Arithmétique (partie 1)

1. Introduction : un axiome de $\mathbb{N}$

AXIOME : Axiome du plus petit élément

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément : autrement dit, si A est une partie non vide de $\mathbb{N}$, alors il existe un entier $p \in A$ tel que pour tout $a \in A$, $p \leqslant a$.

Exemple :

Pour $A = \{7\,;\,9\,;\,11\}$ alors $p = 7$
La partie $B =]2\,;\,3]$ de $\mathbb{R}$ admet-elle un plus petit élément ? Non, car 2 est exclu.

2. Multiples et diviseurs

DÉFINITION :

Soit $(a\,;\,b) \in \mathbb{Z}^2$. On dit que a **est un multiple de** b s'il existe $k \in \mathbb{Z}$ tel que $a = kb$. Dans ce cas, on dit aussi que b **est un diviseur de** a, ou que b **divise** a et on note : $b \mid a$.

Exemple :

Donner l'ensemble des diviseurs de -21 :

$$\mathcal{D}(-21) = \{-21\,;\,-7\,;\,-3\,;\,-1\,;\,1\,;\,3\,;\,7\,;\,21\}$$

Exemple :

0 est-il un diviseur de 3 ? Non, car $\forall k \in \mathbb{Z},\ k \times 0 \neq 3$

3 est il un diviseur de 0 ? Oui, car $\exists k \in \mathbb{Z},\ k \times 3 = 0$.
On prend $k = 0$.
0 est il un diviseur de 0 ? Oui car $\exists k \in \mathbb{Z},\ k \times 0 = 0$.
On prend n'importe quel réel k.
Quels sont les diviseurs de 0 ? $\mathcal{D}(0) = \mathbb{R}$.

Exemple :

Pour tout $n \in \mathbb{Z}$, montrer que $n-1$ divise $n^4 - 1$.
Soit $n \in \mathbb{Z}$.

$$\begin{aligned} n^4 - 1 &= \left(n^2+1\right)\left(n^2-1\right) \\ &= \left(n^2+1\right)(n+1)(n-1) \end{aligned}$$

On pose $k = (n^2+1)(n+1)$.
$k \in \mathbb{Z}$, donc on a montré que $n-1$ divise n^4-1.

Exemple :

Pour tout $n \in \mathbb{Z}$, montrer que 2 divise $n(n+1)$.
Soit n un entier. Alors n est soit pair, soit impair.

- Si n est pair, alors il existe $k \in \mathbb{Z}$ tel que $n = 2k$.
  Alors $n(n+1) = 2k(2k+1)$.
  Posons $k' = k(2k+1)$. $k' \in \mathbb{Z}$, donc on a montré qu'il existe $k' \in \mathbb{Z}$ tel que $n(n+1) = 2k'$. Donc 2 divise $n(n+1)$.
- Si n est impair, alors il existe $k \in \mathbb{Z}$ tel que $n = 2k+1$.
  Alors

$$\begin{aligned} n(n+1) &= (2k+1)(2k+2) \\ &= 2(2k+1)(k+1) \end{aligned}$$

  Posons $k' = (2k+1)(k+1)$. $k' \in \mathbb{Z}$, donc on a montré qu'il existe $k' \in \mathbb{Z}$ tel que $n(n+1) = 2k'$. Donc 2 divise $n(n+1)$.

On conclut par disjonction de cas que 2 divise $n(n+1)$.

PROPRIÉTÉ :

Tout entier relatif non nul admet un nombre fini de diviseurs.

Démonstration. Soit $a \in \mathbb{Z}^*$ et d un diviseur de a. Ainsi, il existe $q \in \mathbb{Z}^*$ tel que $a = dq$. Donc $|a| = |d|\,|q|$ où q est un entier non nul, donc $|q| \geqslant 1$ et donc $|d|\,|q| \geqslant |d|$ c'est-à-dire que $|a| \geqslant |d|$ et donc que $-a \leqslant d \leqslant a$. On en déduit que a admet au plus $2|a|$ diviseurs. □

PROPRIÉTÉ :

Soit $(a\,;\,b\,;\,c) \in \mathbb{Z}^3$. Si $a \mid b$ et $b \mid a$, alors $b = a$ ou $b = -a$.

Démonstration. Si $a \mid b$, alors $|a| \leqslant |b|$ et si $b \mid a$ alors $|b| \leqslant |a|$, donc $|a| = |b|$ et donc $b = a$ ou $b = -a$. □

PROPRIÉTÉ :

Soit $(a\,;\,b\,;\,c) \in \mathbb{Z}^3$. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.

Démonstration. Soit $(a\,;\,b\,;\,c) \in \mathbb{Z}^3$.
Si $a \mid b$, alors il existe $k \in \mathbb{Z}$ tel que $b = ka$.
Si $b \mid c$, alors il existe $k' \in \mathbb{Z}$ tel que $c = k'b$.
Ainsi

$$\begin{aligned} c &= k'b \\ &= k'ka \end{aligned}$$

Posons $K = k'k$. On a $K \in \mathbb{Z}$ et $c = Ka$. Ainsi $a \mid c$.
□

■ PROPRIÉTÉ :

Soit $(a\,;\,b\,;\,c\,;\,m\,;\,n) \in \mathbb{Z}^5$.
Si $a \mid b$ et $a \mid c$, alors $a \mid (mb+nc)$.

Démonstration. Soit $(a\,;\,b\,;\,c\,;\,m\,;\,n) \in \mathbb{Z}^5$.
Si $a \mid b$, alors il existe $k \in \mathbb{Z}$ tel que $b = ka$.
Si $a \mid c$, alors il existe $k' \in \mathbb{Z}$ tel que $c = k'a$.
Ainsi

$$\begin{aligned} mb + nc &= mka + nk'a \\ &= a\,(mk + nk') \end{aligned}$$

Posons $K = mk + nk'$. On a $K \in \mathbb{Z}$, donc il existe un entier $K \in \mathbb{Z}$, $mb + nc = aK$. Ainsi $a \mid mb + nc$. □

Remarque : La propriété précédente est essentielle pour de nombreux raisonnements. On peut la reformuler ainsi : si un entier divise deux entiers, alors il divise toute combinaison linéaire à coefficients entiers de ceux-ci.

3. Nombres premiers

A. Introduction

■ DÉFINITION :

On dit qu'un entier naturel est **premier** s'il admet exactement deux diviseurs positifs.

Exemple :

1 est-il premier ? Non, car 1 n'a qu'un seul diviseur.

Quel est le plus petit nombre premier ? 2
Quels sont les nombres premiers pairs ? 2
Combien y a-t-il de nombres premiers inférieurs à 100 ? Il y a 25 nombres premiers inférieurs à 100.

■ THÉORÈME :

Soit $a \in \mathbb{N}$ tel que $a \geqslant 2$.

1. a admet toujours un diviseur premier.
2. Si a est premier, alors a admet un unique diviseur premier.
3. Si a n'est pas premier, alors il admet un diviseur premier p vérifiant : $2 \leqslant p \leqslant \sqrt{a}$.

Démonstration.

1. Si a est lui-même un nombre premier, alors il admet un diviseur premier : lui-même.
   Comme $a \neq 1$, si a n'est pas premier, il admet plus de deux diviseurs et donc au moins un diviseur strictement supérieur à 1 et distinct de lui-même. On note p le plus petit de ces éléments (*).
   Alors p est un nombre premier : en effet, supposons que p admette un diviseur d tel que $1 < d < p$. Comme $d \mid p$ et $p \mid a$, alors $d \mid a$. Alors d serait un diviseur de a tel que $1 < d < p$, ce qui contredirait le fait que p est le plus petit diviseur de a strictement supérieur à 1 .
   Donc a admet un diviseur premier.
2. Si a est premier, alors a est divisible par 1 et par a. 1 n'est pas premier et a est premier, donc a admet bien un unique diviseur premier : lui-même.
3. On sait, d'après que a admet un diviseur premier p et donc $p \geqslant 2$.
   Puisque, par hypothèse, a n'est pas premier, alors il existe $q > 1$ tel que $a = q \times p$.
   Si $p \leqslant q$ alors : $p \times p \leqslant q \times p = a$ donc $p^2 \leqslant a$ et donc $p \leqslant \sqrt{a}$: donc a admet un diviseur premier p inférieur ou égal à sa racine carrée.
   Si $q \leqslant p$ alors : $q \times q \leqslant q \times p = a$ donc $q^2 \leqslant a$ et donc $q \leqslant \sqrt{a}$: comme $q \geqslant 2$, il admet un diviseur premier qui est aussi un diviseur de a d'où le résultat.

□

Remarque : (*) Justifier l'existence de p : l'ensemble des diviseurs de a est une partie non vide de $\mathbb{N}$, donc elle admet un plus petit élément.

Exemple :

Vérifier que 197 n'est divisible par aucun des premiers $2, 3, 5, 7, 11$ et 13. Que peut-on en déduire ?

- $\frac{197}{2}$ n'est pas un entier ;
- $\frac{197}{3}$ n'est pas un entier ;
- $\frac{197}{5}$ n'est pas un entier ;
- $\frac{197}{7}$ n'est pas un entier ;
- $\frac{197}{11}$ n'est pas un entier ;
- $\frac{197}{13}$ n'est pas un entier ;

Or, $\sqrt{197} \approx 14$. Ainsi, il n'existe pas de nombres premiers inférieurs à la racine carrée de 197 qui divise 197. Donc, d'après le théorème précédent, 197 est un nombre premier.

Exemple :

2021 est-il un nombre premier ?
$\sqrt{2021} \approx 44$, on teste la division de 2021 par p, avec p un nombre premier inférieur à 44. On constate que $\frac{2021}{43} = 47$. Donc 2021 n'est pas un nombre premier.

B. Crible d'Eratosthène [1]

$n \in \mathbb{N}$ étant donné, le Crible d'Eratosthène sert à faire la liste de tous les entiers premiers inférieurs ou égaux à n (ici, $n = 100$).
On commence par barrer tous les multiples de 2 sauf 2, puis tous les multiples de 3 non déjà barrés, sauf 3. Le premier nombre non barré après 3 est 5 et il est donc premier, sinon il aurait un diviseur premier parmi les nombres non barrés qui le précèdent et il aurait déjà été barré. On barre ensuite tous les multiples de 5 sauf 5, etc.

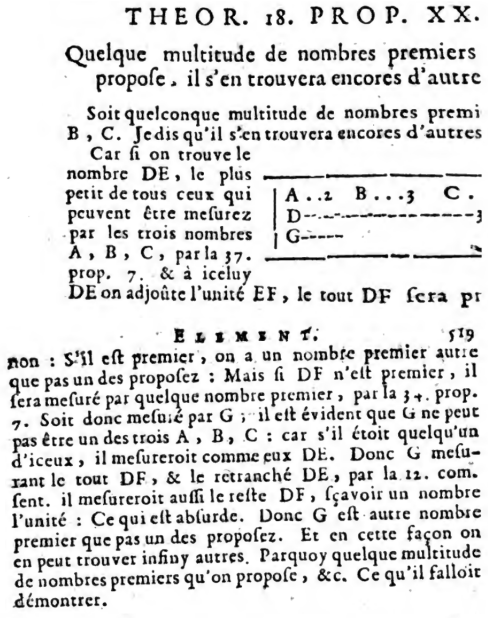
~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Légende	2		3		5		7	

■ PROPRIÉTÉ :

Il existe une infinité de nombres premiers.

Démonstration. La démonstration qui suit est due à Euclide (III^{e} siècle av. J.C.). Nous allons l'étudier à travers le texte historique.



THEOR. 18. PROP. XX.

Quelque multitude de nombres premiers propoſe, il s'en trouvera encores d'autre

Soit quelconque multitude de nombres premi
B, C. Je dis qu'il s'en trouvera encores d'autres
Car ſi on trouve le nombre DE, le plus petit de tous ceux qui peuvent être meſurez par les trois nombres A, B, C, par la 37. prop. 7. & à iceluy DE on adjoûte l'unité EF, le tout DF ſera pr

A..2 B...3 C.
D
G

ELEMENT. 519

non : S'il eſt premier, on a un nombre premier autre que pas un des propoſez : Mais ſi DF n'eſt premier, il ſera meſuré par quelque nombre premier, par la 34. prop. 7. Soit donc meſuré par G ; il eſt évident que G ne peut pas être un des trois A, B, C : car s'il étoit quelqu'un d'iceux, il meſureroit comme eux DE. Donc G meſurant le tout DF, & le retranché DE, par la 12. com. ſent. il meſureroit auſſi le reſte DF, ſçavoir un nombre l'unité : Ce qui eſt abſurde. Donc G eſt autre nombre premier que pas un des propoſez. Et en cette façon on en peut trouver infiny autres. Parquoy quelque multitude de nombres premiers qu'on propoſe, &c. Ce qu'il falloit démontrer.

Raisonnons par l'absurde et supposons qu'il existe un nombre fini n de nombres premiers, dont la liste soit $p_1, p_2, \ldots, p_n$.
Considérons alors l'entier $a = 1 + p_1 p_2 \cdots p_n$.

- Supposons que a est premier. Alors on a trouvé un nombre premier qui est plus grand que les précédents, et il n'appartient donc pas à la liste. D'où contradiction.
- Donc a n'est pas premier et $a \geqslant 2$. Ainsi, d'après le cours, a admet un diviseur premier. Celui-ci se trouve donc dans la liste supposée finie des nombres premiers $p_1, p_2, \ldots, p_n$. Notons p_j ce diviseur premier de a.

  Alors p_j divise a et p_j divise $p_1 p_2 \cdots p_j \cdots p_n$ donc p_j est un facteur dans chacun des deux termes de la différence

  $$a - p_1 p_2 \cdots p_j \cdots p_n$$

  Mais $a - p_1 p_2 \cdots p_j \cdots p_n = 1$. Donc, si l'entier p_j est un diviseur de 1 tel que $p_j > 0$, alors $p_j = 1$. Or p_j est un nombre premier, et on sait que 1 n'est pas un nombre premier.
  D'où contradiction.

Ainsi, dans tous les cas, l'hypothèse de départ est fausse.
On a donc démontré qu'il existe une infinité de nombres premiers. □

Remarques :

1. Il n'existe pas actuellement de formule exploitable pour générer des nombres premiers.
2. En octobre 2024, le plus grand nombre premier connu est $2^{136\,279\,841}$ - 1, nombre qui comporte 41 024 320 chiffres en écriture décimale.
3. En 1896, les mathématiciens Jacques Hadamard [2] et Charles-Jean De la Vallée Poussin [3] ont montré que si x est un réel et $\pi(x)$ le nombre de nombre premiers inférieurs ou égaux à x, alors $\lim\limits_{x \to +\infty} \pi(x) \dfrac{\ln(x)}{x} = 1$.

1. Ératosthène de Cyrène, né vers -276 à Cyrène et mort vers -194 à Alexandrie, est un astronome, géographe, philosophe et mathématicien grec. Érudit reconnu par ses pairs, il est nommé directeur de la bibliothèque d'Alexandrie par le roi d'Égypte Ptolémée III vers -245. Considéré comme le plus grand savant du III^{e} siècle av. J.-C., il est l'inventeur de la géographie.

2. Jacques Salomon Hadamard, né le 8 décembre 1865 à Versailles et mort le 17 octobre 1963 à Paris, est un mathématicien français, connu pour ses travaux en théorie des nombres, en analyse complexe, en analyse fonctionnelle, en géométrie différentielle et en théorie des équations aux dérivées partielles.

3. Charles-Jean Étienne Gustave Nicolas, baron de La Vallée Poussin, né le 15 août 1866 à Louvain en Belgique, mort le 2 mars 1962 à Watermael-Boitsfort, à Bruxelles, est un mathématicien belge.

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

■ THÉORÈME :

Soit $a \in \mathbb{N}$ tel que $a \geqslant 2$.
a se décompose de manière unique, à l'ordre des facteurs près, sous la forme $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ où $p_1, p_2, \dots, p_n$ sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont des entiers naturels.

Exemple :
$2015 = 5 \times 13 \times 31$.

Exemple :
Décomposer 2025 en produit de facteurs premiers.

$$\begin{aligned} 2025 &= 5 \times 405 \\ &= 5 \times 5 \times 81 \\ &= 5^2 \times 3^4 \end{aligned}$$

Remarque : Lorsque le nombre est lui-même premier, pour généraliser l'expression, on parle tout de même de « produit de facteurs premiers ».

Démonstration.

— Existence de la décomposition : On démontre cette existence par récurrence sur l'entier a.
On note (P_a) la propriété dépendant de l'entier a : « Tout entier naturel k tel que $2 \leqslant k \leqslant a$ admet une décomposition sous la forme $k = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ où $p_1, p_2, \dots, p_n$ sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont des entiers naturels. ».

- $2 = 2^1$ où 2 est premier donc (P_2) est vraie.
- Montrons que $(P_a) \Rightarrow (P_{a+1})$:
  Ou bien $a+1$ est premier et alors sa décomposition est convenable.
  Ou bien $a+1$ n'est pas premier et donc il admet un diviseur premier $p < a+1$.
  Donc il existe un entier naturel k tel que $a+1 = k \times p$ avec $0 < k < a+1$.
  Donc k vérifie l'hypothèse de récurrence, donc k s'écrit sous la forme $k = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ où $p_1, p_2, \dots, p_n$ sont des nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_n$ sont des entiers naturels.
  Finalement, $a+1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \times p$, qui est bien de la forme souhaitée, que p soit un des nombres premiers $p_1, p_2, \dots, p_n$ ou un autre.
- Le théorème est vérifié pour tout entier $a \geqslant 2$.

— Unicité de la décomposition : admise.

□

■ THÉORÈME :

Soit $a \in \mathbb{N}$ et $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ sa décomposition en produit de facteurs premiers.
Les diviseurs positifs de a sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ où, pour tout $i \in [\![1; n]\!]$, $\beta_i \in \mathbb{N}$ et $0 \leqslant \beta_i \leqslant \alpha_i$.

Esquisse de preuve : Supposons que $d \mid a$ où $d \geqslant 2$. Alors d admet un diviseur premier p, qui est donc aussi un diviseur premier de a. Comme la décomposition en facteurs premiers de a est unique, p est dans la liste $p_1, p_2, \dots, p_n$. □

Exemple :
Décomposer 16 758 en produit de facteurs premiers.

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

Ainsi $16\,758 = 2 \times 3^2 \times 7^2 \times 19$.
Même question pour 999 999 en trouvant une première factorisation « évidente » de cet entier.

$$\begin{aligned} 999\,999 &= 10^6 - 1 \\ &\left(10^3 - 1\right)\left(10^3 + 1\right) \\ &= 999 \times 1001 \\ &= 111 \times 9 \times 1001 \\ &= 37 \times 3 \times 3^2 \times 7 \times 11 \times 13 \\ &= 3^3 \times 7 \times 11 \times 13 \times 37^1 \end{aligned}$$

Donc $999\,999 = 3^3 \times 7 \times 11 \times 13 \times 37$.

B. Déterminer si un entier en divise un autre

■ PROPRIÉTÉ :

Soit $n = \prod_{i \in \mathbb{N}^*} p_i^{\alpha_i}$ et $d = \prod_{i \in \mathbf{N}^*} p_i^{\beta_i}$. L'entier d divise l'entier n si et seulement si, pour tout entier i, $\beta_i \leqslant \alpha_i$

Exemple :
$360 = 2^3 \times 3^2 \times 5$ et $24 = 2^3 \times 3$. On a $\underbrace{3 \geqslant 3}_{\text{pour 2}}$, $\underbrace{2 \geqslant 1}_{\text{pour 3}}$ et $\underbrace{2 \geqslant 1}_{\text{pour 5}} \geqslant 0$. donc 24 divise 360.

C. Déterminer l'ensemble des diviseurs positifs d'un nombre entier

L'écriture $n = \prod_{i\in\mathbf{N}^*} p_i^{\alpha_i}$ permet d'obtenir tous les diviseurs de n. Tous les diviseurs de n sont de la forme $\prod_{i\in\mathbb{N}^*} p_i^{\beta_i}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$. Donc :

■ PROPRIÉTÉ :

Le nombre de diviseurs positifs de n est alors :

$$ND(n) = \prod_{i\in\mathbb{N}^*} (\alpha_i + 1)$$

Exemple :

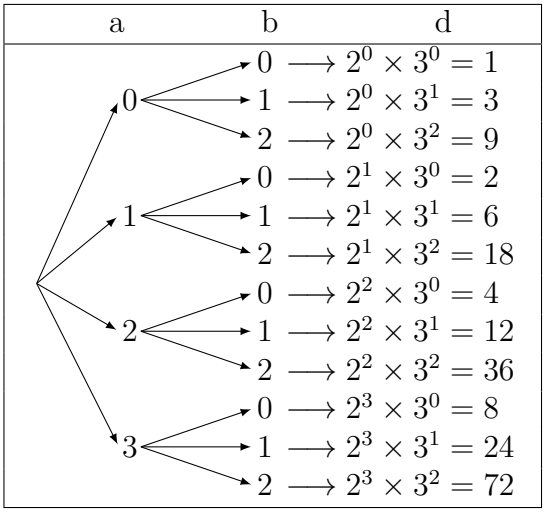
$72 = 2^3 \times 3^2$. Les diviseurs de 72 s'écrivent $2^a \times 3^b$, avec $0 \leqslant a \leqslant 3$ et $0 \leqslant b \leqslant 2$.

Il y a $(3+1) \times (2+1) = 12$ diviseurs.

Liste des diviseurs grâce à un tableau à double entrée :

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	$2^0 \times 3^0 = 1$	$2^1 \times 3^0 = 2$	$2^2 \times 3^0 = 4$	$2^3 \times 3^0 = 8$
$b=1$	$2^0 \times 3^1 = 3$	$2^1 \times 3^1 = 6$	$2^2 \times 3^1 = 12$	$2^3 \times 3^1 = 24$
$b=2$	$2^0 \times 3^2 = 9$	$2^1 \times 3^2 = 18$	$2^2 \times 3^2 = 36$	$2^3 \times 3^2 = 72$

Liste des diviseurs grâce à un « arbre » :



Donc $D(72) = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72\}$.

D. La théorie des nombres et les conjectures actuelles

■ DÉFINITION :

On appelle **nombre parfait** tout entier naturel n dont la somme des diviseurs positifs vaut $2n$.

1. Montrer que 6 et 28 sont parfaits.
   - $\mathcal{D}_+(6) = \{1\,;\,2\,;\,3\,;\,6\}$ et $1+2+3+6 = 2\times 6$, donc 6 est un nombre parfait.
   - $\mathcal{D}_+(28) = \{1\,;\,2\,;\,4\,;\,7\,;\,14\,;\,28\}$ et $1+2+4+7+14+28 = 2\times 28$, donc 28 est un nombre parfait.
2. Euclide a énoncé le théorème suivant : « Si un nombre a s'écrit sous la forme $2^n(2^{n+1}-1)$ et si le facteur $(2^{n+1}-1)$ est premier, alors a est un nombre parfait ».
   Quelle est sous l'hypothèse du théorème, la décomposition de a en produit de facteurs premiers ?
   L'hypothèse du théorème est que $2^{n+1}-1$ est un nombre premier, donc la décomposition en facteurs premiers est $2^n(2^{n+1}-1)$. Ce nombre à $(n+1)\times 2$ diviseurs.
   En déduire la liste de tous les diviseurs de a.
   On liste les diviseurs en deux catégories : ceux qui contiennent le facteur $2^{n+1}-1$ et leur analogue qui ne le contient pas :
   $2^0 \quad 2^0 \times (2^{n+1}-1)$
   $2^1 \quad 2^1 \times (2^{n+1}-1)$
   $\ldots \quad \ldots$
   $2^n \quad 2^n \times (2^{n+1}-1)$
   Montrer que la somme de ces diviseurs est $2a$.
   On calcule $\sum_{k=0}^{n} 2^k + \sum_{k=0}^{n} 2^k\left(2^{k+1}-1\right)$. Grâce à la propriété de la somme des termes de la suite géométrique de raison 2 (qui est différent de 1) et de premier terme $u_0 = 1$, on obtient :

$$\begin{aligned}\sum_{k=0}^{n}\left(2^k + 2^k\left(2^{n+1}-1\right)\right) &= \sum_{k=0}^{n} 2^k + \left(2^{n+1}-1\right)\sum_{k=0}^{n} 2^k \\ &= 2^{n+1}\sum_{k=0}^{n} 2^k \\ &= 2^n \frac{1-2^{n+1}}{1-2} \\ &= 2\times 2^n\left(2^{n+1}-1\right) \\ &= 2a\end{aligned}$$

3. Trouver d'autres nombres parfaits.
   Pour $n=3$, $2^{n+1}-1$ n'est pas premier. Pour $n=4$, on trouve 496, ensuite vient 8 128,
   puis 33 550 336, 8 589 869 056, 137 438 691 328, 2 305 843 008 139 952 128 (découvert par Leonhard Euler... sans calculatrice !)...
   Actuellement, 51 nombres parfaits sont connus. Le plus grands possède 12 640 858 chiffres et est égal à

$$2^{20\,996\,010}\left(2^{20\,996\,011}-1\right)$$

Remarque : Au XVIII$^{\text{e}}$ siècle, Euler a montré que tout nombre parfait pair est de la forme proposée par Euclide. En 2025, on ne sait toujours pas s'il existe des nombres parfaits impairs...