Congruences

Fiche méthode

(Maths expertes Terminale · Arithmétique)

La démarche pour une question de congruences

1. Je choisis le module imposé par la question : le diviseur, le 10 du chiffre des unités, le 26 de l'alphabet…

2. Je réduis chaque nombre : son reste, ou un représentant commode (-1, -2).

3. J'enchaîne les congruences en citant la compatibilité (somme, produit, puissance), avec le module écrit à chaque ligne.

4. Je conclus par un reste compris entre 0 et $n-1$, par une classe $x \equiv c\ [n]$, ou par « divisible par n » si le reste est nul.

Le réflexe — chaque congruence porte son module [n], et le reste final est compris entre 0 et n − 1. Un « reste » négatif ou supérieur au module est une erreur.

Cas 1 · Prouver une congruence, trouver un reste

Réflexe — a ≡ b [n] : j'écris a − b = kn avec k entier ; pour un reste, j'ajoute ou je retire des multiples de n jusqu'à tomber entre 0 et n − 1.

Exemple. Questions types : « Montrer que $a \equiv b\ [n]$ », « Déterminer le reste de … modulo … ». Exemple : reste de -100 modulo 7.

$7 \times 14 = 98$, donc $100 = 7 \times 14 + 2$ et $-100 = 7 \times (-14) - 2$.

-2 n'est pas un reste : $-100 = 7 \times (-15) + 5$, avec $0 \leqslant 5 < 7$.

Donc $-100 \equiv 5\ [7]$: le reste vaut 5.

Attention — un reste est compris entre 0 et n − 1 : on écrit $-2 \equiv 5\ [7]$, jamais « le reste vaut -2 ».

Cas 2 · Calculer modulo n

Réflexe — je remplace chaque nombre par un représentant commode, je calcule avec la compatibilité, puis je ramène le résultat entre 0 et n − 1.

Exemple. Questions types : « Déterminer le reste de $a+b$, de ab, de a^2+2b sachant que … ». Exemple : $a \equiv 5\ [9]$ et $b \equiv 7\ [9]$, reste de a^2+2b.

Représentants commodes : $a \equiv -4$ et $b \equiv -2\ [9]$.

Par compatibilité : $a^2 + 2b \equiv 16 - 4 = 12\ [9]$.

$12 = 9 + 3$: le reste vaut 3.

Attention — on ne divise pas une congruence : 2a ≡ 2b [n] n'entraîne pas toujours a ≡ b [n].

Cas 3 · Reste d'une grande puissance

Réflexe — je réduis la base, je cherche la première puissance congrue à 1 (ou à -1), je divise l'exposant par la longueur du cycle.

Exemple. Questions types : « Reste de a^m modulo n », « Chiffre des unités de … ». Exemple : reste de 5^{2030} modulo 13.

$5^2 = 25 = 26 - 1$, donc $5^2 \equiv -1\ [13]$ et $5^4 \equiv (-1)^2 = 1\ [13]$.

$2\,030 = 4 \times 507 + 2$, donc $5^{2030} = (5^4)^{507} \times 5^2 \equiv -1\ [13]$.

Le reste vaut $13 - 1 = 12$.

Attention — on réduit la base modulo n, jamais l'exposant ; l'exposant se divise par la longueur du cycle.

Cas 4 · Utiliser un critère de divisibilité

Réflexe — somme des chiffres pour 3 et 9, somme alternée depuis les unités pour 11, derniers chiffres pour 2, 4, 5, 8, 10 et 25.

Exemple. Questions types : « Déterminer le reste par 9, par 11 », « Démontrer le critère de divisibilité par . . . ». Exemple : restes de 93 581 modulo 9 et modulo 11.

$10 \equiv 1\ [9] : 9 + 3 + 5 + 8 + 1 = 26 \equiv 8\ [9]$, donc $93\,581 \equiv 8\ [9]$.
$10 \equiv -1\ [11] : 1 - 8 + 5 - 3 + 9 = 4$, donc $93\,581 \equiv 4\ [11]$.

Attention — pour 11, le signe + va au chiffre des unités ; un résultat négatif se corrige en ajoutant 11.

Cas 5 · Raisonner avec un tableau de congruences

Réflexe — une colonne par reste modulo n, une ligne par expression ; je lis le tableau et je conclus pour tout entier.

Exemple. Questions types : « Montrer que pour tout entier n, . . . est divisible par . . . », « Montrer que l'équation . . . n'a pas de solution entière ». Exemple : 3 divise $n(n^2+2)$ pour tout entier n.

n **modulo** 3	0	1	2
n^2+2	2	0	0
$n(n^2+2)$	0	0	0

La dernière ligne ne contient que des 0 : 3 divise $n(n^2+2)$ pour tout entier n.

Attention — toutes les colonnes, sans oubli ; des restes compatibles ne prouvent pas qu'une solution existe.

Cas 6 · Résoudre ax ≡ b [n]

Réflexe — je cherche un inverse u de a parmi n + 1, 2n + 1. . . ; s'il existe, x ≡ ub [n] ; sinon je simplifie par le diviseur commun.

Exemple. Questions types : « Résoudre dans $\mathbb{Z}$ l'équation . . . », « Déterminer les entiers n tels que . . . soit divisible par . . . ». Exemple : $7x \equiv 4\ [10]$.

Inverse de 7 modulo 10 : $7 \times 3 = 21 \equiv 1\ [10]$.
En multipliant par 3 : $x \equiv 12 \equiv 2\ [10]$.
Vérification : $7 \times 2 = 14 \equiv 4\ [10]$. Solutions : $x = 2 + 10k$, $k \in \mathbb{Z}$.

Attention — la réponse est une classe ; si un diviseur de a et n ne divise pas b, il n'y a aucune solution.

Les pièges

- Un reste est compris entre 0 et n − 1 : $-3 \equiv 5\ [8]$, jamais « reste −3 ».
- On ne divise pas une congruence : $2 \times 5 \equiv 2 \times 0\ [10]$, mais 5 n'est pas congru à 0 modulo 10.
- On ne prend pas la racine : $6^2 \equiv 1^2\ [7]$, mais 6 n'est pas congru à 1 modulo 7.
- On réduit la base, jamais l'exposant, modulo n.
- Somme alternée pour 11 : on part du chiffre des unités, avec le signe +.
- Une équation de congruence a pour solution une ou plusieurs classes, pas un seul entier.

Ce document est la propriété intellectuelle de Ben, professeur particulier (benprofparticulier.fr), protégée par le Code de la propriété intellectuelle (art. L. 111-1 et L. 122-4). Il est mis à disposition pour un usage personnel de révision. Toute reproduction, diffusion, mise en ligne ou revente, totale ou partielle, sans autorisation écrite est interdite et constitue une contrefaçon (art. L. 335-2).