

Thème 1: Divisibilité et nombres premiers

1 Divisibilité dans $\mathbb{Z}$

Définition:

Soient a et b deux entiers. 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 :

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

Démonstration:

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

Propriété:

Sont n un entier naturel non-nul, c'est à dire $n \in \mathbb{N}^*$.

Tout diviseur positif d de n est compris entre 1 et n et ainsi tout entier naturel non-nul a a un nombre fini de diviseurs.

Démonstration:

$n \in \mathbb{N}^*$ et soit $d \in \mathbb{N}$ un diviseur de n alors il existe $k \in \mathbb{N}$ tel que $n = kd$. Comme $n > 0$ et $d > 0$ on a $k > 0$ soit $k \geq 1$ d'où $kd \geq d$ c'est à dire $n \geq d$.

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 $\mathbb{N}$ est $D(18) = \{1; 2; 3; 6; 9; 18\}$.

Propriété:

Pour tous entiers 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.

Démonstration:

En exercice.

Exemple:

Si a divise 3 et 11 alors a divise $7 \times 3 - 2 \times 11 = 1$ donc $a = 1$ ou $a = -1$!

2 Division euclidienne

Théorème:

Soient a et b deux entiers naturels, b étant non-nul.

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

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

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

Démonstration:

Soit $(q; r)$ un couple satisfaisant les deux conditions alors $qb \leq qb + r < qb + b$ soit $qb \leq a < (q + 1)b$ donc $q = E\left(\frac{a}{b}\right)$ et l'unicité du couple est prouvée.

Inversement, soit $q = E\left(\frac{a}{b}\right)$. On pose $r = a - qb$. On a $qb \leq a < (q + 1)b$ soit $qb \leq qb + r < qb + b$ donc $0 \leq r < b$ et l'existence du couple vérifiant les deux conditions est prouvée.

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:

Soit $n \geq 2$ un entier naturel. Le plus petit diviseur de n compris entre 2 et n est premier.

Démonstration:

Soit $n \geq 2$ un entier naturel. Supposons que p , le plus petit diviseur de n , n'est pas premier. Il existe alors d et q tel que $p = dq$ et $1 < d < p$. De plus, d divise p donc divise n ce qui contredit la définition de p . On en déduit par l'absurde que p est premier.

Propriété:

Tout entier naturel composé n admet un diviseur premier au plus égal à $\sqrt{n}$.

Démonstration:

Soit n un entier naturel composé. Le plus petit diviseur d de n compris entre 2 et n est premier et $n = dd'$ avec $2 \leq d \leq d' \leq n$ donc $dd \leq dd'$ soit $d \leq \sqrt{n}$.

Propriété:

Il existe une infinité de nombres premiers.

Démonstration:

Supposons qu'il existe un nombre fini de nombres premiers et notons p le plus grand d'entre-eux. Alors le produit de tous ces nombres premiers auxquels on ajoute 1, c'est à dire $2 \times 3 \times 5 \times \dots \times p + 1$, n'est divisible par aucun des nombres premiers donc il est lui aussi premier. Ceci contredit l'hypothèse de finitude initiale.

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.

Démonstration:

Ceci est la contraposée de « Si n est un entier naturel composé alors n admet un diviseur premier au plus égal à $\sqrt{n}$ » est « Si aucun des entiers premiers compris entre 2 et $\sqrt{n}$ ne divise n alors n est un nombre 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 .

Démonstration:

$\Rightarrow$ Si d divise n , soit p un facteur premier de d apparaissant à la puissance α . p^α divise d donc p^α divise n .

$\Leftarrow$ Si $d = p_1^{a_1} \times \dots \times p_r^{a_r}$ et $n = p_1^{b_1} \times \dots \times p_r^{b_r}$ avec $0 \leq a_i \leq b_i$ pour $1 \leq i \leq r$ alors $n = d \times p_1^{b_1-a_1} \times \dots \times p_r^{b_r-a_r}$ où $p_1^{b_1-a_1} \times \dots \times p_r^{b_r-a_r}$ est entier puisque $0 \leq b_i - a_i$ pour $1 \leq i \leq r$ donc d divise n .

Exemple:

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

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

5 Congruence dans $\mathbb{Z}$

Définition:

Soit m un entier naturel. Deux entiers a et b sont dits congrus modulo m lorsque $a - b$ est multiple de m . On écrit alors :

$$a \equiv b(m)$$

Exemple:

$27 \equiv 2(5)$ puisque $27 - 2 = 5 \times 5$.

Théorème:

Soit m un entier naturel. Deux entiers a et b sont congrus modulo m si et seulement si la division euclidienne de a par m a le même reste que la division euclidienne de b par m .

Démonstration:

En exercice.

Propriété:

Soit $m \geq 2$ un entier naturel et a, b et c des entiers alors :

(1) $a \equiv a(m)$;

(2) Si $a \equiv b(m)$ et $b \equiv c(m)$ alors $a \equiv c(m)$.

Démonstration:

En exercice.

Propriété:

Soit $m \geq 2$ un entier naturel et a, b, a', b' des entiers alors :

(1) Si $a \equiv b(m)$ et $a' \equiv b'(m)$ alors $a + a' \equiv b + b'(m)$

(2) Si $a \equiv b(m)$ et $a' \equiv b'(m)$ alors $aa' \equiv bb'(m)$

(3) Pour $n \in \mathbb{N}^*$, si $a \equiv b(m)$ alors $a^n \equiv b^n(m)$

Démonstration:

En exercice.