Arithmétique

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

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

on note alors b/a .

EXEMPLE :

$15 = 5 \times 3$

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

II. Propriétés.

Propriétés :

Soient $(a;b) \in \mathbb{Z}^{\not=}$.

- $\forall a \in \mathbb{Z}^*\,,\ 0/a.$
- $a/b \implies |a| \leq |b|.$
- $a/b\,;\ b/a \implies a =$

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.

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

IV. Théorème fondamental de l'arithmétique.

1. Décomposition en facteurs premiers.

Théorème:

Soit $n \in \mathbb{N}$.L'entier n se décompose de manière unique, à l'ordre près, sous forme de produit de nombres premiers.

$n =$.

2. Division euclidienne.

Théorème:

Soient a et b deux entiers relatifs tels que $b \neq 0$alors Il existe un unique couple d'entiers (q,r) tel que :

Invalid Equation

REMARQUE :

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

3. Congruences.

Définition :

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 Invalid Equation .

EXEMPLE :
18=5x3+3 et 27=8x3+3.

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

donc

Invalid Equation

Propriétés :

$$\bullet a \equiv b[n] \iff a - b \equiv 0[n] \iff \exists k \in \mathbb{N}\,,\ a - b = k \times\ n$$

$$\bullet a \equiv b[n]\ ;\ a' \equiv b'[n] \iff a + a' \equiv b + b'[n] \iff a \times\ a' \equiv b \times\ b'[n] \iff a^p \equiv b^p[n](p \in \mathbb{N})$$

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

a. Definition du pgcd(a,b)

Définition :

Soient a et b deux entiers relatifs.L'ensemble des diviseurs communs à a et b admet un plus grand élément nommé le pgcd(a,b).

On note aussi a^b.

b. Propriétés du pgcd(a,b)

Propriétés :

Soit k un entier non nul.

Si k divise a et b alors :

- $pagcd(\frac{a}{k}, \frac{b}{k}) = \frac{1}{k} pgcd(a,b)$
- $pgcd(ka, kb) = k \times pgcd(a,b).$

REMARQUE :

On peut déterminer le $pgcd(a,b)$ de trois manières :

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

c. Définition du 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 ppcm(a,b).

On note aussi : a v b .

Propriété :

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

Invalid Equation

V. Théorème de Bézout :

Proposition :

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

Invalid Equation

Propriété :

Deux nombres entiers a et b sont premiers entre eux si et seulement si pgcd(a,b)=1 .

Corollaire 1 :

Invalid Equation

Corollaire 2 :

$pgcd(a,b) = d \iff a = a'db =$

VI. Théorème de Gauss:

Théorème :

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 théorème de Gauss 5 divise 10.