Nombres premiers et petit théorème de Fermat

Terminale maths expertes · Chapitre 06

Les repères essentiels

- Premier : entier au moins 2 ayant exactement deux diviseurs positifs.
- Un composé a un diviseur premier au plus égal à sa racine carrée.
- Un premier divisant un produit divise au moins un facteur ; les facteurs premiers d'un entier sont uniques à l'ordre près.
- Fermat : $a^{p-1} \equiv 1 \pmod{p}$ si p est premier et $p \nmid a$; $a^p \equiv a$ pour tout entier a.
- Fermat peut réfuter une primalité ; une congruence réussie pour une base ne la prouve pas.
- Crible, divisions successives et carrés successifs répondent à trois questions différentes : lister, factoriser, calculer une puissance.

Contrôle. Ai-je inclus la borne racine carrée ? Vérifié les hypothèses de Fermat ? Réduit l'exposant modulo p-1 ? Évité de confondre un nombre et un diviseur premier de ce nombre ?

Une méthode à retenir

> **Méthode · Prouver la primalité d'un entier**
>
> Liste les nombres premiers inférieurs ou égaux à $\sqrt{n}$ et vérifie qu'aucun ne divise n. La borne est incluse : pour 49, il faut tester 7. Ne tester que quelques premiers sans atteindre cette borne ne conclut pas.

Un exemple pour se repérer

> **Exemple · Une grande puissance**
>
> Le module 7 est premier et ne divise pas la base 3. Fermat s'applique donc : $3^{7-1} = 3^6 \equiv 1 \pmod{7}$. Divisons l'exposant par 6 : $100 = 6 \times 16 + 4$. Alors
>
> $$\begin{aligned} 3^{100} &= (3^6)^{16} 3^4 \equiv 1^{16} 3^4 \\ &= 81 \equiv 4 \pmod{7}, \end{aligned}$$
>
> car $81 = 7 \times 11 + 4$.
>
> Le reste final 4 appartient à $\{0, \dots, 6\}$. Réduire 100 modulo 7 serait injustifié : Fermat fournit une puissance d'exposant $p - 1 = 6$, et c'est par cet exposant que l'on regroupe les facteurs.

Les erreurs à éviter

> **Attention · Une conclusion plus précise que « le produit plus un est premier »**
>
> La preuve affirme que N possède un facteur premier nouveau, pas que N est lui-même premier. Par exemple
>
> $$\begin{aligned} 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 &= 30031 \\ &= 59 \times 509. \end{aligned}$$
>
> La distinction évite une fausse généralisation.