

**2.9** Puisque  $a \equiv b \pmod{m}$ , il existe  $k \in \mathbb{Z}$  tel que  $b = a + km$ .

De même, il existe  $k' \in \mathbb{Z}$  tel que  $d = c + k'm$ .

1)  $b + d = (a + km) + (c + k'm) = (a + c) + (k + k')m$

En posant  $k'' = k + k'$ , on obtient  $b + d = (a + c) + k''m$  avec  $k'' \in \mathbb{Z}$ .

Ceci revient à dire que  $a + c \equiv b + d \pmod{m}$ .

2)  $bd = (a + km)(c + k'm) = ac + ak'm + ck'm + kk'm^2$   
 $= ac + (ak' + ck + kk'm)m$

En posant  $k'' = ak' + ck + kk'm$ , on trouve  $bd = ac + k''m$  avec  $k'' \in \mathbb{Z}$ .

On en tire que  $ac \equiv bd \pmod{m}$ .

3) Montrons par récurrence que  $a^n \equiv b^n \pmod{m}$  pour tout  $n \in \mathbb{N}$ .

#### Initialisation

$a^1 \equiv b^1 \pmod{m}$  est vérifié, puisque l'on suppose  $a \equiv b \pmod{m}$ .

#### Hérédité

Supposons  $a^n \equiv b^n \pmod{m}$  pour un certain  $n \in \mathbb{N}$ .

En utilisant la propriété 2) avec  $c = a^n$  et  $d = b^n$ , on obtient :

$a \cdot a^n \equiv b \cdot b^n \pmod{m}$ , c'est-à-dire  $a^{n+1} \equiv b^{n+1} \pmod{m}$ .