1 Multiples et diviseurs

A retenir

Soient a , b et c trois entiers naturels non nuls .

1. Transitivité : Si a divise b et b divise c alors a divise c .
2. Combinaison linéaire : Si a divise b et c alors a divise $kb + hc$ pour tous entiers k et h .

Le principe

On utilise simplement les définitions .

Les démonstrations

1. Puisque a divise b , alors **il existe un entier naturel k tel que** $b = ka$
   Puisque b divise c , alors **il existe un entier naturel k' tel que** $c = k'b$
   On peut donc écrire : $c = k'(ka) = kk'a$ **, k et k' étant entiers ,** kk' **est aussi entier et donc a divise c**

2. Puisque a divise b et c alors , il existe n et m entiers tels que $b = ma$ et $c = na$. Alors $kb + hc = kma + hna = (km + hn)a$ **. On sait que k , h , m et n sont entiers donc a divise bien** $kb + hc$

2 Division euclidienne

A retenir

Soient a et b deux entiers naturels avec b non nul . Alors il existe un unique couple (q;r) d'entiers naturels tels que $a = bq + r$ avec $0 \leq r < b$

Le principe

Pour l'existence , on encadre a non multiple de b par deux multiples de b et on en déduit l'encadrement de $a - bq$. Pour l'unicité , on prend deux couples ayant les mêmes propriétés et on montre l'égalité .

La démonstration

1. Existence :

   - Premier cas : on va supposer que a est un multiple de b . Alors , il existe un entier q tel que $a = bq + 0$ donc on peut poser $r = 0$
   - Deuxième cas : on suppose que a n'est pas un multiple de b .
     On peut ranger les multiples de b dans l'ordre croissant et on peut donc encadrer a par deux multiples de b : $qb < a < (q+1)b$. On pose : $r = a - qb$ alors : $0 < r < b$.
   - Conclusion : Dans tous les cas , il existe bien q et r tels que $a = bq + r$ avec $0 \leq r < b$.

2. Unicité :

   - Posons $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$
   - On va montrer que $r = r'$.
     $bq + r = bq' + r' \iff b(q - q') = r' - r$
     On peut donc dire que b divise $r' - r$
     Or $-b < -r \leq 0$ donc
     $-b < r' - r < b$.
     Mais le seul diviseur de b compris entre $-b$ et b c'est **0** donc $r' - r = 0$ et $r' = r$.
   - Montrons maintenant que $q = q'$. On a :
     $b(q - q') = \mathbf{0}$ et puisque b est non nul , alors $q - q' = 0$ **et** $q = q'$

3 Congruences

A retenir

Soient a , b , c et d des entiers relatifs tels que $a \equiv c\ [n]$ et $b \equiv d\ [n]$.

1. $a + b \equiv c + d\ [n]$
2. $a - b \equiv c - d\ [n]$
3. $ab \equiv cd\ [n]$
4. Pour tout p entier naturel non nul , $a^p \equiv c^p\ [n]$

Le principe

On applique simplement les définitions pour les trois premières . Pour la dernière , on utilise un raisonnement par récurrence .

La démonstration

1. $a \equiv c\ [n] \iff a - c = kn \iff a = c + kn$ **pour un k entier relatif**
   $b \equiv d\ [n] \iff b - d = k'n \iff b = d + k'n$ **pour un k' entier relatif**
   Donc $a+b = c+d+kn+k'n = c+d+(k+k')n$ et par définition , on a : $a+b \equiv c+d\ [n]$

2. $a \equiv c\ [n] \iff a - c = kn \iff a = c + kn$ pour un k entier relatif
   $b \equiv d\ [n] \iff b - d = k'n \iff b = d + k'n$ pour un k' entier relatif
   Donc $a-b = c-d+kn-k'n = c-d+(k-k')n$ et par définition , on a : $a-b \equiv c-d\ [n]$

3. $a \equiv c\ [n] \iff a - c = kn \iff a = c + kn$ pour un k entier relatif
   $b \equiv d\ [n] \iff b - d = k'n \iff b = d + k'n$ pour un k' entier relatif
   $ab = (c + kn)(d + k'n) = cd + n(dk + ck' + kk'n)$ **et donc par définition** $ab \equiv cd\ [n]$

4. On procède par récurrence . Pour $p = 1$, l'initialisation est immédiate .
   Hérédité : supposons que pour un p donné , $a^p \equiv c^p\ [n]$
   Alors , $a^{p+1} = a^p a$. Or $a \equiv c\ [n]$ et $a^p \equiv c^p\ [n]$ donc par la propriété 3) , on a : $a^{p+1} = a^p a \equiv c^p c\ [n] \equiv c^{p+1}\ [n]$ **.**