Chapitre 10 : Arithmétique

Introduction :

L'arithmétique est l'art et la manière de manipuler les quantités entières. Cette branche des mathématiques est riche en applications dans notre société, cette science des nombres entiers est très utilisée en informatique et particulièrement dans le domaine de la cryptographie.

I Définitions et premières notations :

1 Ensembles de nombres entiers :

Définition 1.

Pour comparer deux ensembles et introduire les notions d'inclusion, d'égalité et de différence entre ensembles, nous utilisons les symboles suivants :

$$(\subset,\ \subseteq,\ \supset,\ \supseteq,\ =,\ \neq)$$

Exemple 1.

☐ $\{1,\ 2\}$ ..... $\{1,\ 2,\ 3\}$ ☐ $\{1,\ 3,\ 2\}$ ..... $\{1,\ 2,\ 3\}$ ☐ $\{0,\ 2\}$ ..... $\{1,\ 2,\ 3\}$

☐ $\{4,\ 5,\ 6\}$ ..... $\{4,\ 6\}$ ☐ $\{4,\ 5,\ 6\}$ ..... $\{1,\ 2,\ 3\}$ ☐ $\{4,\ 5,\ 6\}$ ..... $\{5\}$

Remarque 1.

Nous noterons $\mathbb{N}^*$ l'ensemble des entiers naturels privé de l'élément 0, ce sont tous les entiers strictement positifs.

Propriété 1.

Nous avons les relations d'inclusions suivantes : $\mathbb{N}^* \subset \mathbb{N} \subset \mathbb{Z}$

Remarque 2.

En mathématiques nous utilisons souvent des lettres de l'alphabet grec ancien.

lettre majuscule	*lettre minuscule*	*nom*
A	α	*alpha*
B	β	*bêta*
Γ	γ	*gamma*
Δ	δ	*delta*
E	ε	*epsilon*
Z	ζ	*zêta*
H	η	*êta*
Θ	θ	*thêta*
I	ι	*iota*
K	κ	*kappa*
Λ	λ	*lambda*
M	μ	*mu*

lettre majuscule	*lettre minuscule*	*nom*
N	ν	*nu*
Ξ	ξ	*ksi ou xi*
O	o	*omicron*
Π	π	*pi*
P	ρ	*rhô*
Σ	σ	*sigma*
T	τ	*tau*
Υ	υ	*upsilon*
Φ	ϕ *ou* φ	*phi*
X	χ	*khi*
Ψ	ψ	*psi*
Ω	ω	*omega*

2 Multiples, diviseurs et critères de divisibilité :

a Multiples et diviseurs :

Définition 2.

Soit $a, b \in \mathbb{Z}$, on dit que a est ..... de b s'il existe un entier $k \in \mathbb{Z}$ tel que : a = ...

Exemple 2.

- ☐ 12 *est un multiple de* 6 *car il existe le nombre* 2 *tel que :* $12 = \ldots\ldots\ldots\ldots$
- ☐ 54 *est un multiple de* 3 *car il existe le nombre* 18 *tel que :* $54 = \ldots\ldots\ldots\ldots$
- ☐ 0 *est un multiple de n'importe quel nombre* $a \in \mathbb{Z}$, *car :* $0 = \ldots\ldots\ldots\ldots$
- ☐ 1 *n'est un multiple que de ..... et de .....*

Définition 3.

Soit $a, b \in \mathbb{Z}$, on dit que b est ..... de a s'il existe un entier $k \in \mathbb{Z}$ tel que : a = ...

Exemple 3.

- ☐ *Les diviseurs de* 12 *sont :* $D_{12} = \left\{ \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots \right\}$
- ☐ *Les diviseurs de* 45 *sont :* $D_{45} = \left\{ \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots, \ldots\ldots\ldots \right\}$
- ☐ 1 *divise tous les nombres car pour tout* $a \in \mathbb{Z}$ *on a :* $\ldots\ldots\ldots = \ldots\ldots\ldots \times \ldots\ldots\ldots$
- ☐ 0 *ne divise personne autre que lui-même.*

Exemple 4. *Contre-exemples et indications :*

- ☐ 3 *ne divise pas* 5 *car il n'existe pas un entier* k *tel que* 5 *soit égale à :* $3 \times k$
- ☐ 32 *n'est pas un multiple de* 11 *car il n'existe pas un entier* k *tel que* 32 *soit égale à :* $11 \times k$
- ☐ *Ne pas avoir peur de nombres négatifs.* 2 *divise* 6 *car* $6 = 2 \times 3$ *mais* -2 *est aussi un diviseur de* 6 *car* $6 = -2 \times -3$

Propriété 2. *Soit $a, b \in \mathbb{Z}$, si b divise a alors $-b$ divise aussi a*

Démonstration.

.....

☐

Propriété 3. *Soit $a, b \in \mathbb{Z}$ deux multiples de $c \in \mathbb{Z}$. Alors $(a+b)$, $(a-b)$ et $(b-a)$ sont des multiples de c*

Démonstration.

.....

.....

.....

.....

☐

b Parité des entiers relatifs :

Définition 4.

☐ *Un entier $n \in \mathbb{Z}$ est ..... si 2 est un diviseur de n. $\leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que : $n = 2k$*

☐ *Un entier $n \in \mathbb{Z}$ est ..... si 2 n'est pas un diviseur de n. $\leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que : $n = 2k + 1$*

Remarque 3.

☐ *Un nombre est pair si la division euclidienne de celui-ci par 2 a un reste égale à 0.*

☐ *Un nombre est impair si la division euclidienne de celui-ci par 2 a un reste égale à 1.*

Propriété 4. *Soit $n, m \in \mathbb{Z}$ on a :*

1. ▷ $n^2 = n \times n$ *est pair si et seulement si n est pair.*
   ▷ $n^2 = n \times n$ *est impair si et seulement si n est impair.*

2. ▷ $nm = n \times m$ *est pair si et seulement si n est pair ou si m est pair.*
   ▷ $nm = n \times m$ *est impair si et seulement si n et m sont tous les deux impairs.*

3. ▷ $n^3 = n \times n \times n$ *est pair si et seulement si n est pair*
   ▷ $n^3 = n \times n \times n$ *est impair si et seulement si n est impair.*

Démonstration.

1. ▷ $n \times n$ est pair si n est pair car si n est un multiple de 2 alors $n \times n = n^2$ est aussi un multiple de 2

   ▷ $n \times n$ est impair si n est impair car si n est impair on a :

   $n^2 =$ .....

   .....

2. ▷ $n \times m$ est pair si n est pair ou si m est pair ou encore si ils sont tous les deux pairs.

   ▷ $n \times m$ est impair si n et m sont tous les deux impairs car :

   $n \times m =$ .....

   .....

   .....

3. ▷ $n \times n \times n$ est pair si n est pair

   ▷ $n \times n \times n$ est impair si n est impair car on a :

   $n^3 =$ .....

   .....

   .....

   .....

□

3 Nombres premiers :

Définition 5.
Un nombre entier naturel est dit ..... s'il admet deux uniques diviseurs positifs distincts qui sont 1 et lui-même.

Exemple 5. *Les nombres suivants sont premiers :*

$$\{2; 3; 5; 7; 11; 13; 17; 19; 23; 29\}$$

Remarque 4.

- ☐ *Le nombre 0 n'est pas premier car il a une infinité de diviseur.*
- ☐ *Le nombre 1 n'admet qu'un seul diviseur positif qui est lui-même. Il n'en a pas deux distinct, 1 n'est donc pas premier.*

Exemple 6. *Les nombres suivants ne sont pas premiers :*

$$\{0; 1; 4; 9; 15; 32; 49; 121\}$$

Exercice 1. *Donner la liste et apprendre les vingt premiers nombres premiers.*

Théorème 1. *(**Théorème fondamental de l'arithmétique**)*
Tout nombre entier supérieure ou égal à deux admet une unique décomposition en produit de facteurs premiers à l'ordre près.

Exemple 7.

☐ $15 =$ ☐ $1617 =$ ☐ $100 =$

Remarque 5. *Tout nombre entier supérieure ou égal à deux admet toujours un diviseur premiers.*

Définition 6.
Un nombre entier supérieure à deux qui n'est pas premier est appelé un nombre .....

Propriété 5. *Soit n un nombre composé alors sont plus petit diviseur premier est inférieur ou égale à $\sqrt{n}$.*

Démonstration.

.....

.....

.....

☐

Propriété 6.

1. *Il existe une infinité de nombres qui ne sont pas premiers*
2. *Il existe une infinité de nombres qui sont premiers*

Démonstration.

.....

.....

.....

.....

.....

.....

☐