Arithmétique

1. Division euclidienne

La division euclidienne a été vue au collège.

Exemple

145	11
−143	13
2	

On a posé ci-contre la division euclidienne de 145 par 11. Le dividende est 145, le diviseur 11, le quotient 13 et le reste 2.
On a alors l'égalité $145 = 11 \times 13 + 2$ et le reste vérifie $0 \leq 2 < 11$.

On admet le résultat suivant.

Théorème (division euclidienne). Pour tout entier naturel a et tout entier naturel b non nul, il existe deux entiers naturels uniques q et r tels que
$$a = bq + r \text{ et } 0 \leq r < b.$$

Définition. *L'entier q s'appelle quotient de la division euclidienne de a par b et r est le* reste *de cette division.*

L'algorithme suivant retourne respectivement le quotient et le reste de la division euclidienne de a par b.

```
q ← 0
Tant que a ≥ b
    a ← a − b
    q ← q + 1
Fin Tant que
Retourner q, a
```

Division euclidienne « naïve »

En python,

- `a%b` donne le reste de la division euclidienne de a par b ;
- `a//b` donne le quotient de division euclidienne de a par b ;

1 Compléter le tableau suivant pour suivre l'exécution de l'algorithme ci-dessus avec $a = 17$ et $b = 5$.

a	17			
b	5			
q	0			
$a \geq b$	oui			

Faire de même avec $a = 20$ et $b = 5$, puis $a = 5$ et $b = 20$.

2 Effectuer les divisions euclidiennes suivantes et écrire l'égalité obtenue. Donner le quotient et le reste.
a. 185 par 13 ;
b. 600 par 24 ;
c. 12345 par 678.

3 Préciser si les égalités suivantes peuvent être des divisions euclidiennes. Préciser le dividende et le diviseur le cas échéant.
a. $792 = 21 \times 37 + 15$;
b. $807 = 21 \times 37 + 30$;
c. $819 = 21 \times 37 + 42$.

4 On écrit les unes à la suite des autres les 26 lettres de l'alphabet. Arrivé à Z, on recommence à A et ainsi de suite.
Quelle est la 10 000^{e} lettre écrite ? Combien d'alphabets entiers ont été écrits ?

5 Un texte saisi avec un logiciel comporte 5070 lignes. L'éditeur étudie quelques possibilités de mise en page du texte :
a. Si l'éditeur décide de mettre 64 lignes par page, combien de lignes comporte la dernière page sachant que toutes les autres sont complètes ?
b. Si l'éditeur décide de mettre 81 pages, combien de lignes comporte chaque page sachant que la dernière en comporte 48 ?

6 On considère l'algorithme suivant.

```
Tant que n > 0
    r ← reste de n par 10
    n ← quotient de n par 10
    Afficher r
Fin Tant Que
```

Grâce au tableau suivant, l'exécuter avec $n = 2547$.
Que retourne l'algorithme ?

$n > 0$		oui				
r						
n	2547					

7 Si a divise b, que peut-on dire :
a. du reste de la division euclidienne de b par a ?
b. du reste de la division euclidienne de a par b ?

2. Multiples, diviseurs

Exemple

Les entiers 4 et 6 sont des diviseurs de 12 car $12 = 4 \times 3$ et $12 = 6 \times 2$. On peut aussi dire que 12 est un multiple de 4 et de 6.

Définition. *Soit a et b des entiers. S'il existe un entier q tel que $a = bq$, on dit que a est un multiple de b. Si $b \neq 0$, on dit que b est dit un diviseur de a (ou que a est divisible par b).*

Remarques.

- 1 a pour seul diviseur 1 ;
- tout entier naturel $n \geq 2$ a au moins deux diviseurs : 1 et n ;
- 0 a pour seul multiple 0 ;
- 0 est un multiple de tout entier.
- a est divisible par b si et seulement si le reste de la division euclidienne de a par b est 0.

Exemple

Vérifions avec Python que $3^{15} + 1$ est divisible par 271 :

```
>>> (3**15+1)%271
0
```

Rappelons quelques critères de divisibilité :

- Un entier est divisible par 2 s'il se termine par 0, 2, 4, 6 ou 8 ;
- un entier est divisible par 3 si la somme de ses chiffres est divisible par 3 ;
- un entier est divisible par 5 s'il se termine par 0 ou 5 ;
- un entier est divisible par 9 si la somme de ses chiffres est divisible par 9.

8 Donner les diviseurs de 12 ; 20 ; 35 et 41.

9 Donner un nombre entre 20 et 30 ayant :

a. exactement 2 diviseurs ;
b. exactement 3 diviseurs ;
c. exactement 4 diviseurs.

10 Rappeler la définition d'un nombre pair.
Montrer que si n est un nombre pair, il en de même de n^2.

11 Rappeler la définition d'un nombre impair.
Montrer que si n est un nombre impair, il en de même de n^2.

12 Montrer que la somme de trois nombres consécutifs est divisible par 3.

13 Voici un critère de divisibilité par 7 : un nombre n est divisible par 7 si et seulement si le nombre de dizaines de n augmenté de 5 fois le chiffre de ses unités est divisible par 7.
Par exemple :

- pour **110**6, on calcule $\mathbf{110} + 5 \times 6 = 140$ et comme 140 est clairement divisible par 7, il en de même de 1106 ;
- pour **61**1, on calcule $\mathbf{61} + 5 \times 1 = 66$ et comme 66 n'est pas divisible par 7, il en de même de 611.

1. Les nombres suivants sont-ils des multiples de 7 ? 231 ; 882 ; 1748.
2. Expliquer pourquoi ce critère revient à montrer la propriété suivante : x et y étant deux entiers, $10x + y$ est divisible par 7 si et seulement si $x + 5y$ est divisible par 7.
3. Supposons que $10x + y$ est un multiple de 7. Justifier qu'il existe un entier k tel que $10x + y = 7k$ et en déduire qu'alors $x + 5y$ est un multiple de 7.

4. Démontrer la réciproque.

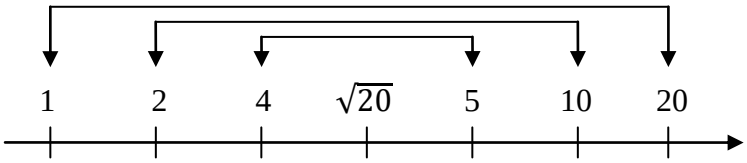
❖ **Recherche des diviseurs d'un entier**

Exemple

Les diviseurs de 20 sont 1 ; 2 ; 4 ; 5 ; 10 et 20. Ils « s'associent » deux à deux de façon à ce que leur produit fasse 20 : on a

$$1 \times 20 = 2 \times 10 = 4 \times 5 = 20.$$

Dans chaque paire de diviseurs « associés », il y en a un dont le carré est inférieur ou égal à 20, c'est-à-dire qui est inférieur ou égal à $\sqrt{20}$, et un dont le carré est supérieur ou égal à 20, c'est-à-dire qui supérieur ou égal à $\sqrt{20}$.



Cette observation est générale : soit n un entier supérieur ou égal à 2, d et d' deux diviseurs « associés » de n, c'est-à-dire tels que $dd' = n$. Si l'on suppose que d est le plus petit de ces deux diviseurs (c'est-à-dire en supposant que $d \leq d'$), alors **on a $\mathbf{1 \leq d \leq \sqrt{n} \leq d'}$.**

Démonstration. En effet, si l'on avait $d > \sqrt{n}$, alors on aurait également $d' > \sqrt{n'}$, d'où $dd' > \sqrt{n} \times \sqrt{n}$, c'est-à-dire $dd' > n$, ce qui serait en contradiction avec $dd' = n$. Cela démontre que $d \leq \sqrt{n}$.
Si l'on avait $d' < \sqrt{n}$, il viendrait $dd' < \sqrt{n} \times \sqrt{n}$, soit $dd' < n$, ce qui encore une fois est impossible. Cela démontre que $d' \geq \sqrt{n}$. ■

La recherche des diviseurs de n peut donc s'écrire sous forme de l'algorithme suivant.

```
Pour k de 1 à √n
   Si k divise n
      Afficher n, n/k
   Fin Si
Fin Pour
```

Recherche des diviseurs de n

```
for k in range(1,int(n**0.5)+1):
   if n%k==0:
      print(k,n//k)
```

Recherche des diviseurs de n (en Python)

Exemple

Exécutons cet algorithme pour $n = 20$. On a $\sqrt{20} \approx 4{,}5$ donc k va varier de 1 à 4.

k	1	2	3	4
k divise n	oui	oui	non	oui
si oui, afficher …	1, 20	2, 10		4, 5

Ainsi les diviseurs de 20 sont : 1, 2, 4, 5, 10 et 20.

Remarque. Si n est un carré ($n = k^2$), l'algorithme retournera deux fois le diviseur k.

14 Faire le tableau pour la recherche des diviseurs de 25, puis 27.

15 Faire la liste des diviseurs de 18, 30, 221, 225 et 227.

16 Proposer une modification de l'algorithme ci-dessous pour éviter le doublon dans le cas où n est un carré.

17 On considère l'algorithme suivant.

```
n=20
L1=[]
L2=[]
for k in range(1,int(n**0.5)+1):
   if n%k==0:
      L1=L1+[k]
      L2=[n//k]+L2
L=L1+L2
print(L)
```

1. Compléter le tableau ci-dessous pour suivre son exécution. Qu'affiche l'algorithme ?

k					
L1	[]				
L2	[]				

2. Donner sans justification l'affichage de l'algorithme s'il est exécuté avec $n = 25$.
3. Écrire l'algorithme en Python gérant le doublon qui apparaît lorsque n est un carré.

3. Rappels sur les puissances, valeurs approchées et arrondis

❖ Rappel sur les puissances

Définition. *Soit a un réel n un entier relatif. On pose*

$$a^0 = 1 \text{ et } a^n = \underbrace{a \times a \times \ldots \times a}_{n\ fois} \text{ si } n \geq 1.$$

Si $a \neq 0$, on pose pour tout entier $n \leq -1$,

$$a^n = \frac{1}{a^{-n}}.$$

Exemple

- $2^4 = 2 \times 2 \times 2 \times 2 = 16$
- $(-2)^3 = (-2) \times (-2) \times (-2) = -8$
- $(-1)^{1789} = -1$ car 1789 est impair
- $3^0 = 1$
- $3^{-2} = \frac{1}{3^2} = \frac{1}{9}$
- $10^7 = 10\,000\,000$
- $10^{-7} = \frac{1}{10^7} = 0,000\,000\,01$

❖ Valeurs approchées et arrondis (source : Chronomaths)

Valeur approchée. Comme son nom l'indique, la valeur approchée d'un nombre N est un nombre dont la valeur est proche de N (presque égale à N). On comprend qu'une valeur approchée n'est pas unique : 4,9 et 5,1 sont proches de 5 ! Voyons cela plus précisément :

- la valeur approchée au dixième par défaut de 3,574 est 3,5 ;
- la valeur approchée au dixième par excès de 3,574 est 3,6. De même pour 3,54.

Règle. Pour une valeur approchée au dixième, (on peut dire aussi à 0,1 près, ou à 10^{-1} près), on étudie le chiffre des centièmes : de 0 à 4 par défaut : on le supprime ; de 5 à 9 : on le supprime en augmentant le chiffre des dixièmes d'une unité.

Cette règle s'applique de manière semblable pour des valeurs approchées à l'unité, au centième, etc. :

- la valeur approchée au centième par défaut de 3,574 est 3,57. Sa valeur approchée au centième par excès de 3,58.

Arrondi. L'arrondi au dixième (on peut dire aussi à 0,1 près, ou à 10^{-1} près) est la valeur approchée au dixième la plus proche du nombre.
Il est incorrect de parler d'un arrondi à 0,1 près par excès (ou par défaut). L'arrondi à la dizaine (resp. à la centaine, etc.) consiste à prendre la valeur approchée à la dizaine (resp. la centaine, etc.) la plus proche.

- L'arrondi au dixième de 3,574 est 3,6. L'arrondi au dixième de 3,547 est 3,5 ;
- l'arrondi à l'unité de 3,54 est 4. L'arrondi à l'unité de 3,49 est 3; celui de 3,5 est 4 ;
- l'arrondi au centième de π = 3,1415926539... est 3,14 ;
- l'arrondi au dix millième de π = 3,1415926539... est 3,1416.

18 On considère le nombre 5,27391. Donner :
a. sa valeur approchée par défaut à 10^{-2} ;
b. sa valeur approchée par défaut à 10^{-3} ;
c. sa valeur approchée par excès à 10^{-4} ;
d. son arrondi à 10^{-2} ;
e. son arrondi à 10^{-3}.

❖ Numération en base 10

Dans la vie courante, nous comptons en base 10.

Exemple

$2018 = 2 \times 1000 + 0 \times 100 + 1 \times 10 + 8 = 2 \times 10^3 + 0 \times 10^2 + 1 \times 10^1 + 8 \times 10^0$.
$5{,}23 = 5 + 2 \times 0{,}1 + 3 \times 0{,}01 = 5 \times 10^0 + 2 \times 10^{-1} + 3 \times 10^{-2}$

19 Donner l'écriture décimale de :
a. 5×10^3 ;
b. $7 \times 10^4 + 9 \times 10^3 + 1 \times 10^1 + 9 \times 10^0$;
c. 10^{-2} ;
d. $2 \times 10^2 + 9 \times 10^{-3}$.

4. Numération en base 2

❖ De la base 2 à la base 10 (facile)

En base 2, on dispose de deux chiffres : 0 et 1.

Exemple

Le nombre 1001_2 vaut, en décimal :

$$1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 8 + 1 = 9.$$

20 Écrire dans le système décimal les nombres suivants.

a. 110_2 ;
b. 1001_2 ;
c. 10011_2 ;
d. 1010011_2.

Comme en base 10, les puissances de 2 d'exposant négatif permettent d'écrire des nombres à virgule en base 2.

Exemple

- $2^{-1} = \frac{1}{2} = 0{,}5$ est noté $0{,}1_2$ en base 2 ;
- $2^{-2} = \frac{1}{2^2} = 0{,}25$ est noté $0{,}01_2$ en base 2 ;
- Le nombre $0{,}101_2$ en base deux est égal à $2^{-1} + 2^{-3} = 0{,}625$ en base 10.

21 Écrire dans le système décimal les nombres suivants.

a. $0{,}1_2$;
b. $11{,}01_2$;
c. $100{,}1_2$;
d. $1001{,}1101_2$.

❖ De la base 10 à la base 2 pour les entiers (un peu plus dur !)

En pratique, la connaissance des puissances de 2 permet de faire rapidement « à la main » la conversion en base 2.

Exemple

Convertissons 13 en base 2.
Comme $2^3 = 8$ et $2^4 = 16$, la plus grande puissance de 2 « rentrant » dans 13 est $2^3 = 8$. Il reste alors $13 - 8 = 5$. Ainsi on a

$$13 = 2^3 + 5$$

On recommence avec 5 : la plus grande puissance de 2 rentrant dans 5 est $2^2 = 4$. Il reste alors $5 - 4 = 1$. On a donc

$$13 = 2^3 + 2^2 + 1$$

Finalement

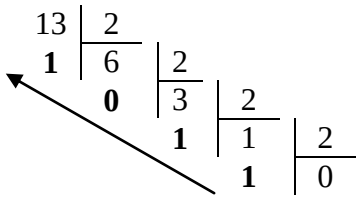
$$13 = 2^3 + 2^2 + 2^0,$$

d'où $13 = 1101_2$.

22 Écrire dans le système binaire les nombres suivants.
a. 21 ;
b. 41 ;
c. 29 ;
d. 85.

Le problème de la méthode précédente est qu'elle est difficile à programmer. En voici une bien plus simple à mettre en œuvre.

On effectue les divisions euclidiennes successives par 2 jusqu'à obtenir 0 pour quotient.



L'écriture en binaire de 13 se lit en remontant la liste des restes : $13 = 1101_2$. Cette méthode s'écrit simplement sous forme d'algorithme :

```
Tant que n > 0
    r ← reste de la division de n par 2
    n ← quotient de la division de n par 2
    Afficher r
Fin Tant que
```

Conversion en binaire

Elle a le petit inconvénient d'afficher les chiffres en base 2 de la droite vers la gauche.
En Python il est préférable d'utiliser les listes pour n'avoir qu'un seul affichage. De plus on peut facilement corriger l'affichage des chiffres et les obtenir de la gauche vers la droite.

```
L=[]
while n>0:
    L=[n%2]+L
    n=n//2
```

Conversion en binaire (Python)

Voici le tableau permettant de suivre l'exécution de l'algorithme avec $n = 13$.

n>0		oui	oui	oui	oui	non
L	[]	[1]	[0,1]	[1,0,1]	[1,1,0,1]	
n	13	6	3	1	0	

23 Compléter le tableau suivant pour suivre l'exécution de l'algorithme pour $n = 26$.

n>0							
L							
n							

❖ **De la base 10 à la base 2 pour les « nombres à virgule » (encore un peu plus dur !)**

Considérons un réel x de l'intervalle $[0; 1[$ que l'on souhaite écrire en binaire avec n chiffres après la virgule (c'est-à-dire que l'on cherche une valeur approchée à 2^{-n} par défaut de x).
Ici un algorithme est quasiment indispensable pour décrire clairement la méthode. Le voici :

```
Pour k de 1 à n
   x ← 2x
   Si x ≥ 1
      c = 1
      x ← x − 1
   Sinon
      c = 0
   Fin Si
   Afficher c
```

Conversion en binaire d'un réel x de $[0; 1[$ avec n chiffres après la virgule

```
L=[]
for k in range(n):
   x=2*x
   if x>=1:
      L=L+[1]
      x=x-1
   else:
      L=L+[0]
print(L)
```

(en Python, avec les chiffres stockés dans une liste)

Exemple

Prenons $x = 0{,}4$ et $n = 5$. L'algorithme peut se représenter de la façon suivante.

0,4 × 2 = **0**,8
0,8 × 2 = **1**,6
0,6 × 2 = **1**,2
0,2 × 2 = 0,4
0,4 × 2 = **0**,8

On déduit qu'une **valeur approchée par défaut de 0,4 à 2^{-5}** est $0{,}01100_2$ (et donc qu'une **valeur approchée par excès à 2^{-5}** est $0{,}01101_2$).

En faisant une étape de plus dans l'algorithme, on constate que le chiffre suivant est un 1, ce qui veut dire qu'une valeur approchée par défaut de 0,4 à 2^{-6} est $0{,}011001_2$ et donc qu'un **arrondi de 0,4 à 2^{-5}** est $0{,}01101_2$.

On remarque que l'algorithme « boucle » rapidement puisqu'on retombe sur 0,8 dans les calculs. Ainsi on a :

$$0{,}4 = 0{,}0110\ 0110\ 0110\ \ldots_2.$$

Il se passe le même phénomène que par exemple pour $\frac{1}{3}$ en décimal qui « ne tombe pas juste » et s'écrit 0,3333333…

Regardons les valeurs approchées et arrondi de 0,4 à 2^{-3} :

- valeur approchée par défaut à 2^{-3} : $0{,}011_2$;
- valeur approchée par excès à 2^{-3} : $0{,}1_2$;
- arrondi à 2^{-3} : $0{,}011_2$.

Pour convertir un nombre à virgule qui n'est pas compris dans $[0; 1[$ on traite séparément la partie entière et la partie à virgule.

Exemple

Donnons un arrondi à 2^{-3} en binaire de 12,4.
On vient de voir que l'arrondi de 0,4 à 2^{-3} est $0{,}011_2$ et comme $12=1010_2$, on en déduit que $12{,}4=1010{,}011_2$.

24 Écrire dans le système binaire les nombres suivants.

a. 17,75 **b.** 54,625
c. 11,375 **d.** 26,3125

25 Donner dans le système binaire une valeur approchée de 0,7 :

a. par défaut à 2^{-4} ;
b. par excès à 2^{-4} ;
c. par excès à 2^{-5}.

26 Donner dans le système binaire une valeur approchée de 23,43 par défaut à 2^{-4} puis une valeur approchée à 2^{-4}.

27 Écrire dans le système binaire le nombre 5,4321 en arrondissant à 2^{-4} :

a. par défaut 2^{-3} ;
b. par excès à 2^{-3}.

28 Donner les 10 premiers chiffres après la virgule de 0,9 en binaire.
Quel est le 50e chiffre ? Le 100e ? Et de façon plus générale, quelle est le n^{e} chiffre, où n est un entier naturel non nul ?

5. Numération en base 16

En base 16 on dispose de 16 chiffres : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E et F.

Exemple

Le nombre $3C5_{16}$ vaut $3 \times 16^2 + 12 \times 16 + 5 = 965$ en décimal.
Le nombre $B{,}A_{16}$ vaut $11 + 10 \times 16^{-1} = 11 + 10 \times \frac{1}{16} = 11{,}625$.

29 Écrire dans le système décimal les nombres suivants.

a. $1A_{16}$ **b.** $7E2_{16}$
c. BAC_{16} **d.** $C0C1_{16}$

30 Écrire dans le système décimal les nombres suivants.

a. $0{,}3_{16}$ **b.** $A{,}B_{16}$
c. $E01{,}5F_{16}$ **d.** $FFF{,}F_{16}$

31 Écrire dans le système hexadécimal les nombres suivants.

a. 541 **b.** 1620
c. 2199 **d.** 10^4

32 Écrire dans le système hexadécimal les nombres suivants.

a. 2199,4375 **b.** 141,34375

6. Nombres premiers

Définition. *Un entier naturel est dit premier s'il a exactement deux diviseurs : 1 et lui-même.*

Exemple

Les entiers 0 et 1 ne sont pas premiers, pas plus que 4 ou 10.
Les entiers premiers inférieurs à 20 sont : 2, 3, 5, 7, 11, 13, 17 et 19.

35 Justifier que les nombres suivants ne sont pas premiers : 21 – 85 – 999 – 1479.

On a vu dans le paragraphe sur la recherche des diviseurs d'un entier n que si d est un diviseur de n et d' son diviseur associé, c'est-à-dire tel que $dd' = n$, alors d ou d' est inférieur à $\sqrt{n}$. Par conséquent, si aucun des entiers compris entre 2 et $\sqrt{n}$ ne divise n, alors n n'a pas de diviseur à part 1 et son diviseur associé n, donc il est premier.
En fait on peut se contenter d'essayer les diviseurs entre 2 et $\sqrt{n}$ qui sont premiers :

Théorème. Soit $n \geq 2$ un entier naturel. Si aucun des entiers premiers compris entre 2 et $\sqrt{n}$ ne divise n, alors n est premier.

Exemple

Les nombres 191 et 187 sont-ils premiers ?

- $\sqrt{191} < 14$. On doit donc tester les diviseurs suivants : 2, 3, 5, 7, 11 et 13.
  - ✓ 191 n'est clairement pas divisible par 2, ni par 5.
  - ✓ 191 n'est pas divisible par 3 car $1 + 9 + 1 = 11$ n'est pas divisible par 3.
  - ✓ $\frac{191}{7} \approx 27{,}3$, donc 7 n'est pas un diviseur de 191.
  - ✓ De même, 11 et 13 ne sont pas des diviseurs de 191.

  Finalement, 191 est premier.
- $\sqrt{187} < 14$, donc on teste si 187 est divisible par les entiers premiers inférieurs strictement à 14, à savoir : 2, 3, 5, 7, 11 et 13. On constate alors que 187 n'est pas premier puisque $187 = 11 \times 17$.

36 Justifier que 281 est un nombre premier.

37 Les nombres suivants sont-ils premiers ? Sinon, donner un diviseur : 91 – 117 – 179 – 429 – 607 – 899 – 1967 – 2207.

38 Existe-t-il une suite de trois nombres consécutifs tous premiers ?

39 Donner 5 nombres entiers consécutifs dont aucun n'est premier.

L'écriture de d'algorithme où l'on teste tous les entiers entre 2 et $\sqrt{n}$ est facile à programmer. La version « raffinée » où l'on ne teste que les premiers est plus difficile.

L'algorithme suivant retourne le booléen Faux ou Vrai selon que l'entier n est premier ou pas. On présente deux versions, l'une utilisant deux « retourner », ce qui a le don d'horripiler certains informaticiens, et l'autre où l'on contourne ce raccourci.

```
Pour d de 2 à √n
    Si d divise n
        Retourner Faux
Fin Pour
Retourner Vrai
```

Test de primalité avec deux « retourner »

```
premier ← Vrai
d ← 2
Tant que d ≤ √n et premier = Vrai
    Si d divise n
        premier ← Faux
    d ← d + 1
Retourner premier
```

Test de primalité avec un « retourner »

Voici l'algorithme avec un « retourner » programmé en Python sous forme d'une fonction nommée `est_premier`, ainsi qu'un exemple d'appel de cette fonction.

```
def est_premier(n):
    premier=True
    d=2
    while d<=int(n**0.5) and premier:
        if n%d==0:
            premier=False
        d=d+1
    return premier
```

```
>>> est_premier(12)
False

>>> est_premier(13)
True
```

40 Pour tout entier naturel n, on pose $a_n = n^2 + n + 41$.

a. Les entiers a_0, a_1, a_2, a_3, a_4, a_5, a_6 sont-ils premiers ?

b. Déterminer, à l'aide d'un algorithme, le plus petit entier naturel n tel que a_n ne soit pas premier.

41 Écrire un algorithme qui détermine 10 nombres entiers consécutifs dont aucun n'est premier.

42 On dit que des nombres premiers sont jumeaux si leur différence est égale à 2. Par exemple 29 et 31 sont des nombres premiers jumeaux.
Écrire un algorithme qui détermine les deux plus petits nombres premiers jumeaux supérieurs à 1000.

7. Décomposition en produit de facteurs premiers

Théorème. Tout nombre entier naturel supérieur ou égal à 2 se décompose de façon unique (à l'ordre des facteurs près) en un produit de nombres premiers.

Exemple

$90 = 2 \times 45 = 2 \times 9 \times 5 = 2 \times 3^2 \times 5$.
De cela on peut déduire tous les diviseurs de 90, ils sont de la forme $2^a \times 3^b \times 5^c$ avec $0 \leq a \leq 1$, $0 \leq b \leq 2$ et $0 \leq c \leq 1$.
Un arbre ou un tableau permet de ne pas en oublier.

			Diviseurs de 90
2^0	3^0	5^0	1
		5^1	5
	3^1	5^0	3
		5^1	$3 \times 5 = 15$
	3^2	5^0	$3^2 = 9$
		5^1	$3^2 \times 5 = 45$
2^1	3^0	5^0	2
		5^1	$2 \times 5 = 10$
	3^1	5^0	$2 \times 3 = 6$
		5^1	$2 \times 3 \times 5 = 30$
	3^2	5^0	$2 \times 3^2 = 18$
		5^1	$2 \times 3^2 \times 5 = 90$

Les diviseurs de 90 sont donc :

1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90.

43 Écrire la décomposition en facteurs premiers des entiers suivants et en déduire la liste de leurs diviseurs : 8 – 9 – 10 – 11 – 12 – 112 – 5423.

44 Écrire la décomposition en facteurs premiers des entiers suivants et en déduire la liste de leurs diviseurs à l'aide d'un arbre : 176 – 252 – 392.

Voici un algorithme retournant la liste des facteurs premiers d'un entier $n \geq 2$. Par exemple, pour l'entier 15, l'algorithme renverra [3,5] et pour 12 il renverra [2,2,3].

```
Pour k de 2 à √n
    Si k divise n
        Retourner k
    Fin Si
Fin Pour
Retourner n
```

fonction premier_diviseur(n)

```
L ← liste vide
Tant que n > 1
    d ← premier_diviseur(n)
    Ajouter d dans la liste L
    n = n/d
Retourner L
```

Algorithme de décomposition

45 Faire fonctionner « à la main » la fonction premier_diviseurs(n) pour $n = 10$, 19, 35 et 59 ? Quel est le rôle de cette fonction ?

46 Faire fonctionner « à la main » l'algorithme de décomposition pour $n = 10$, 19, 40 et 99.

47 Donner la décomposition en facteurs premiers des entiers suivants et donner pour chacun le nombre de diviseurs : 240 – 4896 – 11600.

48 Modifier l'algorithme de décomposition pour qu'il renvoie la liste des diviseurs avec leur puissance. Pour $n = 2^3 \times 7$ on obtiendra [(2,3),(7,1)].

49 Écrire la décomposition en facteurs premiers de 350. Quel est le plus petit entier naturel par lequel il faut multiplier 350 pour obtenir le carré d'un entier naturel ?

8. PGCD

Définition. *Soit a et b deux entiers avec $a \neq 0$ ou $b \neq 0$.*
Le plus grand diviseur commun de deux entiers a et b se note $PGCD(a;b)$.

Exemple

Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12 et ceux de 30 sont 1, 2, 3, 5, 6, 10, 15, 30, donc $\text{PGCD}(12;30) = 6$.

Définition. *Deux entiers naturels sont dits premiers entre eux lorsque leur PGCD est 1.*

Exemple

28 et 15 sont premiers entre eux car les diviseurs de 28 sont 1, 2, 4, 7, 14, 28 et ceux de 15 sont 1, 3, 5, 15, donc $\text{PGCD}(28;15) = 1$.

Il ne faut pas confondre « premiers entre eux » et « premiers ». Deux nombres peuvent être premiers entre eux sans être premiers comme le montre l'exemple précédent.

50 Déterminer le PGCD de
a. 21 et 24 ;
b. 24 et 60 ;
c. 15 et 77 ;
d. 0 et 745.

51 Déterminer si les entiers suivants sont premiers entre eux.
a. 1254 et 2018 ;
b. 444 et 1961 ;
c. 27 et 1 111 111 111 117 (douze « 1 » et un « 7 »).

❖ Calcul du PGCD par l'algorithme d'Euclide

Voici un algorithme extrêmement court pour le calcul du PGCD des deux entiers a et b.

Tant que $b > 0$
  $(a, b) = (b, a\%b)$
Fin Tant que
Retourner a

Fonction pgcd(a,b)

```
def pgcd(a,b):
   while b>0:
      (a,b)=(b,a%b)
return a
```

Fonction pgcd(a,b) en Python

Par exemple le calcul de $\text{PGCD}(81;15)$ donnera les valeurs successives suivantes de a et b :

a	81	15	6	3
b	15	6	3	0

d'où $\text{PGCD}(81;15) = 3$. On a effectué les divisions euclidiennes successives de a par b :

- $81 = 15 \times 5 + 6$
- $15 = 6 \times 2 + 3$
- $6 = 3 \times 2 + 0$

52 Par l'algorithme d'Euclide, calculer le PGCD de
a. 0 et 43 ;
b. 91 et 63 ;
c. 517 et 1128 ;
d. 797 et 122.

53 Cas particuliers.
1. Que renvoie l'algorithme d'Euclide si $b = 0$? (avec $a \neq 0$).
2. Que renvoie l'algorithme d'Euclide si $a = 0$? (avec $b \neq 0$).
3. On suppose que $a < b$. Que fait la première itération de la boucle « tant que » de l'algorithme d'Euclide ?

❖ Calcul du PGCD grâce à la décomposition en facteurs premiers

Le PGCD est le produit des facteurs premiers communs, chacun étant affecté du plus petit exposant avec lequel il figure dans les deux décompositions.

Exemple

$12 = 2^2 \times 3$ et $30 = 2 \times 3 \times 5$, donc $\text{PGCD}(12; 30) = 2^1 \times 3^1 = 6$.

Exemple

28 et 15 sont premiers entre eux car leur décomposition en facteurs premiers n'a aucun facteur commun : $28 = 2^2 \times 7$ et $15 = 3 \times 5$.

54 En utilisant la décomposition en produit de facteurs premiers, déterminer le PGCD de
a. 48 et 216 ;
b. 175 et 385 ;
c. 385 et 1540.

55 Décomposer en produit de facteurs premiers 45. Donner alors, sans calculatrice, tous les entiers compris entre 3250 et 3260 qui sont premiers avec 45.
Écrire un algorithme qui renvoie la liste de ces entiers.

56 On veut répartir la totalité de 760 dragées au chocolat et de 1045 dragées aux amandes dans des sachets ayant la même répartition de dragées de chaque sorte.
a. Peut-on faire 76 sachets ? Justifier la réponse.
b. Quel nombre maximal de sachets peut-on réaliser ?
c. Combien de dragées de chaque sorte y a-t-il alors dans chaque sachet ?

57 Un ouvrier dispose de plaques de métal de 110 cm de longueur et de 88 cm de largeur. Il doit découper des carrés tous identiques, les plus grands possibles, dont les longueurs des côtés sont des nombres entiers de cm et de façon à ne pas avoir de perte.
Déterminer les dimensions de ces carrés et le nombre que l'ouvrier pourra en faire avec une plaque.

9. Congruences

❖ Définitions

Exemple

Admettons qu'aujourd'hui nous soyons le mardi 3 octobre. Les autres mardis du mois d'octobre auront pour date : 10, 17, 24 et 31.
On passe d'un mardi à l'autre en ajoutant ou en enlevant un certain nombre de fois « 7 ».
On dit alors que tous ces nombres : 3, 10, 17, 24 et 31 sont congrus modulo 7.
Par exemple 10 est congru à 31 modulo 7, ou encore 17 est congru à 3 modulo 7. On écrira $10 \equiv 31\ [7]$ et $17 \equiv 3\ [7]$.

Définition. *Soit a et b deux entiers et n un entier naturel non nul.*
On dit que a est congru à b modulo n lorsque que $a - b$ (ou $b - a$) est divisible par n. On note alors $a \equiv b\ [n]$, ou $a \equiv b$ modulo n, ou $a \equiv b \bmod n$.

Exemple

- On a $10 \equiv 31\ [7]$ car $31 - 10 = 21 = 7 \times 3$;
- On a $25 \equiv 17\ [4]$ car $25 - 17 = 8 = 4 \times 2$;
- On a $25 \equiv 41\ [4]$ car $25 - 41 = -16 = 4 \times (-4)$;
- On a $31 \not\equiv 15\ [7]$ car $31 - 15 = 16$ n'est pas un multiple de 7.
- On a $-33 \equiv 2\ [7]$ car $-33 - 2 = -35 = 7 \times (-5)$.

58 À quels entiers 16 est-il congru modulo 5 parmi les entiers suivants ? 1 ; -24 ; 45 ; 151 ; 2018.

59 À quels entiers 16 est-il congru modulo 7 parmi les entiers suivants ? 8 ; 51 ; -19 ; 359 ; 700.

60 Compléter les égalités suivantes avec le plus petit entier positif possible :
a. $21 \equiv \ldots\ [13]$;
b. $28 \equiv \ldots\ [4]$;
c. $57 \equiv \ldots\ [5]$;
d. $124 \equiv \ldots\ [6]$;
e. $2018 \equiv \ldots\ [11]$

Théorème. L'entier a est divisible par n si et seulement si $a \equiv 0\ [n]$.

Démonstration. $a \equiv 0\ [n]$ équivaut par définition à « $a - 0$ est divisible par n ». ■

Exemple

Puisque $30 = 5 \times 6$, on a $30 \equiv 0\ [5]$ (et aussi $30 \equiv 0\ [6]$).

Théorème. La relation de récurrence est transitive, c'est-à-dire que si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$.

Remarque. Toutes les « relations » ne sont pas transitives, par exemple la relation de perpendicularité pour deux droites n'est pas transitive car si $d_1 \perp d_2$ et $d_2 \perp d_3$, on sait qu'alors d_1 et d_3 sont parallèles et non perpendiculaires.

La transitivité permet d'écrire des chaînes d'égalités sans ambigüité, par exemple

$$3 \equiv 10 \equiv 17 \equiv 24 \equiv 31 \ [7].$$

Démonstration. Les congruences $a \equiv b \ [n]$ et $b \equiv c \ [n]$ se traduisent par l'existence de deux entiers k et k' tels que $a - b = kn$ et $b - c = k'n$. Il vient donc

$$a - c = (a - b) + (b - c) = kn + k'n = (k + k')n$$

ce qui montre que $a - c$ est un multiple de n, c'est-à-dire $a \equiv c \ [n]$. ■

❖ Congruences et division euclidienne

D'après la définition, si r est le reste de la division euclidienne de a par n, alors $a \equiv r \ [n]$. En effet, la division euclidienne de a par n se traduit par l'existence de deux entiers q et r tels que $a = qn + r$, ce qui montre que $a - r = qn$ est un multiple de n et donc que $a \equiv r \ [n]$.
On a donc démontré le théorème suivant.

Théorème. Si r est le reste de la division euclidienne de a par n, alors $a \equiv r \ [n]$.

61 Effectuer les divisions euclidiennes de 200 et 900 par 13 et traduire ces résultats par des congruences.

Exemple

Comme la division euclidienne de 20 par 7 est $20 = 7 \times 2 + \mathbf{6}$, on a $20 \equiv \mathbf{6} \ [7]$.

Réciproquement, on a le résultat suivant.

Théorème. La congruence $a \equiv b \ [n]$ équivaut à dire a et b ont le même reste dans la division euclidienne par n.

Démonstration. Soit $a = nq_1 + r_1$ et $b = nq_2 + r_2$ (avec $0 \leq r_1 < n$ et $0 \leq r_2 < n$) les divisions euclidiennes de a et b par n. D'après le théorème précédent, on a

$$a \equiv r_1 \ [n] \text{ et } b \equiv r_2 \ [n].$$

Ainsi

$$a \equiv b \ [n] \Leftrightarrow r_1 \equiv r_2 \ [n] \Leftrightarrow r_1 - r_2 \text{ est divisible par } n.$$

Mais comme $0 \leq r_1 < n$ et $0 \leq r_2 < n$, on en déduit que $-n < r_2 - r_1 < n$ et le seul multiple de n strictement compris entre $-n$ et n étant 0, il vient

$$r_1 - r_2 \text{ est divisible par } n \Leftrightarrow r_1 - r_2 = 0 \Leftrightarrow r_1 = r_2. \ ■$$

Exemple

On a $10 \equiv 31 \ [7]$ et 10 et 31 on bien le même reste dans la division euclidienne par 10, à savoir 7.

Il résulte de ce théorème le suivant :

Théorème. Si $a \equiv r\ [n]$ avec $0 \leq r < n$, alors r est le reste de la division euclidienne de a par n.

62 Dans chacun des cas suivants, donner le reste de la division euclidienne de a par 9.
a. $a \equiv 7\ [9]$;
b. $a \equiv 22\ [9]$;
c. $a \equiv -11\ [9]$.

❖ **Propriétés de calcul sur les congruences**

63 Pour quelques entiers n vérifiant $n \equiv 2\ [7]$, calculer $n^3 + 2n + 2$ modulo 7.
Que semble-t-il se passer ?

Pour éclaircir ce qui se passe dans l'exercice précédent, voici un théorème très important.

Théorème (compatibilité des congruences avec l'addition et la multiplication). Soit a, b, c, d, n des entiers avec $n \geq 1$. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors
1. $a + c \equiv b + d\ [n]$;
2. $a \times c \equiv b \times d\ [n]$;
3. $a^k \equiv b^k\ [n]$ pour tout entier naturel k.

Ce théorème permet de remplacer dans des chaînes de congruences un nombre par un autre qui lui est congru.

Exemple

- On a $24 \equiv 4\ [5]$ et $18 \equiv 3\ [5]$, donc $24 + 18 \equiv 4 + 3 \equiv 7 \equiv 2\ [5]$.
- $24 + 1 \equiv 4 + 1 \equiv 5 \equiv 0\ [5]$.

Exemple

Soit $N = 2^2 \times 3 \times 7 \times 19$. Déterminons le reste de la division euclidienne de N par 10. Il faut donc calculer N modulo 10. La technique est la suivante : on effectue petit-à-petit les multiplications, et dès qu'on dépasse 10, on réduit modulo 10 :

$$N \equiv 12 \times 7 \times 19 \equiv 2 \times 7 \times 9 \equiv 14 \times 9 \equiv 4 \times 9 \equiv 36 \equiv 6\ [10]$$

et comme $0 \leq 6 < 10$, le reste cherché est 6.

64 Sans calculatrice, compléter avec le plus petit entier positif possible.
a. $72 + 706 \equiv \ldots\ [7]$;
b. $72 \times 706 \equiv \ldots\ [7]$;
c. $11 \times 13 \times 17 \times 19 \equiv \ldots\ [9]$;
d. $12^5 \times 45 + 91 \equiv \ldots\ [10]$.

65 Éclaircir le mystère de l'exercice 63.

66 Démontrer que le reste de la division euclidienne de 216^{30} par 7 est 1.
Quelle est le reste de la division euclidienne de 307^{17} par 7 ?

67 Démontrer que $6^{23} \equiv 1\ [5]$, puis que $9^{23} \equiv 4\ [5]$.

Exemple

Montrons que $17^5 + 7$ est divisible par 8.
On a $17 \equiv 1\ [8]$, donc $17^5 \equiv 1^5\ [8]$, ce qui montre que $17^5 \equiv 1\ [8]$. Par conséquent il vient $17^5 + 7 \equiv 1 + 7 \equiv 8 \equiv 0\ [8]$, ce qui prouve que $17^5 + 7$ est divisible par 8.

68 Démontrer que $12^3 + 10$ est divisible par 11.

Exemple

Montrons que $2^{111} + 1$ est divisible par 3.
Comme $2 \equiv -1\ [3]$, on a $2^{111} \equiv (-1)^{111} \equiv -1\ [3]$. On déduit

$$2^{111} + 1 \equiv -1 + 1 \equiv 0\ [3],$$

ce qui montre que N est divisible par 3.

69 Démontrer que $13^8 - 8^8$ est divisible par 7.

Exemple

Soit a un nombre ayant 8 pour reste dans la division euclidienne par 17 et b ayant 11 pour reste dans cette même division. Cela se traduit par $a \equiv 8\ [7]$ et $b \equiv 11\ [7]$.
Le théorème permet d'écrire

- $a + b \equiv 8 + 11 \equiv 19 \equiv 2\ [17]$, donc $a + b$ a pour reste 2 dans la division euclidienne par 17 ;
- $ab \equiv 8 \times 11 \equiv 88 \equiv 3\ [17]$ (car $88 - 3 = 5 \times 17$), donc ab a pour reste 3 dans la division euclidienne par 17.

70 Effectuer les divisions euclidiennes de 200 et 900 par 13 et traduire ces résultats par des congruences. En déduire les restes dans la division euclidienne par 13 des entiers suivants.

a. $200 + 900$
b. 200×900
c. 200^2
d. 900^3

71 Pour $n \in \mathbb{N}$, on pose $u_n = 2^{3n+1} + 5^{6n+1}$.

1. Calculer u_0, u_1 et u_2 et montrer qu'ils sont divisibles par 7.
2. Justifier que $2^3 \equiv 1\ [7]$ puis montrer que pour tout entier naturel n on a $2^{3n} \equiv 1\ [7]$ et en déduire que $2^{3n+1} \equiv 2\ [7]$
3. Montrer de même que $5^{6n+1} \equiv 5\ [7]$ pour tout $n \in \mathbb{N}$.
4. En déduire que u_n est divisible par 7 pour tout $n \in \mathbb{N}$.

72 Pour tout entier naturel n, on pose

$$u_n = n(n+1)(n+2).$$

1. Calculer u_n pour quelques valeurs de n. Par quel entier semble être divisibles toutes ces valeurs de u_n ?
2. Expliquer pourquoi tout entier est congru à 0, 1, 2, 3, 4, ou 5 modulo 6.

3. Compléter le tableau suivant par les entiers les plus petits possibles. Conclusion ?

Si $n \equiv \ldots\ [6]$,	0	1	2	3	4	5
alors $n+1 \equiv \ldots\ [6]$						
et $n+2 \equiv \ldots\ [6]$,						
donc $n(n+1)(n+2) \equiv \ldots\ [6]$						

Exemple

On veut calculer 7^{37} modulo 10. Ici on ne voit pas par quoi remplacer 7 pour simplifier les calculs, alors on calcule les premières puissances de 7 en espérant tomber sur 1 modulo 10.
On a $7^2 \equiv 49 \equiv -1\ [10]$, ce qui en élevant au carré donne $(7^2)^2 \equiv (-1)^2 \equiv 1\ [10]$, c'est-à-dire $7^{2\times 2} \equiv 7^4 \equiv 1\ [10]$. Et voilà ! Il suffit maintenant de faire apparaître 7^4 dans 7^{37}. Pour cela, on effectue la division euclidienne de 37 par 4 : $37 = 4 \times 9 + 1$, puis on se rappelle les cours de seconde sur les puissances :

$$7^{37} = 7^{4\times 9+1} = 7^{4\times 9} \times 7^1 = (7^4)^9 \times 7.$$

En passant aux congruences :

$$7^{38} \equiv (-1)^9 \times 7 \equiv -1 \times 7 \equiv -7 \equiv 3\ [10].$$

73 On souhaite connaître le reste de la division euclidienne de 2018^{2018} par 7.
a. Compléter avec le plus petit entier naturel la congruence $2018^3 \equiv \ldots\ [7]$.
b. Montrer que $2018^{2018} = (2018^3)^{672} \times 2018^2$.
c. En déduire la réponse au problème posé.

74 Compléter les congruences suivantes avec le plus petit entier possible.
a. $2^{2022} \equiv \ldots\ [11]$
b. $5^{2022} \equiv \ldots\ [11]$
c. $5^{2022} \equiv \ldots\ [10]$

75 Démontrer que la seule suite de 3 nombres premiers « consécutifs » est 3 ; 5 ; 7.
De façon plus précise, cela revient à montrer que pour $n > 3$, les entiers n, $n+2$ et $n+4$ ne peuvent pas être tous être premiers.

10. Problèmes

76 *(D'après Chronomaths).* À l'issue de la seconde guerre mondiale, lors de la création de la Sécurité Sociale et afin de vous identifier, l'État a mis en place depuis 1946, un code numérique à 11 chiffres strictement personnel qui vous caractérise sans ambiguïté : c'est aussi votre code INSEE (*Institut National de la Statistique et des Etudes Economiques*) ou code RNIPP (*Répertoire National d'Identification des Personnes Physiques*), en abrégé : code

NIR (*Numéro d'Inscription au Répertoire*). En fait ce code comporte 13 chiffres : les deux derniers représentent la clé de contrôle.

Sur l'exemple fictif ci-dessus, on peut lire que le code de Nathalie Durand est 2 69 05 49 588 157 80. On doit alors comprendre que Nathalie est de sexe féminin (2), qu'elle est née en 1969 (69) du mois de mai de cette année là (05), dans la commune codée 49588 par l'INSEE (code généralement distinct du code postal, lequel peut regrouper plusieurs communes sous un même code) et que dans l'ordre du registre des naissances du mois de mai 1969 de cette localité, elle est notée en 157^{e} position.
Lors de la saisie de votre code, vous ou l'administration peut faire une erreur. Raison pour laquelle il a été prévu une clé de contrôle (80 pour l'exemple donné). Si NIR désigne les 13 premiers chiffres, la clé est calculée par :

$$C = 97 - r$$

où r est le reste de la division euclidienne de NIR par 97.

1. Montrer que la clé de l'exemple est bien 80.
2. Justifier que $1 \leq C \leq 97$.
3. On désigne par
- S le numéro du sexe ;
- A le numéro de l'année ;
- M le numéro du mois ;
- D le numéro du département ;
- C le numéro de la commune ;
- R le numéro de registre.

Exprimer NIR en fonction de S, A, M, D, C et R.
4. Justifier que NIR $\equiv 50S + 49A + 81M + 27D + 30C + R$ [97] et en déduire une façon de calculer la clé qui nécessite des nombres moins gros que par la définition.

77 *(2018, Métropole)*. Les publications en série, comme les journaux et les périodiques, sont toutes identifiées par un numéro ISSN (Intemational Standard Serial Number). En France, ce numéro est attribué par le Centre national d'enregistrement des publications en série.
L'ISSN comporte huit caractères répartis en deux groupes de quatre, ces groupes étant séparés par un tiret. Le tableau ci-après donne les numéros ISSN de quelques journaux ou périodiques français.

Journal ou périodique	Numéro ISSN
Le Monde	1950–6244
Le Figaro	1241–1248
Le Nouvel Observateur	0029–4713
Les Échos	0153–4831
Libération	0335–1793
Le Canard Enchaîné	0008–5405
Courrier International	1154–516X

Les sept premiers caractères d'un numéro ISSN sont des chiffres qui caractérisent la publication.
Le dernier caractère, situé en huitième position, sert de clé de contrôle et est pris dans l'ensemble

$$E = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; X\}$$

où les chiffres de 0 à 9 représentent le nombre correspondant et le caractère *X* représente le nombre 10.
Pour déterminer la clé de contrôle d'un numéro ISSN dont les sept premiers chiffres correspondent aux nombres a, b, c, d, e, f, g :

- on calcule le nombre
$$N = 8a + 7b + 6c + 5d + 4e + 3f + 2g ;$$
- on détermine le reste r de $-N$ dans la division euclidienne par 11 ;
- la clé de contrôle est le caractère de l'ensemble E correspondant au nombre r.

Par exemple, pour *Le Monde*, on a
$$N = 8 \times 1 + 7 \times 9 + 6 \times 5 + 5 \times 0 + 4 \times 6 + 3 \times 2 + 2 \times 4 = 139.$$
D'où $-N \equiv -139 \equiv 4 \bmod 11$. La clé de contrôle est donc bien égale à 4.

1. En détaillant les étapes, retrouver la clé de contrôle du périodique *Courrier International*.

2. Écrire une fonction `calculN(n)` qui calcule N à partir de la donnée des 7 premiers chiffres n. Par exemple exécuté avec 1950624 (pour *Le Monde*), la fonction renverra 4.

```
>>> calculN(1950624)
4
```

3. Écrire une fonction `cle(n)` qui calcule la clé à partir de la donnée des 7 premiers chiffres n. Par exemple pour *Courrier International*,

```
>>> cle(1154516)
'X'
```

4. Le deuxième caractère du numéro ISSN d'un journal est illisible. Si l'on note n ce caractère, le numéro ISSN est $3n08 - 2138$.
a. Montrer que $81 + 7n \equiv 3 \bmod 11$.
b. En déduire la valeur de n.

78 *(2013, Métropole)*. Le but de cet exercice est l'étude d'un procédé de cryptage des lettres majuscules de l'alphabet français. Chacune des 26 lettres est associée à l'un des entiers de 0 à 25, selon le tableau de correspondance suivant.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	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 cryptage se fait à l'aide d'une clé, qui est un nombre entier k fixé, compris entre 0 et 25.
Pour crypter une lettre donnée :

- on repère le nombre x associé à la lettre, dans le tableau de correspondance précédent ;
- on multiplie ce nombre x par la clé k ;
- on détermine le reste r de la division euclidienne de $k \times x$ par 26 ;
- on repère la lettre associée au nombre r dans le tableau de correspondance ; c'est la lettre cryptée.

Par exemple, pour crypter la lettre « P » avec la clé $k = 11$:

- le nombre x associé à la lettre « P » est le nombre 15 ;
- on multiplie 15 par la clé k, ce qui donne
$$11 \times 15 = 165 ;$$
- on détermine le reste de 165 dans la division par 26 : on trouve 9 ;
- on repère enfin la lettre associée à 9 dans le tableau : c'est « J ».

Ainsi, avec la clé $k = 11$, la lettre « P » est cryptée en la lettre « J ».

On crypte un mot en cryptant chacune des lettres de ce mot.

Partie A – Cryptage d'un mot avec la clé $k = 11$

Dans cette partie, la clé de cryptage est $k = 11$. Le but de cette partie est de crypter le mot « BTS ».

1. Déterminer en quelle lettre est cryptée la lettre « S ». On détaillera les différentes étapes du processus de cryptage.

2. Crypter le mot « BTS ». On ne demande pas le détail du cryptage.

Partie B – Décryptage avec la clé $k = 11$

Dans cette partie, la clé de cryptage est toujours $k = 11$.

Le but de cette partie est de retrouver une lettre initiale connaissant la lettre cryptée.

1. Prouver que $19 \times 11 \equiv 1$ modulo 26.

2. Une lettre associée à un nombre x a été cryptée. Le nombre associé à la lettre cryptée est noté y.

a. Justifier que $11 \times x \equiv y$ modulo 26.

b. Montrer que $19 \times y \equiv x$ modulo 26.

Ces propriétés montrent que pour décrypter une lettre codée y avec la clé $k = 11$, il suffit de crypter cette lettre avec la clé de cryptage $k' = 19$.

Exemple : si une lettre est codée par $y = 22$, on multiplie 22 par 19 et on prend le reste du résultat dans la division euclidienne par 26 ; on obtient $x = 2$. Donc la lettre de départ est C.

3. Utiliser les résultats précédents pour décrypter le mot « WGA ».

Partie C – Recherche des bonnes clés de cryptage

Une clé k ne possède pas forcément une clé de décryptage associée.

On dit qu'une clé est une bonne clé de cryptage si elle possède une clé de décryptage associée.

On admet qu'une clé k est une bonne clé de cryptage si et seulement si les nombres k et 26 sont premiers entre eux.

Le but de cette partie est de trouver les bonnes clés de cryptage, parmi les nombres entiers compris entre 0 et 25.

1. Décomposer 26 en un produit de facteurs premiers.

2. En déduire la liste des nombres k compris entre 0 et 25 qui sont de bonnes clés de cryptage.

79 *(2014, Polynésie).* Alice souhaite que Bob lui envoie des données confidentielles par Internet. Pour éviter que ces données puissent être exploitées par une tierce personne, ils ont recours à un cryptage de type RSA.

Partie A – Création des clés publique et privée par Alice

1. Il faut tout d'abord choisir deux nombres premiers distincts notés p et q, puis calculer leur produit noté n. Alice décide de prendre $p = 5$ et $q = 23$, ce qui donne $n = 115$.
Expliquer pourquoi 23 est un nombre premier.

2. Il faut ensuite calculer $K = (p - 1)(q - 1)$, ce qui donne ici $K = 4 \times 22 = 88$, puis trouver un entier naturel c, compris entre 2 et K, qui soit premier avec K. Le couple d'entiers $(n; c)$ est la clé publique. Alice décide de prendre $c = 9$.

a. Donner la décomposition en produit de facteurs premiers de 88.

b. Expliquer pourquoi 9 et 88 sont deux nombres premiers entre eux.

3. Il faut enfin trouver un entier d tel que

$$d \times c \equiv 1 \bmod K.$$

Le couple d'entiers $(n; d)$ est la clé privée. Alice a trouvé $d = 49$.

Expliquer pourquoi $49 \times 9 \equiv 1 \bmod 88$.

Partie B – Cryptage du message à envoyer par Bob avec la clé publique d'Alice

Alice envoie sa clé publique à Bob et celui-ci s'en sert pour crypter un nombre a, qui doit être un entier naturel strictement inférieur à n. Le nombre crypté b est alors égal au reste dans la division euclidienne de a^c par n. C'est ce nombre crypté b que Bob envoie à Alice, Bob veut transmettre à Alice le nombre 12.

Déterminer le nombre crypté b que Bob envoie à Alice.

Partie C – Décryptage d'un message reçu par Alice avec sa clé privée

Alice reçoit un nouveau nombre crypté de la part de Bob : le nombre 2. Pour le décrypter, Alice utilise sa clé privée, c'est-à-dire le couple $(n; d)$.

On admet que le nombre non crypté transmis par Bob, noté a, est égal au reste dans la division euclidienne de 2^{49} par n.

Alice doit donc calculer le reste dans la division euclidienne de 2^{49} par 115 pour trouver a.

Mais sa calculatrice ne permet pas de calculer la valeur exacte de 2^{49}. Cependant,

elle a pu obtenir les résultats suivants :

$$2^{33} = 8589934592 \text{ et } 8589934592 \equiv 47 \bmod 115,$$
$$2^{16} = 65536 \text{ et } 65536 \equiv 101 \bmod 115.$$

À partir de ces résultats, calculer le nombre a transmis par Bob à Alice.