

**1** Soient trois entiers  $a$ ,  $b$  et  $c$ . On dit que  $a$  divise  $b$  lorsqu'il existe un entier relatif  $k$  tel que  $b = k \times a$ .

On note  $a | b$ . De plus, si  $a | b$  et  $a | c$ , alors, pour tous entiers  $m$  et  $n$ ,  $a | (mb + nc)$ . Cela permet de :

- ✓ déterminer les diviseurs d'un entier ;
- ✓ montrer qu'un entier  $b$  est divisible par un entier  $a$  ;
- ✓ déterminer des solutions entières d'équations en se ramenant à une équation du type  $A \times B = C$  où les diviseurs de  $C$  sont connus ;
- ✓ déterminer les diviseurs communs à deux entiers.

**2** Soient deux entiers  $a$  et  $b$  avec  $b$  strictement positif. Effectuer la division euclidienne de  $a$  par  $b$ , c'est déterminer l'unique couple d'entiers  $(q ; r)$  tel que  $a = bq + r$  et  $0 \leq r < b$ . Cela permet de :

- ✓ raisonner par disjonction de cas pour établir une divisibilité ;
- ✓ résoudre des problèmes de codage (clé de contrôle).

**3** Soient deux entiers relatifs  $a$  et  $b$ , et  $m$  un entier naturel non nul.  $a$  et  $b$  sont congrus modulo  $m$  lorsqu'ils ont le même reste dans la division euclidienne par  $m$ . On note  $a \equiv b [m]$ . De plus,  $a \equiv b [m] \Leftrightarrow m | (b - a)$ . Cela permet de :

- ✓ établir les propriétés sur les congruences (compatibilité avec l'addition et la multiplication) ;
- ✓ établir un test de divisibilité ;
- ✓ étudier des problèmes de chiffrement ;
- ✓ résoudre une équation du type  $ax \equiv b [m]$ .

### CARTE MENTALE

