TS spé

Les nombres premiers

Le 5-10-2023

carré magique d'inverses de nombres premiers article Wikipedia

Le 29-12-2022

Crible d'Ératosthène Python

Fonction remove

→ schoolmove

→ prépa d'Arsonval pas mal pour mathplotlib

Le 8-6-2022

La décomposition en facteurs premiers fournit un moyen rapide de simplifier la racine carrée, la racine cubique … la racine *n*-ième d'un entier naturel.

Exemple : 3, 5, 12

$c = 3\times5\times3\times4$

$\sqrt[3]{a} = \sqrt[3]{180}$

J'ai pris cet exemple sur le site wiki-how article sur la moyenne géométrique de plusieurs nombres.
Il proposait le calcul de la moyenne géométrique des nombres 3, 5, 12.

Le 20 avril 2022
Inégalité de Bonse

Pour commencer :

Écrire la liste des diviseurs positifs de 36.
Entourer les diviseurs premiers.
Que peut-on faire de ces diviseurs ?

Programmes Python du chapitre à connaître :

① Programme fondamental de test de primalité

La fonction Python fondamentale « estpremier » peut être programmée de plusieurs façons.
L'argument `n` doit être un entier naturel supérieur ou égal à 2.
La fonction renvoie une valeur booléenne, c'est-à-dire ou bien `True` ou bien `False`.

• Une première version très basique :

On parcourt l'ensemble des entiers naturel entre 2 et `n-1`.
On remarque que dès qu'on trouve un diviseur `k` on peut renvoyer `False`. L'instruction return permet à la fois de renvoyer le résultat attendu et d'interrompre l'itération.
Le programme est écrit dans le cadre de gauche.

• Une deuxième version améliorée :

Pour tester si un entier naturel `n` supérieur ou égal à 2 est premier, il suffit de tester sa divisibilité par les entiers plus petits ou égaux à sa racine carrée.
On a utilisé l'instruction `assert(n>=2)` pour vérifier l'hypothèse faite sur l'argument.
Le programme est écrit dans le cadre de droite.

```
def estprem(n):
    for k in range(2,n):
        if n%k==0:
            return False
    return True
```

```
def estprem(n):
    assert(n>=2)
    d=2
    while d*d<=n:
        if n%d==0:
            return False
        d=d+1
    return True
```

② Autres programmes

Fonction plus petit diviseur premier

```
def ppdp(n):
    d=2
    while n%d!=0:
        d=d+1
    return d
```

Fonction test de primalité

```
def estprem(n):
    if ppdp(n)==n:
        x=True
    else:
        x=False
    return x
```

Liste des nombres premiers inférieurs ou égaux à un entier naturel donné

```
def liste_premiers(n):
    L=[]
    for k in range(2,n+1):
        if estprem(k)==True:
            L.append(k)
    return L
```

ou

```
def liste_premiers(n):
    L=[k for k in range(2,n+1) if estprem(k)==True]
    return L
```

Décomposition en facteurs premiers d'un entier

```
def div_prem(n):
    L=[]
    while n>1:
        d=ppdp(n)
        L.append(d)
        n=n//d
    return L
```

On peut compléter en faisant résoudre certains problèmes :
- nombre et proportion de nombres premiers inférieurs ou égaux à un entier naturel *N* donné ;
- liste de nombres premiers compris entre deux entiers *a* et *b* donnés.

Plan du chapitre :

Commentaires :

• Ce chapitre reprend les notions étudiées dans les chapitres précédents (congruences, PGCD, PPCM etc.).

• Il faut connaître les nombres premiers inférieurs à 50.

• Tous les énoncés des propriétés doivent être sus par cœur.

• Les démonstrations sont toutes à apprendre et à savoir refaire à l'exception de celle qui est mentionnée comme devant seulement être comprise dans le paragraphe **V. 1°)**.

• Les algorithmes donnés en appendice (test de primalité et décomposition en facteurs premiers) doivent être sus par cœur et il est conseillé d'avoir les programmes correspondant dans la calculatrice.

• Les résultats donnés en appendice doivent être connus.

I. Quelques généralités sur les nombres premiers

Rappel : Pour tout entier relatif n, 1 et n sont deux diviseurs associés de n.

1°) Définition [rappel]

On dit qu'un entier naturel est **premier** s'il admet exactement deux diviseurs positifs : 1 et lui-même.

Autrement dit, un entier naturel p est premier si et seulement si il admet exactement deux diviseurs positifs (qui sont donc 1 et p).

2°) Remarques

• 0 n'est pas premier (car il admet une infinité de diviseurs positifs ; en effet, tout entier relatif est un diviseur de 0).

• 1 n'est pas premier (car un seul diviseur positif : 1).

• 2 est le plus petit des nombres premiers et c'est le seul nombre premier pair.
Tout nombre premier supérieur ou égal à 3 est impair. La démonstration est quasiment évidente.

• Les premiers nombres premiers sont : 2, 3, 5, 7, 11, 13, 17, 19 etc. Une liste des nombres premiers inférieurs à 1000 est donnée en appendice à la fin du chapitre.
Nous verrons dans le paragraphe **II** une méthode permettant d'obtenir très facilement la liste de tous les nombres premiers inférieurs ou égaux à un entier naturel $N \geqslant 3$ fixé (crible d'Ératosthène).

3°) Caractérisation d'un nombre non premier

Soit n un entier naturel.

n n'est pas premier $\Leftrightarrow$ n admet un diviseur positif autre que 1 et n.

Soit n un entier naturel.

n n'est pas premier $\Leftrightarrow$ il existe un entier naturel d distinct de 1 et n tel que $d \mid n$.

Un entier naturel supérieur ou égal à 4 qui n'est pas premier est dit « composé ».
Il s'écrit comme le produit de deux entiers naturels supérieurs ou égaux à 2.

On retiendra la petite propriété suivante :

Soit n un entier naturel tel que $n \geqslant 4$.
n non premier $\Leftrightarrow$ $n = pq$ avec $p \geqslant 2$ et $q \geqslant 2$

Un entier naturel supérieur ou égal à 4 n'est pas premier si et seulement si il peut s'écrire comme produit de deux entiers supérieurs ou égaux à 2.

Cette propriété fondamentale permet de reconnaître qu'un entier naturel n'est pas premier.

4°) Quelques questions

- L'ensemble des nombres premiers est-il infini ?
- Comment reconnaître si un nombre est premier ?
- Comment sont répartis les nombres premiers ?

Il y a encore beaucoup d'autres questions sur les nombres premiers. Certaines ont été résolues ; d'autres ne le sont pas encore et font encore l'objet de recherches.

Il y a également de nombreuses curiosités autour des nombres premiers. Nous en verrons quelques unes en exercices (par exemple, les familles de certains nombres premiers).

Ces nombres font l'objet de recherches actives car il faut toujours en trouver de plus grands ; en effet, ils interviennent dans le codage de données (voir méthode RSA).

5°) Test élémentaire de primalité

L'argument de la fonction **estprem** est un entier naturel supérieur ou égal à 2.

```
Fonction estprem(n)
    Pour k allant de 2 à n−1 Faire
        Si k divise n
            Renvoyer Faux
        FinSi
    FinPour
    Renvoyer Vrai
```

La fonction Python est donnée au début.

II. Reconnaissance d'un nombre premier

1°) Lemme

• Énoncé :

Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier : son plus petit diviseur entier naturel autre que 1.

• Exemples :

Les diviseurs positifs de 15 sont 1, 3, 5, 15. Le plus petit diviseur positif de 15 autre que 1 est 3.

Les diviseurs positifs de 13 sont 1 et 13. Le plus petit diviseur positif de 13 autre que 1 est 13.

• Démonstration (à savoir refaire) :

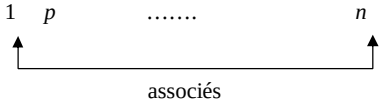
n est un entier naturel supérieur ou égal à 2.

☐ 1er cas : n est premier

Dans ce cas, le lemme est démontré (le plus petit diviseur positif de n autre que 1 est n, qui est premier).

☐ 2e cas : n n'est pas premier

On écrit la liste des diviseurs positifs de n dans l'ordre croissant.



On note p le plus petit diviseur de n strictement supérieur à 1.

On va démontrer que p est premier.

Considérons en effet un diviseur positif d de p.

Comme p est un diviseur de n, d est aussi un diviseur de n.
De plus, $d \leqslant p$.

D'après la liste des diviseurs positifs de n, on en déduit que $d = 1$ ou $d = p$.
p admet donc exactement deux diviseurs positifs (car $p \neq 1$).
On en déduit que p est un nombre premier.

Remarques :

- Cette propriété permet de créer une fonction Python importante : `ppdp(n)` qui renvoie le plus petit diviseur premier puis une fonction `estprem(n)` qui permet de savoir si un entier est premier.

```
Fonction ppdp(n)
    d = 2
    Tantque d ne divise pas n Faire
        d ← d +1
    FinTantque
    Renvoyer d
```

- Si n est un entier naturel pair, alors le plus petit diviseur strictement supérieur à 1 est 2 qui est bien premier.

• Majoration du plus petit diviseur premier d'un entier naturel non premier

On suppose que n est un entier naturel supérieur ou égal à 2 non premier.

On note p son plus petit diviseur positif autre que 1.

On peut dire que p est strictement inférieur à n. Autrement dit, on a $1 < p < n$.

Nous allons préciser cette inégalité.

p est associé à un autre diviseur q, de telle sorte que l'on a $pq = n$ (il est à noter que p peut être égal à q, penser par exemple à 25 et au diviseur 5).
q est donc aussi un diviseur positif de n autre que 1.
En effet, si q était égal à 1, alors p serait égal à n ce qui n'est pas possible puisque l'on a fait l'hypothèse que n n'est pas premier.
Par définition de p, on peut dire que $q \geqslant p$.
On sait que lorsque deux entiers naturels sont deux diviseurs associés d'un entier naturel non nul, alors le plus petit est inférieur ou égal à la racine carrée de cet entier.
On en déduit que $p \leqslant \sqrt{n}$.

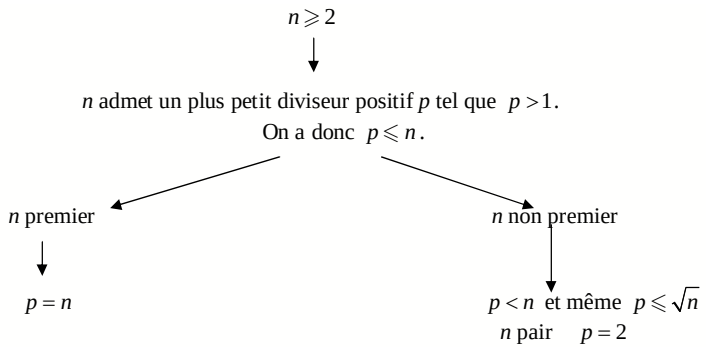
On peut donc énoncer la propriété suivante.

Propriété :

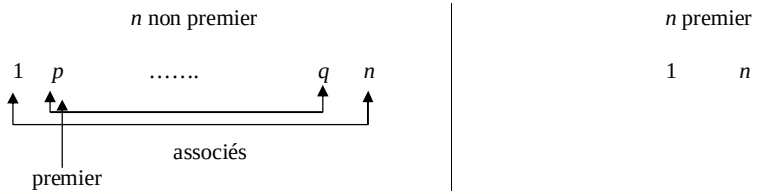
Soit n est un entier naturel supérieur ou égal à 2.
Si n n'est pas premier, alors son plus petit diviseur positif autre que 1 est un nombre premier p tel que $p \leqslant \sqrt{n}$.

Cette propriété fournit un critère d'arrêt dans le test de primalité.

Schéma récapitulatif à retenir :



Diviseurs positifs d'un entier naturel $n > 1$:



2°) Propriété (un test de primalité utilisant le critère d'arrêt)

• Énoncé :

n est un entier naturel supérieur ou égal à 2.
Si n n'est divisible par aucun nombre premier p tel que $p \leqslant \sqrt{n}$, alors n est premier.

• Démonstration (à savoir refaire) :

On raisonne par contraposition.
On a démontré dans le paragraphe 1°) que si n n'est pas premier, alors n admet un diviseur premier p inférieur ou égal à $\sqrt{n}$.

• Application pratique :

Pour déterminer si un entier naturel $n \geqslant 2$ est premier, on teste la divisibilité de n par tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$.

Cette méthode est importante.

3°) Exercice

Dans chaque cas, dire si le nombre est premier sans utiliser la liste des nombres premiers donnée en appendice.

a) 547 b) 133

Solution :

b) D'après la calculatrice, on a : $\sqrt{547} = 23,3880311...$.

La calculatrice n'est pas indispensable. On peut se contenter de dire que $23 < \sqrt{547} < 24$ (car $23^2 = 529$ et $24^2 = 576$).

On teste successivement la divisibilité de 547 par les nombres premiers inférieurs ou égaux à 23 pris dans l'ordre croissant.

547	nombre premier	547 est-il divisible par ce nombre premier ?
	2	non
	3	non
	5	non
	7	non
	11	non
	13	non
	17	non
	19	non
	23	non

547 n'est pas divisible par 2, 3, 5, 7, 11, 13, 17, 19 et 23 donc **547 est premier**.

On peut vérifier ce résultat avec la liste des nombres premiers inférieurs à 1000 donnée en appendice.

a) D'après la calculatrice, on a $\sqrt{133} = 11,5325625...$.

La calculatrice n'est pas indispensable. On peut se contenter de dire que $11 < \sqrt{133} < 12$ (car $11^2 = 121$ et $12^2 = 144$).

On teste successivement la divisibilité de 133 par les nombres premiers inférieurs ou égaux à 11 pris dans l'ordre croissant.

133	nombre premier	133 est-il divisible par ce nombre premier ?	
	2	non	
	3	non	
	5	non	
	7	oui	$133 = 7 \times 19$

133 n'est pas un nombre premier.

On peut vérifier ce résultat avec la liste des nombres premiers inférieurs à 1000 donnée en appendice.
Il y a d'autres méthodes possibles :
- utilisation d'une table de nombres premiers ;
- utilisation d'un programme pour avoir la liste des diviseurs positifs d'un entier (cela peut être assez long) ;
- utilisation du programme « test de primalité » donné dans l'appendice 2 ;
- utilisation d'un logiciel de calcul formel (commande « isprime » sur XCas).

4°) Le crible d'Ératosthène

On cherche la liste des nombres premiers inférieurs ou égaux à un entier naturel $N \geqslant 2$ donné.
On pourrait tester chaque entier de 1 à N mais ce serait long.
Ératosthène, mathématicien grec de l'antiquité (vers – 272 ; – 194), a imaginé une méthode beaucoup plus rapide.

Le crible d'Ératosthène est une méthode qui permet de déterminer une liste de nombre premiers sans tester chaque entier naturel.

Exemple :

On prend $N = 25$. On cherche tous les nombres premiers inférieurs ou égaux à 25.

On écrit les entiers naturels de 1 à 25 (pour notre exemple).

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

On barre le 1 qui n'est pas premier.

~~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

2 est premier. On entoure 2 et ensuite on barre tous les multiples de 2 (différents de 2) qui ne seront donc pas premiers.

~~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

Le premier nombre restant de la liste est 3 et est nécessairement premier. Il n'est pas divisible par un diviseur premier plus petit sinon il serait barré.
On entoure 3 et on barre tous les multiples de 3 (différents de 3).

~~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

Le premier nombre restant est 5 et est donc premier. On entoure 5 et on barre les multiples de 5 (différents de 5). Ici, le seul nouveau nombre barré est 25.

~~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~~

Nous avons entouré tous les nombres premiers inférieurs ou égaux à 25.

~~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~~

À titre d'entraînement, déterminer la liste des nombres premiers inférieurs à 100 par le crible d'Ératosthène.

On pourra présenter la démarche en écrivant tous les entiers naturels de 1 à 100 dans un tableau carré à 10 lignes et 10 colonnes.

Information :

Ératosthène de Cyrène

Considéré comme le premier géographe de l'histoire, Ératosthène (vers – 272 ; – 194) est aussi astronome, philosophe et mathématicien. Né à Cyrène, une ancienne ville grecque (actuellement en Libye), il s'installe à Athènes, où il côtoie des disciples de Platon, puis est appelé à Alexandrie par le souverain Lagide Ptolémée III. Il devient le troisième conservateur de la bibliothèque d'Alexandrie.
Célèbre pour son crible, Ératosthène a également proposé le premier procédé connu de calcul du rayon de la Terre. Son calcul était remarquablement exact et est toujours utilisé.
Dans *Platonicus*, il a abordé des domaines aussi variés que la géométrie, l'arithmétique, la philosophie, la musique (*quadrivium*).

http://www.math93.com/mathematiciens/eratosthene.html

Illustration : carte du monde par Ératosthène

Définition du mot crible :

En mathématiques, les cribles sont des techniques algorithmiques (un crible est une méthode de sélection) permettant de discriminer les nombres possédant certaines propriétés : nombres premiers, carrés parfaits, nombres parfaits etc.

On peut programmer le crible d'Ératosthène sur calculatrice en utilisant des listes.

On trouve sur Internet des animations qui présentent le crible d'Ératosthène, par exemple sur le site : http://therese.eveilleau.pagesperso-orange.fr/pages/truc_mat/pratique/textes/crible_an.htm .

Programmation en Python du crible d'Ératosthène :

Version 1 :

```
def crible(N):
    liste=list(range(2,N+1)) # contient tous les nombres entiers entre 2 et N
    for i in liste:
        for j in liste:
            if (j>i) and (j%i==0):
                liste.remove(j) # on retire les multiples de i
    return liste
```

Version 2 :

```
from math import *

def crible(n):
    L=[i for i in range(0,n+1)]
    for i in range(2,int(floor(sqrt(n)))+1):
        if L[i]>=1:
            for k in range(2,int(floor(n/i))+1):
                L[i*k]=0
    i=0
    while i<len(L):
          if L[i]==0 or L[i]==1:
             L.remove(L[i])
          else:
             i+=1
    return L, len(L)
```

crible : fonction Python d'argument *n* où *n* est un entier naturel supérieur ou égal à 1 qui renvoie la liste des nombres premiers inférieurs ou égaux à *n*.
La liste est notée L.
L'idée est au lieu de rayer des nombres, de leur affecter la valeur 0 puis de les supprimer de la liste L.

III. L'ensemble des nombres premiers

1°) Propriété

• Énoncé :

Il existe une infinité de nombres premiers.

• Démonstration (à comprendre et à savoir refaire) :

On raisonne par l'absurde.

Supposons qu'il existe un nombre fini de nombres premiers que nous pouvons noter p_1, p_2, …, p_n.

Considérons le nombre $N = p_1 \times p_2 \times ... \times p_n + 1$ (c'est la grande astuce du raisonnement).

N est un entier naturel supérieur ou égal à 2.

D'après le lemme du **II. 1°)** (« Tout entier naturel supérieur ou égal à 2 admet au moins un diviseur premier »), ce nombre N admet au moins un diviseur premier.
Il existe donc $k \in \{1; 2; ...; n\}$ tel que $p_k \mid N$.
Par ailleurs, p_k divise le produit $p_1 \times p_2 \times p_3 \times ... \times p_n$ et donc $p_k \mid N - p_1 \times p_2 \times p_3 \times ... \times p_n$ soit $p_k \mid 1$ ce qui donne $p_k = 1$, égalité qui contredit le fait que p_k est premier.

On peut aussi dire que $k \in \{1; 2; ...; n\}$ N est congru à 1 modulo p_k donc n'est pas divisible par p_k.
Il est également possible de dire que le reste de la division euclidienne de N par p_k est égal à 1.

La supposition de départ conduit donc à une contradiction. On en déduit qu'elle est fausse.

Il existe bien une infinité de nombres premiers.

On peut utiliser le lemme suivant :

Soit a_1, a_2, …, a_n des entiers relatifs quelconques.
On pose $N = a_1 \times a_2 \times ... \times a_n + 1$.
Si tous les a_i sont différents de 1 et de – 1, alors N n'est divisible par aucun des a_i.

Il s'agit d'une propriété célèbre à bien comprendre due à Euclide (Archimède).

IV. Propriétés

1°) Propriété 1

• Énoncé :

Deux nombres premiers distincts sont premiers entre eux.

• Démonstration :

Soit p et q deux nombres premiers distincts.
On a : $D^+(p) = \{1; p\}$ et $D^+(q) = \{1; q\}$.

Or $p \neq q$ donc $D^+(p) \cap D^+(q) = \{1\}$ d'où le résultat.

2°) Propriété 2

• Énoncé :

Tout nombre premier p est premier avec ses prédécesseurs entiers naturels non nuls ($p-1$, $p-2$, $p-3$ ... 2, 1).

• Démonstration :

Soit a un entier naturel quelconque tel que $1 \leqslant a \leqslant p-1$.

Les diviseurs positifs de a sont inférieurs ou égaux à a donc strictement inférieurs à p.

Par ailleurs, les diviseurs positifs de p sont 1 et p.

On en déduit que le seul diviseur positif commun à a et p est 1.

3°) Propriété 3

• Énoncé :

Soit p un nombre premier.
Soit a un entier relatif.
On cherche $\text{PGCD}(a; p)$.

• Si p divise a, alors $\text{PGCD}(a; p) = p$.

• Si p ne divise pas a, alors $\text{PGCD}(a; p) = 1$.

• Démonstration :

1er cas : $p \mid a$
Dans ce cas, $\text{PGCD}(a; p) = p$ (propriété vue dans le chapitre sur le PGCD).

2e cas : $p \nmid a$
Soit d un diviseur positif commun à a et p.
Comme $d \mid p$, $d = 1$ ou $d = p$.
Or $p \nmid a$ donc $d = 1$.

4°) Propriété 4

• Énoncé :

Soit p un nombre premier.
Soit a un entier relatif.

***p* est premier avec *a* si et seulement si *p* ne divise pas *a*.**

• Démonstration :

La propriété 4 est une conséquence de la propriété 3.

1er cas : $p \mid a$
Dans ce cas, $\text{PGCD}(a\,;p)=p$. Or $p\neq 1$. Donc $\text{PGCD}(a\,;p)\neq 1$.

2e cas : $p \nmid a$
Dans ce cas, $\text{PGCD}(a\,;p)=1$.

• Corollaire :

Soit p un nombre premier.

p* est premier avec tous les entiers qui ne sont pas multiples de *p (c'est-à-dire que si $p \nmid n$, alors $\text{PGCD}(p\,;n)=1$).

5°) Propriété 5

• Énoncé :

Soit p un nombre premier.
Soit a et b deux entiers relatifs.

p* | *ab* ⇔ *p* | *a* ou *p* | *b

Démonstration (à savoir refaire) :

Démontrons que $p \mid ab \Leftrightarrow p \mid a$ ou $p \mid b$.

On démontre l'équivalence en raisonnant dans les deux sens.

• Si $p \mid a$ ou $p \mid b$, alors de manière évidente $p \mid ab$. Ce sens est toujours vrai, que p soit premier ou non.

• Réciproquement, supposons que $p \mid ab$. Démontrons qu'alors $p \mid a$ ou $p \mid b$.

1er cas : $p \nmid a$
Dans ce cas, p et a sont premiers entre eux (propriété 4).
Or $p \mid ab$. Donc d'après le théorème de Gauss, $p \mid b$.

2e cas : $p \nmid b$
Même démarche.

• Exercice d'application (exercice-type) :

Soit x un entier relatif tel que $3 \mid x^2$.
Démontrer que $3 \mid x$.

Solution :

3 est un nombre premier.
On applique la propriété 5 avec $p=3$ et $a=b=x$.

• Généralisation (propriété) :

Soit p un nombre premier.
p un divise un produit d'entiers relatifs quelconques si et seulement si p divise l'un au moins des facteurs.

V. Décomposition en produit de facteurs premiers

1°) Existence

• Exemples :

$56=7\times 8=7\times 2^3=2^3\times 7$

$540=27\times 2\times 10=3^3\times 2\times 2\times 5=2^2\times 3^3\times 5$

• Propriété :

Tout entier naturel supérieur ou égal à 2 est premier ou produit de nombres premiers.

• Démonstration (à comprendre) :

La démonstration de l'existence de la décomposition en facteurs premiers s'inspire de la méthode pratique systématique.

Soit n un entier naturel supérieur ou égal à 2.

- Si n est premier, la propriété est établie.

- Si n n'est pas premier, nous savons que son plus petit diviseur positif p_1 autre que 1 est premier.

On a donc : $n = p_1 \times n_1$ avec $n_1 < n$.

Si n_1 est premier, alors la propriété est établie.

Sinon, on recommence avec n_1.
n_1 est divisible par le nombre premier p_2, à savoir le plus petit diviseur de n_1 supérieur ou égal à 2.

On a donc : $n = p_1(p_2 n_2) = p_1 p_2 n_2$ avec $n_2 < n_1 < n$.

De proche en proche, on construit une suite strictement décroissante d'entiers naturels n_1, n_2 … tels que

$$1 \leqslant \ldots < n_2 < n_1 < n.$$

Cette suite est finie et le dernier d'entre eux est nécessairement égal à 1.

Donc $n = p_1 \times p_2 \times \ldots \times p_k$.

• Remarque :

Dans ce produit, les nombres premiers p_1, p_2, …, p_n ne sont pas tous nécessairement distincts.
En regroupant les nombres premiers égaux, on obtient $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$, les α_i étant des entiers naturels non nuls.
On dit que n est décomposé en produit de facteurs premiers.

2°) Unicité

Propriété (admise) :

On admet que la décomposition en produit de facteurs premiers d'un entier naturel supérieur ou égal à 2 est unique (à l'ordre des facteurs près).

3°) Théorème (qui rassemble en un seul énoncé l'existence et l'unicité vues au 1°) et au 2°))

Tout entier naturel $n \geqslant 2$ peut s'écrire sous la forme $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ où :
p_1, p_2, …, p_r désignent des nombres premiers deux à deux distincts ;
α_1, α_2, … α_r désignent des entiers naturels supérieurs ou égaux à 1.
Cette écriture est unique à l'ordre près des facteurs.

Avec ces notations, l'ensemble des diviseurs premiers de n est $\{p_1, p_2, \ldots, p_r\}$.

On énonce parfois la propriété sous la forme suivante :

Tout entier naturel supérieur ou égal à 2 s'écrit comme produit de nombres premiers.
Cette écriture est unique à l'ordre près des facteurs.

4°) Pratique de la décomposition

• Méthodes « à la main » :

→ Méthode usuelle :

On essaie d'écrire le nombre comme produit d'entiers naturels de plus en plus petits jusqu'à ne faire apparaître que des nombres premiers (cf. exemples du 1°)).

Exemple 1 : décomposition de 140 en produit de facteurs premiers

$$\begin{aligned} 140 &= 14 \times 10 \\ &= (2 \times 7) \times (2 \times 5) \\ &= 2 \times 2 \times 5 \times 7 \\ &= 2^2 \times 5 \times 7 \end{aligned}$$ (2, 5 et 7 sont des nombres premiers)

Exemple 2 : décomposition de 360 en produit de facteurs premiers

$$\begin{aligned} 360 &= 36 \times 10 \\ &= 6^2 \times (2 \times 5) \\ &= (2 \times 3)^2 \times (2 \times 5) \\ &= 2^2 \times 3^2 \times 2 \times 5 \\ &= 2^3 \times 3^2 \times 5 \end{aligned}$$ (2, 3 et 5 sont des nombres premiers)

Exemple 3 : décomposition de 2020 en produit de facteurs premiers

$$\begin{aligned} 2020 &= 20 \times 100 + 20 \\ &= 20 \times 101 \\ &= 2^2 \times 5 \times 101 \end{aligned}$$ (2, 5 et 101 sont des nombres premiers)

→ Méthode systématique :

On étudie la divisibilité du nombre par les nombres premiers pris dans l'ordre croissant selon la présentation donnée dans les exemples (trait vertical avec nombres premiers à droite et quotients à gauche jusqu'à obtenir un quotient égal à 1).

Exemple 1 : décomposition de 168 en produit de facteurs premiers

168	2
84	2
42	2
21	3
7	7
1	

quotients — diviseurs premiers

La décomposition de 168 en produit de facteurs premiers est $168 = 2^3 \times 3 \times 7$.

Exemple 2 : décomposition de 45 en produit de facteurs premiers

45	3
15	3
5	5
1	

La décomposition de 45 en produit de facteurs premiers est : $45 = 3^2 \times 5$.

Pour cette méthode, il est important de respecter la présentation :
- en testant les nombres premiers dans l'ordre croissant ;
- en épuisant complètement un facteur premier avant de passer au suivant.

• Utilisation de la calculatrice (éventuellement à l'aide d'un programme : voir programme donné dans l'appendice 2) **ou utilisation de logiciel de calcul formel**

Calculatrice Numworks

La calculatrice collège Casio fx-92 possède une commande « Décomp ».
Par exemple, pour obtenir la décomposition de 2888, on tape 2888 EXE puis Décomp .
On obtient $2^3 \times 19^2$.

• Utilisation d'outils de calculs en ligne

Utilisation du site « dcode »
http://calculator.intemodino.com/fr/decomposition-en-produit-de-facteurs-premiers.html
http://alain.pichereau.pagesperso-orange.fr/Decnb1erbis.html

5°) Décomposition en facteurs premiers et opérations algébriques

• On donne les décompositions en facteurs premiers de deux entiers naturels a et b.
On peut en déduire la décomposition en facteurs premiers de ab.
Autrement dit, si l'on connaît la décomposition en facteurs premiers de deux entiers naturels, il est possible d'en déduire immédiatement celle de leur produit.

• On donne la décomposition en facteurs premiers d'un entier naturel a.
On peut en déduire la décomposition en facteurs premiers de a^k pour k entier naturel quelconque.
Autrement dit, si l'on connaît la décomposition en facteurs premiers d'un entier naturel, il est possible d'en déduire immédiatement celle de n'importe quelle puissance de cet entier à un exposant entier naturel.

• Si l'on connaît la décomposition en facteurs premiers de deux entiers naturels, il n'est pas possible d'en déduire celle de leur somme ou de leur différence.
La décomposition en facteurs premiers ne se comporte bien que pour la multiplication.

6°) Programme Python

Voir programme Python donné au début.

VI. Divisibilité et décomposition en facteurs premiers

1°) Propriété [condition nécessaire et suffisante de divisibilité à l'aide de la décomposition en facteurs premiers]

> Deux entiers naturels a et b supérieurs ou égaux à 2 sont décomposés en produit de facteurs premiers.
>
> $b \mid a$ si et seulement si tout facteur premier figurant dans la décomposition de b figure aussi dans celle de a avec un exposant supérieur ou égal à celui qu'il a dans la décomposition de b.

Idée de la démonstration :

• Sens direct :

On suppose que $b \mid a$. Il existe donc un entier naturel q tel que $a = bq$.
En écrivant la décomposition en facteurs premiers de b, il est évident que l'on retrouve tous les facteurs premiers dans la décomposition en facteurs premiers de a avec un exposant supérieur ou égal à celui qu'il a dans la décomposition de b.

• Sens réciproque : quasiment évident

On écrit $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ la décomposition en produit de facteurs premiers de a.
p_1, p_2, …, p_r désignent des nombres premiers deux à deux distincts ; α_1, α_2, … α_r désignent des entiers naturels supérieurs ou égaux à 1.
On pose $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$ avec pour tout i compris entre 1 et r l'inégalité $0 \leqslant \beta_i \leqslant \alpha_i$.
On peut alors écrire $a = \left(p_1^{\alpha_1-\beta_1} \times p_2^{\alpha_2-\beta_2} \times \ldots \times p_r^{\alpha_r-\beta_r}\right) \times \left(p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}\right)$ soit
$a = \left(p_1^{\alpha_1-\beta_1} \times p_2^{\alpha_2-\beta_2} \times \ldots \times p_r^{\alpha_r-\beta_r}\right) \times b$.
Pour tout i compris entre 1 et r, le nombre $\alpha_i - \beta_i$ est un entier naturel.
On en déduit que $b \mid a$.
Complément :

On notera que lorsque $b \mid a$, le quotient de la division euclidienne de a par b s'obtient immédiatement grâce aux décompositions en facteurs premiers.

2°) Autre formulation de la propriété (très importante) : diviseurs positifs d'un entier à l'aide de la décomposition en facteurs premiers

n est un entier naturel dont la décomposition en facteurs premiers s'écrit $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ où

♦ p_1, p_2,… p_r sont des nombres premiers deux à deux distincts ;

♦ α_1, α_2,… α_r sont des entiers naturels non nuls.

Les diviseurs positifs de *n* sont tous les entiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ avec $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, …. $0 \leqslant \beta_r \leqslant \alpha_r$.

Cette formule reste valable même lorsque l'un des exposants α_i est nul (auquel cas, au sens strict, il ne s'agit pas de la décomposition en facteurs premiers de *n*).

3°) Utilisation

Cette propriété donne un moyen pour déterminer de façon systématique tous les diviseurs d'un entier naturel.

4°) Exercice

a) Décomposer 196 en produit de facteurs premiers.

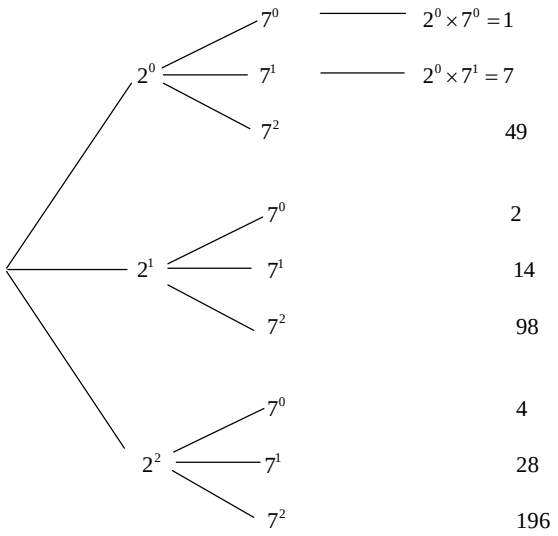
b) À l'aide d'un arbre, déterminer tous les diviseurs positifs de 196.

Solution :

a) $196 = 2^2 \times 7^2$

b) Les diviseurs positifs de 196 sont tous les entiers de la forme $2^\alpha \times 7^\beta$ avec $0 \leqslant \alpha \leqslant 2$ et $0 \leqslant \beta \leqslant 2$.

On obtient les diviseurs positifs de 196 à l'aide d'un arbre de possibilités (arbre à 2 niveaux) :



Les diviseurs positifs de 196 sont 1, 2, 4, 7, 14, 28, 49, 98 et 196.

5°) Autre présentation (fondée sur le même principe), mais nécessitant moins de place

On s'intéresse aux diviseurs positifs de 750.

Ligne	Décomposition en facteurs premiers		Ensemble des diviseurs positifs	Principe
L_0			1	Le nombre 1 est placé sur la ligne L_0. Tout diviseur obtenu à la ligne L_i est le produit d'un diviseur figurant sur une des lignes précédentes par le facteur premier de la ligne L_i .Toutefois, si le facteur premier de la ligne L_i est le même qu'à la ligne L_{i-1}, il suffit de multiplier les diviseurs de la ligne L_{i-1} par le facteur premier de la ligne L_i
L_1	750	2	2	
L_2	375	3	3 6	
L_3	125	5	5 10 15 30	
L_4	25	5	25 50 75 150	
L_5	5	5	125 250 375 750	
L_6	1			

Les diviseurs positifs de 750 sont 1 ; 2 ; 3 ; 6 ; 5 ; 10 ; 15 ; 30 ; 25 ; 50 ; 75 ; 150 ; 125 ; 250 ; 375 ; 750.

6°) Nombre de diviseurs positifs d'un entier naturel supérieur ou égal à 2

• Propriété [cas particulier d'un entier qui n'admet qu'un seul diviseur premier]

p est un nombre premier.

α est un entier naturel.

Le nombre de diviseurs positifs de p^α est égal à $\alpha + 1$.

En effet, les diviseurs positifs de p^α sont 1, *p*, p^2, …, $p^{\alpha-1}$, p^α.

• Propriété [cas général]

Si $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$, les p_i étant des nombres premiers deux à deux distincts et les α_i étant des entiers naturels, le nombre de diviseurs positifs de *n* est égal à $(\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_r + 1)$.

• Démonstration :

Utilisation des principes de dénombrement (principe multiplicatif)

• Exemples :

$\rightarrow\ 1996 = 2^2 \times 499$

Les nombres 2 et 499 sont premiers.

Le nombre de diviseurs positifs de 1996 est égal à : $(2+1)\times(1+1) = 6$.

(Les diviseurs positifs de 1996 sont tous les entiers de la forme $2^{\alpha} \times 499^{\beta}$ avec $0 \leqslant \alpha \leqslant 2$ et $0 \leqslant \beta \leqslant 1$.)

$\rightarrow\ 360 = 2^3 \times 3^2 \times 5$

Le nombre de diviseurs positifs de 360 est égal à 24.

$\rightarrow\ 2020 = 2^2 \times 5 \times 101$

Le nombre de diviseurs positifs de 2020 est égal à 12.

VII. PGCD et PPCM à l'aide de la décomposition en facteurs premiers

1°) Exemple

$a = 13608$

$b = 32076$

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

$b = 2^2 \times 3^6 \times 11$

$\text{PGCD}(a\,;b) = 2^2 \times 3^5$

$\text{PPCM}(a\,;b) = 2^3 \times 3^6 \times 7 \times 11$

2°) Cas général

On considère deux entiers naturels a et b tels que $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_r^{\alpha_r}$ et $b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$ où :
$p_1,\ p_2,\ \ldots,\ p_r$ désignent des nombres premiers deux à deux distincts ;
$\alpha_1,\ \alpha_2,\ \ldots \alpha_r$ désignent des entiers naturels ;
$\beta_1,\ \beta_2,\ \ldots \beta_r$ désignent des entiers naturels.

Attention, certains entiers parmi les α_i ou les β_i peuvent être nuls donc, au sens strict, il ne s'agit pas forcément des décompositions en facteurs premiers de a et b.

• Calcul du PGCD

Propriété (démonstration facile) :

$\text{PGCD}(a\,;b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots \times p_r^{\gamma_r}$ en posant $\gamma_i = \min(\alpha_i\,;\beta_i)$ pour tout entier i tel que $1 \leqslant i \leqslant r$.

Autre formulation de la propriété :

Le PGCD de a et b est égal au produit des facteurs premiers communs aux deux décompositions de a et b, chacun étant élevé au plus petit exposant avec lequel il figure dans la décomposition de a et b.

La démonstration utilise l'écriture des diviseurs positifs d'un entier à l'aide de la décomposition en facteurs premiers.

On utilise la décomposition en facteurs premiers du PGCD.

Exemple :

$a = 196$ $\qquad a = 2^2 \times 7^2$

$b = 140$ $\qquad b = 2^2 \times 5 \times 7$

$\text{PGCD}(a\,;b) = 2^2 \times 7$

Commentaires :

Cette méthode est rapide si l'on connaît les décompositions des deux entiers en facteurs premiers mais longue s'il faut trouver ces décompositions.
On ne l'applique que dans le cas où l'on connaît les décompositions des deux entiers.
La méthode des nombres premiers présentée ici permet de déterminer le PGCD d'une famille finie d'entiers naturels supérieurs ou égaux à 2.

• Calcul du PPCM

Propriété (démonstration facile) :

$\text{PPCM}(a\,;b) = p_1^{\delta_1} \times p_2^{\delta_2} \times \ldots \times p_r^{\delta_r}$ en posant $\delta_i = \max(\alpha_i\,;\beta_i)$ pour tout entier i tel que $1 \leqslant i \leqslant r$.

Autre formulation de la propriété :

Le PPCM de a et b est égal au produit des facteurs premiers intervenant dans les deux décompositions de a et b, chacun étant élevé au plus grand exposant avec lequel il figure dans la décomposition de a et b.

On obtient la décomposition en facteurs premiers du PPCM.

Exemple :

$a = 792$ $\qquad a = 2^3 \times 3^2 \times 11$

$b = 1638$ $\qquad b = 2 \times 3^2 \times 7 \times 13$

$\text{PPCM}(a\,;b) = 2^3 \times 3^2 \times 7 \times 11 \times 13 = 72072$

Commentaires :

Cette méthode est rapide si l'on connaît les décompositions des deux entiers en facteurs premiers mais longue s'il faut trouver ces décompositions.
On ne l'applique que dans le cas où l'on connaît les décompositions des deux entiers.

La méthode des nombres premiers présentée ici permet de déterminer le PPCM d'une famille finie d'entiers naturels supérieurs ou égaux à 2.

• Relation liant PGCD et PPCM

On reprend les notations précédentes.

Les expressions du PGCD et du PPCM sous forme de produits de facteurs premiers permettent de retrouver facilement la relation $\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = ab$ (dans le cas où $a \geqslant 2$ et $b \geqslant 2$).

En effet, $ab = p_1^{\alpha_1+\beta_1} \times p_2^{\alpha_2+\beta_2} \times \ldots \times p_r^{\alpha_r+\beta_r}$ et

$\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = p_1^{\min(\alpha_1\,;\beta_1)+\max(\alpha_1\,;\beta_1)} \times p_2^{\min(\alpha_2\,;\beta_2)+\max(\alpha_2\,;\beta_2)} \times \ldots \times p_r^{\min(\alpha_r\,;\beta_r)+\max(\alpha_r\,;\beta_r)}$.

Or $\min(\alpha_i\,;\beta_i) + \max(\alpha_i\,;\beta_i) = \alpha_i + \beta_i$ pour tout entier i tel que $1 \leqslant i \leqslant r$.

3°) Décomposition en facteurs premiers et nombres premiers entre eux

• Propriété [condition nécessaire et suffisante pour que deux entiers naturels supérieurs ou égaux à 2 soient premiers entre eux] :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si leurs décompositions en facteurs premiers font intervenir des nombres premiers différents.

• Formulation équivalente 1 :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si aucun facteur premier qui intervient dans la décomposition de l'un n'intervient dans la décomposition de l'autre.

• Formulation équivalente 2 :

Deux entiers supérieurs ou égaux à 2 sont premiers entre eux si et seulement si ils n'admettent aucun un diviseur premier commun.

• Conséquence :

Deux entiers supérieurs ou égaux à 2 ne sont pas premiers entre eux si et seulement si ils admettent un diviseur premier commun.

• Généralisation :

La propriété se généralise aisément au cas d'une famille finie quelconque d'entiers naturels supérieurs ou égaux à 2. Des entiers naturels supérieurs ou égaux à 2 (en nombre fini) sont premiers entre eux dans leur ensemble si et seulement si ils n'ont aucun diviseur premier commun.

4°) Retour sur la détermination du PGCD de deux entiers naturels à partir de leur décomposition en facteurs premiers

On considère deux entiers naturels a et b supérieurs ou égaux à 2.

1er cas : a et b n'ont aucun facteur premier commun.
Dans ce cas, le PGCD de a et b est égal à 1.

2e cas : a et b ont au moins un facteur premier commun.
Dans ce cas, le PGCD de a et b est égal au produit des facteurs premiers communs aux décompositions de a et b, chacun étant élevé au plus petit exposant avec lequel il figure dans la décomposition de a et b.

Autrement dit, pour déterminer le PGCD de deux entiers naturels supérieurs ou égaux à 2 :

- On effectue leurs décompositions en facteurs premiers.

- On regarde s'il y a des facteurs premiers qui apparaissent dans les deux décompositions.

- Si oui : on écrit les facteurs premiers communs
on leur affecte le plus petit exposant qui apparaît dans les deux décompositions ;
on effectue le produit.

- Si non : on écrit directement que le PGCD vaut 1.

5°) Utilisation pratique de la décomposition en facteurs premiers pour simplifier une fraction

La décomposition en facteurs premiers fournit une méthode simple pour simplifier une fraction « à la main ».
Cette méthode est en général montrée aux élèves au collège.

Exemple :

On veut simplifier la fraction $\frac{24}{60}$.
On effectue la décomposition en facteurs premiers du numérateur et du dénominateur.

$\frac{24}{60} = \frac{2^3 \times 3}{2^2 \times 3 \times 5}$ que l'on écrit plutôt $\frac{24}{60} = \frac{2 \times 2 \times 2 \times 3}{2 \times 2 \times 3 \times 5}$.

On simplifie les facteurs premiers communs au numérateur et au dénominateur (autrement dit on simplifie par le PGCD).

$$\frac{24}{60}=\frac{\cancel{2}\times\cancel{2}\times 2\times\cancel{3}}{\cancel{2}\times\cancel{2}\times\cancel{3}\times 5}=\frac{2}{5}$$

On raisonne par condition nécessaire et suffisante.

VIII. Carrés et cubes parfaits

1°) Propriété

Un entier naturel supérieur ou égal à 2 est un carré parfait si et seulement si tous les exposants de sa décomposition en facteurs premiers sont pairs.

2°) Démonstration

Soit n un entier naturel tel que $n \geqslant 2$.

• Condition nécessaire pour que n soit un carré parfait :

Supposons que n soit un carré parfait.
Il existe un entier naturel m tel que $n = m^2$.

$m \geqslant 2$ donc m peut se décomposer comme produit de facteurs premiers sous la forme $m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$.

On a alors : $n = \left(p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}\right)^2$
$= \left(p_1^{\alpha_1}\right)^2 \times \left(p_2^{\alpha_2}\right)^2 \times ... \times \left(p_r^{\alpha_r}\right)^2$
$= p_1^{2\alpha_1} \times p_2^{2\alpha_2} \times ... \times p_r^{2\alpha_r}$

Par unicité de la décomposition en facteur premiers d'un entier, on obtient la décomposition en facteurs premiers de n et on voit que chaque exposant est pair.
On en conclut qu'une condition nécessaire pour que n soit un carré parfait est qu'il admette une décomposition en facteurs premiers où tous les exposants sont pairs.

• Condition suffisante pour que n soit un carré parfait :

Ce sens est évident ; il n'est pas lié à la décomposition en facteurs premiers. En effet, si un entier naturel est le produit de puissances d'entiers avec des exposants entiers naturels pairs, alors c'est un carré parfait.
Nous allons tout de même refaire la démonstration.

On suppose que n peut se décomposer sous la forme de facteurs premiers où tous les exposants sont pairs.
Démontrons qu'alors n est un carré parfait.

La décomposition en facteurs premiers de n peut s'écrire sous la forme $n = p_1^{2\alpha_1} \times p_2^{2\alpha_2} \times ... \times p_r^{2\alpha_r}$.
On a donc $n = \left(p_1^{\alpha_1}\right)^2 \times \left(p_2^{\alpha_2}\right)^2 \times ... \times \left(p_r^{\alpha_r}\right)^2$
$= \left(p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}\right)^2$

Donc $n = m^2$ avec $m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$.
On en déduit que n est un carré parfait.

Conclusion :

Une condition nécessaire et suffisante pour qu'un entier naturel supérieur ou égal à 2 soit un carré parfait est que tous les exposants de sa décomposition en facteurs premiers soient pairs.

3°) Généralisation

Un entier naturel supérieur ou égal à 2 est un cube parfait si et seulement si tous les exposants de sa décomposition en facteurs premiers sont des multiples de 3.

Le résultat se généralise à toutes les puissances d'exposant entier naturel.

4°) Quelques résultats qui découlent de la démonstration

• On retiendra que la décomposition en facteurs premiers d'un entier naturel permet immédiatement de savoir si c'est un carré parfait et dans ce cas, elle permet également de donner la racine carrée de cet entier naturel. Idem pour les cubes parfaits.

• On retiendra également que la décomposition en facteurs premiers d'un entier naturel permet également de déterminer le plus grand carré parfait qui divise cet entier naturel. Idem pour les cubes parfaits.

Lorsque l'entier n'est pas un carré parfait, la décomposition en facteurs premiers permet donc de donner sa racine carrée sous la forme $a\sqrt{b}$ où a et b sont des entiers naturels avec b le plus petit possible.

Lorsque l'entier n'est pas un cube parfait, la décomposition en facteurs premiers permet donc de donner sa racine cubique sous la forme $a\sqrt[3]{b}$ où a et b sont des entiers naturels avec b le plus petit possible.

IX. Petit théorème de Fermat

Pierre de Fermat (1601-1665)

1°) Petit théorème de Fermat (admis sans démonstration)

p est un nombre premier et a est un entier premier avec p (c'est-à-dire a non divisible par p).
Alors $a^{p-1} - 1$ est divisible par p c'est-à-dire $a^{p-1} \equiv 1 \pmod{p}$.

2°) Exemples

• On peut écrire directement $24^6 \equiv 1 \pmod{7}$ (petit théorème de Fermat avec $p = 7$ et $a = 24$ premier avec 7).

• On peut écrire directement $34^{10} \equiv 1 \pmod{11}$ (petit théorème de Fermat avec $p = 11$ et $a = 34$ premier avec 11).

3°) Cas de petites valeurs de p

On vérifie aisément le petit théorème de Fermat pour des valeurs particulières de p (petites valeurs de p), par exemple par tableau de congruence.

4°) Corollaire du petit théorème de Fermat

● Énoncé :

p est un nombre premier et *a* est un entier relatif quelconque.
Alors $a^p - a$ est divisible par *p* c'est-à-dire $a^p \equiv a \pmod{p}$.

● Démonstration :

1er cas : *a* n'est pas premier avec *p*

Dans ce cas, *p* divise *a* d'où $a^p \equiv 0 \pmod{p}$.

2e cas : *a* est premier avec *p*

Dans ce cas, le petit théorème de Fermat s'applique. On a : $a^{p-1} \equiv 1 \pmod{p}$.

D'où par produit par *a* de chacun des deux membres, $a^p \equiv a \pmod{p}$.

X. Nombres premiers particuliers

Il existe des familles de nombres premiers très célèbres : les nombres de Fermat, les nombres de Mersenne etc.
Il y a également une famille de nombres entiers intéressants : les nombres de Carmichaël.
Leur étude sera abordée lors de thèmes d'étude.

Appendices

Appendice 1 : Liste des nombres premiers inférieurs ou égaux à 1000

2	31	73	127	179	233	283	353	419	467	547	607	661	739	811	877	947
3	37	79	131	181	239	293	359	421	479	557	613	673	743	821	881	953
5	41	83	137	191	241	307	367	431	487	563	617	677	751	823	883	967
7	43	89	139	193	251	311	373	433	491	569	619	683	757	827	887	971
11	47	97	149	197	257	313	379	439	499	571	631	691	761	829	907	977
13	53	101	151	199	263	317	383	443	503	577	641	701	769	839	911	983
17	59	103	157	211	269	331	389	449	509	587	643	709	773	853	919	991
19	61	107	163	223	271	337	397	457	521	593	647	719	787	857	929	997
23	67	109	167	227	277	347	401	461	523	599	653	727	797	859	937	
29	71	113	173	229	281	349	409	463	541	601	659	733	809	863	941	

Appendice 2 : Algorithmes et programmes (primalité d'un nombre ; décomposition en facteurs premiers)

① Algorithme permettant de savoir si un entier naturel est premier (algorithme de primalité)

On souhaite rédiger en langage naturel un algorithme qui, pour un entier naturel *n* saisi en entrée, affiche en sortie s'il est premier ou non.

On se réfère à la définition d'un nombre premier. Nous proposons ici deux tests de primalité élémentaires.

Algorithme 1

La valeur de *n* saisie en entrée doit être supérieure ou égale à 2.

Entrée :
Saisir *n*

Initialisation :
d prend la valeur 2

Traitement :
Tantque $d \not| n$ **Faire**
    d prend la valeur $d+1$
FinTantque

Sortie :
Si $d = n$
    Alors afficher « le nombre est premier »
    Sinon afficher « le nombre n'est pas premier »
FinSi

Principe :

On teste la divisibilité de *n* par chaque entier strictement supérieur à 1 (c'est-à-dire en commençant par 2).
Il y a deux cas.
Dès que l'on a trouvé un diviseur, on sort de la boucle. Ce diviseur sera strictement inférieur à *n*. Dans ce cas, *n* est premier.
Si l'on n'a pas trouvé de diviseur strictement inférieur à *n* (et supérieur ou égal à 2), la valeur de *d* avant le dernier passage dans la boucle est $n-1$. Du coup, la valeur de *d* après le dernier passage dans la boucle sera *n*. Dans ce cas, le seul diviseur de *n* strictement supérieur à 1 est *n* et, par conséquent, *n* est premier.

Quelques remarques :

• L'algorithme utilise les variables *n* et *d* qui sont des entiers naturels.

• Cet algorithme ne marche pas pour 2.

• Il est intéressant de faire tourner cet algorithme « à la main » sur quelques valeurs de *n* pour voir comment il fonctionne.

Programme sur calculatrice TI :

```
: Prompt N
: 2 → D
: While remainder(N, D) ≠ 0 [ou selon le modèle de calculatrice partDéc(N / D) ≠ 0]
: D+1→ D
: End
: If D = N
: Then
: Disp "LE NOMBRE EST PREMIER"
: Else
: Disp "LE NOMBRE N'EST PAS PREMIER"
: End
```

Quelques remarques :

• Comment trouver les guillemets :

Sur la TI 83-Plus, il faut faire [alpha] puis [+].

• Comment trouver l'apostrophe :

Sur la TI 83-Plus, il faut faire [2nde] puis [0] puis remonter avec la flèche et c'est le deuxième symbole en partant du haut.

• On rappelle ci-dessous comment on traduit la divisibilité d'un entier par un autre en langage de programmation de la calculatrice.

→ Pour les calculatrices TI bleues, on utilise la fonction « partie décimale » (partDéc ou fPart) de la calculatrice que l'on trouve en faisant [math] puis NUM et choix 4.

On traduit « A | B » par « $\text{partDéc}(A/B) = 0$ ».

→ Pour les calculatrices TI noires, on utilise la commande donnant le reste de la division euclidienne (remainder ou reste) que l'on trouve en faisant [math] puis NUM et choix 0.

On traduit « A | B » par « $\text{remainder}(B, A) = 0$ ».

• Il est intéressant de tester le programme pour différentes valeurs de N.
Par exemple, pour le nombre 1789 (qui est un nombre premier), cela met un peu plus de temps. Même chose pour le nombre 2017 qui est premier !

Algorithme 2 (amélioration de l'algorithme 1) :

L'algorithme 2 permet de gagner du temps pour des grands nombres.
On rajoute la condition $d \leqslant \sqrt{n}$ qui est équivalente à $d^2 \leqslant n$.
En effet, on avait vu lors de l'étude des diviseurs positifs d'un entier naturel non nul que les diviseurs fonctionnent par paires.

Entrée :
Saisir n

Initialisation :
d prend la valeur 2

Traitement :
Tantque $d \nmid n$ et $d^2 \leqslant n$ **Faire**
    d prend la valeur $d+1$
FinTantque

Sortie :
Si $d^2 > n$
    Alors afficher « le nombre est premier »
    Sinon afficher « le nombre n'est pas premier »
FinSi

Programme sur calculatrice TI

```
: Prompt N
: 2 → D
: While remainder(N, D) ≠ 0 and D² ≤ N
: D+1 → D
: End
: If D² > N
: Then
: Disp "LE NOMBRE EST PREMIER"
: Else
: Disp "LE NOMBRE N'EST PAS PREMIER"
: End
```

• Le « et » ou « and » se trouve dans [2nde] [math] (tests). Choisir LOGIQUE et sélectionner 1 : et ou 1 : and.

② Algorithme de décomposition d'un entier naturel comme produit de facteurs premiers

On souhaite rédiger un algorithme qui, pour un entier naturel $n \geqslant 2$ saisi en entrée, affiche les diviseurs premiers de n répétés autant de fois qu'ils apparaissent dans la décomposition en facteurs premiers.

On se réfère à la démonstration de l'existence de la décomposition en facteurs premiers, qui est constructive.

On s'appuie sur la démonstration de l'existence de la décomposition en facteurs premiers, qui est constructive.

Langage intermédiaire

• Chercher le plus petit diviseur $d > 1$ de n.
• Remplacer n par $\frac{n}{d}$.
• Recommencer jusqu'à obtenir la valeur 1.

Algorithme 1 [algorithme sans liste à comprendre et à savoir réécrire parfaitement]

On rappelle que la valeur de n saisie en entrée doit être supérieure ou égale à 2.

Entrée :
Saisir n

Initialisation :
d prend la valeur 2

Traitement et sortie :
Tantque $n > 1$ **Faire**
    Si $d \mid n$
        Alors afficher d
            n prend la valeur $\frac{n}{d}$
        Sinon d prend la valeur $d+1$
    FinSi
FinTantque

Quelques remarques :

• L'algorithme utilise les variables n et d qui sont des entiers naturels.

• Il est intéressant de faire tourner cet algorithme « à la main » pour quelques valeurs de n pour voir comment il fonctionne.

• Il est important de comprendre que le contenu de la variable n évolue au fur et à mesure de l'algorithme, en particulier dans la condition (ou test) « $n > 1$ » où elle apparaît (c'est toujours le cas dans les boucles « Tantque »).
• En sortie, les facteurs premiers apparaîtront dans l'ordre croissant.

• On programme aisément cet algorithme sur calculatrice.

Le 16-4-2016

On peut faire tourner le programme « à la main » pour une valeur de n saisie en entrée (par exemple 60).

Étape	Test $n>1$	Test $d \mid n$	n	d
0			60	2
1	vrai	vrai	30	2
2	vrai	vrai	15	2
3	vrai	faux	15	3
4	vrai	vrai	5	3
5	vrai	faux	5	5
6	vrai	vrai	1	5
7	faux			

Variante :

On peut aussi remplacer l'instruction conditionnelle par une deuxième boucle « Tantque » (voir Livre TS spé programme 2012 collection Indice cours sur les nombres premiers).


```
: Prompt N
: 2 → D
: While N > 1
: If remainder(N, D) = 0
: Then
: Disp D
: N/D → N
: Else
: D + 1 → D
: End
: End
```

Algorithme 2 [version non opérationnelle pour la programmation, à savoir réécrire parfaitement]

On utilise une liste L.

Entrée :
Saisir n $(n \geqslant 2)$

Initialisation :
d prend la valeur 2

Traitement :
Tantque $n>1$ **Faire**
  Si $d \mid n$
    Alors ajouter d à la liste L
      n prend la valeur $\frac{n}{d}$
    Sinon d prend la valeur $d+1$
  FinSi
FinTantque

Sortie :
Afficher L

Dans la liste L affichée en sortie, les diviseurs premiers seront donnés dans l'ordre croissant.

Algorithme 2′ [version opérationnelle de l'algorithme 2 pour la programmation]

L'entier naturel *n* saisi en entrée doit vérifier la condition $n \geqslant 2$.

Entrée :
Saisir *n*

Initialisations :
d prend la valeur 2
i prend la valeur 1

Traitement :
Tantque $n > 1$ **Faire**
  Si $d \mid n$
    Alors $L(i)$ prend la valeur *d*
      i prend la valeur $i+1$
      n prend la valeur $\frac{n}{d}$
    Sinon *d* prend la valeur $d+1$
  FinSi
FinTantque

Sortie :
Afficher L

Programme pour calculatrice TI :

```
: EffListe L1  [aller dans stats 4 : ]
: Prompt N
: 2 → D
: 1 → I
: While  N > 1
: If  remainder(N, D) = 0  [ou  fPart(N / D) = 0  ou  partDéc(N / D) = 0 ]
: Then
: D → L1(I)   (bien noter que c'est la lettre I et qu'il faut mettre des
parenthèses}
: I+1 → I
: N/D → N
: Else
: D+1 → D
: End
: End
: Disp L1
```

Pour voir la liste L1, on fait [2nde] [1] (L1) puis on appuie sur la touche [entrer].

Algorithme 3 [amélioration de l'algorithme 2] :

Les diviseurs premiers de *n* peuvent être 2 ou des entiers premiers impairs.
On modifie l'algorithme précédent pour traiter le cas du diviseur 2 éventuel puis les autres diviseurs premiers possibles.

Algorithme 4 [amélioration de l'algorithme 3] :

On sait qu'il suffit de tester les diviseurs inférieurs ou égaux à $\sqrt{n}$.

Entrée :
Saisir *n*

Initialisations :
d prend la valeur 2
c prend la valeur 1
i prend la valeur 1

Traitement :
Tantque $d^2 \leqslant n$ **Faire**
  Si $d \mid n$
    Alors $L(i)$ prend la valeur *d*
      i prend la valeur $i+1$
      n prend la valeur $\frac{n}{d}$
    Sinon *d* prend la valeur $d+c$
      c prend la valeur 2
  FinSi
FinTantque
$L(i)$ prend la valeur *n*

Sortie :
Afficher la liste L

Quelques remarques :

• L'algorithme utilise les variables *n*, *c*, *d*, *i* qui sont des entiers naturels. Il fait aussi intervenir une liste L supposée créée au moment de l'algorithme (déjà vu dans le chapitre « Algorithmes liés à la division euclidienne »).

• Il est intéressant de faire tourner cet algorithme « à la main » pour quelques valeurs de *n* pour voir comment il fonctionne.

• Il est important de comprendre l'intérêt d'utiliser une liste.

• Il est important de comprendre que la variable *n* évolue au fur et à mesure de l'algorithme, en particulier dans la condition (ou test) « $d^2 \leqslant n$ ». De même, sauf si *n* est premier, la valeur de *n* dans l'instruction « $L(i)$ prend la valeur *n* » n'est pas celle saisie en entrée.

• En sortie, les facteurs premiers apparaîtront dans l'ordre croissant.

Programme correspondant sur calculatrice TI

```
: Prompt N
: 2 → D
: 1 → C
: 1 → I
: EffListe L1      [ou ClrList L1]
: While D^2 ⩽ N
: If remainder(N, D) = 0      [ou fPart(N / D) = 0]
: Then
: D → L1(I)
: I+1 → I
: N/D → N
: Else
: D+C → D
: 2 → C
: End
: End
: N→ L1(I)
: Disp L1
```

Quelques remarques :

• Le programme reprend les propriétés du cours (notamment le lemme du **II. 1°)** : le plus petit diviseur positif strictement supérieur à 1 d'un entier naturel est un nombre premier).

• ClrList ou EffListe : touche [stats] EDIT et choisir 4 :

• fPart signifie la partie décimale et pas la partie entière.

Affichage obtenu lorsque l'on fait tourner ce programme :

Par exemple, pour 45, on aura l'affichage suivant :

```
prgmFACTPREM

N = ? 45
{3   3   5}
          DONE
```


Appendice 3 : Somme des diviseurs positifs d'un entier naturel

n est un entier naturel supérieur ou égal à 2 dont la décomposition en facteurs premiers s'écrit $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ où

• $p_1, p_2, \ldots p_r$ sont des nombres premiers deux à deux distincts ;

• $\alpha_1, \alpha_2, \ldots \alpha_r$ sont des entiers naturels non nuls.

Les diviseurs positifs de *n* sont tous les entiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$ avec $0 \leqslant \beta_1 \leqslant \alpha_1,\ 0 \leqslant \beta_2 \leqslant \alpha_2, \ldots .\ 0 \leqslant \beta_r \leqslant \alpha_r$.

Notons $\sigma(n)$ la somme des diviseurs positifs ou nuls de *n*.

On a : $\sigma(n) = \sum_{\substack{0 \leqslant \beta_1 \leqslant \alpha_1 \\ \ldots \\ 0 \leqslant \beta_r \leqslant \alpha_r}} p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r}$

$$= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \ldots \sum_{\beta_r=0}^{\alpha_r} \left(p_1^{\beta_1} \times p_2^{\beta_2} \times ... \times p_r^{\beta_r} \right)$$

$$= \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \times \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \times ... \times \left(\sum_{\beta_r=0}^{\alpha_r} p_r^{\beta_r} \right)$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \times \frac{p_2^{\alpha_2+1}-1}{p_2-1} \times ... \times \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

$$= \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

Grâce à cette formule, on peut aisément démontrer que si *m* et *n* sont deux entiers naturels premiers entre eux, on a : $\sigma(mn) = \sigma(m) \times \sigma(n)$.

Une telle fonction arithmétique est appelée *fonction multiplicative*.

La formule $\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \times \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \times ... \times \left(\sum_{\beta_r=0}^{\alpha_r} p_r^{\beta_r} \right) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$ doit être sue par cœur.

Appendice 4 : Le théorème de Wilson

Énoncé :

Soit p un entier supérieur ou égal à 2.
Si $(p-1)! \equiv -1 \ [p]$ (1), alors p est premier.

John Wilson, né le 6 août 1741, à Applethwaite, dans le Westmorland et mort le 18 octobre 1793, à Kendal, dans le Westmorland, est un mathématicien britannique. Il est connu pour avoir énoncé, sans démonstration, un théorème sur les nombres premiers qui porte son nom.
Wilson étudie à l'université de Cambridge, à Peterhouse. Il y est un étudiant de Edward Waring.
Il devient membre de la Royal Society en 1782. Il se consacre ensuite au barreau.

Le premier texte actuellement connu à faire référence à ce résultat est dû au mathématicien arabe Alhazen (965-1039). Ce théorème est connu à partir du XVII^{e} siècle en Europe. Gottfried Wilhelm von Leibniz (1646-1716) fait référence à ce résultat sans le démontrer. John Wilson redécouvre ce qu'il croit être une conjecture et en partage la découverte avec son professeur Edward Waring, qui publie cette conjecture en 1770.

Démonstration :

1ère démonstration :

D'après (1), il existe $k \in \mathbb{Z}$ tel que $(p-1)! = -1 + kp$ ce qui donne $kp - (p-1)! = 1$.

Donc d'après le théorème de Bezout, p et $(p-1)!$ sont premiers entre eux

Or, $(p-1)!$ est le produit de tous les entiers de 1 à $p-1$.

Donc p n'est divisible par aucun entier inférieur à lui-même.
On en déduit que p est premier.

2^{e} démonstration :

D'après (1), il existe $k \in \mathbb{Z}$ tel que $(p-1)! = -1 + kp$ ce qui donne $kp - (p-1)! = 1$.

Soit d un diviseur positif de p.
Supposons que $d < p$ d'où $d \leqslant p-1$.

On a donc $d \mid (p-1)!$.

Par suite, $d \mid 1$.

On en déduit que $d = 1$ et que p est premier.

Réciproque :

La réciproque est vraie mais nous n'allons pas la démontrer.

Appendice 5 : Représentation des nombres chez Euclide

Appendice 6 : Crible de Sundaram

Le crible de Sundaram permet de lister les entiers naturels impairs non premiers grâce à des suites arithmétiques placées en colonnes. Il est basé sur le fait qu'en déterminant l'ensemble des nombres impairs composés, on peut en déduire l'ensemble des nombres premiers. La colonne numéro n a pour premier terme $(2n+1)^2$ et pour raison $r = 4n+2$. Par conséquent, un nombre impair strictement supérieur à 1, absent de ce tableau, sera premier. En effet, considérons deux nombres impairs quelconques $I_n = 2n+1$ et $I_p = 2p+1$.
Alors on peut écrire que : $I_p = 2p+1 = 2n+1+2k$.
Alors le produit vaut : $I_n \times I_p = (2n+1) \times (2p+1) = (2n+1)^2 + k(4n+2)$.

Ainsi, en faisant varier n et k, on obtient l'ensemble des produits de deux nombres impairs que l'on reproduit dans ce tableau.

9											
15	**25**										
21	**35**	**49**									
27	**45**	**63**	**81**								
33	**55**	**77**	**99**	**121**							
39	**65**	**91**	**117**	**143**	**169**						
45	**75**	**105**	**135**	**165**	**195**	**225**					
51	**85**	**119**	**153**	**187**	**221**	**255**	**289**				
57	**95**	**133**	**171**	**209**	**247**	**285**	**323**	**361**			
63	**105**	**147**	**189**	**231**	**273**	**315**	**357**	**399**	**441**		
69	**115**	**161**	**207**	**253**	**299**	**345**	**391**	**437**	**483**	**529**	
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**

Sundaram était un mathématicien indien. Le crible qu'il publia en 1934 était un peu différent du modèle ci-dessus. Il contenait les valeurs n telles que $2n+1$ ne soit pas premier. Le tableau ci-dessous offre directement les valeurs $2n+1$.

Extrait du livre Math'x TS spé programme 2012 page 73

Point info

Ce crible construit en 1934 par un jeune étudiant indien du nom de Sundaram, permet de conclure sur la primalité d'un entier naturel. Mais comme le crible d'Ératosthène qui date, lui, du III^{e} siècle avant notre ère, son utilisation pour des grands nombres est beaucoup trop gourmande en notre temps…