Nombres premiers

Fiche méthode

(Maths expertes Terminale · Arithmétique)

La démarche pour une question sur les nombres premiers

1. J'identifie la question : primalité, décomposition, diviseurs, PGCD ou PPCM, reste d'une grande puissance, démonstration (infinité, lemme d'Euclide).

2. Je décompose en facteurs premiers, ou j'encadre n entre deux carrés pour savoir jusqu'où tester.

3. Je cite la propriété avec ses hypothèses : test jusqu'à $\sqrt{n}$, unicité de la décomposition, petit théorème de Fermat avec « p premier ne divisant pas a ».

4. Je contrôle : je remultiplie les facteurs, je vérifie pgcd $\times$ ppcm $= ab$, je ramène un reste entre 0 et $p-1$.

Le réflexe — pas de « premier » sans avoir testé tous les nombres premiers jusqu'à $\sqrt{n}$, pas de « d'après Fermat » sans « p premier ne divisant pas a ».

Cas 1 · Décomposer en facteurs premiers

Réflexe — diviser par 2, 3, 5, 7… dans l'ordre, garder le même nombre premier tant qu'il divise, contrôler en remultipliant.

Exemple. Questions types : « Décomposer n en produit de facteurs premiers », « Rendre la fraction irréductible ». Exemple : 1 386.

$1\,386 = 2 \times 693$; $6+9+3 = 18$, donc $693 = 3 \times 231 = 3^2 \times 77$; $77 = 7 \times 11$.

$1\,386 = 2 \times 3^2 \times 7 \times 11$.

Contrôle : $2 \times 9 \times 77 = 1\,386$.

Attention — un 9 ou un 77 dans le produit final : ce ne sont pas des nombres premiers.

Cas 2 · Démontrer qu'un entier est premier

Réflexe — encadrer n entre deux carrés consécutifs, tester les seuls nombres premiers jusqu'à $\sqrt{n}$, conclure par le critère.

Exemple. Questions types : « Montrer que n est premier », « Déterminer le plus petit diviseur premier de n ». Exemple : 389.

$19^2 = 361 \leqslant 389 < 400 = 20^2$: on teste 2, 3, 5, 7, 11, 13, 17, 19.

389 est impair, $3+8+9 = 20$, ni 0 ni 5 ; $7 \times 55 = 385$, $11 \times 35 = 385$, $13 \times 29 = 377$, $17 \times 22 = 374$, $19 \times 20 = 380$: restes 4, 4, 12, 15, 9.

Aucun reste nul : 389 est premier.

Attention — s'arrêter avant $\sqrt{n}$ peut faire déclarer premier un entier composé.

Cas 3 · Rédiger l'infinité des nombres premiers

Réflexe — hypothèse « liste finie », N = produit + 1, diviseur premier p de N, « p divise 1 », contradiction.

Exemple. Question type : « Démontrer que l'ensemble des nombres premiers est infini ». Illustration avec la liste $\{3\,;5\}$.

Si $p_1, \ldots, p_r$ étaient tous les nombres premiers, $N = p_1 \cdots p_r + 1 \geqslant 3$ aurait un diviseur premier $p = p_i$.

p divise N et $p_1 \cdots p_r$, donc 1 : impossible.

Avec $\{3\,;5\}$: $N = 16 = 2^4$, et 2 est hors de la liste.

Attention — N n'est pas forcément premier : on dit seulement qu'il a un diviseur premier.

Cas 4 · Compter et sommer les diviseurs

Réflexe — décomposer, multiplier les exposants augmentés de 1, sommer avec une parenthèse par facteur premier.

Exemple. Questions types : « Combien n a-t-il de diviseurs positifs ? », « Calculer leur somme ». Exemple : 600.

$600 = 2^3 \times 3 \times 5^2$.
Nombre de diviseurs : $(3+1)(1+1)(2+1) = 24$.
Somme : $(1+2+4+8)(1+3)(1+5+25) = 15 \times 4 \times 31 = 1\,860$.

Attention — (a + 1)(b + 1) et non ab : l'exposant 0 compte.

Cas 5 · PGCD et PPCM par décomposition

Réflexe — même liste de nombres premiers, exposants minimaux pour le PGCD, maximaux pour le PPCM, contrôle par le produit.

Exemple. Questions types : « Déterminer $\text{pgcd}(a\,;b)$ et $\text{ppcm}(a\,;b)$ ». Exemple : 252 et 330.

$252 = 2^2 \times 3^2 \times 7$ et $330 = 2 \times 3 \times 5 \times 11$.
pgcd $= 2 \times 3 = 6$; ppcm $= 2^2 \times 3^2 \times 5 \times 7 \times 11$, soit 13 860.
Contrôle : $6 \times 13\,860 = 83\,160 = 252 \times 330$.

Attention — le PGCD ne garde que les facteurs communs ; le PPCM les garde tous.

Cas 6 · Reste d'une grande puissance (Fermat)

Réflexe — vérifier « p premier ne divisant pas a », diviser l'exposant par p − 1, garder le reste.

Exemple. Questions types : « Déterminer le reste de a^m modulo p », « Montrer que p divise $n^p - n$ ». Exemple : 8^{123} modulo 11.

11 est premier et ne divise pas 8 : $8^{10} \equiv 1\ [11]$ (Fermat).
$123 = 10 \times 12 + 3$, donc $8^{123} \equiv 8^3 = 512\ [11]$.
$512 = 46 \times 11 + 6$: le reste est 6.

Attention — module non premier : le théorème ne s'applique pas.

Les pièges

- 1 n'est pas premier, 2 l'est, et un entier impair n'est pas forcément premier.
- Tester jusqu'à $\sqrt{n}$: ni moins (on rate un diviseur), ni plus (inutile).
- $N = p_1 \times \ldots \times p_r + 1$ n'est pas toujours premier : avec $\{3\,;5\}$, $N = 16 = 2^4$.
- Nombre de diviseurs : produit des exposants augmentés de 1, pas des exposants.
- Somme des diviseurs : toutes les puissances de p dans chaque parenthèse, pas seulement 1 et pˆa.
- Fermat : module premier, a non multiple de p, exposant divisé par p − 1.

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).