MATHS EXPERTES / COURS

Divisibilité, division euclidienne et congruences

Astrolab Cours · astrolabcours.fr

01 Le problème

Quel est le chiffre des unités de 7^{2026} ? La calculatrice abandonne : ce nombre a plus de 1 700 chiffres. Pourtant, la réponse tient en trois lignes.

01 L'idée : le cadran de l'horloge

Sur une horloge, après 12 h, on revient à 1 h : on ne compte pas « 15 h », on dit « 3 h ». Sur le cadran, 15 et 3 sont **au même endroit**. On ne garde que le **reste** de la division par 12.

Pour le chiffre des unités, on utilise une horloge à **10 heures** : seul le reste de la division par 10 compte. Et sur une horloge, les puissances finissent toujours par **tourner en rond**.

01 Divisibilité

Pour a et b entiers relatifs, $b \neq 0$: b **divise** a (noté $b \mid a$) s'il existe un entier k tel que $a = kb$.

- Si $b \mid a$ et $a \mid c$, alors $b \mid c$;
- si $b \mid a$ et $b \mid c$, alors b divise toute **combinaison** $ua + vc$ (u, v entiers).

01 Division euclidienne

Pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un **unique** couple $(q\,;r)$ d'entiers tel que

$$a = bq + r \quad \text{et} \quad 0 \leq r < b.$$

q est le **quotient**, r le **reste**.

Congruences

$n \geq 2$. On dit que a est **congru à** b **modulo** n, et on écrit $a \equiv b\ [n]$, si a et b ont le même reste dans la division par n, c'est-à-dire si $n \mid a - b$.

Propriétés : si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors

- $a + c \equiv b + d\ [n]$ et $ac \equiv bd\ [n]$;
- $a^k \equiv b^k\ [n]$ pour tout entier naturel k.

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

On peut donc **remplacer un nombre par son reste** dans les sommes, les produits et les puissances. Mais on ne peut **pas simplifier** par un facteur commun en général.

Tableau de congruences : pour étudier les restes de x^2 modulo 5, on teste les 5 restes possibles de x : $0, 1, 2, 3, 4$ donnent $0, 1, 4, 4, 1$. Un carré n'est donc jamais congru à 2 ou 3 modulo 5.

Retour au problème

On cherche le reste de 7^{2026} modulo 10. Les puissances de 7 tournent sur le cadran :

$$7^1 \equiv 7, \quad 7^2 \equiv 9, \quad 7^3 \equiv 3, \quad 7^4 \equiv 1 \ [10]$$

Comme $7^4 \equiv 1$, et $2026 = 4 \times 506 + 2$:

$$7^{2026} = (7^4)^{506} \times 7^2 \equiv 1^{506} \times 49 \equiv 9 \ [10].$$

Le chiffre des unités de 7^{2026} est 9.

La suite : PGCD, Bézout et Gauss. Les bases (nombres premiers, critères de divisibilité) sont dans l'arithmétique de 3e.

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