

L'ARITHMETIQUE

A) Divisibilité dans \mathbb{Z} .

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

On dit que l'entier relatif b divise a s'il existe un entier relatif k tel que $a = kb$

On écrit : $b|a$. et on dit que a est divisible par b ou a est un multiple de b

b) Si $b|m$ et $b|n$ on dit que b est un diviseur commun de m et n

c) Si $b|m$ et $b'|m$, on dit que m est un multiple commun de b et b'

B) Propriétés de Divisibilité dans \mathbb{Z} .

$a \in \mathbb{Z}$; $b \in \mathbb{Z}$; $c \in \mathbb{Z}$

$$1) |a| \text{ et } -1|a \text{ et } a|a \text{ et } a|-a \quad 2) b|a \Rightarrow |b| \leq |a|$$

$$3) a/b \Rightarrow a/b \times c \quad 4) a/b \Rightarrow |a| \leq |b|$$

$$5) b|1 \Rightarrow b \in \{-1, 1\} \quad 6) a|b \text{ et } b|a \Rightarrow |a| = |b|$$

$$7) a|b \text{ et } c|d \Rightarrow ac|bd \quad 8) a|b \text{ et } b|c \Rightarrow a|c$$

$$9) a|b \Rightarrow a|b \times c \quad 10) a|b \text{ et } b|c \Rightarrow a|c$$

$$11) a|b \Rightarrow a|b \times c \quad 12) a|m \text{ et } a|n \Rightarrow a|m+n$$

$$13) a|m \text{ et } a|n \Rightarrow a|m-n$$

14) $a|m$ et $a|n \Rightarrow a|\alpha m + \beta n$ où α et β sont des entiers relatifs quelconques.

$$15) a/b \Rightarrow a^n/b^n \quad n \in \mathbb{N}$$

C) La division euclidienne dans \mathbb{Z}

a et b deux entiers relatifs tels que $b \neq 0$; ils existent un entier relatif q et un entier naturel r tels que : $a = bq + r$ où $0 \leq r < |b|$

- L'entier a s'appelle : **Le divisé**
- L'entier b s'appelle : **Le diviseur**
- L'entier q s'appelle : **Le quotient**
- L'entier r s'appelle : **Le reste**

Remarque : Si r est le reste de la division euclidienne par b alors : $r \in \{0, 1, \dots, b-1\}$.

D) Les nombres premiers

a) On dit que l'entier d est un diviseur **effectif** de l'entier relatif a si $d|a$ et $|d| \neq 1$ et $|d| \neq |a|$

b) On dit qu'un entier relatif non nul p est **premier** s'il est différent de 1 et s'il n'admet pas de diviseurs effectifs.

• Un nombre premier p admet exactement deux diviseurs positifs 1 et $|p|$.

• Pour l'étude des nombres premiers on se contente d'étudier les nombres premiers positifs.

c) si a un entier naturel non nul différent de 1 et non premier, le plus petit diviseur de a différent de 1 est un nombre premier

d) Soit n un entier naturel non nul, différent de 1 et non premier, il existe un nombre premier p qui divise l'entier n et qui vérifie $p^2 \leq n$.

e) Si un entier n n'est divisible par aucun entier premier p et qui vérifie $p^2 \leq n$ alors n est premier.

Remarque : Cette propriété nous permet de déterminer si un nombre est premier ou non

Théorème : L'ensemble des nombres premiers est infini.

E) Plus grand diviseurs commun

1) On dit que le nombre d est le plus grand diviseur commun de deux entiers relatifs a et b lorsque d divise a et d divise b et qu'il n'y a pas d'autre plus grands diviseurs de ces deux nombres. on note $d = PGDC(a, b) = a \wedge b$

$$\text{Propriétés : } 1) a \wedge a = |a| \quad 2) 1 \wedge a = 1$$

$$3) (a \wedge b) \wedge c = a \wedge (b \wedge c) \quad 4) \text{Si } b|a \text{ alors } a \wedge b = |b|$$

$$5) \text{si } d|a \text{ et } d|b \text{ alors } d|(a \wedge b) \quad 6) a \wedge b = a \wedge (a-b)$$

$$7) a \wedge b = |a| \wedge |b|$$

Définition : On dit que deux entiers relatifs a et b sont premiers entre eux si $a \wedge b = 1$.

F) L'algorithme d'Euclide.

1) Soit a un entier naturel et b un entier naturel non nul on a : $a = bq + r$ Où $0 \leq r < b$ alors on a : $a \wedge b = b \wedge r$

2) Soient a et b deux entiers naturels non nuls. Le plus grand diviseur commun de a et b est le dernier reste non nul dans les divisions euclidiennes successives.

3) Soient a et b deux entiers relatifs non nuls. Les diviseurs communs de a et b sont les diviseurs de $a \wedge b$.

On peut dire que : $D_a \cap D_b = D_{a \wedge b}$

G) Le plus petit multiple commun.

On dit que le nombre entier naturel m est le plus petit multiple commun de deux entiers relatifs a et b lorsque m est un multiple de a et de b et qu'il n'y a pas d'autre plus petit multiple non nuls de ces deux nombres. On note : $m = PPCM(a, b) = a \vee b$

$$\text{Propriétés : } 1) a \vee a = |a| \quad 2) a \vee b = b \vee a$$

$$3) a \vee 1 = |a| \quad 4) \text{Si } b|a \text{ alors } a \vee b = |a|$$

$$5) a \vee (b \vee c) = (a \vee b) \vee c \quad 6) a \vee b = |a| \vee |b|$$

$$7) a|(a \vee b); b|(a \vee b) \text{ et } (a \vee b)|ab$$

8) Si $a \vee b = m$ et M un multiple commun de a et b alors $m|M$.

$$9) (a \wedge b) \times (a \vee b) = |ab| \quad 10) ca \vee cb = c(a \vee b)$$

$$11) ca \wedge cb = c(a \wedge b)$$

12) Soient a et b et des entiers relatifs non nuls :

$$a \wedge b = d \Leftrightarrow \exists (\alpha, \beta) \in \mathbb{Z}^2; \begin{cases} a = \alpha d \\ b = \beta d \\ \alpha \vee \beta = 1 \end{cases}$$

H) LA CONGRUENCE MODULO n

a et b deux entiers relatifs ; et n un entier naturel non nul. On dit que : a est congrue à b modulo n si $n|(b-a)$.

On écrit : $a \equiv b \pmod{n}$

1) Si $a \equiv b \pmod{n}$ alors a et b ont le même reste dans la division euclidienne par n

2) a) $(\forall a \in \mathbb{Z}) (a \equiv a \pmod{n})$ on dit que la relation de congruence est réflexive.

b) $(\forall (a, b) \in \mathbb{Z}^2) (a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n})$: on dit que la relation de congruence est symétrique.

c) $(\forall(a, b, c) \in \mathbb{Z}^3)$

$(a \equiv b [n] \text{ et } b \equiv c [n] \Rightarrow a \equiv c [n])$: on dit que la relation de congruence est transitive.

On dit que la relation de congruence est une relation d'équivalence

3) Soit n un entier naturel non nul.

Si $a \equiv b [n]$ et $c \equiv d [n]$ alors :

a) $a + c \equiv b + d [n]$ On dit que la relation de congruence est compatible avec l'addition dans \mathbb{Z}

b) $ac \equiv bd [n]$; On dit que la relation de congruence est compatible avec la multiplication dans \mathbb{Z}

4) Si $a \equiv b [n]$ alors pour tout k dans \mathbb{N} on a : $a^k \equiv b^k [n]$

I) Les classes d'équivalences.

Soit n un entier naturel non nul. L'ensemble des entiers relatifs qui ont le même reste r dans la division euclidienne par n s'appelle la classe d'équivalence de r et se note :

$$r = \{m \in \mathbb{Z} / m \equiv r [n]\} = \{nk + r \text{ où } k \in \mathbb{Z}\}$$

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \dots; \bar{n-1}\}$ S'appelle ensemble quotient

1) On définit dans $\mathbb{Z}/n\mathbb{Z}$ les deux lois :

a) L'addition : On pose $\bar{a} + \bar{b} = \overline{a+b}$

b) La multiplication : On pose : $\bar{a} \times \bar{b} = \overline{a \times b}$

3) Si p est premier alors

dans $\mathbb{Z}/p\mathbb{Z}$ on a : $(\bar{a} \times \bar{b}) = \bar{0} \Leftrightarrow \bar{a} = \bar{0} \text{ ou } \bar{b} = \bar{0}$

J) DECOMPOSITION D'UN ENTIER EN FACTEURS DES NOMBRES PREMIERS

1) Chaque entier **relatif** m non nul s'écrit d'une façon unique comme le produit des facteurs premiers comme

suite : $m = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$ où $\varepsilon \in \{-1, 1\}$

2) Soit a un entier relatif dont la décomposition est de la

forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

3) un entier d non nul divise l'entier a si et seulement si d à une décomposition de la forme

$d = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$

où $(\forall i \in \llbracket 1, n \rrbracket)(0 \leq \beta_i \leq \alpha_i)$

4) $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

est un entier, le nombre des diviseurs de a

est : $2(\alpha_1+1)(\alpha_2+1)\dots(\alpha_n+1)$

5) Soit a un entier relatif dont la décomposition est de la

forme : $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n} = \prod_{k=1}^{k=n} p_k^{\alpha_k}$

un entier m est un multiple de a si et seulement si

$m = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times p_3^{\beta_3} \times \dots \times p_n^{\beta_n} = \prod_{k=1}^{k=n} p_k^{\beta_k}$

6) Soient $a = \prod_{k=1}^{k=n} p_k^{\alpha_k} = 1$ et $b = \prod_{k=1}^{k=n} p_k^{\beta_k}$ deux entiers

$$a \wedge b = \prod_{k=1}^{k=n} p_k^{\inf(\alpha_k, \beta_k)} \text{ et } a \vee b = \prod_{k=1}^{k=n} p_k^{\sup(\alpha_k, \beta_k)}$$

K) Le P.G.D.C et le P.P.M.C de plusieurs nombres.

1) Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls, le plus grand entier naturel d qui divise en même temps tous les nombres a_1, a_2, \dots, a_n s'appelle le plus grand diviseur commun des nombres a_1, a_2, \dots, a_n et se note : $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$

2) Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls ; on a : $a_1 \wedge a_2 \wedge \dots \wedge a_n = (a_1 \wedge a_2 \wedge \dots \wedge a_{n-2}) \wedge (a_{n-1} \wedge a_n)$

3) On dit que les entiers relatifs non nuls : a_1, a_2, \dots, a_n sont premiers entre eux si : $a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$

5) Soient a_1, a_2, \dots, a_n des entiers relatifs non nuls, le plus petit entier naturel m qui est multiple en même temps tous les nombres a_1, a_2, \dots, a_n s'appelle le plus petit multiple commun des nombres a_1, a_2, \dots, a_n et se note : $m = a_1 \vee a_2 \vee \dots \vee a_n$

L) CRITERES DE DIVISIBILITE DES NOMBRES

5,25,3,9,11 ET 4 : Soit x un entier naturel non nul tel que :

$x \equiv a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10^1 + a_0$ où $0 \leq a_i \leq 9$; on a :

1) $x \equiv 0 [5] \Leftrightarrow a_0 = 0$ ou $a_0 = 5$

2) $x \equiv 0 [25] \Leftrightarrow \overline{a_1 a_0} \in \{0, 25, 50, 75\}$

3) $x \equiv 0 [3] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [3]$

4) $x \equiv 0 [9] \Leftrightarrow \sum_{i=0}^n a_i \equiv 0 [9]$

5) $x \equiv 0 [11] \Leftrightarrow \sum_{i=0}^n (-1)^i a_i \equiv 0 [11]$

6) $x \equiv 0 [4] \Leftrightarrow \overline{a_1 a_0} \equiv 0 [4]$

« C'est en forgeant que l'on devient forgeron » Dit un proverbe.

C'est en s'entraînant régulièrement aux calculs et

exercices

Que l'on devient un mathématicien

