Plaquette 3 – Le petit théorème de Fermat et ses applications

Nombres premiers — Terminale maths expertes

Corrections détaillées

Boîte à outils

Le théorème et sa boîte à outils.

— **Petit théorème de Fermat** : si p est premier et si $p \nmid a$, alors

$$a^{p-1} \equiv 1 \pmod{p}$$

— **Corollaire** valable pour **tout** entier a (même divisible par p) : $a^p \equiv a \pmod{p}$.

— **Méthode pour un reste de puissance** : on divise l'exposant par $p-1$. Si $n = (p-1)q + r$, alors

$$a^n = \left(a^{p-1}\right)^q \times a^r \equiv a^r \pmod{p}$$

— **Inverse modulaire** : si p est premier et $p \nmid a$, alors $a \times a^{p-2} \equiv 1$, donc $a^{-1} \equiv a^{p-2} \pmod{p}$.

— **Résolution de** $ax \equiv b \pmod{p}$: $x \equiv a^{p-2}b \pmod{p}$.

— **Attention au sens du théorème** : il donne une condition **nécessaire** de primalité, pas suffisante. Si $a^{n-1} \not\equiv 1 \pmod{n}$, alors n n'est pas premier ; mais la congruence peut être vraie pour un n composé (**pseudo-premier**).

— **Réduction préalable** : on remplace toujours la base par son reste modulo p avant d'appliquer le théorème.

Correction de l'exercice 1 – Vérifier le théorème

a) Le théorème annonce $3^6 \equiv 1 \pmod{7}$.

— $3^2 = 9 \equiv 2$; $3^3 \equiv 3 \times 2 = 6$; $3^6 = \left(3^3\right)^2 \equiv 6^2 = 36 = 35 + 1 \equiv 1 \pmod{7}$ ✓.

— Contrôle direct : $3^6 = 729 = 7 \times 104 + 1$ ✓.

b) Pour $a = p = 7$: $7^7 \equiv 7 \equiv 0 \pmod{7}$.

— C'est vrai, puisque 7^7 est un multiple de 7 et 7 aussi : le **corollaire** est bien vérifié.

— En revanche, le théorème sous sa forme $a^{p-1} \equiv 1$ exige $p \nmid a$. Ici $7 \mid 7$, et de fait $7^6 \equiv 0$, pas 1.

— **La distinction à retenir** : la forme $a^{p-1} \equiv 1$ demande que p ne divise pas a ; la forme $a^p \equiv a$ est vraie sans condition.

Réponse. a) $3^6 = 729 = 7 \times 104 + 1$ ✓ · b) $7^7 \equiv 0 \equiv 7$, et $7^6 \equiv 0 \neq 1$ car $7 \mid 7$.

Correction de l'exercice 2 – Une grande puissance modulo 7

7 est premier et ne divise pas 3 : le petit théorème de Fermat s'applique.

— $3^6 \equiv 1 \pmod{7}$.

— On divise l'exposant par 6 : $100 = 6 \times 16 + 4$.

— Donc

$$3^{100} = \left(3^6\right)^{16} \times 3^4 \equiv 1^{16} \times 3^4 = 81 \pmod{7}$$

— $81 = 7 \times 11 + 4$, donc $3^{100} \equiv 4 \pmod 7$.

Conclusion. Le reste est 4.

— **Comparaison** : sans Fermat, il aurait fallu construire à la main le cycle des puissances de 3 modulo 7 (de longueur 6). Le théorème donne cette longueur **gratuitement**.

Réponse. $3^{100} \equiv 4 \pmod 7$.

Correction de l'exercice 3 – Modulo 13

13 est premier et $13 \nmid 2$: Fermat donne $2^{12} \equiv 1 \pmod{13}$.

— On divise l'exposant par 12 : $2\,026 = 12 \times 168 + 10$ (car $12 \times 168 = 2\,016$).

— Donc $2^{2026} \equiv 2^{10} \pmod{13}$.

— $2^{10} = 1\,024$, et $1\,024 = 13 \times 78 + 10$.

— **Conclusion** : $2^{2026} \equiv 10 \pmod{13}$.

Contrôle par un autre chemin.

— $2^6 = 64 = 13 \times 4 + 12 \equiv -1 \pmod{13}$.

— Donc $2^{10} = 2^6 \times 2^4 \equiv (-1) \times 16 \equiv -16 \equiv -3 \equiv 10 \pmod{13}$ ✓.

Réponse. $2^{2026} \equiv 10 \pmod{13}$.

Correction de l'exercice 4 – Modulo 11

11 est premier et ne divise pas 7 : $7^{10} \equiv 1 \pmod{11}$.

— $2\,026 = 10 \times 202 + 6$, donc $7^{2026} \equiv 7^6 \pmod{11}$.

— On calcule 7^6 par étapes, en réduisant à chaque fois :

— $7^2 = 49 = 44 + 5 \equiv 5$;

— $7^3 \equiv 7 \times 5 = 35 = 33 + 2 \equiv 2$;

— $7^6 = \left(7^3\right)^2 \equiv 2^2 = 4 \pmod{11}$.

Conclusion. $7^{2026} \equiv 4 \pmod{11}$: le reste est 4.

— **Le bon réflexe** : ne jamais calculer $7^6 = 117\,649$ puis diviser. On réduit à chaque étape, les nombres restent inférieurs au module.

Réponse. $7^{2026} \equiv 4 \pmod{11}$.

Correction de l'exercice 5 – Réduire la base d'abord

Étape 1 : réduire la base.

— $2\,026 = 7 \times 289 + 3$, donc $2\,026 \equiv 3 \pmod{7}$.

— Par compatibilité : $2\,026^{2026} \equiv 3^{2026} \pmod{7}$.

Étape 2 : réduire l'exposant avec Fermat.

— 7 est premier et $7 \nmid 3$: $3^6 \equiv 1 \pmod{7}$.

— $2\,026 = 6 \times 337 + 4$ (car $6 \times 337 = 2\,022$), donc $3^{2026} \equiv 3^4 \pmod{7}$.

— $3^4 = 81 = 7 \times 11 + 4 \equiv 4$.

Conclusion. Le reste est 4.

— **Attention** : les deux réductions ne se font pas modulo le même nombre. La **base** se réduit modulo 7, l'**exposant** modulo $6 = p - 1$. Confondre les deux est l'erreur

classique.

Réponse. $2\,026^{2026} \equiv 3^4 \equiv 4 \pmod 7$.

Correction de l'exercice 6 – Un inverse sans Euclide

a) 13 est premier et $13 \nmid 5$, donc $5^{12} \equiv 1 \pmod{13}$.

— On écrit $5 \times 5^{11} \equiv 1$: l'inverse de 5 est donc 5^{11} modulo 13.
— Calcul par puissances successives : $5^2 = 25 \equiv 12 \equiv -1 \pmod{13}$.
— Donc $5^4 \equiv 1$, et $5^{11} = 5^8 \times 5^2 \times 5 \equiv 1 \times (-1) \times 5 = -5 \equiv 8 \pmod{13}$.
— **L'inverse de** 5 **modulo** 13 **est** 8**.**

b) Plus simplement : on cherche un multiple de 5 qui dépasse un multiple de 13 d'exactement 1.

— $5 \times 8 = 40 = 39 + 1 = 13 \times 3 + 1$ ✓.
— **Conclusion** : $5^{-1} \equiv 8 \pmod{13}$, par les deux méthodes.
— **Quand utiliser quoi** : pour un petit module, on cherche de tête ; pour un grand module premier, la formule $a^{-1} \equiv a^{p-2}$ est systématique, et l'algorithme d'Euclide reste le plus efficace si le module n'est pas premier.

Réponse. $5^{-1} \equiv 5^{11} \equiv 8 \pmod{13}$.

Correction de l'exercice 7 – Résoudre une congruence avec Fermat

17 est premier et ne divise pas 3 : l'inverse de 3 est $3^{15} \pmod{17}$.

— $3^2 = 9$; $3^4 = 81 = 68 + 13 \equiv 13 \equiv -4$; $3^8 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}$.
— Donc $3^{15} = 3^8 \times 3^4 \times 3^2 \times 3 \equiv (-1) \times (-4) \times 9 \times 3 = 108 \pmod{17}$.
— $108 = 17 \times 6 + 6$, donc $3^{-1} \equiv 6 \pmod{17}$ — ce que confirme $3 \times 6 = 18 \equiv 1$ ✓.

On multiplie l'équation par 6 :

— $x \equiv 6 \times 5 = 30 \equiv 13 \pmod{17}$.
— **Vérification** : $3 \times 13 = 39 = 34 + 5 \equiv 5 \pmod{17}$ ✓.

Réponse. $x \equiv 13 \pmod{17}$.

Correction de l'exercice 8 – Une divisibilité pour tout entier

On utilise le **corollaire** du petit théorème de Fermat, celui qui n'exige aucune condition sur n :

$$n^p \equiv n \pmod p \qquad \text{pour } p \text{ premier}$$

— Avec $p = 5$: $n^5 \equiv n \pmod 5$, donc $n^5 - n \equiv 0 \pmod 5$.
— **Conclusion** : 5 divise $n^5 - n$ pour tout entier n.

Contrôles. $n = 2$: $32 - 2 = 30 = 5 \times 6$ ✓ · $n = 3$: $243 - 3 = 240 = 5 \times 48$ ✓.

Pour aller plus loin. $n^5 - n$ est en réalité divisible par 30.

— Par Fermat avec $p = 2$: $2 \mid n^2 - n$, et $n^5 - n = n(n^4 - 1)$ est pair (l'un des facteurs n, $n - 1$ l'est).
— Par Fermat avec $p = 3$: $n^3 \equiv n$, donc $n^5 = n^3 \times n^2 \equiv n \times n^2 = n^3 \equiv n \pmod 3$.
— 2, 3 et 5 étant premiers entre eux deux à deux, leur produit 30 divise $n^5 - n$. Contrôle : $n = 4$ donne $1\,020 = 30 \times 34$ ✓.

Réponse. $n^5 \equiv n \pmod 5$, donc $5 \mid (n^5 - n)$ (et même 30).

Correction de l'exercice 9 – Divisibilité par un premier quelconque

On applique le corollaire du petit théorème de Fermat avec $a = 2$:

— $2^p \equiv 2 \pmod{p}$, donc $p \mid \left(2^p - 2\right)$.

— Aucune hypothèse supplémentaire n'est nécessaire : si $p = 2$, $2^2 - 2 = 2$ est bien divisible par 2 ✓.

Vérification pour $p = 11$.

— $2^{11} = 2\,048$, donc $2^{11} - 2 = 2\,046$.

— $2\,046 = 11 \times 186$ ✓.

Attention à la réciproque. Le fait que $n \mid 2^n - 2$ **ne prouve pas** que n est premier.

— Contre-exemple : $n = 341 = 11 \times 31$ vérifie $2^{341} \equiv 2 \pmod{341}$ alors qu'il est composé.

— On dit que 341 est un **pseudo-premier de base 2** — c'est l'objet de l'exercice suivant.

Réponse. $2^p \equiv 2 \pmod{p}$; pour $p = 11$: $2\,046 = 11 \times 186$.

Correction de l'exercice 10 – Un test de primalité qui échoue

a) $2^{10} = 1\,024$ et $1\,024 = 341 \times 3 + 1$, donc $2^{10} \equiv 1 \pmod{341}$.

— Comme $340 = 10 \times 34$:

$$2^{340} = \left(2^{10}\right)^{34} \equiv 1^{34} = 1 \pmod{341}$$

— La conclusion du petit théorème de Fermat est donc vérifiée pour $a = 2$.

b) Pourtant $341 = 11 \times 31$: **il n'est pas premier**.

— On le voit en testant les premiers jusqu'à $\sqrt{341} \approx 18,5$: $341 = 11 \times 31$.

— **Ce que cela prouve** : la réciproque du petit théorème de Fermat est **fausse**. La congruence $a^{n-1} \equiv 1 \pmod{n}$ ne garantit pas que n soit premier.

— **Ce que le test permet quand même** : si l'on trouve un a tel que $a^{n-1} \not\equiv 1 \pmod{n}$, alors n n'est **certainement pas** premier. Ici, avec $a = 3$: $3^{340} \not\equiv 1 \pmod{341}$, ce qui démasque 341.

— Les nombres composés qui passent le test pour **toutes** les bases s'appellent les **nombres de Carmichael** ; le plus petit est 561.

Réponse. a) $1\,024 = 341 \times 3 + 1$ · b) $341 = 11 \times 31$: la réciproque de Fermat est fausse.

Correction de l'exercice 11 – Somme de deux puissances

On traite séparément les deux termes, avec Fermat pour chacun (7 est premier et ne divise ni 3 ni 4).

Premier terme.

— $3^6 \equiv 1 \pmod{7}$ et $2\,026 = 6 \times 337 + 4$, donc $3^{2026} \equiv 3^4 = 81 \equiv 4 \pmod{7}$.

Second terme.

— $4^6 \equiv 1 \pmod{7}$ et $2\,026 \equiv 4 \pmod{6}$, donc $4^{2026} \equiv 4^4 \pmod{7}$.

— $4^2 = 16 \equiv 2$, donc $4^4 \equiv 2^2 = 4 \pmod{7}$.

Somme.

— $3^{2026} + 4^{2026} \equiv 4 + 4 = 8 \equiv 1 \pmod{7}$.

— **Conclusion** : le reste est 1.
— Contrôle sur un petit exposant de même reste modulo 6 :
$3^4 + 4^4 = 81 + 256 = 337 = 7 \times 48 + 1$ ✓.

Réponse. $3^{2026} + 4^{2026} \equiv 1 \pmod 7$.

Correction de l'exercice 12 – Les racines carrées de 1

On factorise, puis on utilise le **lemme d'Euclide** (un premier qui divise un produit divise l'un des facteurs).

— $x^2 \equiv 1 \pmod p$ signifie $p \mid \left(x^2 - 1\right)$, c'est-à-dire $p \mid (x-1)(x+1)$.
— p étant **premier**, il divise $x - 1$ ou $x + 1$.
— Donc $x \equiv 1 \pmod p$ ou $x \equiv -1 \pmod p$.

Contre-exemple modulo 8 (qui n'est pas premier) :

$x \equiv$	1	3	5	7
$x^2 \equiv$	1	1	1	1

— $3^2 = 9 \equiv 1$ et $5^2 = 25 \equiv 1 \pmod 8$, alors que $3 \not\equiv \pm 1 \pmod 8$.
— **La primalité est donc essentielle** : c'est elle qui empêche un produit d'être nul sans qu'un facteur le soit.
— Cette propriété est le cœur des tests de primalité modernes, qui cherchent précisément des « racines carrées de 1 » inattendues.

Réponse. $p \mid (x-1)(x+1)$ et p premier donne $x \equiv \pm 1$; modulo 8, 3 et 5 conviennent aussi.

Correction de l'exercice 13 – Un chiffre des unités lointain

a) Le chiffre des unités, c'est le reste modulo 10. On cherche le cycle des puissances de 3 :

n	1	2	3	4	5
$3^n \pmod{10}$	3	9	7	1	3

— Le cycle a pour longueur 4 : 3, 9, 7, 1.
— $2\,026 = 4 \times 506 + 2$, donc $3^{2026} \equiv 3^2 = 9 \pmod{10}$.
— **Le chiffre des unités est** 9**.**

b) Non, pas directement : 10 **n'est pas premier**, donc le petit théorème de Fermat ne s'applique pas.

— On peut cependant l'utiliser en coulisses : $10 = 2 \times 5$, et modulo 5 Fermat donne $3^4 \equiv 1$; modulo 2, $3 \equiv 1$. Le cycle de longueur 4 que l'on observe n'est donc pas un hasard.
— **La règle de prudence** : avant d'écrire « d'après le petit théorème de Fermat », toujours vérifier que le module est premier.

Réponse. a) 9 · b) non, 10 n'est pas premier ; on passe par le cycle des puissances.

Correction de l'exercice 14 – Une clé de contrôle modulo 97

a) 97 est premier et $97 \nmid a$: d'après le petit théorème de Fermat,

$$a^{96} \equiv 1 \pmod{97}$$

— Le résultat vaut **toujours** 1, quelle que soit la donnée a.

b) Non, un tel système est inutilisable : toutes les données donnent le même résultat, il est impossible de retrouver a.

— **Avec l'exposant** 7, en revanche, la transformation qui à a associe a^7 est **inversible**.

— On cherche un exposant d tel que $\left(a^7\right)^d = a^{7d} \equiv a \pmod{97}$, c'est-à-dire $7d \equiv 1 \pmod{96}$.

— Inverse de 7 modulo 96 : $7 \times 55 = 385 = 96 \times 4 + 1$, donc $d = 55$.

— On retrouve alors a en élevant à la puissance 55 : c'est **exactement le principe du chiffrement RSA**, où le module est le produit de deux très grands nombres premiers.

— Vérification du mécanisme : $a^{7\times 55} = a^{385} = \left(a^{96}\right)^4 \times a \equiv 1^4 \times a = a \pmod{97}$ ✓.

Réponse. a) toujours 1 · b) inutilisable ; avec l'exposant 7, on déchiffre par l'exposant 55 (car $7 \times 55 \equiv 1 \pmod{96}$).

Correction de l'exercice 15 – Bilan : Fermat en trois questions

a) 19 est premier et ne divise pas 5 : $5^{18} \equiv 1 \pmod{19}$.

— $2\,026 = 18 \times 112 + 10$ (car $18 \times 112 = 2\,016$), donc $5^{2026} \equiv 5^{10} \pmod{19}$.

— $5^2 = 25 \equiv 6$; $5^4 \equiv 6^2 = 36 \equiv 17 \equiv -2$; $5^8 \equiv (-2)^2 = 4$.

— $5^{10} = 5^8 \times 5^2 \equiv 4 \times 6 = 24 \equiv 5 \pmod{19}$.

— **Le reste est** 5**.**

b) 13 est premier : le corollaire du petit théorème de Fermat donne directement $n^{13} \equiv n \pmod{13}$ pour tout entier n.

— Donc $13 \mid \left(n^{13} - n\right)$, y compris lorsque 13 divise n (les deux termes sont alors multiples de 13).

— Contrôle : $n = 2$ donne $8\,192 - 2 = 8\,190 = 13 \times 630$ ✓.

c) 23 est premier et $23 \nmid 8$: on cherche l'inverse de 8 modulo 23.

— De tête : $8 \times 3 = 24 \equiv 1 \pmod{23}$, donc $8^{-1} \equiv 3$.

— On multiplie : $x \equiv 3 \times 3 = 9 \pmod{23}$.

— **Vérification** : $8 \times 9 = 72 = 23 \times 3 + 3 \equiv 3 \pmod{23}$ ✓.

— Par la formule de Fermat, on aurait calculé $8^{21} \pmod{23}$: beaucoup plus long pour le même résultat.

Réponse. a) 5 · b) $n^{13} \equiv n \pmod{13}$ · c) $x \equiv 9 \pmod{23}$.