Leçon d'oral du CAPES de mathématiques

Nombres premiers, décomposition d'un entier en produit de facteurs premiers

Introduction

Les nombres premiers occupent une place fondamentale dans l'arithmétique des entiers. Ils constituent les éléments multiplicatifs de base à partir desquels tout entier naturel supérieur ou égal à 2 peut être construit.

L'étude des nombres premiers permet de comprendre la structure multiplicative des entiers, de justifier les méthodes de calcul du plus grand commun diviseur et du plus petit commun multiple, et de résoudre des problèmes de divisibilité. Elle intervient également dans des domaines plus avancés, notamment en algèbre et en cryptographie.

La leçon s'articule autour de trois questions :

— Comment caractériser un nombre premier ?

— Comment démontrer qu'un entier est premier ou composé ?

— Pourquoi tout entier supérieur ou égal à 2 admet-il une décomposition unique en facteurs premiers ?

Prérequis et objectifs

Prérequis. On suppose connus la division euclidienne dans $\mathbb{N}$, les notions de multiple et de diviseur, les critères élémentaires de divisibilité, ainsi que les opérations sur les entiers naturels. La notion de preuve mathématique, en particulier le raisonnement par l'absurde et le raisonnement par récurrence, pourra être mobilisée selon le niveau auquel la leçon est présentée.

Objectifs. À l'issue de cette leçon, l'élève ou le candidat doit être capable :

— de définir un nombre premier et de distinguer nombres premiers et nombres composés ;

— d'utiliser un critère de primalité fondé sur les diviseurs premiers inférieurs ou égaux à la racine carrée du nombre étudié ;

— de démontrer l'existence et l'unicité de la décomposition en facteurs premiers ;

— de déterminer la décomposition d'un entier en produit de puissances de nombres premiers ;

— d'exploiter cette décomposition pour déterminer les diviseurs, le PGCD et le PPCM de deux entiers ;

— de mettre en oeuvre ces résultats dans des exercices d'arithmétique adaptés au niveau scolaire.

1 Nombres premiers et nombres composés

1.1 Définition

Définition 1.1. Un entier naturel $p \geq 2$ est dit *premier* si ses seuls diviseurs positifs sont 1 et p.

Un entier naturel $n \geq 2$ qui n'est pas premier est dit *composé*.

Exemple 1.2. Les nombres 2, 3, 5, 7, 11 et 13 sont premiers.

Le nombre 1 n'est pas premier. Le nombre 12 est composé, car il possède notamment les diviseurs 2, 3, 4 et 6.

Remarque 1.3. Le nombre 2 est le seul nombre premier pair. En effet, tout entier pair supérieur ou égal à 4 est divisible par 2 et par lui-même, qui lui est distinct.

1.2 Un critère de primalité

Proposition 1.4. *Soit $n \geq 2$. Si n est composé, alors il existe des entiers a, b tels que*

$$n = ab, \qquad 1 < a \leq \sqrt{n}, \qquad b \geq a.$$

En particulier, tout entier composé possède un diviseur a compris entre 2 et $\sqrt{n}$.

Démonstration. Puisque n est composé, il existe deux entiers a, b strictement supérieurs à 1 tels que $n = ab$. Quitte à échanger les facteurs, on peut supposer $a \leq b$.

On a alors

$$a^2 \leq ab = n,$$

d'où $a \leq \sqrt{n}$. □

Théorème 1.5 (Critère de primalité)**.** *Un entier $n \geq 2$ est premier si et seulement s'il n'est divisible par aucun nombre premier p vérifiant*

$$p \leq \sqrt{n}.$$

Démonstration. Si n est premier, il n'est divisible par aucun nombre premier strictement inférieur à n.

Réciproquement, supposons que n ne soit divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$. Si n était composé, la proposition précédente fournirait un diviseur a compris entre 2 et $\sqrt{n}$. Tout entier $a \geq 2$ possède un diviseur premier p, avec $p \leq a$. Ce nombre premier diviserait n, ce qui contredirait l'hypothèse. □

Exemple 1.6. Montrons que 97 est premier. On a

$$\sqrt{97} < 10.$$

Il suffit donc de tester les nombres premiers 2, 3, 5 et 7.

Le nombre 97 n'est divisible par aucun d'eux : il est impair, la somme de ses chiffres vaut 16, son chiffre des unités est 7, et

$$97 = 7 \times 13 + 6.$$

Ainsi, 97 est premier.

1.3 Infinité des nombres premiers

Théorème 1.7 (Euclide)**.** *Il existe une infinité de nombres premiers.*

Démonstration. Supposons, par l'absurde, qu'il n'existe qu'un nombre fini de nombres premiers $p_1, p_2, \ldots, p_r$.

Considérons l'entier

$$N = p_1 p_2 \cdots p_r + 1.$$

Aucun des nombres p_i ne divise N, puisque la division de N par p_i laisse le reste 1.

Or tout entier $N \geq 2$ possède au moins un diviseur premier. Un tel diviseur ne peut donc être aucun des p_i. Cela contredit l'hypothèse selon laquelle la liste $p_1, \ldots, p_r$ contient tous les nombres premiers.

Il existe donc une infinité de nombres premiers. □

Remarque 1.8. L'entier N construit dans cette démonstration n'est pas nécessairement premier. Par exemple, pour les nombres premiers 2, 3 et 5, on obtient $N = 31$, qui est premier, mais d'autres produits peuvent conduire à un entier composé. La contradiction repose sur l'existence d'un diviseur premier nouveau, et non sur la primalité de N lui-même.

2 Décomposition en facteurs premiers

2.1 Existence de la décomposition

Théorème 2.1 (Existence)**.** *Tout entier naturel $n \geq 2$ peut s'écrire comme un produit de nombres premiers.*

Démonstration. On raisonne par récurrence forte sur $n \geq 2$.

Pour $n = 2$, l'entier 2 est premier : le résultat est vérifié.

Supposons que tout entier k tel que $2 \leq k < n$ puisse s'écrire comme un produit de nombres premiers.

Si n est premier, il est lui-même une décomposition convenable.

Si n est composé, il existe a, b tels que

$$n = ab, \qquad 2 \leq a < n, \qquad 2 \leq b < n.$$

Par hypothèse de récurrence, a et b sont chacun des produits de nombres premiers. Leur produit donne donc une décomposition de n en facteurs premiers.

Le résultat est établi pour tout $n \geq 2$. □

2.2 Lemme d'Euclide

Lemme 2.2 (Lemme d'Euclide)**.** *Si un nombre premier p divise un produit ab, alors p divise a ou p divise b.*

Démonstration. Supposons que p divise ab et que p ne divise pas a.

Puisque p est premier, on a

$$\mathrm{pgcd}(p, a) = 1.$$

D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$up + va = 1.$$

En multipliant cette égalité par b, on obtient

$$upb + vab = b.$$

Le nombre p divise upb et, par hypothèse, p divise ab. Il divise donc le membre de gauche, puis b.

Ainsi, $p \mid a$ ou $p \mid b$. □

Remarque 2.3. Le lemme d'Euclide est un résultat essentiel pour établir l'unicité de la décomposition en facteurs premiers. Il relie la primalité à la divisibilité d'un produit.

2.3 Unicité de la décomposition

Théorème 2.4 (Théorème fondamental de l'arithmétique)**.** *Tout entier naturel $n \geq 2$ s'écrit de manière unique, à l'ordre des facteurs près, sous la forme*

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}},$$

où $p_1, \ldots, p_r$ sont des nombres premiers distincts et où $\alpha_1, \ldots, \alpha_r$ sont des entiers strictement positifs.

Démonstration. L'existence vient du théorème précédent.

Pour l'unicité, supposons que l'on ait deux décompositions en facteurs premiers :

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

où les facteurs sont éventuellement répétés.

Le nombre premier p_1 divise le produit $q_1 q_2 \cdots q_s$. Par le lemme d'Euclide, il divise l'un des facteurs q_j. Comme q_j est premier, on obtient $p_1 = q_j$.

On peut alors simplifier les deux membres par ce facteur commun et recommencer le raisonnement. On montre ainsi que les deux listes de facteurs premiers coïncident à l'ordre près, avec les mêmes multiplicités.

La décomposition est donc unique à l'ordre des facteurs près. □

Remarque 2.5. Cette unicité permet de définir sans ambiguïté les exposants des facteurs premiers dans la décomposition d'un entier. Ces exposants sont parfois appelés valuations arithmétiques.

3 Méthodes pratiques de décomposition

3.1 Division successive

Pour décomposer un entier, on le divise successivement par des nombres premiers, en commençant par les plus petits, jusqu'à obtenir le quotient 1.

Exemple 3.1. Décomposons 360 en facteurs premiers :

$$\begin{aligned} 360 &= 2 \times 180 \\ &= 2^2 \times 90 \\ &= 2^3 \times 45 \\ &= 2^3 \times 3 \times 15 \\ &= 2^3 \times 3^2 \times 5. \end{aligned}$$

Ainsi,

$$\boxed{360 = 2^3 \times 3^2 \times 5}.$$

3.2 Crible d'Ératosthène

Le crible d'Ératosthène permet de déterminer tous les nombres premiers inférieurs à une borne fixée.

On écrit les entiers de 2 à cette borne, puis :

1. on conserve 2 et on élimine ses multiples supérieurs à 2 ;
2. on conserve le plus petit entier non éliminé et on élimine ses multiples ;
3. on poursuit jusqu'à ce que le carré du plus petit entier restant dépasse la borne ;
4. les entiers non éliminés sont premiers.

Cette méthode constitue une activité adaptée à l'enseignement de l'arithmétique au collège et au lycée.

4 Applications de la décomposition

4.1 Déterminer les diviseurs d'un entier

Proposition 4.1. *Si*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

est la décomposition en facteurs premiers de n, alors tout diviseur positif d de n s'écrit de manière unique sous la forme

$$d = p_1^{\beta_1} \cdots p_r^{\beta_r}, \qquad 0 \leq \beta_i \leq \alpha_i.$$

Exemple 4.2. Puisque $12 = 2^2 \times 3$, ses diviseurs positifs sont

$$1,\ 2,\ 3,\ 4,\ 6,\ 12.$$

Ils correspondent aux choix des exposants de 2 dans $\{0, 1, 2\}$ et de ceux de 3 dans $\{0, 1\}$. Le nombre de diviseurs positifs de 12 est donc

$$(2 + 1)(1 + 1) = 6.$$

4.2 Calcul du PGCD et du PPCM

Proposition 4.3. *Soient a et b deux entiers naturels non nuls dont les décompositions en facteurs premiers sont*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}, \qquad b = \prod_{i=1}^{r} p_i^{\beta_i},$$

où les exposants nuls sont autorisés et où la liste des p_i contient tous les facteurs premiers présents dans au moins l'une des deux décompositions.

Alors

$$\mathrm{pgcd}(a, b) = \prod_{i=1}^{r} p_i^{\min(\alpha_i, \beta_i)}$$

et

$$\mathrm{ppcm}(a, b) = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}.$$

Exemple 4.4. Calculons le PGCD et le PPCM de 360 et 168.

On a

$$360 = 2^3 \times 3^2 \times 5, \qquad 168 = 2^3 \times 3 \times 7.$$

Les exposants minimaux donnent

$$\boxed{\mathrm{pgcd}(360, 168) = 2^3 \times 3 = 24}.$$

Les exposants maximaux donnent

$$\boxed{\mathrm{ppcm}(360, 168) = 2^3 \times 3^2 \times 5 \times 7 = 2520}.$$

On vérifie que

$$\mathrm{pgcd}(360, 168) \times \mathrm{ppcm}(360, 168) = 360 \times 168.$$

5 Aspects pédagogiques et points de vigilance

5.1 Difficultés fréquentes

Plusieurs erreurs peuvent apparaître :

— considérer 1 comme un nombre premier ;

— confondre un diviseur quelconque et un diviseur premier ;

— affirmer qu'un entier est premier après avoir testé seulement quelques diviseurs sans justifier la borne ;

— oublier un facteur premier ou son exposant dans une décomposition ;

— confondre les exposants minimaux du PGCD avec les exposants maximaux du PPCM ;

— croire que l'entier construit dans la preuve d'Euclide est toujours premier.

5.2 Pistes pour l'enseignement

Une progression possible consiste à partir de recherches de diviseurs et de décompositions simples, puis à introduire la définition des nombres premiers. Le crible d'Ératosthène peut ensuite servir à organiser la recherche des nombres premiers.

Le critère de primalité est justifié par l'étude des paires de facteurs d'un entier composé. La décomposition en facteurs premiers est introduite par divisions successives, avant d'en établir l'existence et l'unicité.

Enfin, des problèmes de partage, de groupements ou de synchronisation permettent de réinvestir les décompositions dans le calcul du PGCD et du PPCM.

6 Liste d'exercices

Les exercices suivants sont classés selon une difficulté croissante. Ils peuvent être proposés à l'oral avec une justification des méthodes utilisées.

Exercice 6.1 (Reconnaître les nombres premiers)**.** Parmi les entiers suivants, déterminer ceux qui sont premiers :

$$1,\ 2,\ 9,\ 17,\ 21,\ 29,\ 49,\ 53.$$

Justifier chaque réponse.

Exercice 6.2 (Critère de primalité)**.** Démontrer que 101 est premier. Puis déterminer si 143 est premier.

Exercice 6.3 (Décomposition en facteurs premiers)**.** Décomposer en facteurs premiers les entiers suivants :

$$252, \qquad 756, \qquad 1001, \qquad 2025.$$

Présenter les calculs par divisions successives.

Exercice 6.4 (Nombre de diviseurs)**.** Déterminer le nombre de diviseurs positifs de

$$72, \qquad 360, \qquad 840.$$

Établir au préalable la formule du nombre de diviseurs à partir de la décomposition en facteurs premiers.

Exercice 6.5 (PGCD et PPCM)**.** Calculer le PGCD et le PPCM de 252 et 360 en utilisant leurs décompositions en facteurs premiers. Vérifier ensuite l'identité

$$\mathrm{pgcd}(a,b) \times \mathrm{ppcm}(a,b) = ab.$$

Exercice 6.6 (Carré parfait)**.** Déterminer les entiers naturels n pour lesquels

$$n = 2^4 \times 3^a \times 5^2$$

est un carré parfait, où a est un entier naturel. Généraliser le critère caractérisant les carrés parfaits à l'aide de leur décomposition en facteurs premiers.

Exercice 6.7 (Problème de partage)**.** On dispose de 168 objets rouges et de 252 objets bleus. On souhaite constituer le plus grand nombre possible de lots identiques, sans reste, chaque lot contenant le même nombre d'objets rouges et le même nombre d'objets bleus.

Combien de lots peut-on constituer ? Combien d'objets de chaque couleur contiendra chaque lot ?

Exercice 6.8 (Infinité des nombres premiers)**.** Présenter la démonstration d'Euclide de l'infinité des nombres premiers. Expliquer pourquoi le nombre

$$N = p_1 p_2 \cdots p_r + 1$$

n'est pas nécessairement premier.

Exercice 6.9 (Approfondissement)**.** Soit $n \geq 2$. On suppose que le carré de n est divisible par un nombre premier p.

Montrer que p divise n. En déduire que si le carré d'un entier est divisible par un nombre premier p, alors l'exposant de p dans la décomposition du carré est au moins égal à 2 dès que p apparaît dans la décomposition de n.

7 Éléments de correction des exercices

Exercice 1

Les nombres premiers sont

$$\boxed{2,\ 17,\ 29,\ 53}.$$

Le nombre 1 n'est pas premier. Les autres entiers composés sont $9 = 3^2$, $21 = 3 \times 7$ et $49 = 7^2$.

Exercice 2

Pour 101, on a $\sqrt{101} < 11$. Il suffit de tester 2, 3, 5 et 7. Aucun ne divise 101 : il est premier.
Pour 143, on trouve

$$143 = 11 \times 13.$$

Il est donc composé.

Exercice 3

Les décompositions sont

$$252 = 2^2 \times 3^2 \times 7,$$

$$756 = 2^2 \times 3^3 \times 7,$$

$$1001 = 7 \times 11 \times 13,$$

$$2025 = 3^4 \times 5^2.$$

Exercice 4

Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, le nombre de diviseurs positifs est

$$d(n) = \prod_{i=1}^{r} (\alpha_i + 1).$$

Ainsi,

$$\begin{aligned} 72 &= 2^3 \times 3^2, & d(72) &= 4 \times 3 = 12, \\ 360 &= 2^3 \times 3^2 \times 5, & d(360) &= 4 \times 3 \times 2 = 24, \\ 840 &= 2^3 \times 3 \times 5 \times 7, & d(840) &= 4 \times 2 \times 2 \times 2 = 32. \end{aligned}$$

Exercice 5

On a

$$252 = 2^2 \times 3^2 \times 7, \qquad 360 = 2^3 \times 3^2 \times 5.$$

Par conséquent,

$$\operatorname{pgcd}(252, 360) = 2^2 \times 3^2 = 36,$$

et

$$\operatorname{ppcm}(252, 360) = 2^3 \times 3^2 \times 5 \times 7 = 2520.$$

On vérifie que $36 \times 2520 = 252 \times 360$.

Exercice 6

Un entier est un carré parfait si et seulement si tous les exposants de sa décomposition en facteurs premiers sont pairs. Ici, n est un carré parfait si et seulement si a est pair. Si 0 est autorisé comme exposant, les valeurs admissibles sont donc $a = 0, 2, 4, \ldots$.

Exercice 7

Le nombre maximal de lots est

$$\operatorname{pgcd}(168, 252) = 84.$$

Chaque lot contient

$$\frac{168}{84} = 2 \quad \text{objets rouges}$$

et

$$\frac{252}{84} = 3 \quad \text{objets bleus.}$$

Exercice 8

La preuve est celle du théorème d'Euclide présenté dans la leçon. L'entier N est supérieur à 1 et possède donc un diviseur premier. Aucun des p_i ne divise N. Un diviseur premier de N est donc distinct de tous les p_i, ce qui contredit l'hypothèse d'une liste exhaustive.

Exercice 9

Si $p \mid n^2 = n \times n$, le lemme d'Euclide donne $p \mid n$ ou $p \mid n$, donc $p \mid n$.

Si n contient le facteur p^k, avec $k \geq 1$, alors n^2 contient le facteur p^{2k}. Son exposant est donc pair et au moins égal à 2.

Conclusion

Les nombres premiers sont les briques fondamentales de la multiplication des entiers naturels. Le critère de primalité permet de les identifier, tandis que le théorème fondamental de l'arithmétique garantit l'existence et l'unicité de la décomposition en facteurs premiers.

Cette décomposition fournit un outil efficace pour déterminer les diviseurs d'un entier, calculer le PGCD et le PPCM, reconnaître les carrés parfaits et résoudre des problèmes concrets de partage.

Pour un oral du CAPES, il importe de distinguer les résultats qui peuvent être admis au niveau scolaire de ceux qui doivent être démontrés dans l'exposé, en particulier le critère de primalité, le lemme d'Euclide et l'unicité de la décomposition.

Références bibliographiques

Références

[1] Euclide, *Les Éléments*, livre VII. Texte fondateur de l'arithmétique des entiers et des propriétés de divisibilité.

[2] G. H. Hardy et E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press. Ouvrage de référence sur les nombres premiers et la décomposition des entiers.

[3] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer. Pour approfondir les propriétés des nombres premiers et les méthodes de la théorie des nombres.

[4] Ministère de l'Éducation nationale, *Programmes de mathématiques du collège et du lycée*, ressources institutionnelles disponibles sur Éduscol : https://eduscol.education.fr/.

[5] Ministère de l'Éducation nationale, *Concours du CAPES externe de mathématiques*, programmes, rapports de jury et ressources officielles : https://www.devenirenseignant.gouv.fr/.