Chapitre 1: Divisibilité et nombres premiers

1 Divisibilité dans $\mathbb{Z}$

Définition:
Soient a et b deux entiers relatifs. On dit que b divise a lorsqu'il existe k entier relatif, c'est à dire $k \in \mathbb{Z}$ tel que :

$$a = kb$$

*On dit aussi que b est un **diviseur** de a ou que a est un **multiple** de b.*

Exemple:
$18 = 2 \times 9$ *donc* 9 *divise* 18, *ce qui s'écrit* $9 \mid 18$.

Propriété:
Soient a et b deux entiers. On a les équivalences suivantes :

$$a \mid b \Longleftrightarrow a \mid (-b) \Longleftrightarrow (-a) \mid b \Longleftrightarrow (-a) \mid (-b)$$

Démonstration:
a divise b donc il existe $k \in \mathbb{Z}$ tel que $b = ka$ d'où $b = (-k)(-a)$; $(-b) = (-k)a$ et $(-b) = k(-a)$.

Exemple:
9 *divise* 18, -9 *divise* 18, 9 *divise* -18 *et* -9 *divise* -18.

Remarque:
Un entier naturel non-nul n a au plus n diviseurs dans $\mathbb{N}$ et au plus $2n$ diviseurs dans $\mathbb{Z}$.
De plus 1 et n divise n donc tout entier n distinct de 1 admet au moins deux diviseurs distincts.

Exemple:
L'ensemble des diviseurs de 18 dans $\mathbb{Z}$ est $D(18) = \{-18; -9; -6; -3; -2; -1; 1; 2; 3; 6; 9; 18\}$.

Propriété:
Pour tous entiers relatifs a, b et c :

- *si a divise b et b divise c alors a divise c.*
- *si a divise b et a divise c alors a divise les entiers de la forme $mb + nc$ avec m et n entiers.*

2 Division euclidienne dans $\mathbb{N}$

Théorème:
Soient a et b deux entiers naturels, b étant non-nul.
Il existe un unique couple d'entiers $(q; r)$ tel que :

$$a = bq + r \quad \texttt{et} \quad 0 \leq r < b$$

L'entier q est égal à la partie entière de $\dfrac{a}{b}$, c'est à dire à l'unique entier tel que $q \leq \dfrac{a}{b} < q + 1$.

Définition:
L'entier q est appelé quotient de la division euclidienne de a par b et l'entier r est appelé reste de la division euclidienne de a par b.

Propriété:
Soient a et b deux entiers naturels, b étant non-nul.
*b **divise** a si et seulement si le reste de la division euclidienne de a par b est nul.*

3 Nombres premiers

Définition:
Un nombre est dit premier s'il admet ***exactement*** *deux diviseurs.*

Remarque:
- 1 *n'admet qu'un diviseur donc il n'est pas premier ;*
- 2, 3, 5 *et* 7 *sont les nombres premiers inférieurs à* 10 *;*
- *tout nombre non-premier distinct de* 1 *est dit composé.*

Propriété:
Il existe une infinité de nombres premiers.

Propriété:
Soit $n \geq 2$ *un entier naturel. Si aucun des entiers premiers compris entre* 2 *et* $\sqrt{n}$ *ne divise* n *alors* n *est premier.*

Exemple:
Soit $n = 211$. *On a :* $\sqrt{211} \simeq 14,5$.
211 *est premier puisqu'il n'est pas divisible par* 2, 3, 5, 7, 11 *et* 13

4 Décomposition en produit de facteurs premiers

Théorème:
Soit $n \geq 2$ *un entier naturel.* n *est premier ou produit de nombres premiers.*

Démonstration:
Supposons que cette propriété n'est pas vraie pour tous les entiers et notons n *le premier entier qui n'est ni premier, ni produit de nombres premiers. Comme* n *n'est pas premier, il admet un diviseur premier* p *et il existe* d *tel que* $n = pd$ *où* $1 < d < n$. d *satisfait alors la propriété et* $n = pd$ *la satisfait alors aussi. Ceci contredit l'hypothèse initiale.*

Théorème:
La décomposition de n *en produit de nombres premiers est unique.*

Exemple:
La décomposition en produit de nombres premiers de 1092 *est* $1092 = 2^2 \times 3 \times 7 \times 13$.

Propriété:
Un entier naturel d *divise un entier naturel* n *si et seulement si les exposants des facteurs premiers de la décomposition de* d *sont au plus égaux à ceux de la décomposition de* n

Exemple:
Les six diviseurs de $45 = 3^2 \times 5$ *sont :*

$$1 = 3^0 \times 5^0 \text{ ; } 3 = 3^1 \times 5^0 \text{ ; } 9 = 3^2 \times 5^0 \text{ ; } 5 = 3^0 \times 5^1 \text{ ; } 15 = 3^1 \times 5^1 \text{ et } 45 = 3^2 \times 5^1$$