

Nombres premiers — Terminale maths expertes

20 exercices corrigés · mathlvl.fr

Énoncés et corrigés détaillés

Présentation

Un nombre premier n'a que deux diviseurs positifs, 1 et lui-même — et de cette définition minuscule découle toute la structure des entiers : tout entier supérieur à 1 s'écrit d'une SEULE façon comme produit de nombres premiers. Ces 20 exercices corrigés couvrent l'ensemble du chapitre en maths expertes : test de primalité et crible d'Ératosthène, décomposition en facteurs premiers, nombre et somme des diviseurs, PGCD et PPCM lus sur les exposants, démonstration de l'infinité des nombres premiers, lemme d'Euclide, irrationalité de $\sqrt{2}$, petit théorème de Fermat et son emploi pour calculer des restes ou un inverse modulaire, nombres de Mersenne et de Fermat, et un chiffrement RSA complet sur de petits nombres. Les corrections sont rédigées étape par étape, avec les vérifications — y compris celle qui montre que la réciproque du petit théorème de Fermat est FAUSSE.

Version en ligne, avec les corrections dépliantes :

mathlvl.fr/exercices-corriges/terminale-maths-expertes/nombres-premiers

Exercice 1 - Reconnaître un nombre premier

Un entier $n \geq 2$ est PREMIER lorsque ses seuls diviseurs positifs sont 1 et n . Pour le tester, il suffit de chercher un diviseur parmi les entiers inférieurs ou égaux à $\sqrt{n}$.

1. Dresser la liste des nombres premiers inférieurs à 60.
2. Le nombre 211 est-il premier ? Et 221 ?
3. Le nombre 2027 est-il premier ?

Exercice 2 - Décomposition en facteurs premiers

Le théorème fondamental de l'arithmétique affirme que tout entier $n \geq 2$ s'écrit comme produit de nombres premiers, et ce d'une SEULE façon à l'ordre près. C'est cette unicité qui donne toute sa force à la décomposition.

1. Décomposer 360 et 2024 en produits de facteurs premiers.
2. Décomposer 3600, et en déduire que c'est un carré parfait.
3. Justifier la méthode : pourquoi divise-t-on par les nombres premiers dans l'ordre croissant ?

Exercice 3 - Compter les diviseurs

La décomposition en facteurs premiers permet de compter les diviseurs sans les énumérer : un diviseur de $n = p^a q^b \dots$ s'obtient en choisissant, pour chaque facteur premier, un exposant entre 0 et le sien.

1. Déterminer le nombre de diviseurs positifs de 360.
2. Déterminer le nombre de diviseurs positifs de 2024.
3. Un entier peut-il avoir exactement 3 diviseurs positifs ?

Exercice 4 - PGCD et PPCM par les exposants

Une fois les décompositions écrites, le PGCD et le PPCM se lisent directement sur les exposants — sans algorithme d'Euclide.

1. Calculer $\text{PGCD}(360 ; 2024)$ et $\text{PPCM}(360 ; 2024)$ par les décompositions.
2. Vérifier la relation $\text{PGCD} \times \text{PPCM} = ab$.
3. Déterminer tous les diviseurs communs de 360 et 2024.

Exercice 5 - L'infinité des nombres premiers

La démonstration qui suit remonte à Euclide, il y a plus de deux mille ans. Elle procède par l'absurde et n'utilise qu'un seul fait : tout entier supérieur à 1 admet un diviseur premier.

1. Démontrer que tout entier $n \geq 2$ admet au moins un diviseur premier.
2. Supposons qu'il n'existe qu'un nombre fini de nombres premiers $p_1, \dots, p_k$. Étudier $N = p_1 \times p_2 \times \dots \times p_k + 1$.
3. Conclure.

Exercice 6 - Pourquoi s'arrêter à la racine carrée

Le test de primalité de l'exercice 1 repose sur une propriété qu'il faut savoir démontrer : si n n'est pas premier, il admet un diviseur premier inférieur ou égal à $\sqrt{n}$.

1. Démontrer cette propriété.
2. Combien de divisions faut-il au maximum pour tester la primalité de 2027 ? de $10^6 + 1$?
3. En déduire une justification du crible d'Ératosthène : jusqu'où faut-il rayer les multiples pour cribler jusqu'à 100 ?

Exercice 7 - Nombres premiers et congruences

Les nombres premiers se répartissent de façon irrégulière, mais leurs restes modulo un petit entier obéissent, eux, à des contraintes strictes.

1. Démontrer que tout nombre premier $p > 3$ vérifie $p \equiv 1$ ou $p \equiv 5$ modulo 6.
2. En déduire que tout nombre premier $p > 3$ s'écrit $6k - 1$ ou $6k + 1$.
3. Démontrer que si $p > 3$ est premier, alors $24 \mid p^2 - 1$.

Exercice 8 - Le lemme d'Euclide

Le lemme d'Euclide énonce : si un nombre PREMIER p divise un produit ab , alors p divise a ou p divise b . C'est cette propriété qui donne l'unicité de la décomposition en facteurs premiers.

1. Démontrer le lemme à l'aide du théorème de Gauss.
2. Montrer par un contre-exemple que l'hypothèse « p premier » est indispensable.
3. En déduire que si p est premier et $p \mid a^2$, alors $p \mid a$.

Exercice 9 - Irrationalité de $\sqrt{2}$

On démontre que $\sqrt{2}$ n'est pas un nombre rationnel. Le raisonnement se fait par l'absurde, et repose sur la conséquence du lemme d'Euclide établie à l'exercice précédent.

1. Démontrer que si $2 \mid n^2$, alors $2 \mid n$.
2. En supposant $\sqrt{2} = \frac{a}{b}$ avec $\frac{a}{b}$ irréductible, aboutir à une contradiction.
3. Adapter la démonstration à $\sqrt{3}$.

Exercice 10 - Somme des diviseurs et nombres parfaits

On note $\sigma(n)$ la somme de tous les diviseurs positifs de n . Un entier est dit PARFAIT lorsqu'il est égal à la somme de ses diviseurs stricts, c'est-à-dire lorsque $\sigma(n) = 2n$.

1. Calculer $\sigma(28)$ et vérifier que 28 est parfait.
2. Établir la formule $\sigma(p^k) = 1 + p + \dots + p^k$, puis calculer $\sigma(360)$.
3. Vérifier que 496 est parfait.

Exercice 11 - Le petit théorème de Fermat

Le petit théorème de Fermat affirme : si p est PREMIER et si p ne divise pas a , alors $a^{p-1} \equiv 1 [p]$. Il donne d'un coup la période des puissances, sans avoir à dresser de tableau.

1. Vérifier le théorème pour $p = 7$ et $a = 2$, puis pour $p = 11$ et $a = 3$.
2. Vérifier que la conclusion tombe si p n'est pas premier, avec $p = 8$ et $a = 3$.
3. Que devient l'énoncé lorsque p divise a ?

Exercice 12 - Fermat au service des grands restes

Le petit théorème de Fermat remplace avantageusement le tableau des puissances du chapitre 5 : il fournit directement un exposant qui ramène à 1.

1. Calculer le reste de 2^{2026} modulo 7.
2. Calculer le reste de 3^{2026} modulo 11.
3. Comparer avec la méthode du tableau des puissances.

Exercice 13 - Nombres de Mersenne

On appelle nombre de Mersenne un entier de la forme $M_n = 2^n - 1$. Ce sont les candidats privilégiés à la recherche de très grands nombres premiers.

1. Démontrer que si n n'est pas premier, alors M_n n'est pas premier.
2. La réciproque est-elle vraie ? On pourra étudier M_{11} .
3. Calculer M_2, M_3, M_5, M_7 et préciser lesquels sont premiers.

Exercice 14 - Nombres de Fermat

Symétriquement, on s'intéresse aux entiers de la forme $2^n + 1$. Fermat conjecturait qu'ils sont premiers dès que n est une puissance de 2 — une conjecture célèbre... et fausse.

1. Démontrer que si $2^n + 1$ est premier, alors n est une puissance de 2.
2. Calculer $F_k = 2^{2^k} + 1$ pour $k = 0, 1, 2, 3, 4$ et vérifier qu'ils sont premiers.
3. Que se passe-t-il pour $k = 5$?

Exercice 15 - Décomposition, carrés et puissances

L'unicité de la décomposition permet de reconnaître les carrés, les cubes, et de résoudre des équations où l'inconnue est un exposant.

1. Démontrer qu'un entier $n \geq 2$ est un carré parfait si et seulement si tous les exposants de sa décomposition sont pairs.
2. Déterminer le plus petit entier k tel que $360k$ soit un carré parfait.
3. Déterminer le plus petit entier k tel que $360k$ soit un cube parfait.

Exercice 16 - Des trous arbitrairement grands entre les nombres premiers

Les nombres premiers sont en nombre infini (exercice 5), mais rien n'empêche de longs intervalles d'en être totalement dépourvus. On le démontre par une construction explicite, à partir de la factorielle $n! = 1 \times 2 \times \dots \times n$.

1. Démontrer que pour tout $n \geq 2$, les entiers $n! + 2, n! + 3, \dots, n! + n$ sont tous composés.
2. Illustrer avec $n = 5$.
3. Comment obtenir un intervalle de 100 entiers consécutifs sans aucun nombre premier ?

Exercice 17 - $p^2 - 1$ est divisible par 24

Soit p un nombre premier supérieur ou égal à 5. Démontrer que $p^2 - 1$ est divisible par 24. Vérifier sur $p = 5, 7$ et 11.

Exercice 18 - Inverse modulaire par le petit théorème de Fermat

Au chapitre précédent, l'inverse modulaire s'obtenait par la remontée de l'algorithme d'Euclide. Quand le module est PREMIER, le petit théorème de Fermat en donne une formule directe.

1. Démontrer que si p est premier et $p \nmid a$, alors a^{p-2} est un inverse de a modulo p .
2. Calculer l'inverse de 3 modulo 7 par cette méthode, puis vérifier.
3. Calculer l'inverse de 5 modulo 11, et comparer les deux méthodes disponibles.

Exercice 19 - La réciproque du théorème de Fermat est fausse

Le petit théorème de Fermat fournit un TEST DE NON-PRIMALITÉ : si $a^{n-1} \not\equiv 1 \pmod{n}$ pour un certain a , alors n n'est pas premier. On étudie ici si la réciproque tient —

c'est-à-dire si la congruence garantit la primalité.

1. Montrer que 9 n'est pas premier en utilisant $a = 2$.
2. Vérifier que $561 = 3 \times 11 \times 17$ n'est pas premier, et pourtant que $2^{560} \equiv 1 [561]$.
3. Que peut-on conclure sur la valeur du test de Fermat comme critère de primalité ?

Exercice 20 - Problème de synthèse : un chiffrement RSA

Le chiffrement RSA repose entièrement sur ce chapitre. On choisit deux nombres premiers $p = 5$ et $q = 11$, on pose $n = pq$ et $\varphi = (p - 1)(q - 1)$. La clé publique est $(n; e)$ avec $e = 3$, la clé privée est l'entier d tel que $ed \equiv 1 [\varphi]$. Un message m est chiffré en $c \equiv m^e [n]$ et déchiffré par $m \equiv c^d [n]$.

1. Calculer n et φ , et justifier que $e = 3$ est un choix valide.
2. Déterminer la clé privée d .
3. Chiffrer le message $m = 8$, puis vérifier que le déchiffrement redonne 8.
4. Expliquer pourquoi la sécurité du système repose sur la difficulté de factoriser n .

Corrigés détaillés

Les corrections des 20 exercices, dans l'ordre des énoncés.

Correction de l'exercice 1 - Reconnaître un nombre premier

On applique le crible d'Ératosthène : on écrit les entiers de 2 à 60, on garde 2 et on raye ses multiples, puis on garde 3 et on raye ses multiples, et ainsi de suite.

Les nombres premiers inférieurs à 60 sont :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59. Il y en a 17.

On remarque que 2 est le seul nombre premier PAIR : tout autre nombre pair a 2 pour diviseur en plus de 1 et de lui-même.

Pour 211 : $\sqrt{211} \approx 14,5$, donc il suffit de tester les diviseurs premiers jusqu'à 14, c'est-à-dire 2, 3, 5, 7, 11, 13.

211 est impair (pas divisible par 2) ; $2 + 1 + 1 = 4$ 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 reste nul.

Aucun diviseur trouvé : 211 est PREMIER.

Pour 221 : $\sqrt{221} \approx 14,9$, mêmes candidats. On teste : $221 = 13 \times 17$.

Un diviseur a été trouvé, donc 221 n'est PAS premier. C'est un piège classique : 221 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, ni par 11 — il faut aller jusqu'à 13.

Pour 2027 : $\sqrt{2027} \approx 45,0$, il faut tester les nombres premiers jusqu'à 43, soit 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43.

Il est impair ; la somme de ses chiffres vaut 11, non multiple de 3 ; il ne finit pas par 0 ou 5.

En poursuivant les divisions, aucun reste n'est nul : 2027 est PREMIER.

À comparer avec $2026 = 2 \times 1013$, qui n'est pas premier (mais dont le facteur 1013, lui, l'est).

Réponse. 17 nombres premiers sous 60 :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 · 211 est premier · $221 = 13 \times 17$ ne l'est pas · 2027 est premier.

Rappel de cours. Pour tester la primalité de n , il suffit de chercher un diviseur PREMIER inférieur ou égal à $\sqrt{n}$. S'il n'y en a pas, n est premier.

Erreur fréquente. S'arrêter trop tôt dans les essais. 221 résiste à 2, 3, 5, 7, 11 et n'est pourtant pas premier : il faut aller jusqu'à $\sqrt{n}$.

Correction de l'exercice 2 - Décomposition en facteurs premiers

Pour 360, on divise successivement par les nombres premiers, en commençant par le plus petit.

$360 = 2 \times 180 = 2 \times 2 \times 90 = 2 \times 2 \times 2 \times 45$.

45 n'est plus divisible par 2 ; on passe à 3 : $45 = 3 \times 15 = 3 \times 3 \times 5$.

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

Contrôle : $8 \times 9 \times 5 = 360$ ✓.

Pour 2024 : $2024 = 2 \times 1012 = 2 \times 2 \times 506 = 2 \times 2 \times 2 \times 253$.

253 est impair, non divisible par 3 (somme des chiffres 10) ni par 5 ni par 7. Mais $253 = 11 \times 23$.

Donc $2024 = 2^3 \times 11 \times 23$. Contrôle : $8 \times 253 = 2024$ ✓.

Pour 3600 : c'est $360 \times 10 = 2^3 \times 3^2 \times 5 \times 2 \times 5 = 2^4 \times 3^2 \times 5^2$.

Tous les exposants sont PAIRS. On peut donc écrire $3600 = (2^2 \times 3 \times 5)^2 = 60^2$.

Contrôle : $60^2 = 3600$ ✓. C'est la règle générale : un entier est un carré parfait si et seulement si tous les exposants de sa décomposition sont pairs.

Justification de la méthode : si n admet un diviseur autre que 1, son PLUS PETIT diviseur $d \geq 2$ est nécessairement premier.

En effet, si d avait un diviseur d' avec $1 < d' < d$, alors d' diviserait aussi n — ce qui contredirait la minimalité de d .

En divisant à chaque étape par le plus petit diviseur, on extrait donc toujours un facteur premier, et le quotient diminue strictement : la méthode se termine.

Réponse. $360 = 2^3 \times 3^2 \times 5$ · $2024 = 2^3 \times 11 \times 23$ · $3600 = 2^4 \times 3^2 \times 5^2 = 60^2$, carré parfait car tous les exposants sont pairs.

Rappel de cours. Décomposition unique en facteurs premiers. Conséquence directe : n est un carré parfait $\Leftrightarrow$ tous les exposants de sa décomposition sont pairs (et un cube $\Leftrightarrow$ tous multiples de 3).

Erreur fréquente. S'arrêter à une décomposition incomplète comme $2024 = 8 \times 253$. Tant qu'un facteur n'est pas premier, la décomposition n'est pas terminée.

Correction de l'exercice 3 - Compter les diviseurs

On part de $360 = 2^3 \times 3^2 \times 5^1$.

Tout diviseur de 360 s'écrit $2^\alpha \times 3^\beta \times 5^\gamma$ avec $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 2$ et $0 \leq \gamma \leq 1$.

Il y a donc 4 choix pour α (les valeurs 0, 1, 2, 3), 3 pour β et 2 pour γ .

Par le principe multiplicatif, le nombre de diviseurs est $4 \times 3 \times 2 = 24$.

Contrôle partiel : le choix $\alpha = \beta = \gamma = 0$ donne le diviseur 1, et le choix maximal donne 360 ✓.

Pour $2024 = 2^3 \times 11^1 \times 23^1$: le nombre de diviseurs vaut $(3+1)(1+1)(1+1) = 4 \times 2 \times 2 = 16$.

Formule générale : si $n = p_1^{a_1} \times \dots \times p_k^{a_k}$, alors n a exactement $(a_1 + 1) \times \dots \times (a_k + 1)$ diviseurs positifs.

Troisième question : on cherche n tel que le produit des $(a_i + 1)$ vaille 3.

Or 3 est premier : le produit ne peut être 3 que s'il comporte un seul facteur, égal à 3.

Cela impose $k = 1$ et $a_1 + 1 = 3$, donc $a_1 = 2$: l'entier est de la forme p^2 avec p premier.

Exemples : $4 = 2^2$ a pour diviseurs 1, 2, 4 ✓ ; $9 = 3^2$ a pour diviseurs 1, 3, 9 ✓ ; $49 = 7^2$ également.

Réponse : oui, exactement les carrés de nombres premiers.

Réponse. 360 a 24 diviseurs positifs · 2024 en a 16 · un entier a exactement 3 diviseurs positifs si et seulement s'il est le carré d'un nombre premier.

Rappel de cours. $n = p_1^{a_1} \dots p_k^{a_k}$ a $(a_1 + 1) \dots (a_k + 1)$ diviseurs positifs. Le +1 vient de l'exposant 0, qui est un choix valide.

Erreur fréquente. Multiplier les exposants sans ajouter 1. Pour 360, cela donnerait

$3 \times 2 \times 1 = 6$ au lieu de 24.

Correction de l'exercice 4 - PGCD et PPCM par les exposants

On aligne les décompositions en faisant apparaître tous les facteurs premiers, avec l'exposant 0 quand un facteur est absent.

$$360 = 2^3 \times 3^2 \times 5^1 \times 11^0 \times 23^0.$$

$$2024 = 2^3 \times 3^0 \times 5^0 \times 11^1 \times 23^1.$$

PGCD : chaque facteur avec le plus PETIT exposant, soit $2^3 \times 3^0 \times 5^0 \times 11^0 \times 23^0 = 8$.

PPCM : chaque facteur avec le plus GRAND exposant, soit $2^3 \times 3^2 \times 5 \times 11 \times 23$.

On calcule : $8 \times 9 = 72$, $72 \times 5 = 360$, $360 \times 11 = 3960$, $3960 \times 23 = 91\,080$.

Donc $\text{PGCD}(360; 2024) = 8$ et $\text{PPCM}(360; 2024) = 91\,080$.

Vérification de la relation : $\text{PGCD} \times \text{PPCM} = 8 \times 91\,080 = 728\,640$.

Et $360 \times 2024 = 728\,640$ ✓. La relation tient — elle s'explique d'ailleurs par les exposants : pour chaque facteur premier, min + max = somme des deux exposants.

Troisième question : les diviseurs communs de deux entiers sont exactement les diviseurs de leur PGCD.

Ici le PGCD vaut $8 = 2^3$, dont les diviseurs positifs sont 1, 2, 4, 8.

Les diviseurs communs de 360 et 2024 sont donc 1, 2, 4 et 8 (et leurs opposés si l'on accepte les entiers négatifs).

Contrôle : 8 divise 360 ($= 8 \times 45$) ✓ et 2024 ($= 8 \times 253$) ✓, alors que 16 ne divise ni l'un ni l'autre ✓.

Réponse. $\text{PGCD}(360; 2024) = 2^3 = 8$ · $\text{PPCM} = 2^3 \times 3^2 \times 5 \times 11 \times 23 = 91\,080$ · $8 \times 91\,080 = 728\,640 = 360 \times 2024$ ✓ · diviseurs communs : 1, 2, 4, 8.

Rappel de cours. PGCD = min des exposants, PPCM = max des exposants. Et surtout : les diviseurs communs de a et b sont exactement les diviseurs de $\text{PGCD}(a; b)$.

Erreur fréquente. Oublier les facteurs absents. Il faut leur donner l'exposant 0, sinon le min est faussé et le PGCD trop grand.

Correction de l'exercice 5 - L'infinité des nombres premiers

Soit $n \geq 2$. L'ensemble de ses diviseurs supérieurs ou égaux à 2 n'est pas vide, puisqu'il contient n lui-même.

Cet ensemble d'entiers positifs admet donc un plus PETIT élément, notons-le d .

Montrons que d est premier. Si ce n'était pas le cas, d aurait un diviseur d' avec $1 < d' < d$.

Mais alors d' diviserait d , qui divise n : donc d' diviserait n , avec $2 \leq d' < d$.

Cela contredirait la minimalité de d . Donc d est premier : tout entier $n \geq 2$ admet un diviseur premier.

Passons à la démonstration principale. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers, notés $p_1, p_2, \dots, p_k$.

Posons $N = p_1 p_2 \cdots p_k + 1$. Comme le produit vaut au moins 2, on a $N \geq 3$, donc $N \geq 2$.

D'après la question 1, N admet un diviseur premier p . Or par hypothèse, p figure dans la liste : $p = p_i$ pour un certain i .

Ce p divise donc le produit $p_1 p_2 \cdots p_k$ (il en est l'un des facteurs), et il divise N par

construction.

Il divise donc leur différence : $N - p_1 p_2 \cdots p_k = 1$.

Mais un nombre premier vaut au moins 2 : il ne peut pas diviser 1. C'est une CONTRADICTION.

L'hypothèse de départ est donc fausse : il existe une INFINITÉ de nombres premiers.

Remarque importante : la démonstration ne dit pas que N est premier. Par exemple, avec $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$, le nombre N est composé — mais ses facteurs premiers sont bien absents de la liste initiale, ce qui suffit à conclure.

Réponse. Tout $n \geq 2$ admet un diviseur premier (le plus petit de ses diviseurs ≥ 2) · si les premiers étaient en nombre fini, $N = p_1 \cdots p_k + 1$ aurait un diviseur premier de la liste, qui diviserait alors 1 : absurde · il y a donc une infinité de nombres premiers.

Rappel de cours. Structure de la preuve : par l'absurde, on construit un entier qui échappe à la liste supposée complète. L'argument décisif est « p divise A et $A + 1$, donc p divise 1 ».

Erreur fréquente. Affirmer que $N = p_1 \cdots p_k + 1$ est premier. C'est faux en général : on montre seulement qu'il a un facteur premier hors de la liste.

Correction de l'exercice 6 - Pourquoi s'arrêter à la racine carrée

Soit $n \geq 2$ non premier. Il s'écrit $n = ab$ avec $2 \leq a \leq b$ (on nomme a le plus petit des deux facteurs).

Supposons par l'absurde que $a > \sqrt{n}$. Comme $b \geq a$, on aurait aussi $b > \sqrt{n}$.

En multipliant ces deux inégalités entre nombres positifs : $ab > \sqrt{n} \times \sqrt{n} = n$.

Or $ab = n$, d'où $n > n$: contradiction. Donc $a \leq \sqrt{n}$.

Enfin, a admet lui-même un diviseur premier p (exercice 5), et $p \leq a \leq \sqrt{n}$. Ce p divise n : la propriété est démontrée.

Conséquence pratique : si aucun nombre premier $\leq \sqrt{n}$ ne divise n , alors n est premier.

Pour 2027 : $\sqrt{2027} \approx 45,02$. Les nombres premiers ≤ 45 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 : il y en a 14.

Quatorze divisions suffisent donc — au lieu des 2025 essais d'une recherche naïve de 2 à 2026.

Pour $10^6 + 1 = 1\,000\,001$: $\sqrt{1\,000\,001} \approx 1000$. Il y a 168 nombres premiers inférieurs à 1000.

Cent soixante-huit divisions suffisent, contre un million d'essais pour la méthode naïve. Le gain est considérable, et c'est ce qui rend le test praticable à la main.

Crible jusqu'à 100 : par la même propriété, tout nombre composé ≤ 100 a un facteur premier $\leq \sqrt{100} = 10$.

Il suffit donc de rayer les multiples de 2, 3, 5 et 7 : les nombres restants sont automatiquement premiers.

Contrôle : après ces quatre passes, 91 devrait être rayé — et il l'est, car $91 = 7 \times 13$ ✓.

Réponse. Si $n = ab$ avec $a \leq b$, alors $a \leq \sqrt{n}$, et a a un diviseur premier $\leq \sqrt{n}$ · 14 divisions suffisent pour 2027, 168 pour $10^6 + 1$ · pour cribler jusqu'à 100, il suffit de rayer les multiples de 2, 3, 5, 7.

Rappel de cours. Tout entier composé n admet un diviseur premier $\leq \sqrt{n}$. D'où le test de primalité et le crible d'Ératosthène, qui s'arrête à $\sqrt{N}$.

Erreur fréquente. Tester tous les entiers jusqu'à $\sqrt{n}$ au lieu des seuls nombres

PREMIERS. C'est correct mais inutilement long : un diviseur composé aurait déjà été détecté par ses facteurs premiers.

Correction de l'exercice 7 - Nombres premiers et congruences

Tout entier est congru à 0, 1, 2, 3, 4 ou 5 modulo 6. Examinons chaque cas pour un nombre premier $p > 3$.

Si $p \equiv 0 [6]$, alors $6 \mid p$, donc $2 \mid p$: impossible pour un premier > 3 .

Si $p \equiv 2 [6]$ ou $p \equiv 4 [6]$, alors p est pair : impossible également.

Si $p \equiv 3 [6]$, alors $3 \mid p$, donc $p = 3$: exclu puisque $p > 3$.

Il ne reste que $p \equiv 1 [6]$ ou $p \equiv 5 [6]$. La propriété est démontrée.

Contrôle : $5 \equiv 5$, $7 \equiv 1$, $11 \equiv 5$, $13 \equiv 1$, $17 \equiv 5$, $19 \equiv 1$, $23 \equiv 5$ ✓ — l'alternance est visible.

Deuxième question : $p \equiv 1 [6]$ s'écrit $p = 6k + 1$, et $p \equiv 5 [6]$ s'écrit $p = 6k + 5 = 6(k + 1) - 1$.

En renommant l'entier, tout nombre premier > 3 est donc de la forme $6k - 1$ ou $6k + 1$: il est toujours voisin d'un multiple de 6.

Attention à la réciproque : $25 = 6 \times 4 + 1$ n'est pas premier. La condition est nécessaire, pas suffisante.

Troisième question : $p^2 - 1 = (p - 1)(p + 1)$, produit des deux entiers voisins de p .

p étant premier > 3 , il est impair : $p - 1$ et $p + 1$ sont deux entiers PAIRS CONSÉCUTIFS (au sens où ils diffèrent de 2).

L'un des deux est donc divisible par 4, et l'autre par 2 : leur produit est divisible par 8.

Par ailleurs, parmi les trois entiers consécutifs $p - 1$, p , $p + 1$, l'un est divisible par 3.

Comme p est premier > 3 , ce n'est pas p .

Donc 3 divise $(p - 1)(p + 1)$. Le produit est ainsi divisible par 8 et par 3, qui sont premiers entre eux, donc par 24.

Contrôle : $p = 5$ donne 24 ✓ ; $p = 7$ donne $48 = 24 \times 2$ ✓ ; $p = 11$ donne $120 = 24 \times 5$ ✓ ; $p = 13$ donne $168 = 24 \times 7$ ✓.

Réponse. Un premier $p > 3$ vérifie $p \equiv 1$ ou $5 [6]$: il s'écrit donc $6k \pm 1$ et $p^2 - 1 = (p - 1)(p + 1)$ est divisible par 8 et par 3, donc par 24.

Rappel de cours. Méthode : éliminer les classes de congruence incompatibles avec la primalité. Un premier > 3 est toujours de la forme $6k \pm 1$ — mais la réciproque est fautive (25, 35...).

Erreur fréquente. Transformer la condition nécessaire en critère de primalité. $6k \pm 1$ ne garantit rien : 25, 35, 49 sont de cette forme sans être premiers.

Correction de l'exercice 8 - Le lemme d'Euclide

Soit p premier tel que $p \mid ab$. Deux cas se présentent, selon que p divise a ou non.

Premier cas : $p \mid a$. La conclusion est immédiate.

Second cas : $p \nmid a$. Calculons $\text{PGCD}(p; a)$. Ce PGCD divise p , qui est premier : il vaut donc 1 ou p .

Il ne peut pas valoir p , car p ne divise pas a . Donc $\text{PGCD}(p; a) = 1$: p et a sont premiers entre eux.

On applique alors le théorème de Gauss : $p \mid ab$ et $\text{PGCD}(p; a) = 1$ entraînent $p \mid b$.

Dans les deux cas, p divise a ou b : le lemme est démontré.

Contre-exemple pour un module non premier : prenons $p = 6$, $a = 4$ et $b = 3$.

Alors $ab = 12$ et $6 \mid 12$ ✓. Pourtant $6 \nmid 4$ et $6 \nmid 3$.

Le lemme est donc en défaut : c'est bien la primalité qui le fait fonctionner, en garantissant que le PGCD ne peut valoir que 1 ou p .

Troisième question : appliquons le lemme avec $b = a$. Si $p \mid a^2 = a \times a$, alors $p \mid a$ ou $p \mid a$.

Dans les deux cas, $p \mid a$. La propriété est démontrée.

Par récurrence immédiate, on en déduit plus généralement : $p \mid a^n \Rightarrow p \mid a$, pour tout entier $n \geq 1$.

C'est exactement l'outil de la démonstration d'irrationalité de l'exercice suivant.

Réponse. Si $p \nmid a$, alors $\text{PGCD}(p; a) = 1$ et Gauss donne $p \mid b \cdot$ contre-exemple : $6 \mid 4 \times 3$ mais 6 ne divise ni 4 ni 3 · conséquence : $p \mid a^2 \Rightarrow p \mid a$.

Rappel de cours. Lemme d'Euclide : p premier et $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$. C'est ce lemme qui assure l'UNICITÉ de la décomposition en facteurs premiers.

Erreur fréquente. Appliquer le lemme à un module composé. $6 \mid 4 \times 3$ sans que 6 divise l'un des facteurs : seuls les nombres premiers ont cette propriété.

Correction de l'exercice 9 - Irrationalité de $\sqrt{2}$

Premier point : 2 est premier, donc par le lemme d'Euclide (exercice 8), $2 \mid n^2$ entraîne $2 \mid n$.

On peut aussi le voir directement : si n est impair, $n = 2k + 1$ et $n^2 = 4k^2 + 4k + 1$ est impair. Par contraposée, n^2 pair impose n pair.

Supposons maintenant $\sqrt{2}$ rationnel : $\sqrt{2} = \frac{a}{b}$ avec a et b entiers, $b \neq 0$, et la fraction IRRÉDUCTIBLE (donc $\text{PGCD}(a; b) = 1$).

En élevant au carré : $2 = \frac{a^2}{b^2}$, donc $a^2 = 2b^2$.

Ainsi a^2 est pair, donc a est pair d'après la question 1. Écrivons $a = 2a'$.

En reportant : $(2a')^2 = 2b^2$, soit $4a'^2 = 2b^2$, c'est-à-dire $b^2 = 2a'^2$.

Donc b^2 est pair, et b est pair à son tour.

Mais alors a et b sont tous deux pairs, donc divisibles par 2 : cela contredit l'irréductibilité de $\frac{a}{b}$.

L'hypothèse est donc fausse : $\sqrt{2}$ est IRRATIONNEL.

Pour $\sqrt{3}$, le raisonnement est identique, à condition d'établir d'abord que $3 \mid n^2 \Rightarrow 3 \mid n$ — ce qui découle du lemme d'Euclide, 3 étant premier.

On suppose $\sqrt{3} = \frac{a}{b}$ irréductible, d'où $a^2 = 3b^2$, donc $3 \mid a$, puis $a = 3a'$ et $9a'^2 = 3b^2$, soit $b^2 = 3a'^2$.

Donc $3 \mid b$ également : contradiction avec l'irréductibilité. $\sqrt{3}$ est irrationnel.

Attention : la méthode échoue pour $\sqrt{4}$, et c'est heureux — car 4 est un carré parfait, et $\sqrt{4} = 2$ est bien rationnel. Le point de blocage est que 4 n'est pas premier.

Réponse. 2 premier et $2 \mid n^2$ donnent $2 \mid n$ · de $a^2 = 2b^2$ on déduit a puis b pairs, ce qui contredit l'irréductibilité : $\sqrt{2}$ est irrationnel · même schéma pour $\sqrt{3}$.

Rappel de cours. Schéma : supposer la fraction irréductible, montrer que numérateur et dénominateur sont tous deux divisibles par p , conclure à la contradiction. Valable pour

$\sqrt{p}$ avec p premier.

Erreur fréquente. Oublier de préciser que la fraction est irréductible. C'est cette hypothèse qui rend la conclusion contradictoire : sans elle, il n'y a aucune contradiction.

Correction de l'exercice 10 - Somme des diviseurs et nombres parfaits

Diviseurs positifs de 28 : 1, 2, 4, 7, 14, 28.

Leur somme vaut $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

Or $2 \times 28 = 56$: on a bien $\sigma(28) = 2 \times 28$, donc 28 est PARFAIT.

Autre lecture : la somme des diviseurs STRICTS (tous sauf 28) vaut $1 + 2 + 4 + 7 + 14 = 28$ ✓.

Formule pour une puissance de premier : les diviseurs de p^k sont exactement $1, p, p^2, \dots, p^k$, puisque tout diviseur s'écrit p^α avec $0 \leq \alpha \leq k$.

Leur somme est donc $\sigma(p^k) = 1 + p + \dots + p^k$, soit $\frac{p^{k+1} - 1}{p - 1}$ par la somme géométrique.

Pour un entier quelconque, la fonction σ est MULTIPLICATIVE sur les facteurs premiers distincts : $\sigma(ab) = \sigma(a)\sigma(b)$ lorsque a et b sont premiers entre eux.

Cela vient de ce que tout diviseur de $360 = 2^3 \times 3^2 \times 5$ s'écrit de façon unique comme produit d'un diviseur de 2^3 , d'un de 3^2 et d'un de 5 : développer le produit des trois sommes redonne exactement la somme de tous les diviseurs.

Donc $\sigma(360) = (1 + 2 + 4 + 8)(1 + 3 + 9)(1 + 5)$.

On calcule : $15 \times 13 \times 6 = 15 \times 78 = 1170$. Donc $\sigma(360) = 1170$.

Comme $2 \times 360 = 720 \neq 1170$, le nombre 360 n'est pas parfait (il est même « abondant », sa somme dépassant $2n$).

Pour 496, commençons par décomposer : $496 = 2^4 \times 31$, et 31 est premier.

Donc $\sigma(496) = (1 + 2 + 4 + 8 + 16)(1 + 31) = 31 \times 32 = 992$.

Or $2 \times 496 = 992$ ✓ : 496 est parfait.

On remarque la forme $496 = 2^4(2^5 - 1)$, avec $2^5 - 1 = 31$ premier — de même que $28 = 2^2(2^3 - 1)$ avec 7 premier. C'est le lien avec les nombres de Mersenne de l'exercice 13.

Réponse. $\sigma(28) = 56 = 2 \times 28$, donc 28 est parfait · $\sigma(p^k) = 1 + p + \dots + p^k$ et $\sigma(360) = 15 \times 13 \times 6 = 1170 \neq 2 \times 360$ et $\sigma(496) = 31 \times 32 = 992 = 2 \times 496$: parfait.

Rappel de cours. σ se calcule facteur par facteur :

$\sigma(p^a q^b) = (1 + p + \dots + p^a)(1 + q + \dots + q^b)$. Un nombre est parfait lorsque $\sigma(n) = 2n$.

Erreur fréquente. Confondre « somme des diviseurs » et « somme des diviseurs stricts ». La condition de perfection s'écrit $\sigma(n) = 2n$ avec la première convention, $\sigma(n) - n = n$ avec la seconde.

Correction de l'exercice 11 - Le petit théorème de Fermat

Pour $p = 7$ et $a = 2$: le théorème annonce $2^6 \equiv 1 [7]$.

Calcul : $2^6 = 64$, et $64 = 7 \times 9 + 1$, donc $2^6 \equiv 1 [7]$ ✓.

On peut d'ailleurs le retrouver de proche en proche : $2^3 = 8 \equiv 1 [7]$, donc

$$2^6 = (2^3)^2 \equiv 1 [7].$$

Remarque utile : la période réelle est ici 3, qui DIVISE 6. Le théorème donne un exposant qui fonctionne, pas nécessairement le plus petit.

Pour $p = 11$ et $a = 3$: le théorème annonce $3^{10} \equiv 1 [11]$.

Calcul : $3^5 = 243 = 11 \times 22 + 1$, donc $3^5 \equiv 1 [11]$, et par élévation au carré $3^{10} \equiv 1 [11]$ ✓.

Vérification directe : $3^{10} = 59\,049$, et $59\,049 = 11 \times 5368 + 1$ ✓.

Deuxième question : prenons $p = 8$, qui n'est pas premier, et $a = 3$ (avec $8 \nmid 3$).

Le théorème « donnerait » $3^7 \equiv 1 [8]$. Calculons : $3^2 = 9 \equiv 1 [8]$, donc $3^6 \equiv 1$ et $3^7 \equiv 3 [8]$.

On trouve 3 et non 1 : la conclusion est FAUSSE. L'hypothèse de primalité est donc indispensable.

Troisième question : si $p \mid a$, alors $a \equiv 0 [p]$, donc $a^{p-1} \equiv 0 [p]$ (pour $p \geq 2$) : la conclusion $a^{p-1} \equiv 1$ est évidemment fausse.

Il existe cependant une version qui couvre tous les cas : $a^p \equiv a [p]$, valable pour TOUT entier a , que p divise a ou non.

Vérification dans le cas gênant : si $p \mid a$, les deux membres sont congrus à 0 ✓. Et sinon, on multiplie $a^{p-1} \equiv 1$ par a ✓.

Réponse. $2^6 = 64 \equiv 1 [7]$ ✓ et $3^{10} = 59\,049 \equiv 1 [11]$ ✓ · avec $p = 8$ non premier, $3^7 \equiv 3 [8]$: la conclusion tombe · si $p \mid a$, on utilise la forme générale $a^p \equiv a [p]$.

Rappel de cours. Petit théorème de Fermat : p premier et $p \nmid a \Rightarrow a^{p-1} \equiv 1 [p]$. Forme générale valable sans condition : $a^p \equiv a [p]$. La période réelle divise $p - 1$.

Erreur fréquente. Croire que $p - 1$ est la plus petite période. Pour $a = 2$ et $p = 7$, la période est 3 : le théorème donne un exposant qui marche, pas le plus petit.

Correction de l'exercice 12 - Fermat au service des grands restes

7 est premier et ne divise pas 2, donc le petit théorème de Fermat donne $2^6 \equiv 1 [7]$.

On réduit l'exposant modulo 6 : $2026 = 6 \times 337 + 4$, donc $2026 \equiv 4 [6]$.

$$\text{D'où } 2^{2026} = (2^6)^{337} \times 2^4 \equiv 1^{337} \times 16 [7].$$

Et $16 = 7 \times 2 + 2$, donc $2^{2026} \equiv 2 [7]$. Le reste est 2.

Deuxième calcul : 11 est premier et ne divise pas 3, donc $3^{10} \equiv 1 [11]$.

On réduit l'exposant modulo 10 : $2026 = 10 \times 202 + 6$, donc $2026 \equiv 6 [10]$.

D'où $3^{2026} \equiv 3^6 [11]$. Or $3^6 = 729$, et $729 = 11 \times 66 + 3$.

Donc $3^{2026} \equiv 3 [11]$: le reste est 3.

On peut alléger le calcul de 3^6 : $3^5 \equiv 1 [11]$ (vu à l'exercice 11), donc $3^6 \equiv 3 [11]$ directement ✓.

Comparaison des méthodes. Avec le tableau du chapitre 5, il fallait calculer les puissances successives jusqu'à retomber sur 1 : six lignes pour $p = 7$, cinq ou dix pour $p = 11$.

Avec Fermat, l'exposant $p - 1$ est connu D'AVANCE : on réduit immédiatement modulo $p - 1$, sans aucun tableau.

Le gain devient décisif pour un grand module : modulo 101, le tableau exigerait jusqu'à cent lignes, alors que Fermat donne aussitôt $a^{100} \equiv 1 [101]$.

Seule précaution : vérifier que le module est bien PREMIER, et qu'il ne divise pas la base.

Réponse. $2^{2026} \equiv 2 [7]$ (car $2^6 \equiv 1$ et $2026 \equiv 4 [6]$) · $3^{2026} \equiv 3 [11]$ (car $3^{10} \equiv 1$ et $2026 \equiv 6 [10]$).

Rappel de cours. Avec p premier ne divisant pas a : on réduit l'exposant modulo $p - 1$, puis on calcule la petite puissance restante. Deux modules interviennent : p pour le résultat, $p - 1$ pour l'exposant.

Erreur fréquente. Réduire l'exposant modulo p au lieu de $p - 1$. C'est $p - 1$ qui est la période fournie par le théorème.

Correction de l'exercice 13 - Nombres de Mersenne

Supposons n non premier : $n = ab$ avec $2 \leq a$ et $2 \leq b$.

On utilise l'identité de factorisation $x^b - 1 = (x - 1)(x^{b-1} + \dots + x + 1)$, appliquée à $x = 2^a$.

Comme $2^n = 2^{ab} = (2^a)^b$, on obtient $2^n - 1 = (2^a - 1)((2^a)^{b-1} + \dots + 2^a + 1)$.

Le premier facteur $2^a - 1$ vaut au moins 3 (car $a \geq 2$) et il est strictement inférieur à $2^n - 1$.

M_n admet donc un diviseur strict autre que 1 : il n'est pas premier.

Contrôle : $n = 6 = 2 \times 3$ donne $M_6 = 63$, et la factorisation prédit le diviseur $2^2 - 1 = 3$. Effectivement $63 = 7 \times 9$ ✓.

Conclusion : pour que M_n soit premier, il est NÉCESSAIRE que n le soit.

La réciproque est-elle vraie ? Testons $n = 11$, qui est premier :

$$M_{11} = 2^{11} - 1 = 2048 - 1 = 2047.$$

On cherche un diviseur : $\sqrt{2047} \approx 45,2$, on teste les premiers jusqu'à 43.

On trouve $2047 = 23 \times 89$. Donc M_{11} n'est PAS premier alors que 11 l'est.

La réciproque est donc FAUSSE : la condition « n premier » est nécessaire, pas suffisante.

Petites valeurs : $M_2 = 3$ (premier ✓), $M_3 = 7$ (premier ✓), $M_5 = 31$ (premier ✓), $M_7 = 127$ (premier ✓).

Vérification pour 127 : $\sqrt{127} \approx 11,3$, et 127 n'est divisible ni par 2, 3, 5, 7 ni 11 ✓.

Le premier échec est donc $M_{11} = 2047$. C'est ce qui rend la recherche de premiers de Mersenne intéressante : le critère élimine énormément de candidats, mais il faut encore tester chaque n premier.

Lien avec l'exercice 10 : lorsque M_n est premier, $2^{n-1}M_n$ est un nombre parfait — c'est ainsi que $2^2 \times 7 = 28$ et $2^4 \times 31 = 496$ ont été obtenus.

Réponse. $n = ab$ donne la factorisation $2^n - 1 = (2^a - 1)(\dots)$, donc M_n n'est pas premier · réciproque fautive : 11 est premier mais $M_{11} = 2047 = 23 \times 89$ · $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ sont tous premiers.

Rappel de cours. $M_n = 2^n - 1$ premier $\Rightarrow n$ premier (condition nécessaire, non suffisante). Et si M_n est premier, $2^{n-1}M_n$ est un nombre parfait.

Erreur fréquente. Conclure de « n premier » que M_n l'est. $M_{11} = 2047 = 23 \times 89$ suffit à réfuter cette implication.

Correction de l'exercice 14 - Nombres de Fermat

Raisonnons par contraposée : supposons que n ne soit PAS une puissance de 2.

Alors n admet un diviseur impair $m \geq 3$, et l'on écrit $n = m\ell$.

On utilise l'identité $x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \dots - x + 1)$, valable précisément parce que m est IMPAIR.

Appliquée à $x = 2^\ell$, elle donne $2^n + 1 = (2^\ell)^m + 1 = (2^\ell + 1)(\dots)$.

Le facteur $2^\ell + 1$ vaut au moins 3 et est strictement inférieur à $2^n + 1$: ce dernier n'est donc pas premier.

Par contraposée, si $2^n + 1$ est premier, alors n est une puissance de 2.

Contrôle : $n = 5$ (impair, non puissance de 2) donne $2^5 + 1 = 33 = 3 \times 11$ ✓, et le facteur $3 = 2^1 + 1$ est bien celui que prédit l'identité.

Calcul des nombres de Fermat. $F_0 = 2^1 + 1 = 3$ ✓ premier.

$F_1 = 2^2 + 1 = 5$ ✓ premier. $F_2 = 2^4 + 1 = 17$ ✓ premier.

$F_3 = 2^8 + 1 = 257$. Test : $\sqrt{257} \approx 16,0$, et 257 n'est divisible ni par 2, 3, 5, 7, 11, 13 : il est premier ✓.

$F_4 = 2^{16} + 1 = 65\,537$. C'est également un nombre premier (le test demande les premiers jusqu'à 256).

Fermat, ayant vérifié ces cinq cas, conjectura que tous les F_k sont premiers.

Pour $k = 5$: $F_5 = 2^{32} + 1 = 4\,294\,967\,297$.

Euler montra en 1732 que $F_5 = 641 \times 6\,700\,417$: la conjecture est FAUSSE.

Et la situation est pire que prévu : à ce jour, aucun F_k premier n'a été trouvé au-delà de F_4 . Cinq cas favorables ne font pas une démonstration — c'est la leçon de méthode de cet exercice.

Réponse. Si n a un diviseur impair $m \geq 3$, alors $2^\ell + 1$ divise $2^n + 1$: donc n doit être une puissance de 2. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$ sont premiers · mais $F_5 = 2^{32} + 1 = 641 \times 6\,700\,417$ ne l'est pas.

Rappel de cours. $x^m + 1$ se factorise par $x + 1$ quand m est IMPAIR : c'est ce qui force n à être une puissance de 2. La condition est nécessaire, jamais suffisante.

Erreur fréquente. Conclure d'une vérification sur cinq cas. Fermat lui-même s'y est trompé : F_5 réfute la conjecture.

Correction de l'exercice 15 - Décomposition, carrés et puissances

Sens direct : si $n = m^2$, écrivons $m = p_1^{b_1} \dots p_r^{b_r}$.

Alors $n = m^2 = p_1^{2b_1} \dots p_r^{2b_r}$: tous les exposants sont pairs. Et cette décomposition est LA décomposition de n , par unicité.

Sens réciproque : si $n = p_1^{2c_1} \dots p_r^{2c_r}$ avec tous les exposants pairs, on pose $m = p_1^{c_1} \dots p_r^{c_r}$.

Alors $m^2 = n$: l'entier n est bien un carré parfait.

Deuxième question : $360 = 2^3 \times 3^2 \times 5^1$.

Pour que $360k$ soit un carré, il faut que chaque exposant de sa décomposition soit pair.

L'exposant de 2 vaut 3 : impair, il faut lui ajouter au moins 1. Celui de 3 vaut 2 : déjà pair, rien à ajouter. Celui de 5 vaut 1 : il faut ajouter au moins 1.

Le plus petit k est donc $2^1 \times 5^1 = 10$.

Vérification : $360 \times 10 = 3600 = 2^4 \times 3^2 \times 5^2$, tous exposants pairs, et $3600 = 60^2$ ✓.

Troisième question : pour un CUBE, il faut que chaque exposant soit multiple de 3.

Exposant de 2 : il vaut 3, déjà multiple de 3 — rien à ajouter.

Exposant de 3 : il vaut 2, il faut atteindre 3, donc ajouter 1.

Exposant de 5 : il vaut 1, il faut atteindre 3, donc ajouter 2.

Le plus petit k est donc $3^1 \times 5^2 = 3 \times 25 = 75$.

Vérification : $360 \times 75 = 27\,000 = 2^3 \times 3^3 \times 5^3 = 30^3 \checkmark$.

Méthode à retenir : on complète chaque exposant jusqu'au prochain multiple de l'exposant visé — 2 pour un carré, 3 pour un cube.

Réponse. n est un carré $\Rightarrow$ tous les exposants de sa décomposition sont pairs · plus petit k pour que $360k$ soit un carré : $k = 10$ (et $3600 = 60^2$) · pour un cube : $k = 75$ (et $27\,000 = 30^3$).

Rappel de cours. Carré $\Rightarrow$ exposants pairs · cube $\Rightarrow$ exposants multiples de 3 · puissance m -ième $\Rightarrow$ exposants multiples de m . On complète chaque exposant au multiple suivant.

Erreur fréquente. Multiplier par 360 lui-même pour obtenir un carré. Cela marche (360^2), mais ce n'est pas le plus petit k : seuls les exposants manquants sont à compléter.

Correction de l'exercice 16 - Des trous arbitrairement grands entre les nombres premiers

Soit k un entier avec $2 \leq k \leq n$. Considérons l'entier $n! + k$.

Comme $2 \leq k \leq n$, le facteur k apparaît dans le produit $n! = 1 \times 2 \times \dots \times n$: donc k divise $n!$.

k divise aussi k , donc k divise la somme $n! + k$.

Or $n! + k > k > 1$: l'entier $n! + k$ admet donc un diviseur strictement compris entre 1 et lui-même. Il est COMPOSÉ.

Cela vaut pour chaque k de 2 à n : on obtient $n - 1$ entiers consécutifs tous composés.

Illustration avec $n = 5$: $5! = 120$, et les entiers concernés sont 122, 123, 124, 125.

$122 = 2 \times 61$ (divisible par 2, comme annoncé) $\checkmark$.

$123 = 3 \times 41$ (divisible par 3) $\checkmark$.

$124 = 4 \times 31$ (divisible par 4) $\checkmark$.

$125 = 5^3$ (divisible par 5) $\checkmark$.

Quatre entiers consécutifs sans aucun nombre premier — et le diviseur de chacun est exactement le k ajouté, ce qui rend la construction transparente.

Pour un intervalle de 100 entiers consécutifs, il suffit de prendre $n = 101$.

Les entiers $101! + 2$, $101! + 3$, ..., $101! + 101$ sont alors tous composés : cela fait 100 entiers consécutifs sans nombre premier.

Le nombre $101!$ est astronomique (environ $9,4 \times 10^{159}$), mais la démonstration n'exige pas de le calculer : elle exhibe seulement un diviseur pour chaque terme.

Conclusion de méthode : on peut donc trouver des trous AUSSI GRANDS QU'ON VEUT entre deux nombres premiers, alors même qu'il en existe une infinité. Les deux faits sont parfaitement compatibles.

Réponse. Pour $2 \leq k \leq n$, k divise $n!$ et k , donc $k \mid n! + k$: ces $n - 1$ entiers sont composés · pour $n = 5$: 122, 123, 124, 125 · pour 100 entiers consécutifs, prendre $n = 101$.

Rappel de cours. Construction de trous : $n! + 2, \dots, n! + n$ sont composés. Il existe donc des intervalles arbitrairement longs sans nombre premier, ce qui n'empêche pas leur infinité.

Erreur fréquente. Commencer à $n! + 1$. Cet entier-là peut très bien être premier : la construction ne fonctionne qu'à partir de $n! + 2$.

Correction de l'exercice 17 - $p^2 - 1$ est divisible par 24

$p^2 - 1 = (p - 1)(p + 1)$. Comme $p \geq 5$ est premier, il est impair : $p - 1$ et $p + 1$ sont deux entiers pairs consécutifs.

Parmi deux entiers pairs consécutifs, l'un est multiple de 4 : le produit $(p - 1)(p + 1)$ est donc divisible par $2 \times 4 = 8$.

Parmi les trois entiers consécutifs $p - 1, p, p + 1$, l'un est multiple de 3. Ce n'est pas p (premier et différent de 3) : 3 divise $(p - 1)(p + 1)$.

3 et 8 sont premiers entre eux et divisent tous deux $p^2 - 1$: d'après le théorème de Gauss, 24 divise $p^2 - 1$.

Vérification : $24 = 24 \times 1$, $48 = 24 \times 2$, $120 = 24 \times 5$.

Réponse. $24 \mid p^2 - 1$ pour tout premier $p \geq 5$.

Rappel de cours. Si $a \mid n$, $b \mid n$ et $\text{PGCD}(a, b) = 1$, alors $ab \mid n$.

Erreur fréquente. Le résultat est faux pour $p = 2$ (3) et $p = 3$ (8) : les hypothèses p impair et $p \neq 3$ sont indispensables.

Correction de l'exercice 18 - Inverse modulaire par le petit théorème de Fermat

Par le petit théorème de Fermat, $a^{p-1} \equiv 1 [p]$.

Or $a^{p-1} = a \times a^{p-2}$, à condition que $p - 2 \geq 0$, ce qui est vrai pour $p \geq 2$.

Donc $a \times a^{p-2} \equiv 1 [p]$: par définition, a^{p-2} est un inverse de a modulo p .

C'est une formule EXPLICITE : contrairement à Bézout, elle ne demande aucun algorithme, seulement une exponentiation modulaire.

Application : inverse de 3 modulo 7. La formule donne $3^{7-2} = 3^5$.

Calcul modulo 7, en réduisant à chaque étape : $3^2 = 9 \equiv 2$; $3^4 \equiv 2^2 = 4$; $3^5 \equiv 4 \times 3 = 12 \equiv 5 [7]$.

L'inverse de 3 modulo 7 est donc 5.

Vérification : $3 \times 5 = 15 = 14 + 1 \equiv 1 [7]$ ✓.

Inverse de 5 modulo 11 : la formule donne 5^9 .

Calcul par élévations au carré successives : $5^2 = 25 \equiv 3 [11]$; $5^4 \equiv 3^2 = 9$; $5^8 \equiv 9^2 = 81 \equiv 4 [11]$.

Puis $5^9 = 5^8 \times 5 \equiv 4 \times 5 = 20 \equiv 9 [11]$.

L'inverse de 5 modulo 11 est donc 9. Vérification : $5 \times 9 = 45 = 44 + 1 \equiv 1 [11]$ ✓.

Comparaison. Par Bézout : $11 = 2 \times 5 + 1$, donc $1 = 11 - 2 \times 5$, d'où $-2 \times 5 \equiv 1 [11]$ et l'inverse est $-2 \equiv 9$ ✓ — même résultat, en deux lignes.

Bilan : sur de petits nombres, Bézout est plus rapide. La formule de Fermat, elle, ne demande aucune réflexion — c'est ce qui la rend précieuse en programmation, où l'exponentiation rapide est immédiate.

Limite à retenir : la formule de Fermat exige un module PREMIER, alors que Bézout fonctionne dès que a et n sont premiers entre eux.

Réponse. $a \times a^{p-2} = a^{p-1} \equiv 1 [p]$, donc a^{p-2} est l'inverse de a · inverse de 3 modulo 7 : $3^5 \equiv 5 \cdot \text{inverse de 5 modulo 11} : 5^9 \equiv 9$, résultat identique à celui de Bézout.

Rappel de cours. Module PREMIER : l'inverse de a est $a^{p-2} \bmod p$. Module quelconque (avec $\text{PGCD}(a; n) = 1$) : il faut passer par Bézout.

Erreur fréquente. Appliquer la formule à un module composé. Modulo 26, a^{24} n'est pas un inverse : le petit théorème de Fermat ne s'applique pas.

Correction de l'exercice 19 - La réciproque du théorème de Fermat est fausse

Si 9 était premier, le petit théorème de Fermat donnerait $2^8 \equiv 1 [9]$.

Calculons : $2^3 = 8 \equiv -1 [9]$, donc $2^6 \equiv 1 [9]$, puis $2^8 = 2^6 \times 2^2 \equiv 4 [9]$.

On trouve 4 et non 1 : la conclusion du théorème est en défaut, donc 9 n'est PAS premier.

C'est bien sûr évident ici ($9 = 3^2$), mais la méthode est remarquable : elle prouve la non-primalité SANS exhiber de diviseur.

C'est exactement ce qui la rend utile sur de très grands nombres, où chercher un diviseur serait hors de portée.

Deuxième question : $561 = 3 \times 11 \times 17$, il n'est donc manifestement pas premier.

Vérifions pourtant la congruence de Fermat. Comme $561 = 3 \times 11 \times 17$, on examine 2^{560} modulo chacun des trois facteurs.

Modulo 3 : $2^2 \equiv 1 [3]$ par Fermat, et $560 = 2 \times 280$, donc $2^{560} \equiv 1 [3]$.

Modulo 11 : $2^{10} \equiv 1 [11]$, et $560 = 10 \times 56$, donc $2^{560} \equiv 1 [11]$.

Modulo 17 : $2^{16} \equiv 1 [17]$, et $560 = 16 \times 35$, donc $2^{560} \equiv 1 [17]$.

Ainsi $2^{560} - 1$ est divisible par 3, 11 et 17, qui sont premiers entre eux deux à deux : il est donc divisible par leur produit 561.

Autrement dit $2^{560} \equiv 1 [561]$ ✓, alors que 561 n'est pas premier.

Le nombre 561 est le plus petit nombre de CARMICHAEL : la congruence de Fermat y est vérifiée pour TOUTE base premier avec 561, et pas seulement pour 2.

Conclusion : le test de Fermat est une condition NÉCESSAIRE de primalité, jamais suffisante.

Concrètement : si la congruence échoue, on est CERTAIN que le nombre est composé. Si elle réussit, on a seulement une présomption — le nombre est dit « pseudo-premier » pour cette base.

Cette asymétrie est la raison d'être des tests de primalité modernes (Miller-Rabin), qui raffinent celui de Fermat pour éliminer précisément les nombres de Carmichael.

Réponse. $2^8 \equiv 4 \not\equiv 1 [9]$, donc 9 n'est pas premier · $561 = 3 \times 11 \times 17$ n'est pas premier, et pourtant $2^{560} \equiv 1 [561]$ · le test de Fermat prouve la NON-primalité, jamais la primalité.

Rappel de cours. $a^{n-1} \not\equiv 1 [n]$ prouve que n est composé, sans donner de diviseur. La réciproque est fausse : les nombres de Carmichael (561, 1105, 1729...) passent le test sans être premiers.

Erreur fréquente. Conclure « n est premier » d'une congruence vérifiée. C'est précisément ce que 561 interdit.

Correction de l'exercice 20 - Problème de synthèse : un chiffrement RSA

$$n = pq = 5 \times 11 = 55.$$

$$\varphi = (p - 1)(q - 1) = 4 \times 10 = 40.$$

Pour que e soit valide, il doit être premier avec φ — c'est la condition d'existence de son inverse d modulo φ .

Ici $\text{PGCD}(3; 40) = 1$ ✓ : le choix $e = 3$ convient.

Détermination de d : on cherche d tel que $3d \equiv 1 [40]$.

Par Bézout ou par essais : $3 \times 27 = 81 = 2 \times 40 + 1$, donc $3 \times 27 \equiv 1 [40]$.

La clé privée est donc $d = 27$.

Chiffrement de $m = 8$: $c \equiv 8^3 [55]$.

$$8^3 = 512, \text{ et } 512 = 55 \times 9 + 17 = 495 + 17, \text{ donc } c = 17.$$

Le message chiffré est 17. Déchiffrons-le : $m \equiv 17^{27} [55]$.

On procède par élévations au carré, en réduisant à chaque étape. $17^2 = 289$, et $289 = 55 \times 5 + 14$, donc $17^2 \equiv 14 [55]$.

$$17^4 \equiv 14^2 = 196, \text{ et } 196 = 55 \times 3 + 31, \text{ donc } 17^4 \equiv 31 [55].$$

$$17^8 \equiv 31^2 = 961, \text{ et } 961 = 55 \times 17 + 26, \text{ donc } 17^8 \equiv 26 [55].$$

$$17^{16} \equiv 26^2 = 676, \text{ et } 676 = 55 \times 12 + 16, \text{ donc } 17^{16} \equiv 16 [55].$$

On décompose l'exposant : $27 = 16 + 8 + 2 + 1$.

Donc $17^{27} \equiv 16 \times 26 \times 14 \times 17 [55]$. On réduit au fur et à mesure : $16 \times 26 = 416 \equiv 31 [55]$ (car $416 = 385 + 31$).

Puis $31 \times 14 = 434 \equiv 49 [55]$ (car $434 = 385 + 49$).

Enfin $49 \times 17 = 833$, et $833 = 55 \times 15 + 8 = 825 + 8$, donc $17^{27} \equiv 8 [55]$ ✓.

On retrouve bien le message $m = 8$: le déchiffrement fonctionne.

Pourquoi ça marche : $ed \equiv 1 [\varphi]$ signifie $ed = 1 + k\varphi$, et l'on montre, à l'aide du petit théorème de Fermat appliqué modulo p puis modulo q , que $m^{ed} \equiv m [n]$.

Sécurité : la clé publique est $(n; e)$, donc $n = 55$ et $e = 3$ sont connus de tous. Pour retrouver d , il faut connaître $\varphi = (p - 1)(q - 1)$.

Or calculer φ exige de connaître p et q , c'est-à-dire de FACTORISER n .

Ici, $55 = 5 \times 11$ se factorise en une seconde. Mais avec deux nombres premiers de 300 chiffres chacun, aucun algorithme connu ne permet de factoriser n en un temps raisonnable — alors que le chiffrement, lui, reste immédiat.

Toute la sécurité tient dans cette asymétrie : multiplier deux grands nombres premiers est facile, retrouver les facteurs ne l'est pas.

Réponse. $n = 55$, $\varphi = 40$, et $\text{PGCD}(3; 40) = 1$ valide $e = 3$ · clé privée $d = 27$ (car $3 \times 27 = 81 \equiv 1 [40]$) · $8^3 \equiv 17 [55]$ et $17^{27} \equiv 8 [55]$ ✓ · la sécurité repose sur l'impossibilité pratique de factoriser n pour retrouver φ , donc d .

Rappel de cours. RSA en une ligne : $n = pq$, $\varphi = (p - 1)(q - 1)$, $ed \equiv 1 [\varphi]$, chiffrement $c \equiv m^e$, déchiffrement $m \equiv c^d [n]$. Les grandes puissances se calculent par élévations au carré successives.

Erreur fréquente. Calculer 17^{27} directement. Ce nombre a plus de trente chiffres : on réduit modulo 55 à CHAQUE étape, en décomposant l'exposant en somme de puissances de 2.