Arithmétique - Chapitre 7

I. Nombres premiers

I.1. Définition et propriétés

Définition (Nombre premier)
Soit $p \in \mathbb{N}$.
On dit que p est un nombre premier si :

- $p \geqslant 2$,
- $\forall q \in \mathbb{N}^*, \quad (q \mid p \quad \Leftrightarrow \quad q = 1 \ \texttt{OU} \ q = p)$
  (les seuls diviseurs **positifs** *de p sont 1 et p)*

Un nombre qui n'est pas premier est dit composé.

Commentaire

Le nombre 2 est le seul nombre premier pair.

Proposition 1.

1) *Soit $a \in \mathbb{N}^*$. Soit p un nombre premier. Alors :*
- × *soit : $p \mid a$*
- × *soit : $a \wedge p = 1$*

2) *Deux entiers premiers distincts sont premiers entre eux.*

3) *Soit $a \in \mathbb{N}^*$. Soient p et q deux nombres premiers distincts.*

$$\left.\begin{array}{l} p \mid a \\ q \mid a \end{array}\right\} \quad \Rightarrow \quad pq \mid a$$

4) *Soit $a \in \mathbb{N}^*$. Soient $p_1, \ldots, p_r$ r nombres premiers distincts.*

$$\forall i \in [\![1, r]\!], \ p_i \mid a \qquad \Rightarrow \qquad \prod_{i=1}^{r} p_i \mid a$$

Démonstration.

1) Soit $a \in \mathbb{N}^*$. Soit p un nombre premier.
Comme p est premier : $Div(p) = \{1, p\}$. Or : $Div(a, p) \subset Div(p)$. On en déduit :
- × soit $Div(a, p) = \{1, p\}$, et donc : $p \mid a$.
- × soit $Div(a, p) = \{1\}$ et donc : $p \wedge a = 1$.

2) Évident avec le point précédent.

3) Soit $a \in \mathbb{N}^*$. Soient p et q deux nombres premiers distincts.
Supposons : $p \mid a$ et $q \mid a$.
Comme p et q sont premiers et distincts, d'après ***2)*** : $p \wedge q = 1$. Ainsi :

$$p \mid a, \qquad q \mid a \qquad \text{et} \qquad p \wedge q = 1$$

Par corollaire du théorème de Gauss : $pq \mid a$.

4) Soit $a \in \mathbb{N}^*$. Démontrons par récurrence : $\forall r \in \mathbb{N}^*$, $\mathcal{P}(r)$
où $\mathcal{P}(r)$: pour tout $(p_1, \ldots, p_r) \in [\![2, +\infty[\![^r$ premiers distincts :

$$\forall i \in [\![1, r]\!],\ p_i \mid a \qquad \Rightarrow \qquad \prod_{i=1}^{r} p_i \mid a$$

- **Initialisation**
  Soit $p_1 \in [\![2, +\infty[\![$ premier. Supposons : $p_1 \mid a$.
  Alors : $\prod_{i=1}^{1} p_i = p_1$. Donc : $p_1 \mid a$.
  D'où $\mathcal{P}(1)$.
- **Hérédité** : soit $r \in \mathbb{N}^*$.
  Supposons $\mathcal{P}(r)$ et démontrons $\mathcal{P}(r+1)$ (*i.e.* pour tout $(p_1, \ldots, p_{r+1}) \in [\![2, +\infty[\![^{r+1}$ premiers distincts : $\forall i \in [\![1, r+1]\!],\ p_i \mid a \quad \Rightarrow \quad \prod_{i=1}^{r+1} p_i \mid a$)
  Soit $(p_1, \ldots, p_{r+1}) \in [\![2, +\infty[\![^{r+1}$ premiers distincts. Supposons : $\forall i \in [\![1, r+1]\!]$, $p_i \mid a$.
  × Par hypothèse de récurrence : $\prod_{i=1}^{r} p_i \mid a$.
  × Ainsi :

$$\prod_{i=1}^{r} p_i \mid a, \quad p_{r+1} \mid a \quad \text{et} \quad \left(\prod_{i=1}^{r} p_i\right) \wedge p_{r+1} = 1$$

  Par corollaire du théorème de Gauss : $\prod_{i=1}^{r+1} p_i \mid a$.
  D'où : $\mathcal{P}(r+1)$.

□

Proposition 2.
Soit $a \in \mathbb{N}^*$. Soit p un nombre premier.

1) $p \mid a^2 \quad \Rightarrow \quad p \mid a$

2) Pour tout $n \in \mathbb{N}^*$:

$$p \mid a^n \quad \Rightarrow \quad p \mid a$$

Démonstration.

1) Supposons : $p \mid a^2$.
Raisonnons par l'absurde. Supposons : $p \nmid a$.
Comme p est premier, on en déduit : $p \wedge a = 1$. On obtient donc :

$$p \mid a \times a \qquad \text{et} \qquad p \wedge a = 1$$

Par théorème de Gauss : $p \mid a$.
Absurde !

2) Démontrons par récurrence : $\forall n \in \mathbb{N}^*$, $\mathcal{P}(n)$ où $\mathcal{P}(n) : p \mid a^n \ \Rightarrow\ p \mid a$.

- **Initialisation**
  Supposons : $p \mid a^1$. Alors : $p \mid a$.
  D'où $\mathcal{P}(1)$.

- **Hérédité** : soit $n \in \mathbb{N}^*$.
  Supposons $\mathcal{P}(n)$ et démontrons $\mathcal{P}(n+1)$ (*i.e.* $p \mid a^{n+1} \;\Rightarrow\; p \mid a$)
  Supposons : $p \mid a^{n+1}$.
  Raisonnons par l'absurde.
  Supposons : $p \nmid a$. Comme p est premier, alors : $p \wedge a = 1$. Ainsi :

$$p \mid a^n \times a \qquad \text{et} \qquad p \wedge a = 1$$

  Par théorème de Gauss : $p \mid a^n$.
  Par hypothèse de récurrence ; on obtient : $p \mid a$.
  Absurde !
  On en déduit : $p \mid a$.
  D'où $\mathcal{P}(n+1)$.

□

Proposition 3.
Tout entier naturel au moins égal à 2 admet au moins un diviseur premier.

Démonstration.
Démontrons par récurrence (forte) : $\forall n \in [\![2, +\infty[\![, \mathcal{P}(n)$ où $\mathcal{P}(n)$: n admet au moins un diviseur premier.

- **Initialisation**
  Le nombre 2 admet 2 comme diviseur premier.
  D'où $\mathcal{P}(2)$.
- **Hérédité** : soit $n \in [\![2, +\infty[\![$.
  Supposons : $\forall d \in [\![2, n]\!]$, $\mathcal{P}(d)$. Démontrons $\mathcal{P}(n+1)$ (*i.e.* $n+1$ admet au moins un diviseur premier).
  Deux cas se présentent :
  - × si $n+1$ est premier, alors il admet un diviseur premier : lui-même.
  - × si $n+1$ n'est pas premier, alors il admet des diviseurs autres que 1 et $n+1$.
    Notons d l'un de ces diviseurs. Alors il existe $k \in \mathbb{N}$ tel que : $n+1 = k\,d$. De plus :

$$\begin{array}{rccccl} & 1 & < & d & < & n+1 \\ \text{donc} & 2 & \leqslant & d & \leqslant & n \qquad (\textit{car } d \in \mathbb{N}) \end{array}$$

    Par hypothèse de récurrence, d admet un diviseur premier. Notons le δ. Alors il existe $k' \in \mathbb{N}$ tel que : $d = k'\,\delta$. D'où :

$$n+1 \;=\; k\,d \;=\; k\,k'\,\delta$$

    Ainsi : $\delta \mid n+1$. Comme δ est premier, on en déduit que $n+1$ admet bien un diviseur premier.
    D'où $\mathcal{P}(n+1)$.

□

Commentaire

On peut utiliser cette propriété pour démontrer que deux entiers a et b sont premiers entre eux en raisonnant par l'absurde.

1) On suppose : $a \wedge b \neq 1$.
Alors il existe $p \in [\![2, +\infty[\![$ premier tel que : $p \mid a \wedge b$.

2) On démontre : $p \mid 1$. Absurde !

Exercice 1
Soit $(a, b) \in \mathbb{Z}^2$ tel que :

$$a \wedge b = 1, \qquad a \text{ impair} \qquad \text{et} \qquad b \text{ impair}$$

Démontrer : $(a^2 + b^2) \wedge ab = 1$.

Démonstration.
Raisonnons par l'absurde.
Supposons : $d = (a^2 + b^2) \wedge ab \neq 1$.
Alors il existe $p \in [\![2, +\infty[\![$ premier tel que : $p \mid d$.

- Alors, par définition du PGCD :

  $$p \mid (a^2 + b^2) \qquad \text{et} \qquad p \mid ab$$

  On en déduit :

  $$\begin{array}{ccccc} p & \mid & (a^2 + b^2 + 2\,ab) & \text{et} & p \mid (a^2 + b^2 - 2\,ab) \\ & & \| & & \| \\ & & (a+b)^2 & & (a-b)^2 \end{array}$$

  Comme p est premier, on en conclut :

  $$p \mid (a + b) \qquad \text{et} \qquad p \mid (a - b)$$

  Ainsi : $p \mid 2a$ et $p \mid 2b$.
- Par ailleurs, comme a est impair et b est impair, on en déduit que ab est impair.
  Or : $p \mid ab$. D'où : $p \neq 2$. Ainsi :
  - $\times$ $p \mid 2a$ et $p \wedge 2 = 1$ (2 est le seul nombre premier pair). Par théorème de Gauss : $p \mid a$.
  - $\times$ $p \mid 2b$ et $p \wedge 2 = 1$. Par théorème de Gauss : $p \mid b$.

  On en déduit : $p \mid a \wedge b$. C'est-à-dire : $p \mid 1$.

Absurde ! (car $p \geqslant 3$)
On en conclut : $(a^2 + b^2) \wedge ab = 1$. □

Proposition 4.
L'ensemble des nombres premiers est infini.

Démonstration.
Raisonnons par l'absurde.
Supposons que l'ensemble $\mathcal{P}$ des nombres premiers est fini.
Alors il existe $N \in \mathbb{N}^*$ et $(p_1, \ldots, p_N) \in \mathbb{N}^N$ tel que : $\mathcal{P} = \{p_1, \ldots, p_N\}$.

- On considère l'entier :

  $$n \;=\; p_1\, p_2 \cdots p_N + 1$$

  Comme $n \in [\![2, +\infty[\![$, d'après la proposition précédente, cet entier n admet au moins un diviseur premier.
  Or l'ensemble des nombres premiers est $\mathcal{P} = \{p_1, \ldots, p_N\}$. Il existe donc $k \in [\![1, N]\!]$ tel que : $p_k \mid n$.
- On obtient alors :

  $$p_k \mid n \qquad \text{et} \qquad p_k \mid p_1\, p_2 \cdots p_N$$

  On en déduit :

  $$\begin{array}{ccc} p_k & \mid & (n - p_1\, p_2 \cdots p_N) \\ & & \| \\ & & 1 \end{array}$$

  Absurde ! (car $p_k \geqslant 2$)

□

I.2. Comment savoir si un nombre est premier ?

I.2.a) Condition suffisante de primalité

Proposition 5.
Soit $n \in [\![2, +\infty[\![$.
Si n n'est pas premier, alors il admet au moins un diviseur d tel que : $2 \leqslant d^2 \leqslant n$.

Démonstration.
Soit $n \in [\![2, +\infty[\![$.
Supposons que n n'est pas premier.
Alors il admet un diviseur autre que 1 et n. Il existe donc $(d_1, d_2) \in \mathbb{N}^2$ tel que :

$$n = d_1 \times d_2 \qquad \text{et} \qquad 2 \leqslant d_1 \leqslant d_2$$

Comme $d_1 > 0$, on obtient :

$$\begin{array}{ccccc} 2\,d_1 & \leqslant & d_1^2 & \leqslant & d_1\,d_2 \\ & & & & \shortparallel \\ & & & & n \end{array}$$

De plus, comme $d_1 > 1$, alors : $d_1^2 \geqslant 2\,d_1 \geqslant 2$. Ainsi, on a bien :

$$2 \leqslant d_1^2 \leqslant n$$

□

Commentaire

- Soit $n \in [\![2, +\infty[\![$. Le théorème précédent implique en particulier que si n n'est pas premier, alors il admet au moins un diviseur **premier** p tel que : $p^2 \leqslant n$, *i.e.* $p \leqslant \sqrt{n}$.
- En pratique, c'est plutôt la contraposée de cette implication qui est utilisée : « si l'entier n n'admet aucun diviseur premier p tel que $p \leqslant \sqrt{n}$, alors n est premier ».

Exercice 2
Le nombre 163 est-il premier ?

Démonstration.
On teste la divisibilité de 163 par tous les nombres premiers p tels que : $p^2 \leqslant 163$.

- Comme $2^2 = 4 \leqslant 163$, on teste la divisibilité par 2.
  On a : $163 = 81 \times 2 + 1$ et $0 < 1 < 2$. L'entier 163 n'est donc pas divisible par 2.
- Comme $3^2 = 9 \leqslant 163$, on teste la divisibilité par 3.
  On a : $163 = 54 \times 3 + 1$ et $0 < 1 < 3$. L'entier 163 n'est donc pas divisible par 3.
- Comme $5^2 = 25 \leqslant 163$, on teste la divisibilité par 5.
  On a : $163 = 32 \times 5 + 3$ et $0 < 3 < 5$. L'entier 163 n'est donc pas divisible par 5.
- Comme $7^2 = 49 \leqslant 163$, on teste la divisibilité par 7.
  On a : $163 = 23 \times 7 + 2$ et $0 < 2 < 7$. L'entier 163 n'est donc pas divisible par 7.
- Comme $11^2 = 121 \leqslant 163$, on teste la divisibilité par 11.
  On a : $163 = 14 \times 11 + 9$ et $0 < 9 < 11$. L'entier 163 n'est donc pas divisible par 11.
- Comme $13^2 = 169 > 163$, on ne teste pas la divisibilité par 13.

Le nombre 163 est donc un nombre premier. □

I.2.b) Crible d'Ératostène

L'algorithme suivant, dû à Ératostène de Cyrène (176-194 av. J.-C.), permet de déterminer les nombres premiers inférieurs à un nombre donné n.

1) On commence par représenter dans un tableau les entiers naturels successifs compris entre 2 et n.

2) Le nombre 2 est premier. On barre alors tous les multiples de 2 autre que 2.

3) Le nombre non barré suivant est 3, qui est donc premier. On barre alors tous les multiples de 3 autres que 3.

4) On itère le procédé jusqu'à ce qu'il ne reste plus de nombres composés.

Exercice 3
À l'aide du crible d'Ératostène, déterminer le nombre de nombres premiers inférieurs ou égaux à 127.

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

Notons que, comme :

$$11^2 \leqslant 127 \qquad \text{et} \qquad 12^2 \leqslant 144$$

après avoir rayé les multiples de 11, on est sûr d'avoir barré tous les nombres composés inférieurs à 127.

Codons maintenant en **Python**, à l'aide du crible d'Eratostène, une fonction permettant d'obtenir l'ensemble des nombres premiers inférieurs ou égaux à un entier `n` (où $n \in [\![2, +\infty[\![$).

```
1  def Eratostene(n) :
2      L = list(range(2, n+1))
3      i = 0
4      d = L[i]
5      p = len(L)
6      while d**2 <= n :
7          for k in L[i+1:p] :
8              if k % d == 0 :
9                  L.remove(k)
10         i = i + 1
11         d = L[i]
12         p = len(L)
13     return L
```

Détaillons les éléments de ce script.

- **Début de la fonction**
  On commence par préciser la structure de la fonction :
  - × cette fonction se nomme `Eratostene`,
  - × elle prend en entrée le paramètre `n`,
  - × elle admet pour variable de sortie la variable `L`.

```
1  def Eratostene(n) :
```

```
13     return L
```

  On initialise ensuite différentes variables :
  - × la liste `L` qui contient tous les entiers de 2 à `n`. À l'issue de ce script, on souhaite que cette liste contienne seulement les nombres premiers inférieurs à `n`.

```
2      L = list(range(2, n+1))
```

  - × l'entier `i` qui prend la valeur 0. Cette variable désigne la coordonnée, dans la liste `L`, du nombre premier dont on souhaite supprimer les multiples.

```
3  i = 0
```

  - × l'entier `d` qui prend la valeur 2. Cette variable désigne le nombre premier dont on souhaite supprimer les multiples.

```
4  d = L[i]
```

  - × l'entier `p` qui est la longueur de la liste `L`.

```
5      p = len(L)
```

- **Structure itérative**
  Les lignes 6 à 12 consistent à supprimer les nombres composés de la liste `L` afin de n'en conserver que les nombres premiers. On considère donc chaque nombre `d` de la liste `L` pour en supprimer les multiples. D'après la condition suffisante de primalité d'un nombre entier, il suffit de considérer les entiers `d` tels que $d^2 \leqslant n$.

```
6        while d**2 <= n :
```

  À chaque tour de boucle, on doit donc supprimer tous les multiples de `d` de la liste `L` :

  1) supprimer de la liste `L` tous les multiples de `d`, qui sont donc strictement supérieurs à `d = L[i]`. Pour cela on met en place une nouvelle structure itérative (boucle for).

```
7            for k in L[i+1:p] :
8                if k % d == 0 :
9                    L.remove(k)
```

  2) mettre à jour `i` et `d` pour que la variable `d` contienne le nombre premier suivant dans la liste `L`.

```
10           i = i + 1
11           d = L[i]
```

  On met enfin à jour la variable `p` pour qu'elle contienne la nouvelle longueur de la liste `L`.

```
12           p = len(L)
```

II. Décomposition d'un entier en produit de facteurs premiers

II.1. Théorème

Théorème 1. (Théorème fondamental de l'arithmétique)
Tout entier naturel au moins égal à 2 se décompose, de façon unique, en un produit de facteurs premiers. En d'autres termes, pour tout $n \in [\![2, +\infty[\![$, il existe des entiers premiers p_1, ..., p_r et des entiers naturels α_1, ..., α_r non nuls tels que :

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

Cette écriture est unique à l'ordre près des facteurs.
(notons que les p_i sont deux à deux distincts)

Démonstration.

- Existence. Démontrons par récurrence (forte) : $\forall n \in [\![2, +\infty[\![$, $\mathcal{P}(n)$
  où $\mathcal{P}(n)$: n peut s'écrire comme un produit de nombres premiers.
  - **Initialisation**
    L'entier 2 s'écrit bien comme un produit de nombres premiers puisqu'il est premier.
  - **Hérédité** : soit $n \in [\![2, +\infty[\![$.
    Supposons : $\forall k \in [\![2, n-1]\!]$, $\mathcal{P}(k)$. Démontrons $\mathcal{P}(n)$ (*i.e.* $n+1$ peut s'écrire comme un produit de nombres premiers).
    L'entier n admet au moins un diviseur premier p. Deux cas se présentent alors :
    × si $p = n$, alors n est bien un produit de facteurs premiers.

× si $p \leq n$, alors, il existe $q \in \mathbb{N}^*$ tel que : $n = p \times q$ et $1 < q < n$.
Comme q est un entier, on en déduit : $2 \leqslant q \leqslant n-1$. Ainsi, par hypothèse de récurrence, q s'écrit comme produit de nombres premiers.
Donc $n = p \times q$ aussi.

D'où $\mathcal{P}(n)$.

- Unicité.
Soit $(r,s) \in \left(\mathbb{N}^*\right)^2$, soit $(p_1,\ldots,p_r,p'_1,\ldots,p'_s) \in \left([\![2,+\infty[\![\right)^{r+s}$ des entiers premiers et soit $(\alpha_1,\ldots,\alpha_r,\alpha'_1,\ldots,\alpha'_s) \in \left(\mathbb{N}^*\right)^{r+s}$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{et} \qquad n = \prod_{i=1}^{s} (p'_i)^{\alpha'_i}$$

- Alors : $p'_1 \mid n$.
Raisonnons par l'absurde. Supposons : $p'_1 \notin \{p_1,\ldots,p_r\}$. Alors, comme p'_1 est premier :

$$p'_1 \wedge p_1 = 1, \quad p'_1 \wedge p_2 = 1, \quad \ldots, \quad p'_1 \wedge p_r = 1$$

Toujours parce que p'_1 est premier :

$$p'_1 \wedge p_1^{\alpha_1} = 1, \quad p'_1 \wedge p_2^{\alpha_2} = 1, \quad \ldots, \quad p'_1 \wedge p_r^{\alpha_r} = 1$$

Et enfin :

$$p'_1 \wedge \left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = 1$$

Ainsi : $p'_1 \wedge n = 1$.
Absurde ! On en déduit : $p'_1 \in \{p_1,\ldots,p_r\}$.
- De même, on conclut : $\forall i \in [\![1,s]\!]$, $p'_i \in \{p_1,\ldots,p_r\}$. Ainsi :

$$\{p'_1,\ldots,p'_s\} \subset \{p_1,\ldots,p_r\}$$

- Toujours de même, en inversant le rôle des p_i et p'_i :

$$\{p_1,\ldots,p_r\} \subset \{p'_1,\ldots,p'_s\}$$

On en déduit :

$$\{p_1,\ldots,p_r\} = \{p'_1,\ldots,p'_s\}$$

Et donc :

× $r = s$

× à renumérotation près : $\forall i \in [\![1,r]\!]$, $p_i = p'_i$.

- On obtient :

$$\prod_{i=1}^{r} p_i^{\alpha_i} = n = \prod_{i=1}^{r} p_i^{\alpha'_i}$$

Raisonnons par l'absurde. Supposons : $\alpha_1 \neq \alpha'_1$. Deux cas se présentent :

× si $\alpha_1 \leq \alpha'_1$, alors :

$$\cancel{p_1^{\alpha_1}} \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = \cancel{p_1^{\alpha_1}}\, p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right)$$

D'où :

$$\left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right)$$

Or :

$$p_1 \nmid \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) \qquad \text{et} \qquad p_1 \mid p_1^{\alpha'_1-\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha'_i}\right) \qquad (car\ \alpha'_1 - \alpha_1 > 0)$$

Absurde !

× si $\alpha_1 > \alpha'_1$, alors :

$$\cancel{p_1^{\alpha_1}} \left(\prod_{i=2}^{r} p_i^{\alpha'_i} \right) = \cancel{p_1^{\alpha'_1}}\, p_1^{\alpha_1 - \alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i} \right)$$

D'où :

$$\left(\prod_{i=2}^{r} p_i^{\alpha'_i} \right) = p_1^{\alpha_1 - \alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i} \right)$$

Or :

$$p_1 \nmid \left(\prod_{i=2}^{r} p_i^{\alpha'_i} \right) \qquad \text{et} \qquad p_1 \mid p_1^{\alpha_1 - \alpha'_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i} \right) \qquad (\textit{car } \alpha_1 - \alpha'_1 > 0)$$

Absurde !

On en déduit : $\alpha_1 = \alpha'_1$.

- De même : $\forall i \in [\![2, r]\!]$, $\alpha_i = \alpha'_i$.

On a donc bien obtenu l'unicité à l'ordre des facteurs près.

□

II.2. Application au calcul de PGCD et PPCM

Proposition 6.
Soit $n \in [\![2, +\infty[\![$. Si la décomposition en facteurs premiers de n est :

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

(les p_i sont des entiers premiers distincts et $\alpha_i \in \mathbb{N}^*$)
alors un entier naturel m divise n si et seulement si la décomposition en facteurs premiers de m est :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} \qquad \textit{avec } 0 \leqslant \beta_i \leqslant \alpha_i$$

Démonstration.
On raisonne par double implication.

(⇐) Supposons que la décomposition en facteurs premiers d'un entier m est :

$$m = p_1^{\beta_1} \cdots p_r^{\beta_r} \qquad \text{avec } 0 \leqslant \beta_i \leqslant \alpha_i$$

Alors :

$$n = \left(\prod_{i=1}^{r} p_i^{\alpha_i - \beta_i} \right) \times m$$

Comme $\prod_{i=1}^{r} p_i^{\alpha_i - \beta_i} \in \mathbb{N}$ (car : $\forall i \in [\![1, r]\!]$, $\alpha_i \geqslant \beta_i$), on en déduit que m divise n.

(⇒) Supposons qu'un entier m divise n.
Alors tout nombre premier p intervenant dans la décomposition de m doit diviser n, donc doit appartenir à $\{p_1, \ldots, p_r\}$. Ainsi :

$$m = \prod_{i=1}^{r} p_i^{\beta_i}$$

Il reste à démontrer : $\forall i \in [\![1, r]\!]$, $\alpha_i \geqslant \beta_i$.

× Démontrons par l'absurde : $\alpha_1 \geqslant \beta_1$.
Supposons : $\alpha_1 > \beta_1$. Comme : $m \mid n$, alors :

$$p_1^{\beta_1} \left(\prod_{i=2}^{r} p_i^{\beta_i} \right) \mid p_1^{\alpha_1} \left(\prod_{i=2}^{r} p_i^{\alpha_i} \right)$$

D'où :

$$p_1^{\beta_1-\alpha_1}\left(\prod_{i=2}^{r} p_i^{\beta_i}\right) \mid \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right)$$

Or, comme $\alpha_1 < \beta_1$:

$$p_1 \mid p_1^{\beta_1-\alpha_1}\left(\prod_{i=2}^{r} p_i^{\beta_i}\right) \qquad \text{mais} \qquad p_1 \wedge \left(\prod_{i=2}^{r} p_i^{\alpha_i}\right) = 1$$

Absurde !

× De même : $\forall i \in [\![2, r]\!]$, $\alpha_i \geqslant \beta_i$.

□

Exercice 4
Déterminer l'ensemble des diviseurs positifs de 224.

Démonstration.

- La décomposition en facteur premier de 224 est :

$$224 \;=\; 2^5 \times 7$$

- Les diviseurs positifs de 224 sont donc les entiers naturels d qui peuvent s'écrire sous la forme : $d = 2^\alpha \times 7^\beta$, avec $\alpha \in [\![0, 5]\!]$ et $\beta \in \{0, 1\}$. On en déduit :

$$Div(224) \;=\; \{1, 2, 4, 8, 16, 32, 7, 14, 28, 56, 112, 224\}$$

□

Proposition 7.
Soient a et b deux entiers dont on connaît les décompositions en facteurs premiers. On peut écrire en rassemblant tous ces facteurs :

$$a \;=\; \prod_{i=1}^{r} p_i^{\alpha_i} \qquad et \qquad b \;=\; \prod_{i=1}^{r} p_i^{\beta_i} \qquad (\forall i \in [\![1, r]\!],\ (\alpha_i, \beta_i) \in \mathbb{N}^2)$$

Alors :

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

$$a \vee b \;=\; \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)}$$

III. Petit théorème de Fermat

Théorème 2. (Petit théorème de Fermat)

1) *Soient p un nombre* **premier** *et $a \in \mathbb{Z}$. Supposons de plus : $a \wedge p = 1$. Alors :*

$$a^{p-1} \equiv 1 \ [p]$$

2) *Soient p un nombre* **premier** *et $a \in \mathbb{Z}$.*

$$a^p \equiv a \ [p]$$

Démonstration.

1) Soient p un nombre premier et $a \in \mathbb{Z}$. Supposons : $a \wedge p = 1$.
On définit la fonction f suivante :

$$\begin{array}{rccc} f : & [\![1, p-1]\!] & \to & [\![1, p-1]\!] \\ & r & \mapsto & \begin{array}{c}\text{reste de la division} \\ \text{euclidienne de } a\,r \text{ par } p\end{array} \end{array}$$

Démontrons que f est bijective.

- Démontrons que f est injective. Rappelons la définition de « f est injective » :

$$\forall (r_1, r_2) \in [\![1, p-1]\!]^2, \qquad \big(f(r_1) = f(r_2)\big) \ \Rightarrow \ (r_1 = r_2)$$

Soit $(r_1, r_2) \in [\![1, p-1]\!]^2$. Démontrons la contraposée de l'implication ci-dessus, c'est-à-dire :

$$(r_1 \neq r_2) \quad \Rightarrow \quad \big(f(r_1) \neq f(r_2)\big)$$

Supposons : $r_1 \neq r_2$.

× Comme $(r_1, r_2) \in [\![1, p-1]\!]^2$, alors : $|r_2 - r_1| < p$. On en déduit : $p \nmid (r_2 - r_1)$.
D'où, comme p est premier : $p \wedge (r_2 - r_1) = 1$.

× De plus : $p \wedge a = 1$. D'où : $p \wedge \big(a\,(r_2 - r_1)\big) = 1$. En particulier :

$$\begin{array}{rrcll} & a\,(r_2 - r_1) & \not\equiv & 0 & [p] \\ \text{donc} & a\,r_2 & \not\equiv & a\,r_1 & [p] \\ \text{d'où} & f(r_2) & \neq & f(r_1) & \textit{(par définition de } f\textit{)} \end{array}$$

On en déduit que f est injective.

- Démontrons que f est surjective. Rappelons la définition de « f est surjective » :

$$\forall s \in [\![1, p-1]\!], \ \exists r \in [\![1, p-1[\![, \ s = f(r)$$

(autrement dit, tout élément $s \in [\![1, p-1]\!]$ admet un antédent $r \in [\![1, p-1]\!]$ par f)
Soit $s \in [\![1, p-1]\!]$. Raisonnons par l'absurde.
Supposons que s n'admet pas d'antécédent par f, c'est-à-dire :

$$\forall r \in [\![1, p-1]\!], \quad s \neq f(r)$$

On en déduit : $\forall r \in [\![1, p-1]\!], \ f(r) \in [\![1, p-1]\!] \setminus \{s\}$.
Or : $\text{Card}\big([\![1, p-1]\!] \setminus \{s\}\big) = \text{Card}\big([\![1, p-1]\!]\big) - 1$. Ainsi, il existe $(r_1, r_2) \in [\![1, p-1]\!]^2$ tel que :

$$r_1 \neq r_2 \qquad \text{et} \qquad f(r_1) = f(r_2)$$

Absurde ! (car f est injective)
On en déduit que f est surjective.

- Par définition de f, pour tout $r \in [\![1, p-1]\!]$:

$$a\,r \;\equiv\; f(r)\;[p]$$

Par compatibilité des congruences avec le produit :

$$\begin{array}{ccc} \prod_{r=1}^{p-1}(a\,r) & \equiv & \prod_{r=1}^{p-1} f(r) \quad [p] \\ \| & & \\ a^{p-1}\prod_{r=1}^{p-1} r & & \end{array}$$

De plus, par bijectivité de f :

$$\prod_{r=1}^{p-1} f(r) \;=\; \prod_{r=1}^{p-1} r \;=\; (p-1)!$$

Ainsi :

$$a^{p-1}\,(p-1)! \;\equiv\; (p-1)!\;[p]$$

- On en déduit : $p \mid \big((p-1)!\,(a^{p-1}-1)\big)$. Or, comme p est premier : $\forall r \in [\![1, p-1]\!]$, $p \wedge r = 1$. Toujours comme p est premier, on obtient :
  - $\times$ $p \wedge \big((p-1)!\big) = 1$
  - $\times$ $p \mid \big((p-1)!\,(a^{p-1}-1)\big)$

  Par théorème de Gauss, on en déduit : $p \mid (a^{p-1}-1)$. D'où :

$$a^{p-1} \;\equiv\; 1\;[p]$$

2) Soit p un nombre premier. Soit $a \in \mathbb{Z}$. Deux cas se présentent :

- $\times$ si $a \wedge p = 1$, alors d'après ***1)*** : $a^{p-1} \equiv 1\;[p]$. On en déduit, par compatibilité des congruences avec le produit :

$$a^p \;\equiv\; a\;[p]$$

- $\times$ si $a \wedge p \neq 1$, comme p est premier, alors : $p \mid a$. On en déduit : $p \mid a^p$. D'où : $p \mid (a^p - a)$. Ainsi :

$$a^p \;\equiv\; a\;[p]$$

□

Exercice 5
Démontrer que, pour tout $n \in \mathbb{Z}$, $n^7 - n$ est multiple de 42.

Démonstration.
Soit $n \in \mathbb{Z}$. Comme $42 = 2 \times 3 \times 7$, on souhaite démontrer que $n^7 - n$ est divisible par 2, 3 et 7, puis conclure que $n^7 - n$ est divisible par 42 avec le théorème de Gauss.

- Comme 7 est premier, d'après le petit théorème de Fermat :

$$n^7 \;\equiv n\;[7]$$

Autrement dit : $7 \mid (n^7 - n)$.

- De plus :

$$n^7 - n \;=\; n\,(n^6-1) \;=\; n\left((n^2)^3 - 1^3\right) \;=\; n\,(n^2-1)\,(n^4+n^2+1) \;=\; (n^3-n)\,(n^4+n^2+1)$$

  Comme 3 est premier, d'après le petit théorème de Fermat :

$$n^3 \;\equiv\; n\;[3]$$

  Autrement dit : $3 \mid (n^3 - n)$. Comme de plus $n^4 + n^2 + 1 \in \mathbb{N}$, on en déduit : $3 \mid (n^7 - n)$.
- On reprend la décomposition du point précédent :

$$n^7 - n \;=\; n\,(n^2-1)\,(n^4+n^2+1) \;=\; n\,(n-1)\,(n+1)\,(n^4+n^2+1) \;=\; (n^2-n)\,(n+1)\,(n^4+n^2+1)$$

  Comme 2 est premier, d'après le petit théorème de Fermat :

$$n^2 \;\equiv\; n\;[2]$$

  Autrement dit : $2 \mid (n^2 - n)$. Comme de plus $(n+1)\,(n^4+n^2+1) \in \mathbb{N}$, on en déduit : $2 \mid (n^7 - n)$.
- Finalement :

$$2 \mid (n^7 - n) \qquad 3 \mid (n^7 - n) \qquad 7 \mid (n^7 - n)$$

  Or $2 \wedge 3 = 1$ et $6 \wedge 7 = 1$. Ainsi, par théorème de Gauss : $42 \mid (n^7 - n)$.

□

IV. Chiffrement RSA

Le chiffrement RSA est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman.

IV.1. Principe

Le chiffrement RSA nécessite 2 clés (une clé est un nombre entier) :

× une *clé publique* pour chiffrer des données,

× une *clé privée* pour les déchiffrer.

On dit que le chiffrement RSA est *asymétrique*.

Mettons qu'Alice souhaite envoyer des données confidentielles à Bob.

1) Alice commence par créer les 2 clés (publique et privée). Elle procède de la manière suivante :

- ***a)*** elle choisit p et q, deux nombres premiers distincts (en pratique ces nombres sont choisis très grands, de l'ordre de 10^{300} à 10^{600} : 1024 ou 2048 bits),
- ***b)*** elle calcule leur produit $n = p\,q$, appelé *module de chiffrement*,
- ***c)*** elle calcule $m = (p-1)\,(q-1)$
- ***d)*** elle choisit $e \in \mathbb{N}$ tel que : $e \wedge m = 1$ et $e < m$. Ce nombre est appelé *exposant de chiffrement*.
- ***e)*** elle détermine $d \in \mathbb{N}$, inverse de e modulo m tel que : $d < m$. Ce nombre est appelé *exposant de déchiffrement*.

  Le couple (n, e) est la clé publique du chiffrement et d est sa clée privée (on considère parfois le triplet (p, q, d) comme clé privée).

2) Alice fournit sa clé publique (n, e) à Bob qui peut maintenant chiffrer son message. Plus précisément, si on note $M \in \mathbb{N}$ tel que $M < n$ le message de Bob, alors le message chiffré C sera l'entier $C \in \mathbb{N}$ tel que :

$$M^e \;\equiv\; C\;[n] \qquad \text{et} \qquad C < n$$

3) Une fois le message C reçu, Alice peut alors le déchiffrer avec sa clé privée d. Plus précisément, Alice obtient le message M avec l'opération suivante :

$$C^d \;\equiv\; M\;[n]$$

IV.2. Démonstration de la validité de l'algorithme

1) Démontrons l'étape ***1.e)***, c'est-à-dire qu'il existe bien $d \in \mathbb{N}$ tel que d est l'inverse de e modulo m et : $d < n$. Autrement dit, on souhaite trouver $d \in \mathbb{N}$ tel que :

$$de \equiv 1\ [m] \qquad \text{et} \qquad d < n$$

- D'après ***1.d)*** : $e \wedge m = 1$. Ainsi, par théorème de Bezout, il existe $(u_0, v_0) \in \mathbb{Z}^2$ tels que :

$$u_0\, e - v_0\, m = 1$$

- Déterminons alors l'ensemble des solutions de l'équation diophantienne $e\,x - m\,y = 1$.
(notons que cette équation admet bien des solutions car : $e \wedge m = 1$)
On procède par analyse-synthèse.

  × Analyse.
  Soit $(x, y) \in \mathbb{Z}^2$. Supposons que (x, y) est solution de l'équation $e\,x + m\,y = 1$. Alors :

$$\begin{cases} e\,x & - & m\,y & = & 1 \\ e \times u_0 & - & m \times v_0 & = & 1 \end{cases}$$

$$\begin{aligned} \text{donc} \quad & e\,(x - u_0) - m\,(y - v_0) = 0 \\ \text{d'où} \quad & e\,(x - u_0) = m\,(y - v_0) \end{aligned}$$

  Or : $m \mid m\,(y - v_0)$. Ainsi :
  - ▸ $m \mid e\,(x - u_0)$
  - ▸ $e \wedge m = 1$

  Par théorème de Gauss : $m \mid x - u_0$. On en déduit qu'il existe $k \in \mathbb{Z}$ tel que : $x - u_0 = k\,m$. Alors :

$$\begin{aligned} & e\,(u_0 + km) - m\,y = 1 \\ \text{donc} \quad & m\,ke + e\,u_0 - 1 = m\,y \\ \text{d'où} \quad & m\,ke + m\,v_0 = m\,y \qquad \textit{(par définition de } u_0 \textit{ et } v_0\textit{)} \\ \text{ainsi} \quad & \cancel{m}\,(v_0 + ke) = \cancel{m}\,y \\ \text{enfin} \quad & v_0 + ke = y \end{aligned}$$

  × Synthèse.
  Soit $k \in \mathbb{Z}$. Vérifions que le couple $(u_0 + km, v_0 + ke)$ est solution de l'équation $e\,x - m\,y = 1$.

$$e \times (u_0 + km) - m \times (v_0 + ke) = e\,u_0 - m\,v_0 + \cancel{ekm} - \cancel{ekm} = 1 \qquad \textit{(par définition de } u_0 \textit{ et } v_0\textit{)}$$

L'ensemble des solutions de l'équation $e\,x + m\,y = 1$ est donc l'ensemble :

$$\{(u_0 + km, v_0 + km) \mid k \in \mathbb{Z}\}$$

- On choisit alors $k \in \mathbb{Z}$ tel que $d = u_0 + km$ vérifie :

$$d \in \mathbb{N} \qquad \text{et} \qquad d < m$$

Ceci est bien possible. En effet :

$$\begin{array}{rrcccl} & 0 & \leqslant & d & < & m \\ \Leftrightarrow & 0 & \leqslant & u_0 + km & < & m \\ \Leftrightarrow & -u_0 & \leqslant & km & < & -u_0 + m \\ \Leftrightarrow & -\dfrac{u_0}{m} & \leqslant & k & < & -\dfrac{u_0}{m} + 1 \qquad \textit{(car } m > 0\textit{)} \end{array}$$

En choisissant : $k_0 = \left\lfloor -\dfrac{u_0}{m} \right\rfloor \in \mathbb{Z}$, le dernier encadrement est bien vérifié. Ainsi, grâce au raisonnement par équivalence, le premier encadrement aussi.

- De plus, comme le couple $(d, w) = (u_0 + k_0 m, v_0 + k_0 m)$ est solution de l'équation $e\,x + m\,y = 1$, on obtient :

$$\begin{array}{ll} & e\,d - m\,w \;=\; 1 \\ \text{donc} & e\,d \;=\; 1 + m\,w \\ \text{d'où} & e\,d \;\equiv\; 1\;[m] \qquad \textit{(car } m\,w \;\equiv\; 0\;[m]\textit{)} \end{array}$$

Finalement, on a donc bien trouvé $d \in \mathbb{N}$ tel que :

$$e\,d \;\equiv\; 1\;[m] \qquad \text{et} \qquad d < m$$

3) Démontrons qu'avec les étapes ***2)*** et ***3)***, on retrouve bien le message codé M. Autrement dit, en notant C le message codé (*i.e.* l'entier $C \in \mathbb{N}$ tel que $C < n$ et : $M^e \equiv C\;[n]$), on souhaite vérifier :

$$M \;\equiv\; C^d\;[n] \qquad \text{ou encore} \qquad M \;\equiv\; (M^e)^d\;[n] \qquad \textit{i.e.} \qquad M \;\equiv\; M^{de}\;[n]$$

- Démontrons d'abord : $M^{de} \equiv M\;[p]$. Deux cas se présentent :

× Si $p \not| M$, alors, comme p est premier : $p \wedge M = 1$. Ainsi, par le petit théorème de Fermat :

$$M^{p-1} \;\equiv\; 1\;[p]$$

- Démontrons : $M^{mw} \equiv 1\;[p]$.
Comme $M^{p-1} \equiv 1\;[p]$, alors :

$$\begin{array}{lrcll} & \left(M^{p-1}\right)^{q-1} & \equiv & 1^{q-1} & [p] \\ \text{donc} & M^m & \equiv & 1 & [p] \qquad \textit{(car } m = (p-1)(q-1)\textit{)} \\ \text{d'où} & \left(M^m\right)^w & \equiv & 1^w & [p] \\ \text{ainsi} & M^{mw} & \equiv & 1 & [p] \end{array}$$

- Démontrons : $M^{de} \equiv M\;[p]$.
D'après ce qui précède :

$$\begin{array}{lrcll} & M^{mw} & \equiv & 1 & [p] \\ \text{donc} & M^{mw} \times M & \equiv & M & [p] \\ \text{d'où} & M^{mw+1} & \equiv & M & [p] \\ \text{ainsi} & M^{de} & \equiv & M & [p] \qquad \textit{(par définition de } d \textit{ et } w\textit{)} \end{array}$$

× Si $p \mid M$, alors : $M \equiv 0\ [p]$. On en déduit : $M^{de} \equiv 0^{de}\ [p]$. D'où : $M^{de} \equiv 0\ [p]$. Et ainsi, par transitivité des congruences :

$$M^{de} \ \equiv \ M\ [p]$$

- De manière analogue, on démontre : $M^{de} \equiv M\ [q]$.
- On obtient alors :
  - ▸ $p \mid (M^{de} - M)$
  - ▸ $q \mid (M^{de} - M)$
  - ▸ $p \wedge q = 1$ (car p et q sont des nombres premiers distincts)

  Par corollaire du théorème de Gauss : $pq \mid (M^{de} - M)$. Comme $n = pq$, on obtient : $n \mid (M^{de} - M)$. Autrement dit :

$$M^{de} \ \equiv \ M\ [n]$$

IV.3. Application sur un exemple simple

Alice doit choisir une clé publique (n, e) et sa clé privée d.
Elle choisit :

$$p = 5 \qquad \text{et} \qquad q = 11$$

Ainsi : $n = 55$.

1) Démontrons qu'elle peut choisir $e = 9$ et $d = 9$.

Démonstration.

- On commence par calculer :

$$m \ = \ (p-1)\,(q-1) \ = \ 4 \times 10 \ = \ 40$$

- On peut effectivement choisir $e = 9$ puisque :

$$9 \in \mathbb{N}, \qquad 9 \wedge m = 1 \qquad 9 < m$$

- Enfin, en choisissant $d = 9$, on a bien tout d'abord : $d \in \mathbb{N}$ et $d < m$.
  De plus : $de = 81 = 2 \times m + 1$. Ainsi : $de \equiv 1\ [m]$.

□

2) Les lettres de l'alphabet sont chiffrées de la façon suivante :

A	B	C	$\cdots$	X	Y	Z
1	2	3	$\cdots$	24	25	26

Bob, qui possède la clé publique d'Alice, chiffre le message « TESTONS RSA » et lui envoie. Quel message chiffré reçoit Alice ?

Démonstration.
Détaillons proprement le chiffrement de T et E. Le procédé étant identique pour toutes les lettres.

- Chiffrement de T
  La lettre T est codée par 20. Or : $20^e \equiv 5\ [n]$.
  (on rappelle que Bob possède la clé publique d'Alice et connaît donc le couple (n, e))
  Ainsi T est chiffré par 5.
- Chiffrement de E
  La lettre E est codée par 5. Or : $5^e \equiv 20\ [n]$. Ainsi E est chiffré par 20.

On obtient le message chiffré suivant :

$$(5,\ 20,\ 29,\ 5,\ 25,\ 4,\ 29,\ 8,\ 29,\ 1)$$

□

3) Comment Alice décode-t-elle le message de Bob ?

Démonstration.
Une fois le message chiffré reçu, Alice le décode nombre par nombre de la manière suivante :

- À l'aide de sa clé privée $d = 9$, Alice détermine d'abord le reste de la division euclidienne de 5^d par 55. Elle trouve : $5^d \equiv 20\ [m]$.
  Or 20 est le nombre qui code T.
- Elle procède de même pour tous les nombres du message. Et on retrouve bien le message initial (et c'est bien rassurant !)

□