Divisibilité et congruences

Astrolab Cours · astrolabcours.fr

L'image. Une horloge : après n, on revient à 0. Seul le reste compte, et les puissances finissent par tourner en rond.

01 Divisibilité

- $b \mid a \iff a = kb$, k entier.
- $b \mid a$ et $b \mid c \Rightarrow b \mid ua + vc$.

Division euclidienne

- $a = bq + r$ avec $0 \leq r < b$, unique.
- $-17 = 5 \times (-4) + 3$: reste 3.

03 Congruences

Si $a \equiv b$ et $c \equiv d\ [n]$	Alors
somme	$a + c \equiv b + d\ [n]$
produit	$ac \equiv bd\ [n]$
puissance	$a^k \equiv b^k\ [n]$

- $a \equiv b\ [n] \iff n \mid a - b$.

04 Méthode des grandes puissances

1. Chercher une puissance $a^p \equiv 1$ (ou $\equiv -1$).
2. Diviser l'exposant par p : $k = pq + r$.
3. $a^k = (a^p)^q a^r \equiv a^r$.

Les pièges

- Reste toujours entre 0 et $n - 1$.
- On ne divise pas une congruence.
- Tableau de congruences : tester **tous** les restes.

© Astrolab Cours · astrolabcours.fr/maths/maths-expertes/divisibilite-et-congruences/ · Tous droits réservés : usage personnel uniquement, republication et usage commercial interdits