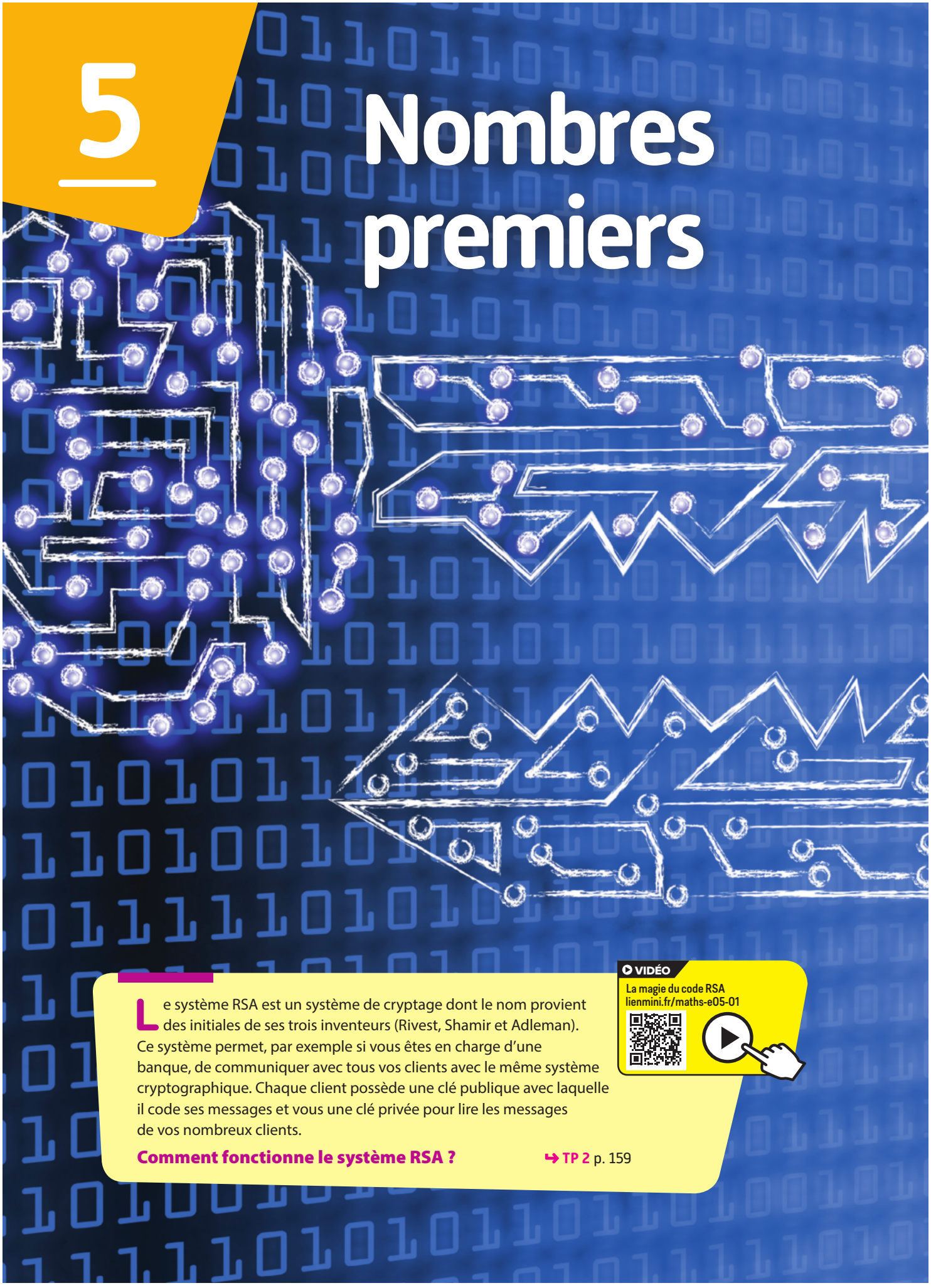
5 Nombres premiers



Le système RSA est un système de cryptage dont le nom provient des initiales de ses trois inventeurs (Rivest, Shamir et Adleman). Ce système permet, par exemple si vous êtes en charge d'une banque, de communiquer avec tous vos clients avec le même système cryptographique. Chaque client possède une clé publique avec laquelle il code ses messages et vous une clé privée pour lire les messages de vos nombreux clients.

Comment fonctionne le système RSA ?

↪ TP 2 p. 159

VIDÉO
La magie du code RSA
lienmini.fr/maths-e05-01

Pour prendre un bon départ

EXOS Prérequis
lienmini.fr/maths-e05-02

Les rendez-vous Sésamath

1 Connaître les nombres premiers inférieurs à 100

1. Donner les 15 nombres premiers inférieurs à 50.
2. Donner les 10 nombres premiers compris entre 50 et 100.

2 Montrer qu'un nombre n'est pas premier

À l'aide des critères de divisibilité par 3, 5 et 11 ou de la division par 7, montrer que les nombres suivants ne sont pas premiers.
a) 57 **b)** 91 **c)** 143 **d)** 265 **e)** 341 **f)** 427 **g)** 319 **h)** 1581

3 Décomposer un nombre

Décomposer les nombres suivants en produit de facteurs premiers.
a) 72 **b)** 98 **c)** 90 **d)** 91 **e)** 97 **f)** 121 **g)** 128 **h)** 225

4 Déterminer l'ensemble des diviseurs d'un entier

Donner tous les diviseurs des nombres suivants.
a) 24 **b)** 36 **c)** 45 **d)** 51 **e)** 63 **f)** 91

5 Définir la divisibilité à l'aide de la congruence

Traduire à l'aide des congruences les propositions suivantes.
a) n est divisible par 6.
b) n est divisible par 3 et par 5.
c) n est divisible par 4 et par 6.
d) n est divisible par 6 et par 9.

6 Traduire une proposition mathématique en français usuel

Traduire par une phrase, sans utiliser le mot « congruence », les propositions suivantes.
a) $n \equiv 0\ (5)$.
b) si $n \equiv 0\ (4)$ et si $n \equiv 0\ (5)$ alors $n \equiv 0\ (20)$.
c) Si $n \leqslant 25$ et si $n \not\equiv 0\ (2)$, $n \not\equiv 0\ (3)$, $n \not\equiv 0\ (5)$ alors, n est premier.
d) Si p est premier et si $ab \equiv 0\ (p)$ alors, $a \equiv 0\ (p)$ ou $b \equiv 0\ (p)$.

7 Comprendre un algorithme en langage Python

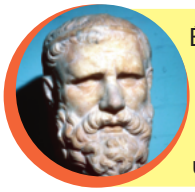
Que retourne cet algorithme pour `fonct(154)` ?

```
from math import *
def fonct(n) :
d=2
c=1
L=[ ]
while d<=sqrt(n):
if n%d==0:
L.append(d)
n = n/d
else:
d=d+c
c=2
L.append(n)
return L
```

Activités

Algo | Histoire des maths | 20 min

1 Découvrir le crible d'Ératosthène



Ératosthène de Cyrène, astronome, géographe, philosophe et mathématicien grec du IIIe siècle av. J.- C., a été le directeur de la bibliothèque d'Alexandrie et est connu notamment pour avoir mesuré géométriquement la circonférence de la Terre en utilisant les rayons du Soleil. En mathématiques, il invente un procédé, le crible d'Ératosthène, permettant de trouver une liste de nombres premiers.

A ▸ Élaboration manuelle de la liste des nombres premiers inférieurs ou égaux à 150

On se propose de déterminer la liste des nombres premiers inférieurs à 150.
On utilise la méthode dites du crible d'Ératosthène, un crible étant une sorte de tamis qui retient les nombres premiers. On donne le tableau suivant.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

1. Rayer le nombre 1 et entourer le nombre 2. Rayer les multiples de 2 à partir de 4.

2. Entourer 3. Rayer les multiples de 3 à partir de 9 qui ne sont pas déjà rayés.

3. Entourer 5. Rayer les multiples de 5 à partir de 25 qui ne sont pas déjà rayés.

4. Entourer 7. Rayer les multiples de 7 à partir de 49 qui ne sont pas déjà rayés.

5. Entourer 11. Rayer les multiples de 11 à partir de 121 qui ne sont pas déjà rayés.

6. Entourer tous les nombres de la liste qui ne sont pas rayés. Vérifier qu'il y a 35 nombres entourés et qu'ils correspondent aux nombres premiers inférieurs à 150.

B ▸ Justification

1. Pourquoi est-on sûr, lorsqu'on entoure 7, que les multiples de 7 inférieurs à 49 sont déjà rayés de la liste ?

2. Pourquoi est-on sûr, parmi les entiers naturels inférieurs ou égaux à 150, qu'une fois rayés tous les multiples de 2 à 11, tous les nombres non rayés sont premiers ?

↪ Cours 1 p. 136

TICE 30 min

2 Généraliser le crible d'Ératosthène par un algorithme

On désire généraliser la méthode de l'activité 1 à une liste de nombres premiers inférieurs ou égaux à n et automatiser ce procédé par une fonction en **Python** d'argument n. On appelle alors cette fonction `crible` et la liste `L`. L'idée est, au lieu de rayer des nombres, de leur affecter la valeur 0 puis de les supprimer de la liste `L`. On obtient la fonction ci-dessous.

PYTHON Programme
lienmini.fr/maths-e05-03

```
1 from math import *
2 def crible(n):
3     L=[i for i in range(0,n+1)]
4     for i in range(2,int(floor(sqrt(n)))+1):
5         if L[i]>=1:
6             for k in range(2,int(floor(n/i))+1):
7                 L[i*k]=0
8     i=0
9     while i<len(L):
10        if L[i]==0 or L[i]==1:
11            L.remove(L[i])
12        else:
13            i+=1
14    return L, len(L))
```

1. Que fait-on à la ligne 3 ?

2. À la ligne 4 :

a) expliquer la borne supérieure du compteur `i`.

b) pourquoi applique-t-on le type `int` à cette borne ?

3. Expliquer ce que l'on fait aux lignes 5 et 6.

4. Que fait-on aux lignes 9, 10, 11 ?

5. Expliquer les affectations aux lignes 8 et 13.

6. Que renvoie la fonction `crible` ?

7. Exécuter ce programme et retrouver le résultat pour $n = 150$ de l'activité 1.

↪ Cours 1 p. 136

20 min

3 Déterminer le nombre de diviseurs

Le but de cette activité est de déterminer tous les diviseurs d'un entier donné à l'aide d'une décomposition en facteurs premiers.

1. Décomposer 567 en produit de facteurs premiers et vérifier qu'il existe deux entiers p et q tels que :

$$567 = p^4q.$$

2. Pourquoi un diviseur de 567 est-il de la forme $p^\alpha q^\beta$ avec $0 \leqslant \alpha \leqslant 4$ et $0 \leqslant \beta \leqslant 1$?

3. Remplir le tableau suivant.

×	p^0	p^1	p^2	p^3	p^4
q^0					
q^1					

4. Donner alors l'ensemble des diviseurs de 567.
Combien 567 a-t-il de diviseurs ? Pouvait-on prévoir ce résultat ?

5. Proposer une autre méthode à partir de la décomposition en facteurs premiers permettant de déterminer tous les diviseurs de 567.

6. **a)** Décomposer 735 en produit de facteurs premiers.
b) Peut-on prévoir le nombre de diviseurs de 735 ?
c) Vérifier ce résultat par la méthode de son choix.

7. Peut-on avoir un entier possédant un nombre impair, autre que 1, de diviseurs ?
Proposer un nombre possédant 3 diviseurs puis un nombre possédant 7 diviseurs.

↪ Cours 3 p. 138 et 4 p. 140

Cours

1 Définition et conséquences

Définition Nombre premier

Un nombre premier est un entier naturel qui admet exactement deux diviseurs : 1 et lui-même.

Remarques

- 1 n'est pas un nombre premier car il n'a qu'un seul diviseur : lui-même.
- Un nombre premier p est un entier naturel supérieur ou égal à 2, soit $p \geqslant 2$.
- À part 2, tous les nombres premiers sont impairs.
- Il y a 25 nombres premiers inférieurs à 100 :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

- Si un entier naturel $n \geqslant 2$ n'est pas premier, il admet un diviseur strict d tel que $1 < d < n$.
- Un entier naturel non premier est appelé nombre composé.

Théorème Critère d'arrêt ou test de primalité

- **Tout entier naturel n tel que $n \geqslant 2$ admet un diviseur premier.**
- **Si n n'est pas premier, alors il admet un diviseur premier p tel que : $2 < p \leqslant \sqrt{n}$.**

Démonstration

Si n est premier, il admet un diviseur premier : lui-même.

Si n n'est pas premier, l'ensemble D des diviseurs stricts de n (non premiers avec n) n'est pas vide.

D'après le principe du bon ordre, D admet un plus petit élément p.

Si p n'était pas premier, il admettrait un diviseur strict d' qui diviserait aussi n et serait donc dans D.

Ceci est impossible car p est le plus petit élément de D.

Donc p est premier. n admet donc un diviseur premier p donc $p \geqslant 2$ et $n = p \times q$ avec $p \leqslant q$.

En multipliant cette inégalité par p, on obtient :

$$p^2 \leqslant pq \text{ donc } p^2 \leqslant n \text{ soit } p \leqslant \sqrt{n}.$$

Remarque

Pour déterminer une liste de nombres premiers, on peut utiliser le crible d'Ératosthène ↪ **Activité 1**.

Théorème Théorème de Gauss appliqué aux nombres premiers

Soit a et b deux entiers relatifs non nuls.

Si un nombre premier p divise le produit ab, alors p divise a ou p divise b.

Démonstration

↪ **Exercice 50** p. 146

Remarques

- Si p premier divise une puissance a^k, alors p divise a.
- Si p premier divise un produit de facteurs premiers, alors p est l'un d'entre eux.

EXOS Méthodes lienmini.fr/maths-e05-04 — Les rendez-vous Sésamath

Exercices résolus

Méthode 1 Déterminer si un nombre est premier

Énoncé

Montrer que 419 est un nombre premier.

Solution

Comme $20 < \sqrt{419} < 21$, on teste les diviseurs premiers inférieurs à 21 soit :

2, 3, 5, 7, 11, 13, 17 et 19. 1

- D'après les critères de divisibilité, 419 n'est pas divisible par 2, 3, 5 et 11.
- En effectuant les divisions euclidiennes, 419 n'est pas divisible par 7, 13, 17 et 19 :

$419 = 7 \times 59 + 6$, $419 = 13 \times 42 + 3$,
$419 = 17 \times 24 + 11$, $419 = 19 \times 22 + 1$

- D'après la contraposée du critère d'arrêt, 419 est un nombre premier. 2

Conseils & Méthodes

1 Il est utile de mémoriser les nombres premiers inférieurs à 50 : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47.

2 Pour montrer qu'un nombre $n \geqslant 2$ est premier, on utilise la contraposée du critère d'arrêt :

« Si n ne possède pas de diviseurs premiers inférieurs ou égaux à $\sqrt{n}$ alors n est premier. »

À vous de jouer !

1 Démontrer que 317 est un premier.

2 L'entier 437 est-il premier ?

↪ Exercices 39 à 46 p. 146

Méthode 2 Utiliser le théorème de Gauss appliqué aux nombres premiers

Énoncé

Soit p un nombre premier supérieur ou égal à 5.

Montrer que $p^2 - 1$ est divisible par 3 et 8. En déduire qu'il est divisible par 24.

Solution

- Divisibilité par 3 :

$p \geqslant 5$ premier donc p n'est pas divisible par 3.
Les deux seuls restes possibles dans la division par 3 sont 1 et 2. 1

$p \equiv 1\ (3) \Rightarrow p^2 - 1 \equiv 1^2 - 1 \equiv 0\ (3)$
$p \equiv 2\ (3) \Rightarrow p^2 - 1 \equiv 2^2 - 1 \equiv 3 \equiv 0\ (3)$

Donc $p^2 - 1$ est divisible par 3.

- Divisibilité par 8 :

$p \geqslant 5$ premier donc p impair et $p^2 - 1 = (p - 1)(p + 1)$. 2
$p - 1$ et $p + 1$ sont deux nombres pairs consécutifs donc l'un d'eux est divisible par 4.
Le produit $(p - 1)(p + 1)$ est donc divisible par 8.

- 3 et 8 divise $p^2 - 1$ comme 3 et 8 sont premiers entre eux, d'après le corollaire du théorème de Gauss :
$3 \times 8 = 24$ divise $p^2 - 1$. 3

Conseils & Méthodes

1 Dissociation des cas : penser à analyser les différents restes.

2 Factoriser et utiliser la parité.

3 Pour le produit des diviseurs, argumenter avec le corollaire du théorème de Gauss.

À vous de jouer !

3 Soit p un nombre premier supérieur à 3.
1. Quels sont les restes possibles dans la division par 12 ?
2. Montrer que $(p^2 + 11)$ est divible par 12.

4 p est un nombre premier supérieur à 5.
1. Montrer que $(p^4 - 1)$ est divisible par 3 et 5.
2. Montrer que $(p^4 - 1)$ est divisible par 16.
3. En déduire que $(p^4 - 1)$ est divisible par 240.

↪ Exercices 47 à 50 p. 146

Cours

2 L'infinité des nombres premiers

Théorème **Infinité des nombres premiers**

Il existe une infinité de nombres premiers.

Démonstration

Démontrons ce théorème par l'absurde.

Supposons qu'il existe un nombre fini n de nombres premiers : $p_1, p_2, \dots, p_n$.

Soit $N = p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n + 1$.

- $N \geqslant 2$ et $N \geqslant p_n$ par construction donc N n'est pas premier.
- D'après le critère d'arrêt, N admet un diviseur premier parmi $p_1, p_2, \dots, p_n$.
- Soit p_i ce diviseur premier.

p_i divise ainsi N et $P = p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n$ donc p_i divise la différence $N - P = 1$; on en déduit alors que $N = 1$.

- Ceci est contradictoire car $N \geqslant 2$.

L'hypothèse qu'il existe un nombre fini de nombres premiers est donc à rejeter.

VIDÉO
Démonstration
lienmini.fr/maths-e05-05

3 Théorème fondamental de l'arithmétique

Théorème **Décomposition en facteurs premiers**

Tout entier $n \geqslant 2$ peut se décomposer de façon unique (à l'ordre des facteurs près) en produit de facteurs premiers.
Soit m nombres premiers distincts $p_1, p_2, \dots, p_m$ et m entiers naturels non nuls $\alpha_1, \alpha_2, \dots, \alpha_m$ alors :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_m^{\alpha_m}.$$

Démonstration

Montrons par récurrence que tout entier $n \geqslant 2$ admet une décomposition en facteurs premiers.

Initialisation : $n = 2$. L'entier 2 étant premier, il se décompose en lui-même.

La proposition est initialisée.

Hérédité : soit $n \geqslant 2$, on suppose que tout entier jusqu'à n se décompose en facteurs premiers (hypothèse de récurrence). Montrons qu'il en est de même pour $n + 1$.

- Soit $n + 1$ est premier, il se décompose alors en lui-même.
- Soit $n + 1$ est composé, il admet alors un diviseur strict $d \geqslant 2$. On a alors $n + 1 = dq$ avec $d \leqslant n$ et $q \leqslant n$, les facteurs d et q d'après l'hypothèse de récurrence se décomposent en facteurs premiers et donc par produit $n + 1$ aussi.

La proposition est héréditaire.

Conclusion : par initialisation et hérédité, tout entier $n \geqslant 2$ admet une décomposition en facteurs premiers.

Remarques

- Lorsque, dans un raisonnement par récurrence, on suppose, dans l'hérédité, la proposition vraie jusqu'au rang n, on dit que la récurrence est forte.
- Pour montrer l'unicité à l'ordre des facteurs près, on utilise également une récurrence forte.

On admettra l'unicité de cette décomposition.

Exercices résolus

Méthode 3 Décomposer un nombre en produit de facteurs premiers

Énoncé

1. Décomposer 16 758 en produit de facteurs premiers.

2. À l'aide d'une décomposition en facteurs premiers, déterminer PGCD(126 , 735).

Solution

1. Tant qu'on peut diviser par un facteur premier, on ne passe pas au suivant : 1 et 2

16 738	2
8 379	3
2 793	3
931	7
133	7
19	19
1	

On a alors : $16\,758 = 2 \times 3^2 \times 7^2 \times 19$.

2. On décompose chaque entiers en facteurs premiers

126	2
63	3
21	3
7	7
1	

$126 = 2 \times 3^2 \times 7$

735	2
245	5
49	7
7	7
1	

$735 = 3 \times 5 \times 7^2$

On obtient alors : PGCD(126 , 735) = $3 \times 7 = 21$. 3

Remarque

Bien que cette méthode permette de calculer le PGCD, on lui préférera l'algorithme d'Euclide plus performant.

Conseils & Méthodes

1 Présenter la décomposition avec une barre verticale et écrire à droite les diviseurs premiers et à gauche le quotient de la division du nombre au-dessus à gauche par celui au-dessus à droite.

2 Tester les diviseurs premiers dans l'ordre croissant jusqu'à obtenir 1 dans la colonne de gauche.

3 Après avoir décomposer chaque nombre, déterminer le PGCD en multipliant tous les facteurs premiers communs à la puissance la plus petite.

À vous de jouer !

5 **1.** Décomposer en produit de facteurs premiers : 6 468 et 16 380.

2. En déduire PGCD(6 468 , 16 380).

6 **1.** Déterminer PGCD(8 316 , 5 670) à l'aide :
a) d'une décomposition en facteurs premiers.
b) de l'algorithme d'Euclide.

2. Quelle est la méthode la plus « économe » en opérations ?

7 **1.** Déterminer PGCD(5 455 , 3 570) à l'aide :
a) d'une décomposition en facteurs premiers.
b) de l'algorithme d'Euclide.

2. Quelle est la méthode la plus « économe » en opérations ?

8 À l'aide d'une décomposition en facteurs premiers, déterminer le couple d'entiers naturels $(a\,;b)$ tel que :

$$\frac{a}{b} = \frac{5\,292}{5544} \text{ et } a + b = 903.$$

9 **1.** Expliquer comment procède cette fonction **facteurs** en **Python** pour trouver la décomposition en facteurs premiers de n.

2. Expliquer l'avant dernière ligne : `L.append(n)`.

```
from math import*
def facteurs(n):
    L=[]
    d=2
    i=1
    while d<=sqrt(n):
        if n%d==0:
            L.append(d)
            n=n/d
        else:
            d=d+i
            i=2
    L.append(n)
    return L
```

↪ Exercices 51 à 59 p. 146

Cours

4 Décomposition et nombre de diviseurs

Propriété **Décomposition et nombre de diviseurs**

Soit un entier $n \geqslant 2$ dont la décomposition en facteurs premiers est :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}.$$

Alors, tout diviseur d de n a pour décomposion :

$$d = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_m^{\beta_m} \quad \text{avec pour tout } i \in [1\,;m],\ 0 \leqslant \beta_i \leqslant \alpha_i.$$

Le nombre N de diviseurs de n est alors : $N = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_m + 1)$.

Remarque

Le nombre de diviseurs se déduit facilement car chaque puissance des facteurs primaires p_i de n peut varier de 0 à α_i. Il y a donc $(1 + \alpha_i)$ choix possibles.

Pour qu'un entier naturel n admette un nombre impair de diviseurs, chaque facteurs $(1 + \alpha_i)$ de N doit être impair, ce qui entraine que les puissances α_i sont paires. Le nombre n est alors un carré.

Exemples

- $126 = 2 \times 3^2 \times 7$ possède $(1 + 1)(2 + 1)(1 + 1) = 12$ diviseurs.
- $196 = 2^2 \times 7^2$ possède $(2 + 1)(2 + 1) = 9$ diviseurs ($196 = 14^2$).

5 Petit théorème de Fermat

Théorème **Petit théorème de Fermat**

Soit un nombre premier p et un entier naturel a non multiple de p, alors : $a^{p-1} \equiv 1\ (p)$.
Si a est un entier naturel quelconque, on a : $a^p \equiv a\ (p)$.

Démonstration

Considérons les $p - 1$ premiers multiples de a : a, $2a$, $3a$, …, $(p - 1)a$.

Considérons les restes de la division de ces multiples de a par p : $r_1, r_2, r_3, \ldots, r_{p-1}$.

- Ces restes sont deux à deux distincts.

En effet s'il existait deux restes identiques $r_i = r_j$ avec $i > j$, alors :

$$ia - ja \equiv r_i - r_j\ (p) \Leftrightarrow a(i - j) \equiv 0\ (p)$$

donc $(i - j)a$ serait multiple de p, qui d'après le théorème de Gauss appliqué aux nombres premiers, impliquerait a ou $(i - j)$ multiples de p, ce qui n'est pas le cas.

- Ces restes sont donc tous différents et comme il y a $(p - 1)$ multiples de a, on trouve ainsi tous les restes non nuls possibles dans la division par p.
- On a alors :

$$a \times 2a \times \ldots \times (p - 1)a \equiv r_1 \times r_2 \times \ldots \times r_{p-1}\ (p) \Leftrightarrow (p - 1)! \times a^{p-1} \equiv 1 \times 2 \times 3 \times \ldots \times (p - 1) \equiv (p - 1)!\ (p)$$

Soit $(p - 1)! \times (a^{p-1} - 1) \equiv 0\ (p)$ donc p divise $(p - 1)! \times (a^{p-1} - 1)$.

Comme $(p - 1)!$ est premier avec p car tous les facteurs de $(p - 1)!$ sont inférieurs à p, d'après le théorème de Gauss, $a^{p-1} - 1$ est alors un multiple de p donc : $a^{p-1} - 1 \equiv 0\ (p) \Leftrightarrow a^{p-1} \equiv 1\ (p)$

- En multipliant par a, on obtient : $a^p \equiv a\ (p)$.

Cette dernière égalité reste vraie si a est multiple de p car alors $a \equiv 0\ (p)$.

Exemples

- 13 est premier et ne divise pas 4, donc d'après le petit théorème de Fermat : $4^{12} \equiv 1\ (7)$.
- 11 est premier et ne divise par 5, donc d'après le théorème de Fermat, $5^{11} \equiv 5\ (11)$.

Exercices résolus

Méthode 4 Trouver tous les diviseurs d'un entier

Énoncé

1. Trouver le nombre de diviseurs de 120 à l'aide de sa décomposition en facteurs premiers.

2. À l'aide d'un tableau double entrée et d'un arbre, trouver tous les diviseurs de 120.

Solution

1.

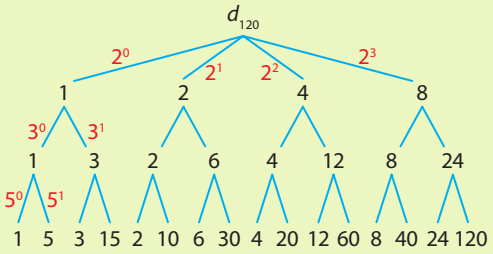
120	2
60	2
30	2
15	3
5	5
1	

$120 = 2^3 \times 3 \times 5$ 1
On a alors 16 diviseurs :
$(3 + 1)(1 + 1)(1 + 1) = 16$

2. On fait un tableau à double entrée en séparant les puissances de 2 et les puissances de 3 et 5. 2

×	2^0	2^1	2^2	2^3
$3^0 5^0$	1	2	4	8
$3^1 5^0$	3	6	12	24
$3^0 5^1$	5	10	20	40
$3^1 5^1$	15	30	60	120

On construit un arbre dont les coefficients sont les puissances des facteurs premiers.



Conseils & Méthodes

1 Le nombre de diviseurs est lié à la décomposition en facteurs premiers.

2 Pour dénombrer les diviseurs avec un tableau ou un arbre, répartir équitablement les choix.

À vous de jouer !

10 **1.** Trouver le nombre de diviseurs de 2 025 à l'aide d'une décomposition en facteurs premiers.

2. À l'aide d'un tableau double entrée, trouver tous les diviseurs de 2 025.

11 **1.** Trouver le nombre de diviseurs de 1 575 à l'aide d'une décomposition en facteurs premiers.

2. À l'aide d'un arbre pondéré, trouver tous les diviseurs de 2 025.

↪ Exercices 60 à 65 p. 147

Méthode 5 Appliquer le petit théorème de Fermat

Énoncé

Montrer que pour tout $n \in \mathbb{N}$, $3^{6n} - 1$ est divisible par 7.

Solution

7 est premier et 3 non divisible par 7. Donc, d'après le petit théorème de Fermat : $3^{7-1} \equiv 1\ (7)$. 1
On a $3^6 \equiv 1\ (7)$ donc en élevant à la puissance n :
$(3^6)^n \equiv 1^n\ (7) \Leftrightarrow 3^{6n} \equiv 1\ (7) \Leftrightarrow 3^{6n} - 1 \equiv 0\ (7)$.

Conseils & Méthodes

1 Dès qu'il y a des puissances et un nombre premier, il faut penser au petit théorème de Fermat.

À vous de jouer !

12 Soit p un nombre premier différent de 3.
Démontrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

13 Soit $n \in \mathbb{N}$ et $a = n^5 - n$.
1. Montrer que a est divisible par 5.
2. Montrer que $a = n(n^2 - 1)(n^2 + 1)$ puis que a est divisible par 2 et 3. Pourquoi a est-il divisible par 30 ?

↪ Exercices 66 à 72 p. 147

Exercices résolus

EXOS Méthodes Lienmini.fr/maths-e05-04 — Les rendez-vous Sésamath

Méthode 6 Déterminer un entier conditionné par le nombre de ses diviseurs

↪ Cours 4 p. 140

Énoncé

Un entier naturel n possède 15 diviseurs. On sait de plus que n est divisible par 6 mais pas par 8. Quel est cet entier ?

Solution

• L'entier n possède 15 diviseurs. On établit le nombre de décomposition de 15 en produit de facteurs supérieurs à 1.

Deux décompositions sont possibles ; soit un facteur :15 ; soit deux facteurs : 3×5. 1

• On sait que n est divisible par $6 = 2 \times 3$ qui possède deux facteurs premiers. Le nombre de diviseurs doit donc se décomposer en au moins deux facteurs.

• Comme 15 se décompose au plus en deux facteurs, n ne possède que deux facteurs premiers primaires : 2 et 3. 2

On a alors $n = 2^{\alpha} \times 3^{\beta}$ avec $(\alpha + 1)(\beta + 1) = 15$.

• Deux choix sont possibles pour le couple $(\alpha ; \beta)$:

1) $\begin{cases} \alpha + 1 = 3 \\ \beta + 1 = 5 \end{cases} \Leftrightarrow \begin{cases} \alpha = 2 \\ \beta = 4 \end{cases}$ ou 2) $\begin{cases} \alpha + 1 = 5 \\ \beta + 1 = 3 \end{cases} \Leftrightarrow \begin{cases} \alpha = 4 \\ \beta = 2 \end{cases}$

• Comme n n'est pas divisible par $8 = 2^3$ alors $\alpha < 3$. 3

• La seule solution est alors $\alpha = 2$ et $\beta = 4$; on a alors $n = 2^2 \times 3^4 = 4 \times 81 = 324$.

Conseils & Méthodes

1 Comme le nombre de diviseurs N est égal au produit des puissances plus un des facteurs premiers, dans la décomposition de n, on cherche à décomposer N en produit de facteurs.

2 Chercher à réduire la décomposition de N à l'aide des diviseurs de n.

3 Éliminer les différents choix à l'aide contraintes de l'énoncé : ici n n'est pas divisible par 8.

À vous de jouer !

14 α et β sont deux naturels et $n = 2^{\alpha} \times 3^{\beta}$.
Le nombre de diviseurs de n^2 est le triple du nombre de diviseurs de n.
1. Prouver que $(\alpha - 1)(\beta - 1) = 3$.
2. Déduire les valeurs possibles pour n.

15 L'entier parmi les nombres inférieurs ou égaux à 50 qui possède le plus de diviseurs en possède 10.
Trouver cet entier.

16 Parmi les nombres inférieurs ou égaux à 100, quatre possèdent 12 diviseurs.
1. Montrer qu'il existe quatre configurations pour un entier de posséder 12 diviseurs.
2. Trouver ces quatre entiers inférieurs à 100 parmi ces configurations.

17 On cherche le plus petit entier naturel n possédant 8 diviseurs.
1. Montrer qu'il existe trois configurations pour un entier de posséder 8 diviseurs.
2. Tester ces trois configurations et en déduire la solution du problème.

18 Un entier naturel n possède 21 diviseurs.
On sait de plus que n est divisible par 18 mais pas par 27.
Quel est cet entier ?

19 α et β sont deux naturels et $n = 2^{\alpha} \times 3^{\beta}$.
Le nombre de diviseurs de $18n$ est le double du nombre de diviseurs de n.
1. Montrer que : $18n = 2^{\alpha+1} \times 3^{\beta+2}$.
2. Montrer alors que $\alpha(\beta - 1) = 4$.
3. Déduire les valeurs possibles pour n.

20 Parmi les nombres inférieurs ou égaux à 200, un seul possède 18 diviseurs.
1. Montrer qu'il existe quatre configurations pour un entier de posséder 18 diviseurs.
2. Trouver cet entier inférieur à 200 parmi ces configurations.

↪ Exercices 73 à 79 p. 148

Méthode 7 Travailler modulo p avec p premier

↪ Cours 5 p. 140

Énoncé

Soit p un nombre premier et a, b, n des entiers relatifs.

1. Montrer que si $na \equiv nb\ (p)$ avec $n \not\equiv 0\ (p)$ alors :

$$a \equiv b\ (p).$$

2. Montrer que si a est premier avec p et si n est un multiple de $p-1$ alors :

$$a^n \equiv 1\ (p).$$

3. Montrer que si a est premier avec p alors il existe un entier b tel que :

$$ab \equiv 1\ (p).$$

En déduire que tout entier a non nul inférieur à p possède un inverse inférieur à p modulo p.

Solution

1. $na \equiv nb\ (p) \Leftrightarrow na - nb \equiv 0\ (p) \Leftrightarrow n(b-a) \equiv 0\ (p)$. 1
p divise $n(b-a)$ et comme $n \not\equiv 0\ (p)$, p ne divise pas n
p est alors premier avec n et donc, d'après le théorème de Gauss, p divise $(a-b)$. 2

$$a - b \equiv 0\ (p) \Leftrightarrow a \equiv b\ (p)$$

2. $n = k(p-1)$ avec $k \in \mathbb{Z}$.
Comme a est premier avec p, a n'est pas un multiple de p, 3
d'après le petit théorème de Fermat : 4

$$a^{p-1} \equiv 1\ (p) \overset{\uparrow k}{\Rightarrow} (a^{p-1})^k \equiv 1^k\ (p)$$
$$\Rightarrow a^{k(p-1)} \equiv a^n \equiv 1\ (p)$$

3. Si p est premier alors $p \geqslant 2$ et donc $p - 2 \geqslant 0$.

Comme a est premier avec p, a n'est pas un multiple de p,
d'après le petit théorème de Fermat :

$a^{p-1} \equiv 1\ (p) \Leftrightarrow a \times a^{p-2} \equiv 1\ (p)$
donc il existe $b = a^{p-2}$ tel que $ab \equiv 1\ (p)$.

Si a est non nul et inférieur à p, alors a est premier avec p.
Il existe alors un réel $b \equiv a^{p-2}\ (p)$ tel que $ab \equiv 1(p)$.

Soit r le reste de la division de b par p, le reste r est inférieur à p.
On a alors $ar \equiv 1(p)$.

Remarque

On vient de montrer que tout entier non multiple de p admet un inverse modulo p avec p premier.

Il est alors possible de diviser par un entier non nul dans la congruence modulo p.

Conseils & Méthodes

1. Attention, on ne peut pas diviser généralement avec les congruences.
2. Revenir à la définition de la congruence pour argumenter.
3. Penser au théorème de Fermat.
4. Compatibilité des congruences avec la puissance.

À vous de jouer !

21 Soit a un entier naturel pair non nul.
Soit p un nombre premier divisant $a^2 + 1$.
1. Montrer que p est de la forme $4n + 1$ ou $4n + 3$.
2. On suppose que p est de la forme $4n + 3$.
a) Montrer que p ne divise pas a.
b) Montrer que $(a^4)^n \times a^2 \equiv 1\ (p)$.
c) En déduire une contradiction.
3. Conclure.

22 Soit N un entier supérieur ou égal à 2 et a un entier naturel pair non nul.
On pose $a = N!$
1. Montrer qu'il existe un nombre premier p divisant $(a^2 + 1)$.
2. En utilisant le résultat de l'exercice précédent :
a) montrer que $p > 1$.
b) Justifier alors qu'il existe une infinité de nombres premiers p de la forme $4n + 1$.

↪ Exercices 80 à 81 p. 148

Exercices apprendre à démontrer

Le théorème à démontrer Infinité des nombres premiers

Il existe une infinité de nombres premiers.

On utilisera un raisonnement par l'absurde.

VIDÉO
Démonstration
lienmini.fr/maths-e05-05

Comprendre avant de rédiger

- Quand on veut montrer qu'une propriété P est vraie par un raisonnement par l'absurde, on suppose que P est fausse et l'on montre alors qu'on obtient une contradiction.
- Supposons qu'il n'existe que trois nombres premiers : 2, 3 et 5. On forme un entier n qui est le produit de ces trois nombres premiers auquel on ajoute 1 : $n = 2 \times 3 \times 5 + 1 = 31$.
- D'après le théorème fondamental de l'arithmétique, 31 doit se décomposer de façon unique en produit de puissances de 2, 3 et 5. Ce n'est bien sûr pas le cas. Il y a donc une contradiction.

Rédiger

Étape 1
On prend les nombres premiers dans l'ordre croissant $p_1 = 2, p_2 = 3, p_3 = 5$ et ainsi de suite jusqu'au dernier p_n.

L'unicité de la décomposition est obtenue en ordonnant les facteurs premiers du plus petit au plus grand.

Étape 2
On forme un entier N produit de tous les nombres premiers auquel on ajoute 1.

Étape 3
D'après le théorème fondamental de l'arithmétique, N se décompose en produit de facteurs premiers.

C'est possible car on a pris les n premiers nombres dans l'expression de n.

Étape 4
Si un entier divise a et b, cet entier divise la différence $a - b$.

Étape 5
1 n'a qu'un seul diviseur positif lui-même.
n possède au moins le facteur 2 donc il est supérieur à 3.

Étape 6
Par construction $N \geqslant 2$.

La démonstration rédigée

On suppose qu'il existe un nombre fini de nombres premiers :

$$p_1, p_2, p_3, \ldots, p_n.$$

On pose :

$$N = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1.$$

Il existe au moins un nombre premier p_i dans la décomposition de N, donc p_i divise N.

p_i divise N et le produit de tous les nombres premiers

$$P = p_1 \times p_2 \times p_3 \times \ldots \times p_n.$$

p_i divise donc la différence : $N - P = 1$.

On en déduit alors que $N = 1$.

Contradiction, donc l'hypothèse de départ est fausse. Il y a un nombre infini de nombres premiers

Pour s'entraîner

Montrer l'irrationnalité de $\sqrt{2}$ par l'absurde.

On rappelle qu'un nombre rationnel x peut s'écrire $x = \frac{p}{q}$ avec PGCD$(p, q) = 1$.