

cours de mathématiques en terminale

Arithmétique - spécialité.

I. Divisibilité :

Définition :

Soient a et b deux entiers relatifs non nuls.

On dit que b divise a ou que a est divisible par b ou bien encore que a est un multiple de b

$$\iff \exists k \in \mathbb{Z}, a = k \times b$$

on note alors b/a .

Exemple :

Donc 5 divise 15, 3 divise 15, 15 est un multiple de 5 et de 3.

II. Propriétés :

Propriétés :

Soient $(a;b) \in \mathbb{Z}^2$.

- $\forall a \in \mathbb{Z}^*, 0/a$.
- $a/b \implies |a| \leq |b|$.
- $a/b ; b/a \implies a = \pm b$
- $a/b ; b/c \implies a/c$.
- $a/b ; a/c \implies a/(b+c) ; a/(b-c) ; \forall (x,y) \in \mathbb{Z}^2, a/(bx+cy)$.
- $a/b \implies (a \times c)/(b \times c)$

III. Définition :

Définition :

Un entier $n \geq 2$ est dit premier s'il n'admet dans $\mathbb{N}$ aucun autre diviseur que lui-même et 1 .

Ensemble des nombres premiers

L'ensemble des nombres premiers, noté $\mathbb{P}$ est un ensemble infini.

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\} .$$

IV. Theoreme fondamental de l'arithmetique :

1. Décomposition en facteurs premiers :

Theoreme:

Soit $n \in \mathbb{N}$.

L'entier n se decompose de maniere unique, à l'ordre près, sous forme de produit de nombres premiers.

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_r^{a_r} = \prod_{k=1}^r p_k^{a_k} .$$

Exemple :

$$150 = 3 \times 25 \times 2 = 2 \times 3 \times 5^2$$

2. Division euclidienne :

Theoreme:

Soient a et b deux entiers relatifs tels que $b \neq 0$

alors :

Il existe un unique couple d'entiers (q, r) tel que :

$$a = bq + r, 0 \leq r < |b|$$

Remarque :

Que l'on soit dans $\mathbb{N}$ ou $\mathbb{Z}$, le reste r est toujours positif ou nul.

3. Congruences :

Definition :

On dit que deux entiers relatifs sont congrus modulo n s'ils ont le même reste dans la division euclidienne par n .

Si c'est le cas, on note $a \equiv b[n]$.

Exemple :

$18=5 \times 3 + 3$ et $27=8 \times 3 + 3$.

18 et 27 ont le même reste ($r=3$) lors de la division euclidienne par 3
donc

$$27 \equiv 18[3]$$

Propriétés :

$$\begin{aligned} & \bullet a \equiv b[n] \iff a - b \equiv 0[n] \\ & \iff \exists k \in \mathbb{N}, a - b = k \times n \quad \bullet a \equiv b[n]; a' \equiv b'[n] \iff aa' \equiv bb'[n] \\ & \iff a \times a' \equiv b \times b'[n] \\ & \iff a^p \equiv b^p[n] (p \in \mathbb{N}) \end{aligned}$$

4. Plus commun diviseur (pgcd) et plus petit commun multiple (ppcm) :

a. Definition du pgcd(a,b)

Definition :

Soient a et b deux entiers relatifs.

L'ensemble des diviseurs communs à a et b admet un plus grand élément nommé le $\text{pgcd}(a,b)$.

On note aussi $\mathbf{a \wedge b}$.

b. Propriétés du $\text{pgcd}(a,b)$

Propriétés :

Soit k un entier non nul.

Si k divise a et b alors :

$$\bullet \text{pgcd}\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{1}{k} \text{pgcd}(a,b)$$

$$\bullet \text{pgcd}(ka, kb) = k \times \text{pgcd}(a,b).$$

Remarque :

On peut déterminer le $\text{pgcd}(a,b)$ de trois manières :

- par décomposition des deux nombres ;
- par une succession de divisions euclidiennes, le dernier reste non nul étant le $\text{pgcd}(a,b)$ (théorème d'Euclide);
- par le théorème de Bezout (voir plus loin....)

c. Définition du $\text{ppcm}(a,b)$

Définition :

Soient a et b deux entiers relatifs.

L'ensemble des multiples communs à a et b admet un plus petit élément nommé le $\mathbf{\text{ppcm}(a,b)}$.

On note aussi : $\mathbf{a \vee b}$.

Propriété :

Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}$.

$$\boxed{\text{pgcd}(a,b) \times \text{ppcm}(a,b) = |ab|}.$$

V. Théorème de Bezout :

Proposition :

Soit $d = \text{pgcd}(a, b)$ alors il existe deux entiers relatifs u et v tels que :

$$\boxed{a \times u + b \times v = d}.$$

Propriete :

Deux nombres entiers a et b sont premiers entre eux si et seulement si $\text{pgcd}(a, b) = 1$.

Corollaire 1 :

$$\boxed{\text{pgcd}(a, b) = 1 \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1}.$$

Corollaire 2 :

$$\begin{aligned} \text{pgcd}(a, b) = d &\iff \begin{aligned} a &= a'd \\ b &= b'd \end{aligned} \\ &\quad \exists (u, v) \in \mathbb{Z}^2, a'u + b'v = 1. \end{aligned}$$

VI. Theoreme de Gauss:

Theoreme :

Si a divise bc et a premier avec b alors a divise c

Exemple :

5 divise $70 = 7 \times 10$

or 5 est premier avec 7

donc d'après le theoreme de Gauss 5 divise 10.