

Plaque 2 - Primalité, crible et décomposition en facteurs premiers

Nombres premiers — Terminale maths expertes

Corrections détaillées

Boîte à outils

Définitions, théorèmes et méthodes.

- Un entier $p \geq 2$ est **premier** s'il n'a que deux diviseurs positifs, 1 et lui-même. 1 **n'est pas** premier ; 2 est le seul premier pair.
- **Test de primalité** : si aucun nombre premier $p \leq \sqrt{n}$ ne divise n , alors n est premier.
- **Pourquoi $\sqrt{n}$ suffit** : si $n = ab$ avec $1 < a \leq b$, alors $a^2 \leq ab = n$, donc $a \leq \sqrt{n}$. Le plus petit facteur est toujours sous la racine.
- **Crible d'Ératosthène** : on écrit les entiers de 2 à N , on garde 2 et on raye ses multiples, puis on garde le premier non rayé et on recommence, jusqu'à $\sqrt{N}$.
- **Théorème fondamental de l'arithmétique** : tout entier $n \geq 2$ s'écrit de manière unique, à l'ordre près,

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

- **Méthode de décomposition** : on divise par 2 tant que c'est possible, puis par 3, 5, 7, 11... en s'arrêtant dès que le quotient est premier.
- **Nombre de diviseurs** : $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ — on choisit indépendamment l'exposant de chaque facteur premier, de 0 à α_i .
- **Carré parfait** : n est un carré si et seulement si **tous** les exposants de sa décomposition sont pairs ; **cube parfait** : tous multiples de 3.

Correction de l'exercice 1 - Tester la primalité

Le test : il suffit d'essayer les nombres premiers inférieurs ou égaux à $\sqrt{n}$.

a) $\sqrt{211} \approx 14,5$: on teste 2, 3, 5, 7, 11, 13.

- 211 est impair ; $2 + 1 + 1 = 4$ n'est pas multiple de 3 ; il ne finit ni par 0 ni par 5.
- $211 = 7 \times 30 + 1$; $211 = 11 \times 19 + 2$; $211 = 13 \times 16 + 3$.
- Aucun ne divise 211 : 211 **est premier**.

b) $\sqrt{221} \approx 14,9$: mêmes candidats.

- $221 = 13 \times 17$: 221 **n'est pas premier**.
- On le trouve au test de 13 ; les tests précédents échouaient tous.

c) $\sqrt{323} \approx 18$: on teste jusqu'à 17.

- $323 = 17 \times 19$: 323 **n'est pas premier**.
- **La morale** : un nombre « qui a l'air premier » peut être le produit de deux premiers proches. Il faut aller jusqu'à $\sqrt{n}$, pas s'arrêter aux premiers essais.

Réponse. a) premier · b) $221 = 13 \times 17$ · c) $323 = 17 \times 19$.

Correction de l'exercice 2 - Le crible d'Ératosthène

a) On écrit les entiers de 2 à 60, puis on raye successivement les multiples de 2, de 3, de 5 et de 7 (autres que ces nombres eux-mêmes).

- Après la rayure des multiples de 2 : il reste 2 et les impairs.
- Multiples de 3 : on raye 9, 15, 21, 27, 33, 39, 45, 51, 57.
- Multiples de 5 : on raye 25, 35, 55 (les autres l'étaient déjà).
- Multiples de 7 : on raye 49 (les autres l'étaient déjà).

Les nombres restants sont les **17 premiers** inférieurs à 60 :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59

b) Il suffit de rayer les multiples des premiers $p \leq \sqrt{60} \approx 7,7$, donc 2, 3, 5 et 7.

- **Justification** : si un nombre $n \leq 60$ n'est pas premier, il s'écrit $n = ab$ avec $1 < a \leq b$, donc $a \leq \sqrt{n} \leq \sqrt{60}$: il a déjà été rayé comme multiple d'un premier ≤ 7 .

Réponse. a) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 · b) jusqu'à 7, car $7 \leq \sqrt{60} < 11$.

Correction de l'exercice 3 - Un grand test de primalité

a) Supposons $n \geq 2$ non premier : il s'écrit $n = ab$ avec $1 < a \leq b < n$.

- Si l'on avait $a > \sqrt{n}$, alors $b \geq a > \sqrt{n}$, donc $ab > n$: contradiction.
- Donc $a \leq \sqrt{n}$. Or $a \geq 2$ admet un diviseur premier p , et $p \leq a \leq \sqrt{n}$.
- Comme $p \mid a$ et $a \mid n$, la transitivité donne $p \mid n$.

b) $\sqrt{2027} \approx 45,02$: il suffit de tester les premiers jusqu'à 43.

p	2	3	5	7	11	13	17
Reste de 2027	1	2	2	4	3	12	4

p	19	23	29	31	37	41	43
Reste de 2027	13	3	26	12	29	18	6

- Détail de trois calculs : $2027 = 7 \times 289 + 4$; $2027 = 17 \times 119 + 4$; $2027 = 43 \times 47 + 6$.
- Les critères usuels règlent les premiers cas : 2027 est impair, $2 + 0 + 2 + 7 = 11$ n'est pas multiple de 3, et il ne finit ni par 0 ni par 5.
- Aucun reste n'est nul : 2027 **est premier**.

Réponse. a) le plus petit facteur est $\leq \sqrt{n}$ · b) aucun premier ≤ 43 ne divise 2027 : il est premier.

Correction de l'exercice 4 - Décomposer en facteurs premiers

On divise successivement par 2, 3, 5, 7, ... jusqu'à obtenir 1.

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

$$360 = 2^3 \times 3^2 \times 5$$

b) 1001 est impair, la somme de ses chiffres vaut 2, il ne finit pas par 0 ni 5 : on essaie 7.

- $1001 = 7 \times 143$, puis $143 = 11 \times 13$.
- $1001 = 7 \times 11 \times 13$ — une décomposition à connaître, elle explique le critère de divisibilité par 7, 11 et 13 des nombres $\overline{abcabc}$.

c) 2025 finit par 25 : il est divisible par 25.

— $2025 = 25 \times 81 = 5^2 \times 3^4$.

— Tous les exposants sont pairs : 2 025 est un **carré parfait**, celui de $5 \times 3^2 = 45$. En effet $45^2 = 2\,025$ ✓.

d) $5\,040 = 2 \times 2\,520 = 2^2 \times 1\,260 = 2^3 \times 630 = 2^4 \times 315 = 2^4 \times 3^2 \times 35$.

— $5\,040 = 2^4 \times 3^2 \times 5 \times 7$ (c'est 7!, le produit des entiers de 1 à 7).

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

Correction de l'exercice 5 - L'année 2026

a) 2 026 est pair : $2\,026 = 2 \times 1\,013$.

— Pour 1 013 : $\sqrt{1\,013} \approx 31,8$, on teste les premiers jusqu'à 31.

— Il est impair ; $1 + 0 + 1 + 3 = 5$ n'est pas multiple de 3 ; il ne finit pas par 0 ou 5.

— $1\,013 = 7 \times 144 + 5$; $= 11 \times 92 + 1$; $= 13 \times 77 + 12$; $= 17 \times 59 + 10$; $= 19 \times 53 + 6$;
 $= 23 \times 44 + 1$; $= 29 \times 34 + 27$; $= 31 \times 32 + 21$.

— Aucun ne convient : 1 013 est premier, donc $2\,026 = 2 \times 1\,013$.

b) Un diviseur s'obtient en choisissant l'exposant de chaque facteur premier :

— exposant de 2 dans $\{0; 1\}$, exposant de 1 013 dans $\{0; 1\}$: $2 \times 2 = 4$ diviseurs.

— Liste : 1, 2, 1 013 et 2 026.

— **Remarque** : 2 026 est donc le double d'un nombre premier, ce qui en fait un entier très « pauvre » en diviseurs — à l'opposé de $2\,024 = 2^3 \times 11 \times 23$, qui en a 16.

Réponse. a) $2\,026 = 2 \times 1\,013$ · b) 1, 2, 1 013, 2 026.

Correction de l'exercice 6 - Compter les diviseurs

a) $360 = 2^3 \times 3^2 \times 5^1$.

— Nombre de diviseurs : $(3 + 1)(2 + 1)(1 + 1) = 4 \times 3 \times 2 = 24$.

b) $2\,025 = 3^4 \times 5^2$: $(4 + 1)(2 + 1) = 15$ diviseurs.

— $5\,040 = 2^4 \times 3^2 \times 5 \times 7$: $(4 + 1)(2 + 1)(1 + 1)(1 + 1) = 5 \times 3 \times 2 \times 2 = 60$ diviseurs.

c) **Justification de la formule.** Un diviseur de $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ s'écrit $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$.

— Pour chaque facteur premier, il y a $\alpha_i + 1$ choix d'exposant, et ces choix sont indépendants.

— Le produit $(\alpha_1 + 1) \cdots (\alpha_k + 1)$ compte donc exactement les diviseurs, chacun une seule fois — c'est l'**unicité** de la décomposition qui garantit qu'on ne compte pas deux fois le même.

— **Remarque** : un nombre de diviseurs **impair** signale un carré parfait, car il faut alors que tous les $\alpha_i + 1$ soient impairs. C'est bien le cas de $2\,025 = 45^2$ ✓.

Réponse. a) 24 · b) 15 et 60 · c) $(\alpha_1 + 1) \cdots (\alpha_k + 1)$, un choix d'exposant par facteur.

Correction de l'exercice 7 - Le plus petit entier à 12 diviseurs

On cherche une décomposition $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ telle que $(\alpha_1 + 1) \cdots (\alpha_k + 1) = 12$.

On liste les factorisations de 12, et pour chacune on affecte les **plus grands exposants aux plus petits premiers** — c'est ce qui minimise n :

Exposants	Forme	Plus petit n
12	p^{11}	$2^{11} = 2\,048$
6×2	$p^5 q$	$2^5 \times 3 = 96$
4×3	$p^3 q^2$	$2^3 \times 3^2 = 72$
$3 \times 2 \times 2$	$p^2 q r$	$2^2 \times 3 \times 5 = 60$
$2 \times 2 \times 3$	$p q r^2$	$2 \times 3 \times 5^2 = 150$

- Le minimum est atteint pour $60 = 2^2 \times 3 \times 5$.
- **Vérification** : $(2+1)(1+1)(1+1) = 12$ ✓, et les diviseurs de 60 sont 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60 : il y en a bien 12.
- **Conclusion** : le plus petit entier à 12 diviseurs est 60. C'est d'ailleurs pour cette richesse en diviseurs que 60 sert d'unité de temps et d'angle depuis les Babyloniens.

Réponse. $60 = 2^2 \times 3 \times 5$.

Correction de l'exercice 8 - Exactement trois diviseurs

Soit n un tel entier, de décomposition $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

- Son nombre de diviseurs est $(\alpha_1 + 1) \cdots (\alpha_k + 1) = 3$.
- 3 est **premier** : ce produit ne peut avoir qu'un seul facteur différent de 1, donc $k = 1$ et $\alpha_1 + 1 = 3$.
- Ainsi $n = p^2$ avec p premier.

Réciproque. Si $n = p^2$ avec p premier, ses diviseurs sont 1, p et p^2 : il y en a exactement trois ✓.

Conclusion. Les entiers à trois diviseurs sont exactement les **carrés de nombres premiers** :

- $4 = 2^2$, $9 = 3^2$, $25 = 5^2$, $49 = 7^2$, $121 = 11^2$, ...
- **Le même raisonnement** montre que les entiers à exactement deux diviseurs sont les nombres premiers, et ceux à quatre diviseurs sont les p^3 et les pq (avec $p \neq q$ premiers).

Réponse. Les carrés de nombres premiers : 4, 9, 25, 49, 121, ...

Correction de l'exercice 9 - La forme $6k \pm 1$

a) Tout entier s'écrit $6k + r$ avec $r \in \{0; 1; 2; 3; 4; 5\}$. On élimine les cas impossibles pour un premier $p > 3$:

$p =$	$6k$	$6k + 1$	$6k + 2$	$6k + 3$	$6k + 4$	$6k + 5$
Divisible par	6	—	2	3	2	—

- Si $r = 0$, 2 ou 4, alors p est pair et $p > 3$: il n'est pas premier.
- Si $r = 3$, alors $p = 3(2k + 1)$ est divisible par 3 et $p > 3$: pas premier non plus.
- Il ne reste que $p = 6k + 1$ ou $p = 6k + 5 = 6(k + 1) - 1$, c'est-à-dire $6k \pm 1$.

b) **Non**, la réciproque est fausse.

- $25 = 6 \times 4 + 1$ n'est pas premier ; $35 = 6 \times 6 - 1$ non plus ($35 = 5 \times 7$).
- La condition est **nécessaire** mais pas suffisante : elle sert à accélérer un test de primalité (on ne teste que les diviseurs de la forme $6k \pm 1$), pas à conclure.

Réponse. a) les restes 0, 2, 3, 4 modulo 6 sont exclus · b) non : 25 et 35.

Correction de l'exercice 10 - Un faux nombre premier

a) 1 729 est impair, $1 + 7 + 2 + 9 = 19$ n'est pas multiple de 3, il ne finit pas par 0 ou 5.

— On essaie 7 : $1\,729 = 7 \times 247$.

— Puis 247 : il n'est divisible ni par 2, ni par 3, ni par 5, ni par 7 ($247 = 7 \times 35 + 2$), ni par 11 ($2 - 4 + 7 = 5$), mais $247 = 13 \times 19$.

— Donc $1\,729 = 7 \times 13 \times 19$.

b) Trois facteurs premiers distincts à l'exposant 1 :

— Nombre de diviseurs : $(1 + 1)(1 + 1)(1 + 1) = 8$.

— Liste : 1, 7, 13, 19, 91, 133, 247, 1 729.

— **Anecdote** : 1 729 est le « nombre de Hardy-Ramanujan », le plus petit entier qui s'écrit de deux façons comme somme de deux cubes :

$$1\,729 = 1^3 + 12^3 = 9^3 + 10^3$$

— Vérification : $1 + 1\,728 = 1\,729 \checkmark$ et $729 + 1\,000 = 1\,729 \checkmark$.

Réponse. a) $1\,729 = 7 \times 13 \times 19$ · b) 8 diviseurs.

Correction de l'exercice 11 - Rendre un produit carré

a) $360 = 2^3 \times 3^2 \times 5$. Un carré parfait a **tous ses exposants pairs**.

— Exposant de 2 : 3, impair → il manque un facteur 2.

— Exposant de 3 : 2, déjà pair → rien à ajouter.

— Exposant de 5 : 1, impair → il manque un facteur 5.

— Donc $k = 2 \times 5 = 10$, et $360 \times 10 = 3\,600 = 2^4 \times 3^2 \times 5^2$.

— **Vérification** : $3\,600 = 60^2 \checkmark$.

b) $500 = 2^2 \times 5^3$. Un cube parfait a tous ses exposants **multiples de 3**.

— Exposant de 2 : 2 → il faut atteindre 3, donc un facteur 2.

— Exposant de 5 : 3 → déjà multiple de 3.

— Donc $m = 2$, et $500 \times 2 = 1\,000 = 2^3 \times 5^3 = 10^3 \checkmark$.

— **La méthode générale** : on complète chaque exposant jusqu'au multiple de 2 (ou de 3) immédiatement supérieur.

Réponse. a) $k = 10$ ($3\,600 = 60^2$) · b) $m = 2$ ($1\,000 = 10^3$).

Correction de l'exercice 12 - Le contre-exemple de Mersenne

a) $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$: tous premiers.

— On pourrait croire que $2^p - 1$ est premier dès que p l'est.

b) $2^{11} - 1 = 2\,048 - 1 = 2\,047$.

— $\sqrt{2\,047} \approx 45,2$. On teste : $2\,047 = 23 \times 89$.

— 2 047 **n'est pas premier**, alors que 11 l'est : la conjecture de a) est **fausse**.

c) Supposons $n = ab$ avec $1 < a < n$ et $1 < b < n$. On utilise l'identité

$$x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \dots + x + 1)$$

— Avec $x = 2^a$: $2^n - 1 = (2^a)^b - 1$ est divisible par $2^a - 1$.

- Or $1 < 2^a - 1 < 2^n - 1$ (car $1 < a < n$) : on a trouvé un diviseur strict, donc $2^n - 1$ n'est pas premier.
- **Conclusion** : « n premier » est **nécessaire** pour que $2^n - 1$ soit premier, mais pas suffisant — c'est exactement ce que montre $n = 11$.

Réponse. a) 3, 7, 31, 127, tous premiers · b) $2\,047 = 23 \times 89$ · c) $2^a - 1$ divise $2^{ab} - 1$.

Correction de l'exercice 13 - Des rectangles d'aire imposée

- a) Un format correspond à un couple de diviseurs $(a; b)$ de 360 tels que $ab = 360$ et $a \leq b$.
- $360 = 2^3 \times 3^2 \times 5$ possède $(3+1)(2+1)(1+1) = 24$ diviseurs.
 - Chaque diviseur a détermine $b = \frac{360}{a}$: les 24 diviseurs se groupent en **paires** $\{a; b\}$.
 - 360 n'étant pas un carré parfait (l'exposant de 5 est impair), aucun diviseur n'est son propre partenaire.
 - Il y a donc $\frac{24}{2} = 12$ formats.
- b) On cherche le couple dont les termes encadrent $\sqrt{360} \approx 18,97$.
- Les diviseurs voisins sont 18 et 20, et $18 \times 20 = 360$ ✓.
 - Le format le plus proche du carré est donc 18×20 cm.
 - **Contrôle** : son périmètre, $2(18 + 20) = 76$ cm, est le plus petit de tous les formats — à aire fixée, le périmètre décroît quand on se rapproche du carré.

Réponse. a) 12 formats · b) 18×20 cm.

Correction de l'exercice 14 - Décomposition et racine carrée

- a) On part de la décomposition : $5\,040 = 2^4 \times 3^2 \times 5 \times 7$.
- On sort de la racine tous les facteurs d'exposant pair :
- $$\sqrt{5\,040} = \sqrt{2^4 \times 3^2 \times 35} = 2^2 \times 3 \times \sqrt{35} = 12\sqrt{35}$$
- $35 = 5 \times 7$ n'a aucun facteur carré : on ne peut pas simplifier davantage.
 - **Vérification numérique** : $12\sqrt{35} \approx 12 \times 5,916 = 70,99$, et $70,99^2 \approx 5\,040$ ✓.
- b) $\sqrt{360} \times \sqrt{10} = \sqrt{3\,600}$.
- $3\,600 = 2^4 \times 3^2 \times 5^2$: tous les exposants sont pairs, c'est un carré parfait.
 - $\sqrt{3\,600} = 2^2 \times 3 \times 5 = 60$: **oui**, c'est l'entier 60.
 - **Le critère** : $\sqrt{n}$ est entier si et seulement si tous les exposants de la décomposition de n sont pairs.

Réponse. a) $12\sqrt{35}$ · b) oui, $\sqrt{3\,600} = 60$.

Correction de l'exercice 15 - Bilan : décomposer et conclure

- a) $4\,900 = 49 \times 100 = 7^2 \times 2^2 \times 5^2$.
- Nombre de diviseurs : $(2+1)(2+1)(2+1) = 27$.
 - Tous les exposants sont pairs : c'est un **carré parfait**, celui de $2 \times 5 \times 7 = 70$. En effet $70^2 = 4\,900$ ✓.
 - Le nombre impair de diviseurs (27) confirme qu'il s'agit d'un carré.
- b) $1\,176 = 8 \times 147 = 2^3 \times 3 \times 7^2$.
- Exposants : 3 pour 2 (impair), 1 pour 3 (impair), 2 pour 7 (pair).
 - Il faut multiplier par $2 \times 3 = 6$: $k = 6$.

— **Vérification** : $1\,176 \times 6 = 7\,056 = 2^4 \times 3^2 \times 7^2 = (4 \times 3 \times 7)^2 = 84^2 \checkmark$.

c) L'effectif d'un groupe doit diviser 221, en étant strictement supérieur à 1.

— $221 = 13 \times 17$: ses diviseurs sont 1, 13, 17 et 221.

— Les répartitions possibles sont donc : 17 groupes de 13, 13 groupes de 17, ou un seul groupe de 221.

— **Remarque** : si l'effectif avait été un nombre premier, aucune répartition non triviale n'aurait été possible.

Réponse. a) $2^2 \times 5^2 \times 7^2$, 27 diviseurs, carré de 70 · b) $k = 6 \cdot$ c) 17×13 , 13×17 ou 1×221 .