

Nombres premiers et décomposition — cours de maths 4e

Certains nombres ne se cassent pas : 7, 13, 31 n'ont d'autres diviseurs qu'eux-mêmes et 1. Tous les autres se fabriquent en les multipliant, et d'une seule façon. C'est ce qui fait des nombres premiers les briques élémentaires de l'arithmétique — et ce qui rend la décomposition si utile pour simplifier, compter ou comparer.

LA DÉFINITION

EXACTEMENT deux diviseurs : 1 et lui-même

CE QU'IL FAUT SAVOIR

La liste jusqu'à 30 · et savoir TROUVER jusqu'à 100

LE PIÈGE

1 n'est pas premier, et 91 non plus — il vaut 7×13

À quoi ça sert : Nombres premiers et décomposition

Les nombres premiers ont longtemps passé pour la partie la plus inutile des mathématiques — le mathématicien anglais Hardy s'en félicitait encore en 1940, y voyant une science pure que rien ne pourrait salir. Trente-cinq ans plus tard, ils sont devenus la clé de tout ce qui se paie en ligne. Le chiffrement RSA, qui protège les connexions bancaires, repose sur un déséquilibre : multiplier deux très grands nombres premiers est instantané, mais retrouver ces deux facteurs à partir du produit demanderait des siècles à un ordinateur. Chacun peut donc publier le produit — c'est la clé publique — sans que personne ne puisse en déduire les facteurs, qui sont la clé privée. C'est exactement la décomposition en facteurs premiers de cette fiche, avec des nombres de plusieurs centaines de chiffres. Le cadenas d'un site marchand, un paiement sans contact, une messagerie chiffrée : tous reposent sur le fait qu'on sait multiplier bien mieux qu'on ne sait décomposer.

Un peu d'histoire : Nombres premiers et décomposition

Euclide démontre vers 300 avant notre ère qu'il existe une infinité de nombres premiers, et sa preuve tient en trois lignes qu'on comprend encore aujourd'hui : si la liste était finie, on multiplierait tous ses éléments et on ajouterait 1 ; le nombre obtenu ne serait divisible par aucun d'eux, ce qui est absurde. Ératosthène, bibliothécaire d'Alexandrie au siècle suivant, invente la méthode pour les trouver — on écrit tous les nombres, on garde 2 puis on barre ses multiples, on garde 3 puis on barre les siens, et ainsi de suite. C'est le crible qui porte son nom, et c'est encore la méthode enseignée. Le même Ératosthène avait mesuré la circonférence de la Terre à quelques pour cent près, en comparant l'ombre de deux bâtons dans deux villes éloignées. Les nombres premiers restent, vingt-trois siècles plus tard, un sujet de recherche ouvert : personne ne sait s'il existe une infinité de nombres premiers jumeaux — deux premiers séparés de 2, comme 11 et 13, ou 29 et 31.

Définition : Nombres premiers et décomposition

Un nombre premier est un entier qui a **EXACTEMENT** deux diviseurs : 1 et lui-même. 7 est premier, car aucun autre nombre ne le divise. 12 ne l'est pas, car 2, 3, 4 et 6 le divisent aussi. ⚠ Le mot important est « exactement » : 1 n'a qu'UN seul diviseur — « 1 » et « lui-même » désignent ici le même nombre — donc 1 n'est pas premier. ★ Le plus petit nombre premier est 2, et c'est aussi le seul qui soit pair.

Données	nombre	ses diviseurs	premier ?
	1	1	non : un seul
	2	1 et 2	OUI
	7	1 et 7	OUI
	12	1,2,3,4,6,12	non : six

on compte les diviseurs

Tout se joue sur un décompte. Deux diviseurs exactement : le nombre est premier. Un seul, ou plus de deux : il ne l'est pas. C'est la seule définition à retenir, et elle règle aussi le cas de 1.

Propriétés : Nombres premiers et décomposition

Exactement deux diviseurs, ni plus ni moins

Tout nombre entier plus grand que 1 possède au moins deux diviseurs : 1 et lui-même. Ceux qui n'en ont QUE ces deux-là sont les nombres premiers. ⚠ Pour montrer qu'un nombre n'est pas premier, un seul autre diviseur suffit — inutile de tous les chercher.

Données	combien de diviseurs
	1 seul
	exactement 2
	3 ou plus

La liste jusqu'à 30, à connaître par cœur

2, 3, 5, 7, 11, 13, 17, 19, 23, 29 : dix nombres, et le programme demande de les savoir. ⚠ Les faux amis les plus fréquents sont les multiples de 3 impairs — 9, 15, 21, 27 — qui n'ont pas l'air composés parce qu'ils sont impairs. Le critère par 3 les démasque en une seconde.

Données	premiers ≤ 30	faux
	2, 3, 5, 7	9
	11, 13, 17, 19	15, 21, 27
	23, 29	33

impair ne veut pas dire premier

Jusqu'à 100, quatre tests suffisent

Les diviseurs vont par paires : si d divise n , alors $n \div d$ le divise aussi. Dans chaque paire, l'un des deux est au plus la racine carrée de n . ★ Pour un nombre inférieur à 100, il suffit donc de tester 2, 3, 5 et 7 — car $11^2 = 121$ dépasse déjà 100.

Données	on teste	car
	2	$2^2 = 4 \leq 100$
	3	$3^2 = 9 \leq 100$
	5	$5^2 = 25 \leq 100$

le décompte décide

Données	on teste	car
	7	$7^2 = 49 \leq 100$
	11 : inutile	$11^2 = 121 > 100$

quatre tests, et on s'arrête

91 a l'air premier — il vaut 7×13

Il est impair, il ne finit pas par 5, et $9 + 1 = 10$ n'est pas divisible par 3. Trois tests passent, et l'élève conclut trop vite. ⚠ Le quatrième est celui qu'on oublie : $91 \div 7 = 13$. C'est exactement pour ce genre de nombre que la liste jusqu'à 30 ne suffit pas, et que la MÉTHODE est demandée.

$$91 \div 7$$

quotient **reste**
: 13 **: 0**

Vérification :
dividende =
diviseur $\times$
quotient +
reste

$91 = 7 \times 13$, **reste 0** : il n'est pas premier

Toute décomposition est unique

Tout entier plus grand que 1 s'écrit comme un produit de nombres premiers, et d'UNE SEULE façon — à l'ordre près. $60 = 2 \times 2 \times 3 \times 5$, et il n'existe aucune autre écriture.

★ C'est cette unicité qui interdit à 1 d'être premier : sinon on pourrait ajouter autant de 1 qu'on veut, et l'écriture ne serait plus unique.

Données	on divise	par
	60	2
	30	2
	15	3
	5	5

$$60 = 2 \times 2 \times 3 \times 5$$

La décomposition compte les diviseurs sans les lister

Dans $12 = 2 \times 2 \times 3$, le facteur 2 apparaît deux fois et le 3 une fois.

Pour fabriquer un diviseur, on choisit combien de fois on prend chacun : 0, 1 ou 2 fois le 2, et 0 ou 1 fois le 3. Cela fait $3 \times 2 = 6$ diviseurs. ★ On les a comptés sans en écrire un seul.

Données	facteur	app
	2	2
	3	1
	total	

12 a bien 6 diviseurs

La formule : Nombres premiers et décomposition

TOUT ENTIER PLUS GRAND QUE 1

$$n = p_1 \times p_2 \times \dots \times p_k$$

où chaque facteur est un nombre premier — et cette écriture est **UNIQUE**, à l'ordre près. C'est le théorème fondamental de l'arithmétique, et c'est lui qui fait des nombres premiers les briques élémentaires : tout nombre se construit avec, et d'une seule façon.

Données	nombre	décomposition
	36	$2 \times 2 \times 3 \times 3$
	60	$2 \times 2 \times 3 \times 5$
	97	97 (déjà premier)

un nombre premier est sa propre décomposition

Méthode : Nombres premiers et décomposition

1. Décider si un nombre est premier

On teste les nombres premiers dont le carré ne dépasse pas le nombre : 2, 3, 5, 7 pour tout ce qui est inférieur à 100. Dès qu'une division tombe juste, c'est fini : le nombre n'est pas premier. Si les quatre échouent, il l'est.

Données	pour 83	résultat
	par 2 ?	non, il est impair
	par 3 ?	$8+3=11$ non
	par 5 ?	non, fin par 3
	par 7 ?	$83 = 7 \times 11 + 6$ non

83 est premier

2. Construire le crible d'Ératosthène

On écrit les nombres de 2 à 100. On entoure 2, puis on barre tous ses multiples. On entoure le plus petit nombre non barré — 3 — et on barre les siens. Puis 5, puis 7. ★ On s'arrête là : tout ce qui reste est premier, et il y en a 25.

Données	on entoure	on barre
	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100
	3	9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99
	5	25, 35, 45, 55, 65, 75, 85, 95
	7	49, 77, 91, 98

après 7, tout ce qui reste est premier

3. Décomposer un nombre

On divise par le plus petit nombre premier possible, on recommence sur le quotient, et on s'arrête quand on tombe sur 1. ⚠ Deux contrôles avant de conclure : chaque facteur doit être PREMIER, et leur produit doit redonner le nombre de départ.

$$84 \div 2$$

quotient : 42 reste : 0

Vérification :
dividende =
diviseur ×
quotient +
reste

on commence par 2, puis on recommence sur 42

4. Simplifier une fraction par la décomposition

On décompose le numérateur et le dénominateur, puis on barre tous les facteurs communs. ★ C'est ici que la décomposition SERT vraiment : elle montre d'un coup tout ce qui peut se barrer, au lieu de simplifier par petits pas au hasard.

Données		décom
	84	2×2
	126	2×3
	reste	

on barre 2, 3 et 7

5. Compter les diviseurs sans les lister

On décompose, on compte combien de fois chaque facteur premier apparaît, on ajoute 1 à chacun de ces comptes, et on multiplie le tout. Pour $36 = 2^2 \times 3^2 : (2 + 1) \times (2 + 1) = 9$ diviseurs.

Données	36 =	2×2
	le 2 apparaît	2 fois 3 c
	le 3 apparaît	2 fois 3 c
	en tout	$3 \times$

neuf diviseurs, sans en écrire un

Selon ce que l'on cherche : Nombres premiers et décomposition

On me demande si un nombre est premier

On teste 2, 3, 5 et 7 si le nombre est inférieur à 100. Une seule division juste suffit à conclure que non.

On me demande de décomposer un nombre

On divise par le plus petit premier possible, encore et encore, jusqu'à 1. Puis on vérifie en refaisant le produit.

On me demande de simplifier une fraction

On décompose le haut et le bas, et on barre les facteurs communs. Ce qui reste est irréductible.

On me demande combien un nombre a de diviseurs

On décompose, on ajoute 1 à chaque exposant, et on multiplie.

Aucun diviseur n'a besoin d'être écrit.

Exemples corrigés : Nombres premiers et décomposition

Le nombre qui a l'air premier

On demande si 91 est un nombre premier.

Que répondre, et comment le justifier ?

$$91 \div 7$$

quotient :
13

reste : 0

Vérification : $\text{dividende} = \text{diviseur} \times \text{quotient} + \text{reste}$

On teste les nombres premiers dont le carré ne dépasse pas 91 : 2, 3, 5 et 7. Par 2 : 91 est impair, non. Par 3 : $9 + 1 = 10$, qui n'est pas un multiple de 3, non. Par 5 : il ne finit ni par 0 ni par 5, non. Par 7 : $91 \div 7 = 13$, sans reste — OUI. 91 n'est donc pas premier : $91 = 7 \times 13$. ⚠️ Trois tests sur quatre passaient. C'est exactement pour ce genre de nombre que la liste jusqu'à 30 ne suffit pas et que le programme demande la MÉTHODE : un élève qui s'arrête après 5 conclut faux.

Décomposer 84

On veut écrire 84 comme un produit de nombres premiers.

Quelle est sa décomposition ?

Données	on divise	par	reste
	84	2	42
	42	2	21
	21	3	7
	7	7	1

On divise par le plus petit premier possible, à chaque étape. $84 \div 2 = 42$, puis $42 \div 2 = 21$. 21 n'est plus pair, on passe à 3 : $21 \div 3 = 7$. Enfin 7 est premier, et $7 \div 7 = 1$: on s'arrête. Donc $84 = 2 \times 2 \times 3 \times 7$. ★ Contrôle : $2 \times 2 = 4$, $4 \times 3 = 12$, $12 \times 7 = 84$. Le produit redonne bien le nombre de départ — et chaque facteur est premier. Sans ces deux vérifications, une décomposition n'est pas terminée.

Simplifier avec la décomposition

On veut rendre la fraction $\frac{84}{126}$ irréductible.

Quelle est la fraction simplifiée ?

Données	décomposition
84	$2 \times 2 \times 3 \times 7$

Données		décomposition
	126	$2 \times 3 \times 3 \times 7$

On décompose les deux : $84 = 2 \times 2 \times 3 \times 7$ et $126 = 2 \times 3 \times 3 \times 7$. Les facteurs communs sont un 2, un 3 et un 7. On les barre en haut et en bas. Il reste 2 au numérateur et 3 au dénominateur : la fraction vaut $\frac{2}{3}$. ★ C'est là que la décomposition gagne du temps. En simplifiant au hasard, on aurait divisé par 2, puis par 3, puis par 7 — trois étapes, avec le risque de s'arrêter trop tôt et de rendre une fraction encore réductible. La décomposition montre TOUT ce qui se barre, d'un seul coup d'œil.

Pièges à éviter : Nombres premiers et décomposition

Croire que 1 est premier. Il n'a qu'UN seul diviseur, alors que la définition en demande exactement deux.

Croire que tous les nombres impairs sont premiers. 9, 15, 21 et 27 sont impairs et composés.

Croire que tous les premiers sont impairs. 2 est premier et pair — c'est le seul, mais il suffit à réfuter.

S'arrêter après avoir testé 2, 3 et 5. 91 passe ces trois tests et vaut pourtant 7×13 .

Tester tous les nombres jusqu'au nombre lui-même. Jusqu'à 100, quatre tests suffisent.

Écrire 1 dans une décomposition. Il ne change rien au produit et détruit l'unicité de l'écriture.

Oublier de vérifier que le produit redonne le nombre de départ. C'est le seul contrôle d'une décomposition.

À retenir : Nombres premiers et décomposition

Un nombre premier a EXACTEMENT deux diviseurs : 1 et lui-même.

1 n'est pas premier : il n'en a qu'un seul.

2 est le plus petit nombre premier, et le seul qui soit pair.

La liste jusqu'à 30 est à connaître : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Jusqu'à 100, il suffit de tester 2, 3, 5 et 7 — car $11^2 = 121$ dépasse déjà 100.

Tout entier plus grand que 1 s'écrit comme un produit de nombres premiers, et d'une SEULE façon.

Décomposer sert à simplifier une fraction d'un coup, au lieu de la simplifier par petits pas.

Le nombre de diviseurs se lit sur la décomposition : on ajoute 1 à chaque exposant, et on multiplie.

Exercices corrigés : Nombres premiers et décomposition

1. Le nombre 1 est-il premier ? Justifie.

Correction :

Non. Un nombre premier a exactement deux diviseurs, or 1 n'en a qu'un seul — « 1 » et « lui-même » désignent ici le même nombre.

2. Dans la liste 17, 21, 23, 29, lequel n'est pas premier ?

Correction :

21, car $21 = 3 \times 7$. Il est impair, mais impair ne veut pas dire premier.

3. Y a-t-il un nombre premier pair ? Lequel ?

Correction :

Oui, un seul : 2. Tout autre nombre pair est divisible par 2, donc il a au moins trois diviseurs.

4. Le nombre 83 est-il premier ?

Correction :

Oui. Il est impair, $8 + 3 = 11$ n'est pas multiple de 3, il ne finit pas par 0 ou 5, et $83 = 7 \times 11 + 6$. Les quatre tests échouent, donc il est premier.

5. Le nombre 91 est-il premier ?

Correction :

Non : $91 = 7 \times 13$. C'est le piège classique — il passe les tests par 2, 3 et 5.

6. Jusqu'où faut-il tester pour savoir si un nombre inférieur à 100 est premier ?

Correction :

Jusqu'à 7, car $11^2 = 121$ dépasse déjà 100. Quatre tests suffisent : 2, 3, 5 et 7.

7. Décompose 60 en produit de facteurs premiers.

Correction :

$60 = 2 \times 2 \times 3 \times 5$. Contrôle : $2 \times 2 \times 3 \times 5 = 60$, et chaque facteur est premier.

8. Décompose 225.

Correction :

225 est impair, mais $2 + 2 + 5 = 9$: il est divisible par 3 et par 9. $225 = 3 \times 3 \times 5 \times 5$.

9. Rends $\frac{90}{126}$ irréductible.

Correction :

$90 = 2 \times 3 \times 3 \times 5$ et $126 = 2 \times 3 \times 3 \times 7$. On barre le 2 et les deux 3 : il reste $\frac{5}{7}$.

10. Le nombre 45 se décompose en $3 \times 3 \times 5$. Combien a-t-il de diviseurs ?

Correction :

Le 3 apparaît 2 fois, donc 3 choix ; le 5 apparaît 1 fois, donc 2 choix. En tout $3 \times 2 = 6$ diviseurs — ce sont 1, 3, 5, 9, 15 et 45.