

Nombres premiers — Terminale maths expertes

20 exercices corrigés · mathlvl.fr

Énoncés

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 .