = kbp + kr$ avec $0 \leqslant r < b$. En appliquant l'algorithme d'Euclide, le dernier reste non nul est alors kr_n.
Ainsi, on a bien $PGCD(ka; kb) = kPGCD(a; b)$.

Propriétés

Soient a et b deux entiers naturels.

1. Si d divise a et d divise b alors d divise $a \wedge b$.
2. Deux entiers sont premiers entre eux si et seulement si $a \wedge b = 1$.
3. Il existe deux entiers naturels a' et b' tels que $a = a' \times a \wedge b$ et $b = b' \times a \wedge b$, avec $a' \wedge b' = 1$.

Démonstration

1. Soit d un diviseur commun de a et b. En utilisant l'algorithme d'Euclide, on constate que d divise les restes successifs des divisions euclidiennes et donc également le dernier reste non nul qui est le PGCD de a et de b.
2. — Si a et b sont premiers entre eux, leurs seul diviseur commun est 1, donc $a \wedge b = 1$.
   — Si $a \wedge b = 1$ alors le plus grand diviseur commun de a et b est 1, donc le seul diviseur commun est 1. Et donc a et b sont premiers entre eux.
3. Soient $d' = a' \wedge b'$ et k_1 et k_2 les entiers tels que $a' = d'k_1$ et $b' = d'k_2$.
   On doit montrer que $d' = 1$
   On a, $a = d'k_1 a \wedge b$ et $b = d'k_2 a \wedge b$ donc $d'a \wedge b$ est un diviseur commun de a et b.
   Ainsi, $d'a \wedge b \leqslant a \wedge b$. Par conséquent, $d' = 1$ (car $d > 0$).

5 Théorème de Bézout et théorème de Gauss

Théorème

Théorème de Bézout : Soient a et b deux entiers naturels non nuls.

$$a \wedge b = 1 \Leftrightarrow \exists (u; v) \in \mathbb{Z}^2,\ au + bv = 1.$$

Démonstration

Propriété

Identité de Bézout : Soient a et b deux entiers naturels non nuls.

$$a \wedge b = d \Longrightarrow \exists (u; v) \in \mathbb{Z}^2,\ au + bv = d.$$

Démonstration

Soient a et b deux entiers relatifs non nuls et on pose $d = a \wedge b$.
Il existe deux entiers a' et b' tels que $a = a'd$ et $b = b'd$ et tels que $a' \wedge b' = 1$.
D'après le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $a'u + b'v = 1$.
On obtient alors, $au + bv = a'du + b'dv = d(a'u + b'v) = d$.

Théorème

Théorème de Gauss : Soient a, b et c trois entiers naturels non nuls.
Si a divise bc et si $a \wedge b = 1$ alors a divise c.

Démonstration

6 Nombres premiers

Définition

Un entier naturel est premier s'il n'est divisible que par 1 et lui-même.

Remarque : Notez bien dans la définition la présence de la conjonction « et » qui induit nécessairement que le nombre doit admettre exactement deux diviseurs.
Ainsi, le nombre 1 n'est pas premier car il n'admet qu'un diviseur : lui-même.

Propriété

Il existe une infinité de nombres premiers.

Démonstration

Supposons que l'ensemble des nombres premiers soit fini. Notons alors cet ensemble :

$$\{p_1; p_2; \cdots ; p_n\}.$$

Considérons alors le nombre :

$$N = p_1 \times p_2 \times \cdots \times p_n + 1.$$

Il est immédiat que N n'appartient pas à l'ensemble des nombres premiers considéré.
Or, N n'est divisible par aucun des p_k, pour $1 \leqslant k \leqslant n$.
Par conséquent, il est premier. Ce qui est contradictoire avec le fait que N n'appartient pas à l'ensemble des nombres premiers considéré.

Ainsi, notre hypothèse selon laquelle l'ensemble des nombres premiers est fini est fausse.

Propriété

Soit n un entier naturel non nul.
Si n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ alors n est premier.

Démonstration

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

Exemple : $\sqrt{137} \approx 11,7$.
De plus, 137 n'est pas divisible par 2, 3, 5, 7 et 11 donc $137 \in \mathbb{P}$ avec $\mathbb{P}$ l'ensemble des nombres premiers.

Théorème

Tout entier naturel n supérieur ou égal à 2 peut s'écrire sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

où k est un entier naturel non nul et $p_i \in \mathbb{P}$ pour $1 \leqslant i \leqslant k$.

Cette écriture est appelée la décomposition en produit de facteurs premiers de n et elle est unique.

Théorème

Petit théorème de Fermat : Si p est un nombre premier et si a est un entier non divisible par p alors $a^{p-1} \equiv 1 \mod p$.

Démonstration

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

Exemple : Prenons $a = 27$ et $p = 5$.
p est premier et a n'est pas divisible par p donc $27^4 \equiv 1 \mod 5$.

Remarque : La congruence de ce théorème est aussi présentée sous la forme suivante :

$$a^p \equiv a \mod p.$$