

### Propriétés :

- (1)  $a$  est divisible par  $n$  ssi  $a \equiv 0 \pmod{n}$ .
- (2)  $n \equiv 0 \pmod{n}$ .
- (3)  $a \equiv a \pmod{n}$ .
- (4) Si  $a \equiv b \pmod{n}$  et  $b \equiv c \pmod{n}$ , alors  $a \equiv c \pmod{n}$ ; on dit que la relation de congruence modulo  $n$  est transitive.
- (5) Si  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ , alors  $a + a' \equiv b + b' \pmod{n}$ .
- (6) Si  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ , alors  $aa' \equiv bb' \pmod{n}$ .
- (7) Si  $a \equiv b \pmod{n}$  et  $p \in \mathbf{N}^*$ , alors  $a^p \equiv b^p \pmod{n}$ .

### Démonstrations :

- (1)  $a$  est divisible par  $n$  si, et seulement si,  $a$  admet pour reste 0 dans la division euclidienne par  $n$ , c'est-à-dire si, et seulement si,  $a \equiv 0 \pmod{n}$ .
- (2)  $n$  a pour reste 0 dans la division euclidienne par  $n$ , donc  $n \equiv 0 \pmod{n}$ .
- (3)  $a$  et  $a$  ont bien le même reste dans la division euclidienne par  $n$ .
- (4) Si  $a$  et  $b$  ont même reste dans la division euclidienne par  $n$  et,  $b$  et  $c$  aussi, alors  $a$  et  $c$  ont même reste dans la division euclidienne par  $n$ .
- (5) Si  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ , alors il existe des entiers  $q$  et  $q'$  tels que  $a - b = qn$  et  $a' - b' = q'n$ .  
Par addition,  $(a + a') - (b + b') = qn + q'n = (q + q')n$ . Comme  $q + q'$  est un entier, alors  $(a + a') - (b + b')$  est divisible par  $n$ , ce qui prouve que  $a + a'$  et  $b + b'$  sont congrus modulo  $n$ .
- (6) Si  $a \equiv b \pmod{n}$  et  $a' \equiv b' \pmod{n}$ , alors il existe des entiers  $q$  et  $q'$  tels que  $a - b = qn$  et  $a' - b' = q'n$ .  
Par produit,  $aa' = (b + qn)(b' + q'n)$ . D'où  $aa' - bb' = n(bq' + qb' + nqq')$ ; comme  $bq' + qb' + nqq'$  est un entier, alors  $aa' - bb'$  est divisible par  $n$ , ce qui montre que  $aa'$  et  $bb'$  sont congrus modulo  $n$ .
- (7) Supposons que  $a \equiv b \pmod{n}$ .

Soit  $\mathcal{P}(p)$  la propriété : « pour tout entier  $p$  supérieur ou égal à 1,  $a^p \equiv b^p \pmod{n}$  ».

➤ Initialisation : si  $p = 1$ , on a :  $a^1 \equiv b^1 \pmod{n}$ ; ce qui est vraie par hypothèses.

Alors  $\mathcal{P}(1)$  est vraie.

➤ Hérédité : soit  $p \geq 1$ , supposons que  $a^p \equiv b^p \pmod{n}$ . Vérifions si  $\mathcal{P}(p+1)$  est vraie. Comme  $a^p \equiv b^p \pmod{n}$  et que  $a \equiv b \pmod{n}$ , alors  $a^{p+1} \equiv b^{p+1} \pmod{n}$  (d'après la propriété 6). D'où  $\mathcal{P}(p+1)$  est vraie.

➤ Conclusion : On vient de prouver que  $\mathcal{P}(1)$  est vraie et que, pour tout  $p \geq 1$ ,

$\mathcal{P}(p) \Rightarrow \mathcal{P}(p+1)$ .

Du principe de raisonnement par récurrence, on en déduit que, pour tout entier  $p$  supérieur ou égal à 1,  $a^p \equiv b^p \pmod{n}$  lorsque  $a \equiv b \pmod{n}$ .