Plaquette 1 – Primalité, décomposition et petit théorème de Fermat

Nombres premiers — Terminale maths expertes

Corrections détaillées

Boîte à outils

Définitions et théorèmes du cours.

— Un entier $p \geq 2$ est **premier** s'il n'admet que deux diviseurs positifs : 1 et p. (1 n'est pas premier.)

— **Test de primalité** : si n n'est divisible par aucun nombre premier $p \leq \sqrt{n}$, alors n est premier.

— **Théorème fondamental** : tout entier $n \geq 2$ s'écrit de façon **unique** (à l'ordre près) comme produit de facteurs premiers :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_k^{\alpha_k}$$

— **Nombre de diviseurs** de n : $(\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1)$.

— **PGCD par décomposition** : produit des facteurs communs affectés du **plus petit** exposant ; **PPCM** : tous les facteurs affectés du **plus grand** exposant.

— **Lemme d'Euclide** : si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

— **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 a : $a^p \equiv a \pmod{p}$.

— Il existe une **infinité** de nombres premiers (démonstration d'Euclide par l'absurde).

Correction de l'exercice 1 – Tester la primalité

Critère du cours : on teste les nombres premiers jusqu'à $\sqrt{n}$.

— a) $\sqrt{91} \approx 9{,}5$: on teste 2, 3, 5, 7. Or $91 = 7 \times 13$: **non premier**.

— b) $\sqrt{97} \approx 9{,}8$: on teste 2, 3, 5, 7. Aucun ne divise 97 (il est impair, la somme des chiffres vaut 16, il ne finit pas par 0 ou 5, et $97 = 7 \times 13 + 6$). Donc 97 est **premier**.

— c) $\sqrt{221} \approx 14{,}9$: on teste 2, 3, 5, 7, 11, 13. Or $221 = 13 \times 17$: **non premier**.

— **Intérêt du critère** : pour 221, il suffit de six essais au lieu de 219.

Réponse. a) non (7×13) · b) oui · c) non (13×17).

Correction de l'exercice 2 – Décomposer en facteurs premiers

On divise successivement par les nombres premiers croissants.

— a) $360 = 2 \times 180 = 2^2 \times 90 = 2^3 \times 45 = 2^3 \times 3^2 \times 5$.

— b) 1 001 est impair ; $1\,001 = 7 \times 143 = 7 \times 11 \times 13$.

— c) $2\,025 = 5 \times 405 = 5^2 \times 81 = 5^2 \times 3^4$.

— Contrôles : $8 \times 9 \times 5 = 360$; $7 \times 11 \times 13 = 1\,001$; $25 \times 81 = 2\,025$. Correct.

Réponse. a) $2^3 \times 3^2 \times 5$ · b) $7 \times 11 \times 13$ · c) $3^4 \times 5^2$.

Correction de l'exercice 3 – Compter les diviseurs

Formule du cours : si $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, le nombre de diviseurs vaut $(\alpha_1 + 1)\cdots(\alpha_k + 1)$.

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).

— a) $360 = 2^3 \times 3^2 \times 5^1$, donc $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$ diviseurs.
— b) $2\,025 = 3^4 \times 5^2$, donc $(4+1)(2+1) = 5 \times 3 = 15$ diviseurs.
— Justification : un diviseur s'obtient en choisissant, pour chaque facteur premier, un exposant entre 0 et α_i — soit $\alpha_i + 1$ possibilités indépendantes.

Réponse. a) 24 diviseurs · b) 15 diviseurs.

Correction de l'exercice 4 – PGCD et PPCM par décomposition

a) PGCD : facteurs **communs**, plus **petit** exposant.

— Communs : 2 (exposants 3 et 2 → on garde 2^2) et 3 (exposants 2 et 1 → on garde 3).
— pgcd $= 2^2 \times 3 = 12$.

b) PPCM : **tous** les facteurs, plus **grand** exposant.

-

$$\text{ppcm} = 2^3 \times 3^2 \times 5 \times 7 = 8 \times 9 \times 35 = 2\,520$$

c) $a = 360$ et $b = 84$, donc $ab = 30\,240$.

— Et pgcd × ppcm $= 12 \times 2\,520 = 30\,240$. La relation est vérifiée.

Réponse. a) 12 · b) 2 520 · c) $12 \times 2\,520 = 30\,240 = 360 \times 84$.

Correction de l'exercice 5 – Lemme d'Euclide

a) **Lemme d'Euclide** : si p est premier et si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

b) 7 est premier et $7 \mid 5 \times n$. Comme $7 \nmid 5$, on conclut $7 \mid n$.

c) **Non.** Contre-exemple : $6 \mid 4 \times 3 = 12$, mais $6 \nmid 4$ et $6 \nmid 3$.

— La **primalité** est donc essentielle : c'est elle qui interdit au diviseur de se « répartir » entre les deux facteurs.

Réponse. b) $7 \mid n$ · c) non ($6 \mid 4 \times 3$ mais 6 ne divise ni 4 ni 3).

Correction de l'exercice 6 – Petit théorème de Fermat

a) **Petit théorème de Fermat** : si p est premier et si $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.

b) $p = 11$ est premier et $11 \nmid 2$, donc $2^{10} \equiv 1 \pmod{11}$.

— Contrôle : $2^{10} = 1\,024 = 11 \times 93 + 1$. Correct.
— $p = 7$ est premier et $7 \nmid 3$, donc $3^6 \equiv 1 \pmod{7}$.
— Contrôle : $3^6 = 729 = 7 \times 104 + 1$. Correct.

Réponse. b) $2^{10} \equiv 1 \pmod{11}$ et $3^6 \equiv 1 \pmod{7}$.

Correction de l'exercice 7 – Reste d'une grande puissance

On applique le petit théorème de Fermat avec $p = 11$.

— $2^{10} \equiv 1 \pmod{11}$.
— On divise l'exposant par 10 : $2\,026 = 10 \times 202 + 6$.

$$2^{2026} = \left(2^{10}\right)^{202} \times 2^6 \equiv 1^{202} \times 2^6 = 64 \pmod{11}$$

— Enfin $64 = 11 \times 5 + 9$, donc $2^{2026} \equiv 9 \pmod{11}$.
— Le reste est 9.

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).

Réponse. Le reste est 9.

Correction de l'exercice 8 – Utiliser Fermat pour une divisibilité

On utilise le **corollaire** du petit théorème de Fermat : pour p premier et **tout** entier a,

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

— Ici $p = 13$ est premier, donc $a^{13} \equiv a \pmod{13}$.
— Donc $a^{13} - a \equiv 0 \pmod{13}$, c'est-à-dire $13 \mid \left(a^{13} - a\right)$.
— Remarque sur les deux cas : si $13 \mid a$, les deux termes sont divisibles par 13 ; sinon, Fermat donne $a^{12} \equiv 1$, donc $a^{13} \equiv a$. La conclusion est la même.
— Contrôle avec $a = 2$: $2^{13} - 2 = 8\,192 - 2 = 8\,190 = 13 \times 630$. Correct.

Réponse. $a^{13} \equiv a \pmod{13}$, donc $13 \mid (a^{13} - a)$.

Correction de l'exercice 9 – Nombres premiers entre eux

On utilise la propriété : tout diviseur commun divise toute combinaison linéaire.

— **Premier cas** : soit d un diviseur commun de n et $n + 1$. Alors $d \mid ((n + 1) - n) = 1$, donc $d = 1$.
— Ainsi $\text{pgcd}(n\,;n + 1) = 1$: deux entiers **consécutifs** sont toujours premiers entre eux.
— **Second cas** : soit d un diviseur commun de n et $2n + 1$. Alors $d \mid ((2n + 1) - 2n) = 1$, donc $d = 1$.
— Contrôle pour $n = 6$: $\text{pgcd}(6\,;7) = 1$ et $\text{pgcd}(6\,;13) = 1$. Cohérent.

Réponse. Dans les deux cas, un diviseur commun divise 1, donc le PGCD vaut 1.

Correction de l'exercice 10 – Infinité des nombres premiers

On raisonne **par l'absurde**.

— $N \geq 2$, donc N admet au moins un diviseur premier p ; d'après l'hypothèse, p est l'un des p_i.
— Or p_i divise le produit $p_1 p_2 \cdots p_k$. Si p_i divisait aussi N, il diviserait la différence $N - p_1 \cdots p_k = 1$ — ce qui est impossible pour un nombre premier (qui est ≥ 2).
— **Contradiction** : l'hypothèse d'un nombre fini de premiers est donc fausse.
— Conclusion : il existe une **infinité** de nombres premiers.
— Illustration : avec $\{2\,;3\,;5\}$, on obtient $N = 31$, qui est premier et n'est pas dans la liste.

Réponse. N n'est divisible par aucun p_i (sinon $p_i \mid 1$) : contradiction, donc l'infinité.

Correction de l'exercice 11 – Décomposition et carré parfait

a) $1\,176 = 2 \times 588 = 2^2 \times 294 = 2^3 \times 147 = 2^3 \times 3 \times 49 = 2^3 \times 3 \times 7^2$.

b) Un entier est un **carré parfait** si et seulement si tous les exposants de sa décomposition sont **pairs**.

— Ici : 2^3 (exposant impair), 3^1 (impair), 7^2 (pair). Donc 1 176 n'est pas un carré parfait.
— Pour rendre tous les exposants pairs, il faut multiplier par $2 \times 3 = 6$.
— Contrôle : $1\,176 \times 6 = 7\,056 = 2^4 \times 3^2 \times 7^2 = \left(2^2 \times 3 \times 7\right)^2 = 84^2$. Correct.

Réponse. a) $2^3 \times 3 \times 7^2$ · b) non ; multiplier par 6 donne $7\,056 = 84^2$.

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).

Correction de l'exercice 12 – Diviseurs et problème concret

a) $84 = 2^2 \times 3 \times 7$.

— Nombre de diviseurs : $(2+1)(1+1)(1+1) = 12$.
— Liste : 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84.

b) On retient les diviseurs compris entre 5 et 15 : 6, 7, 12 et 14.

— Cela correspond respectivement à 14, 12, 7 et 6 groupes.
— Contrôle : $6 \times 14 = 84$, $7 \times 12 = 84$, $12 \times 7 = 84$, $14 \times 6 = 84$. Correct.

Réponse. b) Groupes de 6, 7, 12 ou 14 élèves.

Correction de l'exercice 13 – Crible d'Ératosthène

a) On écrit les entiers de 2 à 50. On garde 2 et on barre ses multiples, puis on garde le premier nombre non barré, 3, et on barre ses multiples, et ainsi de suite avec 5 puis 7. Il reste :

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47$$

soit 15 nombres premiers.

b) Un entier composé $n \leq 50$ s'écrit $n = ab$ avec $2 \leq a \leq b$; alors $a^2 \leq ab = n \leq 50$, donc $a \leq 7$, puisque $8^2 = 64 > 50$. Tout nombre composé jusqu'à 50 a donc un diviseur premier parmi 2, 3, 5, 7, et il a déjà été barré. **Contrôle** : $49 = 7 \times 7$ est barré avec les multiples de 7.

Réponse. a) $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ · b) un nombre composé ≤ 50 a un facteur premier ≤ 7, car $8^2 > 50$.

Correction de l'exercice 14 – Choisir un nombre par son nombre de diviseurs

Un diviseur positif de $2^a \times 3^b$ s'écrit $2^i \times 3^j$ avec $0 \leq i \leq a$ et $0 \leq j \leq b$: il y a $a+1$ choix pour i et $b+1$ pour j. Le nombre de diviseurs vaut donc

$$(a+1)(b+1) = 12$$

Avec $a+1 \geq 2$ et $b+1 \geq 2$, les décompositions de 12 sont 2×6, 3×4, 4×3 et 6×2, ce qui donne :

— $(a\,;b) = (1\,;5)$: $n = 2 \times 243 = 486$;
— $(a\,;b) = (2\,;3)$: $n = 4 \times 27 = 108$;
— $(a\,;b) = (3\,;2)$: $n = 8 \times 9 = 72$;
— $(a\,;b) = (5\,;1)$: $n = 32 \times 3 = 96$.

La plus petite valeur est 72. **Contrôle** : les diviseurs de 72 sont $1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72$, soit bien 12.

Réponse. 486, 108, 72 et 96 ; la plus petite est $72 = 2^3 \times 3^2$.

Correction de l'exercice 15 – Synthèse : reste et Fermat

a) $p = 7$ est premier et $7 \nmid 5$: par Fermat, $5^6 \equiv 1 \pmod 7$.

— $100 = 6 \times 16 + 4$, donc $5^{100} \equiv 5^4 \pmod 7$.
— $5^2 = 25 \equiv 4$, donc $5^4 \equiv 4^2 = 16 \equiv 2 \pmod 7$.
— Le reste est 2.

b) $p = 13$ est premier et $13 \nmid 5$: $5^{12} \equiv 1 \pmod{13}$.

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).

— $100 = 12 \times 8 + 4$, donc $5^{100} \equiv 5^4 \pmod{13}$.
— $5^2 = 25 \equiv 12 \equiv -1 \pmod{13}$, donc $5^4 \equiv (-1)^2 = 1 \pmod{13}$.
— Le reste est 1.
— **Astuce utilisée** : remplacer 12 par -1 simplifie beaucoup le calcul de la puissance.

Réponse. a) 2 · b) 1.

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).