Plaquette 4 – Démontrer avec les nombres premiers

Nombres premiers — Terminale maths expertes

Corrections détaillées

Boîte à outils

Théorèmes et schémas de démonstration.

- **Lemme d'Euclide** : si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$. Il se démontre à partir du théorème de Gauss.
- **Généralisation** : si p est premier et $p \mid a^n$, alors $p \mid a$.
- **Unicité de la décomposition** : deux décompositions en facteurs premiers d'un même entier ont les mêmes facteurs avec les mêmes exposants. C'est l'outil des démonstrations d'irrationalité.
- **Théorème d'Euclide** : il existe une infinité de nombres premiers. Schéma : supposer qu'il n'y en a qu'un nombre fini $p_1, \ldots, p_k$, considérer $N = p_1 p_2 \cdots p_k + 1$, et observer qu'aucun p_i ne divise N.
- **Raisonnement par l'absurde pour une irrationalité** : supposer $\sqrt{n} = \dfrac{a}{b}$ avec la fraction **irréductible**, élever au carré, puis faire apparaître une contradiction sur les facteurs premiers.
- **Disjonction sur les restes** : pour démontrer une propriété des premiers $p > 3$, on utilise $p \equiv \pm 1 \pmod 6$, ou p impair et non multiple de 3.
- **Un contre-exemple suffit** à détruire une conjecture ; aucune quantité d'exemples ne suffit à la démontrer.

Correction de l'exercice 1 – Le lemme d'Euclide

a) Supposons $p \mid ab$ et $p \nmid a$: montrons alors que $p \mid b$.

- Les diviseurs positifs de p sont 1 et p, donc $\text{pgcd}(p\,;a)$ vaut 1 ou p.
- Si ce PGCD valait p, alors p diviserait a, ce que l'on a exclu : donc $\text{pgcd}(p\,;a) = 1$.
- p divise le produit ab et p est premier avec a : d'après le **théorème de Gauss**, $p \mid b$.
- **Conclusion** : $p \mid a$ ou $p \mid b$.

b) Prenons $p = 6$, $a = 4$ et $b = 3$.

- $ab = 12$ et $6 \mid 12$ ✓.
- Pourtant $6 \nmid 4$ et $6 \nmid 3$: l'énoncé est **faux** pour 6.
- **Là est toute la force de la primalité** : $6 = 2 \times 3$ peut « répartir » ses facteurs entre a et b, ce qu'un nombre premier ne peut pas faire.

Réponse. a) Gauss appliqué à $\text{pgcd}(p\,;a) = 1$ · b) $6 \mid 4 \times 3$ mais $6 \nmid 4$ et $6 \nmid 3$.

Correction de l'exercice 2 – Un premier qui divise une puissance

a) $a^2 = a \times a$: on applique le **lemme d'Euclide** au produit.

- p est premier et divise $a \times a$, donc $p \mid a$ ou $p \mid a$: dans les deux cas, $p \mid a$.

b) On raisonne par **récurrence** sur $n \geq 1$.

- **Initialisation** : pour $n = 1$, l'implication « $p \mid a$ donc $p \mid a$ » est évidente.
- **Hérédité** : supposons la propriété vraie au rang n, et supposons $p \mid a^{n+1}$.
- $a^{n+1} = a \times a^n$: d'après le lemme d'Euclide, $p \mid a$ ou $p \mid a^n$.

— Dans le premier cas c'est fini ; dans le second, l'hypothèse de récurrence donne $p \mid a$.
— **Conclusion** : pour tout $n \geq 1$, $p \mid a^n \Longrightarrow p \mid a$.
— **Contre-exemple sans primalité** : $4 \mid 2^2$ mais $4 \nmid 2$.

Réponse. a) lemme d'Euclide sur $a \times a$ · b) récurrence : $p \mid a \times a^n$.

Correction de l'exercice 3 – L'infinité des nombres premiers

Raisonnement par l'absurde (démonstration d'Euclide, vieille de vingt-trois siècles).

— Supposons qu'il n'existe qu'un nombre fini de nombres premiers, notés $p_1, p_2, \ldots, p_k$.
— Posons $N = p_1 \times p_2 \times \cdots \times p_k + 1$. On a $N \geq 3$.
— $N \geq 2$ admet donc un diviseur premier q, et q figure nécessairement dans la liste : $q = p_i$ pour un certain i.
— Mais p_i divise aussi le produit $p_1 p_2 \cdots p_k$.
— Donc p_i divise la différence $N - p_1 p_2 \cdots p_k = 1$: c'est **impossible**, car $p_i \geq 2$.
— L'hypothèse de départ est donc fausse : **il existe une infinité de nombres premiers**.

Attention à une erreur fréquente. La démonstration ne dit **pas** que N est premier.

— Contre-exemple : $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$.
— N n'est pas premier, mais ses facteurs premiers (59 et 509) sont bien **absents** de la liste, ce qui suffit à la contradiction.

Réponse. $N = p_1 \cdots p_k + 1$: tout diviseur premier de N est hors de la liste.

Correction de l'exercice 4 – L'irrationalité de racine de 2

Raisonnement par l'absurde. Supposons $\sqrt{2} = \dfrac{a}{b}$ avec a et b entiers, $b \neq 0$, et la fraction **irréductible** : $\text{pgcd}(a\,;b) = 1$.

— En élevant au carré : $2 = \dfrac{a^2}{b^2}$, donc $a^2 = 2b^2$.
— Ainsi $2 \mid a^2$; comme 2 est premier, $2 \mid a$ (propriété démontrée plus haut).
— On écrit $a = 2a'$: alors $4a'^2 = 2b^2$, donc $b^2 = 2a'^2$.
— Le même argument donne $2 \mid b$.
— Donc 2 divise à la fois a et b : cela contredit $\text{pgcd}(a\,;b) = 1$.

Conclusion. L'hypothèse est absurde : $\sqrt{2}$ est **irrationnel**.

— **Variante par les exposants** : dans $a^2 = 2b^2$, l'exposant de 2 est **pair** à gauche et **impair** à droite, ce qui contredit l'unicité de la décomposition en facteurs premiers. Cette version se généralise immédiatement.

Réponse. $a^2 = 2b^2$ force $2 \mid a$ puis $2 \mid b$: contradiction avec l'irréductibilité.

Correction de l'exercice 5 – Généraliser à racine de p

Supposons $\sqrt{p} = \dfrac{a}{b}$ avec $\text{pgcd}(a\,;b) = 1$ et $b \neq 0$.

— $a^2 = p\,b^2$, donc $p \mid a^2$, et comme p est premier, $p \mid a$.
— On pose $a = pa'$: $p^2 a'^2 = pb^2$, d'où $b^2 = p\,a'^2$ et de même $p \mid b$.
— p divise a et b : contradiction avec $\text{pgcd}(a\,;b) = 1$.
— **Conclusion** : $\sqrt{p}$ est irrationnel pour tout p premier.

Cas de $\sqrt{6}$. $6 = 2 \times 3$ n'est pas premier : on reprend l'argument des exposants.

— Si $\sqrt{6} = \frac{a}{b}$ irréductible, alors $a^2 = 6b^2$.
— $2 \mid a^2$ donne $2 \mid a$, donc $a = 2a'$ et $4a'^2 = 6b^2$, soit $2a'^2 = 3b^2$.
— Alors $2 \mid 3b^2$, et comme $\text{pgcd}(2\,;3) = 1$, le théorème de Gauss donne $2 \mid b^2$, donc $2 \mid b$.
— Contradiction avec l'irréductibilité : $\sqrt{6}$ est irrationnel.
— **Le critère général** : $\sqrt{n}$ est rationnel **si et seulement si** n est un carré parfait.

Réponse. $a^2 = pb^2$ donne $p \mid a$ puis $p \mid b$; $\sqrt{6}$: même raisonnement avec $p = 2$.

Correction de l'exercice 6 – Des premiers en progression

a) $p = 3$ donne 3, 5 et 7 : trois nombres premiers.

b) Soit p un premier tel que p, $p+2$ et $p+4$ soient tous premiers. On regarde les restes **modulo 3**.

$p \equiv$	0	1	2
$p+2 \equiv$	2	0	1
$p+4 \equiv$	1	2	0

— Dans chacun des trois cas, **l'un des trois nombres est divisible par** 3 : les trois restes 0, 1, 2 sont représentés.
— Ce nombre divisible par 3 ne peut être premier que s'il **vaut** 3.
— Si $p = 3$: le triplet est $(3\,;5\,;7)$, effectivement tous premiers ✓.
— Si $p+2 = 3$ ou $p+4 = 3$, alors $p \leq 1$: impossible.
— **Conclusion** : $(3\,;5\,;7)$ est le seul triplet.
— **Pour comparaison** : on conjecture qu'il existe une infinité de couples $(p\,;p+2)$ de premiers jumeaux — $(11\,;13)$, $(17\,;19)$, $(29\,;31)$… mais personne ne l'a démontré.

Réponse. a) $(3\,;5\,;7)$ · b) parmi p, $p+2$, $p+4$, l'un est toujours multiple de 3.

Correction de l'exercice 7 – Une conjecture qui s'effondre

a) $P(0) = 41$; $P(1) = 43$; $P(2) = 47$; $P(10) = 100 + 10 + 41 = 151$.

— 41, 43, 47 sont premiers, et 151 aussi ($\sqrt{151} \approx 12,3$; ni 2, 3, 5, 7, 11 ne le divisent).
— On pourrait conjecturer que $P(n)$ est premier pour tout n — et cette conjecture résiste aux **quarante** premiers essais, ce qui est troublant.

b) $P(40) = 1\,600 + 40 + 41 = 1\,681$.

— $1\,681 = 41^2$: ce n'est **pas** un nombre premier.
— On le voyait sans calculer :
$P(40) = 40^2 + 40 + 41 = 40(40+1) + 41 = 41 \times 40 + 41 = 41 \times 41$.
— **Conclusion** : la conjecture est fausse. $P(41) = 1\,763 = 41 \times 43$ échoue également.
— **La leçon** : quarante vérifications ne démontrent rien. En arithmétique, seule une démonstration vaut preuve — et un seul contre-exemple suffit à tout renverser.

Réponse. a) 41, 43, 47, 151 : tous premiers · b) $P(40) = 1\,681 = 41^2$: la conjecture est fausse.

Correction de l'exercice 8 – Divisible par 24

On écrit $p^2 - 1 = (p-1)(p+1)$ et on montre séparément la divisibilité par 8 et par 3.

Divisibilité par 8.

— p est premier et $p > 3$, donc p est **impair** : $p-1$ et $p+1$ sont deux entiers pairs **consécutifs**.
— L'un des deux est divisible par 4 (deux pairs consécutifs), l'autre l'est par 2 : leur produit est divisible par 8.

Divisibilité par 3.

— p est premier et $p > 3$, donc $3 \nmid p$: $p \equiv 1$ ou $p \equiv 2 \pmod 3$.
— Si $p \equiv 1$, alors $3 \mid (p-1)$; si $p \equiv 2$, alors $p+1 \equiv 0$, donc $3 \mid (p+1)$.
— Dans les deux cas, 3 divise le produit.

Conclusion. $8 \mid p^2-1$, $3 \mid p^2-1$ et $\text{pgcd}(8\,;3)=1$: d'après le corollaire du théorème de Gauss, $24 \mid p^2-1$.

— Contrôles : $p=5$ donne 24 ✓ · $p=7$ donne $48 = 24\times 2$ ✓ · $p=13$ donne $168 = 24\times 7$ ✓.

Réponse. $(p-1)(p+1)$ est divisible par 8 et par 3, donc par 24.

Correction de l'exercice 9 – Somme de deux nombres premiers

a) Une somme est impaire lorsque ses deux termes sont de parités **différentes**.

— L'un des deux premiers est donc pair.
— Or le seul nombre premier pair est 2 (tout autre pair a 2 comme diviseur strict).
— **Conclusion** : l'un des deux premiers vaut 2.
— Exemple : $2+11=13$, impair ✓ ; $3+11=14$, pair, conformément à la règle.

b) 2 026 est pair : on cherche deux premiers **impairs**.

— $2\,026 = 3 + 2\,023$, mais $2\,023 = 7\times 17^2$: non premier.
— $2\,026 = 5 + 2\,021$, et $2\,021 = 43\times 47$: non premier.
— $2\,026 = 17 + 2\,009$, et $2\,009 = 7\times 287$: non premier.
— $2\,026 = 23 + 2\,003$, et 2 003 est premier (aucun premier ≤ 44 ne le divise).
— **Une écriture possible** : $2\,026 = 23 + 2\,003$ ✓.
— **Remarque** : que tout entier pair supérieur à 2 soit somme de deux premiers est la **conjecture de Goldbach**, vérifiée par ordinateur jusqu'à des tailles gigantesques, mais toujours non démontrée.

Réponse. a) l'un des deux est pair, donc vaut 2 · b) $2\,026 = 23 + 2\,003$.

Correction de l'exercice 10 – Des trous dans la suite des premiers

Soit k un entier tel que $2 \le k \le n$. On étudie $n! + k$.

— k figure parmi les facteurs de $n! = 1\times 2\times \cdots \times n$, donc $k \mid n!$.
— k divise aussi k, donc k divise la somme $n! + k$.
— Or $n! + k > k > 1$: le nombre $n! + k$ admet donc un diviseur k strictement compris entre 1 et lui-même.
— **Conclusion** : $n! + k$ n'est pas premier, et ce pour chacune des $n-1$ valeurs de k.

Ce que cela signifie. On peut construire des **suites de nombres composés aussi longues que l'on veut**.

— Exemple avec $n=5$: $5! = 120$, et $122, 123, 124, 125$ sont quatre entiers consécutifs non premiers ($2 \mid 122$, $3 \mid 123$, $4 \mid 124$, $5 \mid 125$) ✓.
— Les nombres premiers se raréfient donc autant qu'on veut — tout en restant en nombre **infini** : les deux faits coexistent.

Réponse. k divise $n!$ et k, donc $k \mid (n! + k)$ avec $1 < k < n! + k$.

Correction de l'exercice 11 – Le produit des premiers plus un

a) $2 \times 3 \times 5 \times 7 = 210$, donc le nombre vaut 211.

— On l'a vu : 211 est premier (aucun premier ≤ 14 ne le divise).

b) $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30\,030$, donc le nombre vaut 30 031.

— Il n'est divisible ni par 2, 3, 5, 7, 11, 13 (par construction, chacun laisse le reste 1).
— En poursuivant les essais : $30\,031 = 59 \times 509$.
— **Il n'est donc pas premier**, alors que le cas a) pouvait le laisser croire.

c) Ce qui reste vrai dans tous les cas : **aucun** des premiers du produit ne divise $N = p_1 \cdots p_k + 1$.

— Si p_i divisait N et le produit, il diviserait leur différence 1 : impossible.
— Donc les facteurs premiers de N sont **tous nouveaux** — ici 59 et 509, absents de la liste $2, 3, 5, 7, 11, 13$.
— C'est précisément ce dont on a besoin dans la démonstration d'Euclide : on n'a jamais besoin que N soit premier.

Réponse. a) 211, premier · b) $30\,031 = 59 \times 509$ · c) ses facteurs premiers ne sont pas dans la liste.

Correction de l'exercice 12 – Unicité de la décomposition à l'œuvre

On compare les **exposants de** 3 dans les décompositions des deux membres — c'est l'argument le plus rapide.

— $12 = 2^2 \times 3$.
— Notons α l'exposant de 3 dans la décomposition de a, et β celui de 3 dans b.
— À gauche, a^2 contient 3 à l'exposant 2α : un nombre **pair**.
— À droite, $12b^2$ contient 3 à l'exposant $1 + 2\beta$: un nombre **impair**.
— L'unicité de la décomposition en facteurs premiers impose $2\alpha = 1 + 2\beta$: un entier pair égal à un entier impair, c'est impossible.

Conclusion. Aucun couple $(a\,;b)$ ne convient.

— **Interprétation** : cela revient à dire que $\sqrt{12} = 2\sqrt{3}$ est irrationnel.
— **La méthode générale** : pour montrer que $a^2 = nb^2$ est impossible, on cherche un facteur premier dont l'exposant est impair dans n.

Réponse. L'exposant de 3 serait pair à gauche et impair à droite : impossible.

Correction de l'exercice 13 – Premiers et carrés

a) On travaille **modulo 3**.

— p est premier et $p \geq 5$, donc $3 \nmid p$: $p \equiv 1$ ou $p \equiv 2 \pmod 3$.
— Dans les deux cas, $p^2 \equiv 1 \pmod 3$: en effet $1^2 = 1$ et $2^2 = 4 \equiv 1$.
— Donc $p^2 + 2 \equiv 1 + 2 = 3 \equiv 0 \pmod 3$: le nombre est divisible par 3.
— Or $p \geq 5$ entraîne $p^2 + 2 \geq 27 > 3$: il a donc un diviseur strict, il n'est **pas premier**.

b) Vérifications :

p	5	7	11
$p^2 + 2$	27	51	123
Factorisation	3^3	3×17	3×41

— Tous divisibles par 3 ✓.
— **Le cas exclu** : $p = 3$ donne $p^2 + 2 = 11$, qui **est** premier — d'où l'hypothèse $p \geq 5$.

Réponse. a) $p^2 \equiv 1 \pmod 3$ donc $3 \mid (p^2 + 2)$ · b) 27, 51, 123.

Correction de l'exercice 14 – Combien de facteurs premiers ?

a) Si n est composé, $n = ab$ avec $1 < a \leq b < n$, donc $a^2 \leq ab = n$ et $a \leq \sqrt{n}$.

— $a \geq 2$ admet un diviseur premier $p \leq a \leq \sqrt{n}$, et $p \mid a \mid n$ donne $p \mid n$.

b) Soit $n < 121$ non divisible par 2, 3, 5 ni 7, avec $n \geq 2$.

— Si n était composé, il aurait un facteur premier $p \leq \sqrt{n} < \sqrt{121} = 11$.
— Les nombres premiers strictement inférieurs à 11 sont 2, 3, 5 et 7 : aucun ne divise n par hypothèse.
— Contradiction : donc n est premier.
— **Application pratique** : pour tester un nombre inférieur à 121, quatre divisions suffisent. Pour un nombre inférieur à 2 000, il faut aller jusqu'à 43, soit quatorze divisions.
— **Vérification** : 89 n'est divisible ni par 2, 3, 5, 7 : il est premier ✓. $91 = 7 \times 13$ est éliminé dès le test de 7 ✓.

Réponse. a) le plus petit facteur est $\leq \sqrt{n}$ · b) sinon n aurait un facteur premier < 11.

Correction de l'exercice 15 – Bilan : trois démonstrations

a) $45 = 3^2 \times 5$, donc $\sqrt{45} = 3\sqrt{5}$.

— Supposons $\sqrt{45}$ rationnel : alors $\sqrt{5} = \dfrac{\sqrt{45}}{3}$ le serait aussi (quotient de deux rationnels).
— Or 5 est premier, donc $\sqrt{5}$ est irrationnel (démonstration de l'exercice 5).
— Contradiction : $\sqrt{45}$ est **irrationnelle**.

b) p est premier et $p > 3$, donc p est impair et non divisible par 3.

— **Modulo 2** : p impair donne p^2 impair, donc $p^2 + 5$ est **pair**.
— **Modulo 3** : $3 \nmid p$ donne $p^2 \equiv 1 \pmod 3$, donc $p^2 + 5 \equiv 1 + 5 = 6 \equiv 0 \pmod 3$.
— 2 et 3 sont premiers entre eux et divisent tous deux $p^2 + 5$: d'après le corollaire de Gauss, $6 \mid p^2 + 5$.
— Contrôle : $p = 7$ donne $54 = 6 \times 9$ ✓ ; $p = 11$ donne $126 = 6 \times 21$ ✓.

c) Soit d un diviseur commun de $n^2 + n$ et $n^2 + n + 1$.

— d divise leur différence : $\left(n^2 + n + 1\right) - \left(n^2 + n\right) = 1$.
— Donc $d = 1$: les deux nombres sont premiers entre eux, pour tout n.
— **Plus général** : deux entiers **consécutifs** sont toujours premiers entre eux — c'est le cas ici, quel que soit n.

Réponse. a) sinon $\sqrt{5}$ serait rationnel · b) pair et multiple de 3 · c) leur différence vaut 1.