Divisibilité et congruence

1 Divisibilité dans $\mathbb{Z}$

Définition

Soient a et b deux entiers relatifs.
On dit que b **divise** a s'il existe un entier relatif k tel que $a = k \times b$.
On note alors $b|a$.

Remarques

On dit aussi que b est un diviseur de a, ou que a est divisible par b ou encore que a est un multiple de b.

Exemples

Les diviseurs de 45 dans $\mathbb{Z}$ sont -45 ; -1 ; 45 ; 1 ; 15 ; 3 ; -15 ; -3 ; 9 ; 5 ; -9 et -5.
On peut donc dire que 45 est un multiple de -3.
On peut aussi dire que -5 divise 45 ou que 45 est divisible par -5.

L'ensemble des multiples de 5 est $\{... ; -20 ; -15 ; -10 ; -5 ; 0 ; 5 ; 10 ; ...\}$. Cet ensemble est aussi noté $5\mathbb{Z}$.

Propriétés

- 0 est un multiple de tout nombre entier. On peut aussi dire que 0 est divisible par n'importe quel nombre entier.
- 1 divise tout nombre entier.
- Deux entiers relatifs opposés ont les mêmes diviseurs.

Propriété : transitivité

Soient a, b et c trois entiers relatifs.
Si a divise b et que b divise c alors a divise aussi c.

Démonstration

Puisque a divise b, il existe un entier relatif k tel que $b = ka$.
Puisque b divise c, il existe un entier relatif k' tel que $c = k'b$.
Avec ces deux égalités, on peut écrire $c = k'b = k'ka$. Or kk' est un entier relatif, que l'on peut noter λ. On a donc trouvé un entier relatif tel que $c = \lambda a$. Ainsi, a divise c.

Propriété : combinaison linéaire

Soient a, b et c trois entiers relatif.
Si a divise b et si a divise c, alors a divise toute combinaison linéaire de b et c.
On peut ainsi noter :

$$a|b \text{ et } a|c \Rightarrow \forall (u\,;\,v) \in \mathbb{Z}^2,\ a|ub+vc.$$

Démonstration

Puisque a divise b et c, il existe deux relatifs k et k' tels que : $b = ka$ et $c = k'a$.
Ainsi, $ub + vc = u(ka) + v(k'a) = a(uk + vk')$. Or le nombre $uk + vk'$ est un entier relatif. On a donc trouvé un entier relatif $\lambda = uk + vk'$ tel que $ub + vc = \lambda a$.
Cela signifie que a divise $ub + vc$.

2 Division euclidienne dans $\mathbb{Z}$

Théorème

Pour tout entier naturel a et pour tout entier naturel b non nul, il existe un unique couple d'entiers naturels $(q\,;\,r)$ tels que

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

Définitions

Dans le précédent théorème, q est appelé le **quotient** de la **division euclidienne** de a par b et r et son **reste**.

Démonstration

Montrons d'abord l'existence.

Supposons que $b \leqslant a$. Notons E l'ensemble des multiples de b strictement supérieurs à a. E est non vide puisque $2b \times a$ appartient à E.
Or, toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
E possède donc un plus petit élément, c'est à dire un multiple de b strictement supérieur à a tel que le multiple précédent soit inférieur ou égal à a.

Il existe donc un entier q tel que $qb \leqslant a < (q+1)b$.
Puisque $b \leqslant a$, on a $b \leqslant a < (q+1)b$. Puisque $b > 0$, on a également $0 < (q+1)b$ ce qui implique $0 < q$.
On peut alors poser $r = a - bq$. Puisque a, b et q sont des entiers, r l'est également.
Puisque $qb \leqslant a$, on a $r \geqslant 0$ donc r est un entier naturel.
Enfin, puisque $a < (q+1)b$ on en déduit que $r < b$.

Démonstration : suite et fin

Montrons maintenant l'unicité.

Supposons que $a = bq_1 + r_1$ et que $a = bq_2 + r_2$ avec $0 \leqslant r_1 < b$ et $0 \leqslant r_2 < b$.
On a donc $-b < r_1 - r_2 < b$ et $r_1 - r_2 = b(q_2 - q_1)$.
Cela implique que $r_1 - r_2$ est un multiple de b strictement compris entre $-b$ et b.
Cela implique donc que $r_1 - r_2 = 0$, autrement dit que $r_1 = r_2$.
Puisque $b \neq 0$, $q_1 = q_2$ montant ainsi l'unicité du couple $(q\,;\,r)$.

Théorème

On peut étendre ces résultat à $\mathbb{Z}$:
Pour tout entier relatif a et pour tout entier entier naturel b non nul, il existe un unique couple $(q\,;\,r)$ d'entiers relatifs tels que :

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

Exemples

- Effectuons la division euclidienne de 534 par 5.

$$\begin{array}{r|l} 534 & 5 \\ \hline -5 & 106 \\ \hline 03 & \\ -0 & \\ \hline 34 & \\ -30 & \\ \hline 4 & \end{array}$$

  On peut donc écrire que $534 = 5 \times 106 + 4$.

- La division euclidienne de 114 par 8 donnera $114 = 8 \times 14 + 2$.
  On a également $-114 = -8 \times 14 - 2$ Mais -2 ne peut pas être un reste de division euclidienne car non positif.
  Mais $-114 = 8 \times (-14) - 8 + 6 = 8 \times (-15) + 6$.

3 Congruences dans $\mathbb{Z}$

Définition

Soit n un entier naturel non nul. Soient a et b deux entiers relatifs.
On dit que a **est congru à** b **modulo** n si a et b ont le même reste dans la division euclidienne par n.
On note alors $a \equiv b\ (n)$.

On dit aussi que a et b sont **congrus modulo** n.

Propriétés

Soit n un entier naturel non nul.

- Si $a \equiv b\ (n)$ alors $a - b$ est divisible par n.
- Si $a \equiv 0\ (n)$ alors a est divisible par n.
- Si $a \equiv b\ (n)$ et si $b \equiv c\ (n)$ alors $a \equiv c\ (n)$. (transitivité)
- Si $a \equiv b\ (n)$ alors $b \equiv a\ (n)$.

Démonstration

- Si $a \equiv b\ (n)$ alors a et b ont le même reste dans la division euclidienne par n. On peut donc utiliser la définition de la division euclidienne et écrire que $a = nq + r$ et $b = nq' + r$ avec $0 \leqslant r < n$.
  On obtient ainsi $a - b = n(q - q')$ avec $q - q'$ un entier donc n divise $a - b$.

  Réciproquement, si $n|a - b$ alors il existe un entier k tel que $a - b = kn$ ou encore $a = b + kn$.
  Notons r le reste de la division euclidienne de b par n :
  $b = nq + r$ avec $0 \leqslant r < n$ donc $a = nq + r + kn = n(q + k) + r$.
  Cette dernière égalité veut dire que r est le reste de la division euclidienne de a par n.
  Puisque a et b ont le même reste dans la division euclidienne par n, ils sont congrus modulo n.

- Il s'agit d'un cas particulier de ce que l'on vient de montrer en posant $b = 0$.

- D'après le premier point, n divise $a - b$ et n divise $b - c$ donc il divise leur somme $a - c$ et donc $a \equiv c\ (n)$.

- Immédiat

Exemples

- $31 \equiv 10\ (7)$.
  En effet, $31 - 10 = 21$ qui est divisible par 7.

- $8 \equiv -7\ (3)$
  En effet, $8 - (-7) = 15$ qui est un multiple de 3.

Propriétés

Soient a, b, c et d quatre entiers relatifs quelconques et soit n en entier naturel non nul.
Si $a \equiv b\ (n)$ et si $c \equiv d\ (n)$ alors :

- $a + c \equiv b + d\ (n)$
- $ac \equiv bd\ (n)$

La relation de congruence est compatible avec l'addition et la multiplication.

Démonstration

Si $a \equiv b\ (n)$ alors il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ ou encore $a = kn + b$.
Si $c \equiv d\ (n)$ alors il existe $k' \in \mathbb{Z}$ tel que $c - d = k'n$ ou encore $c = kn + d$.

Ainsi $a + c = kn + b + k'n + d = n(k + k') + b + d$.
Or $n(k + k') + b + d \equiv b + d\ (n)$. Ainsi, $a + c \equiv b + d\ (n)$.

La démonstration est similaire pour la multiplication.

Propriétés : conséquences

Soit n un entier naturel non nul et soient a et b deux entiers relatifs.

- Pour tout entier relatif k, si $a \equiv b\ (n)$ alors $a + k \equiv b + k\ (n)$.
- Pour tout entier relatif k, si $a \equiv b\ (n)$ alors $ka \equiv kb\ (n)$.
- Pour tout entier naturel non nul p, si $a \equiv b\ (n)$ alors $a^p \equiv b^p\ (n)$.

Démonstration

Pour les deux premiers points, il suffit d'appliquer les précédentes propriétés en posant $b = k$.

Montrons la troisième conséquence par récurrence sur l'entier p.

Initialisation

Pour $p = 0$, la formule est vérifiée de façon triviale.

Hérédité

Supposons que pour un entier naturel p supérieur ou égal à 0, la propriété soit vraie.
$a^{k+1} \equiv a^k \times k \equiv b^k \times b \equiv b^{k+1}\ (n)$
La proposition est donc héréditaire.

Conclusion

La propriété est vraie pour $p = 0$ et héréditaire à partir de cet entier. La propriété est donc vraie pour tout entier naturel p supérieur ou égal à 0.

Remarque

La réciproque est fausse !
$6 \times 5 \equiv 6 \times 2\ (2)$ mais 5 et 2 ne sont pas congrus modulo 2.
De même, $5^2 \equiv 2^2\ (7)$ mais 5 et 2 ne sont pas congrus modulo 7.