Plaquette 3 – Le petit théorème de Fermat et ses applications

Nombres premiers — Terminale maths expertes

Exercices

Méthode

Un seul théorème, mais un outil redoutable : $a^{p-1} \equiv 1 \pmod{p}$ quand p est premier. On s'en sert pour calculer des **restes de puissances gigantesques**, pour trouver un **inverse modulaire** sans algorithme d'Euclide, pour démontrer des divisibilités valables pour tout entier, et l'on voit aussi ce qu'il ne permet **pas** de conclure.

Exercice 1 – Vérifier le théorème

a) Vérifier le petit théorème de Fermat pour $a = 3$ et $p = 7$.

b) Vérifier le corollaire $a^p \equiv a \pmod{p}$ pour $a = 7$ et $p = 7$, et expliquer pourquoi le théorème lui-même ne s'applique pas ici.

Exercice 2 – Une grande puissance modulo 7

Déterminer le reste de 3^{100} dans la division par 7.

Exercice 3 – Modulo 13

Déterminer le reste de 2^{2026} dans la division par 13.

Exercice 4 – Modulo 11

Montrer que l'entier $7^{2026} - 4$ est divisible par 11.

Exercice 5 – Réduire la base d'abord

Déterminer le reste de $2\,026^{2026}$ dans la division par 7.

Exercice 6 – Un inverse sans Euclide

a) En utilisant le petit théorème de Fermat, déterminer l'inverse de 5 modulo 13.

b) Retrouver le résultat par une simple lecture.

Exercice 7 – Résoudre une congruence avec Fermat

Résoudre $3x \equiv 5 \pmod{17}$ en utilisant le petit théorème de Fermat.

Exercice 8 – Une divisibilité pour tout entier

Montrer que pour **tout** entier n, le nombre $n^5 - n$ est divisible par 5.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 9 – Divisibilité par un premier quelconque

Soit p un nombre premier. Montrer que p divise $2^p - 2$.

Vérifier pour $p = 11$.

Exercice 10 – Un test de primalité qui échoue

On veut tester si 341 est premier avec le petit théorème de Fermat.

a) Montrer que $2^{10} \equiv 1 \pmod{341}$, puis que $2^{340} \equiv 1 \pmod{341}$.

b) 341 est-il premier ? Que conclure sur ce test ?

Exercice 11 – Somme de deux puissances

Déterminer le reste de $3^{2026} + 4^{2026}$ dans la division par 7.

Exercice 12 – Les racines carrées de 1

Soit p un nombre premier. Montrer que si $x^2 \equiv 1 \pmod{p}$, alors $x \equiv 1$ ou $x \equiv -1 \pmod{p}$.

Vérifier que la conclusion est fausse modulo 8.

Exercice 13 – Un chiffre des unités lointain

a) Déterminer le chiffre des unités de 3^{2026}.

b) Le petit théorème de Fermat s'applique-t-il directement ici ? Justifier.

Exercice 14 – Une clé de contrôle modulo 97

Dans un système de codage, une donnée a (non divisible par 97) est transformée en $a^{96} \bmod 97$. On rappelle que 97 est premier.

a) Que vaut le résultat, quelle que soit la donnée ?

b) Le système est-il utilisable pour transmettre de l'information ? Et si l'on transformait a en $a^7 \bmod 97$?

Exercice 15 – Bilan : Fermat en trois questions

a) Déterminer le reste de 5^{2026} dans la division par 19.

b) Montrer que pour tout entier n, 13 divise $n^{13} - n$.

c) Résoudre $8x \equiv 3 \pmod{23}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).