# Nombres premiers

## Activités

1) Rappels

*Définition* : un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts, 1 et lui-même.

Un entier naturel, différent de 0 et 1, qui n'est pas premier est composé.

*Remarques* (*à compléter*):

- 0 n'est pas premier car
- 1 n'est pas premier car
- 2 est l'unique nombre premier pair

*Exemples remarquables* :

- 8281807978…10987654321 est premier
- Le nombre $u_0 = 1122659$ est premier, mais également les termes de la suite finie $u_{n+1} = 2u_n + 1$ sept fois de suite (chaîne de Cunningham, de nombres de Sophie Germain, 1776-1831).
- Le nombre $1_{1031}$ est premier (nombre formé de 1031 fois le chiffre 1). Idem avec 2, 19, 23, 317, 1031, 49081, 86453, 109297, 270343, 5794777, et 8177207 fois le chiffre 1. Ces nombres sont appelés rep-unit. Vous remarquerez que le nombre de chiffres de chacun de ces nombres… est premier. Défi : trouvez (seul.e) l'idée de la preuve de cette propriété.
- Le nombre $1_{10080}0_{2135}1$ est premier.
- Le nombre $1_{111}2_{1111}2_{111}...8_{111}9_{1111}0_{2284}1$ est premier.
- L'Electronic Frontier Fundation offre 250000 dollars pour la découverte d'un nombre premier d'un milliard de chiffres ou plus.
- Les nombres premiers « illégaux » sont à la fois des nombres premiers, et une critique pour montrer le ridicule de lois qui rendent la détention de certaines informations illégales. Cf. l'article Wikipedia, qui donne des nombres premiers permettant de craquer un DVD ou un code CSS.

*Conjectures sur les nombres premiers* :

Il y a de très nombreuses conjectures irrésolues sur les nombres premiers, en voici un extrait (directement de Wikipedia) :

- Les quatre problèmes de Landau :
  - conjecture de Goldbach : tout nombre pair strictement supérieur à 2 peut s'écrire comme somme de deux nombres premiers ;
  - conjecture des nombres premiers jumeaux : il existe une infinité de jumeaux premiers ;
  - conjecture de Legendre : il existe toujours au moins un nombre premier entre $n^2$ et $(n + 1)^2$ ; cette conjecture est liée à l'hypothèse de Riemann et, comme cette dernière, reste non démontrée à ce jour ;
  - existence d'une infinité de nombres premiers de la forme $n^2 + 1$.
- L'existence d'une infinité de nombres premiers de Sophie Germain.
- La conjecture de Polignac (dont celle des nombres premiers jumeaux est le cas particulier $n = 2$) : tout entier naturel pair $n$ peut s'écrire comme différence de deux nombres premiers consécutifs et cela d'une infinité de manières.
- Y a-t-il une infinité de nombres premiers factoriels (du type $n ! + 1$ ou $-1$) ou primoriels (similaire à la factorielle, mais le produit se fait uniquement sur les nombres premiers inférieurs ou égaux à $n$) ?

- Une conjecture de Daniel Shanks : soit la suite, dite d'Euclide-Mullin, de premier terme $u_1 = 2$ et telle que le terme $u_n$ soit le plus petit diviseur premier du successeur du produit des termes $u_i$ pour $i < n$. La conjecture énonce que tous les nombres premiers apparaissent dans cette suite.
- La spirale d'Ulam (ou horloge d'Ulam) n'est à ce jour pas encore pleinement expliquée.

*Rappel* sur les propriétés de $\mathbb{N}$ :

- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute partie majorée de $\mathbb{N}$ est finie, et réciproquement toute partie finie de $\mathbb{N}$ est majorée.

2) Diviseurs premiers d'un entier naturel

*Théorème* : Tout entier naturel $n$ supérieur ou égal à 2 admet au moins un diviseur premier. Si $n$ est composé, alors il admet un diviseur premier $p$ compris entre 0 et $\sqrt{n}$.

*Démonstration* :

- Si $n$ est premier, il se divise lui-même.
- Sinon, l'ensemble des diviseurs $d$ de $n$ tels que $2 \le d < n$ n'est pas vide. D'après les rappels sur $\mathbb{N}$, il admet donc un plus petit élément, que l'on note $p$.
- Montrons que $p$ est premier par l'absurde. Si $p$ n'est pas premier, alors il admettrait un diviseur $d$ tel que $2 \le d < p$. Or tout diviseur de $p$ divise $n$, donc $d$ serait plus petit que $p$ : absurde par définition de $p$.
- De plus on en déduit dans ce cas que $n = pq$ avec $2 \le p < q$, donc $p^2 \le pq = n$ p^2, donc $p \le \sqrt{n}$ .

*Exemples* : à la main (pour les courageux), tester si $2^7 - 1$ et $2^{11} - 1$ sont premiers.

3) Nombre de nombres premiers

*Théorème* : il existe une infinité de nombres premiers.

*Démonstration 1* : Par l'absurde (Euclide).

Supposons qu'il n'existe qu'un nombre fini de nombres premiers, et soit $q$ le plus grand d'entre eux.

Soit $N$ le produit de tous ces nombres premiers auquel on ajoute 1 :
$N = 2 \times 3 \times 5 \times 7 \times \ldots \times q + 1$.

On sait qu'il existe un nombre premier $p$ divisant $N$, d'après le théorème précédent du 2).

Alors $\begin{cases} p \mid N \\ p \in \{2,3,5,7,\ldots,q\} \end{cases}$, donc $p \mid 2 \times 3 \times 5 \times 7 \times \ldots \times q$.

Donc $p \mid N - 2 \times 3 \times 5 \times 7 \times \ldots \times q$ , c'est-à-dire que $p \mid 1$. Ce qui est absurde car $p$ est premier.

*Démonstration 2* : Avec les propriétés de $\mathbb{N}$.

Soit $n$ un entier naturel supérieur ou égal à 3, $N = n! - 1$ et $p$ un nombre premier tel que $p$ divise $n$. On est sûr que $p$ existe d'après le théorème du paragraphe 2) ci-dessus.

$p > n$, en effet sinon comme dans la démonstration 1 on aurait $p \mid N - n! = 1$, ce qui serait absurde.

On en déduit que comme $n$ est aussi grand que l'on veut, alors $p$ aussi. Donc l'ensemble des nombres premiers n'admet pas de majorant. Par contraposée sur les propriétés de $\mathbb{N}$ rappelées au 1), on en déduit que l'ensemble des nombres premiers est infini.

■

## II Théorème fondamental de l'arithmétique

1) Décomposition en facteurs premiers

*Théorème* : tout entier naturel supérieur ou égal à 2 se décompose en un produit de facteurs premiers. Cette décomposition est unique à l'ordre près.

On note souvent $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ $p_1, p_2, \dots, p_k$ premiers et $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$

*Démonstration* :

- Existence

  *n* admet au moins un diviseur premier $p_1$ d'après I.2°)

  Si $n \neq p_1$, alors $n = p_1 q_1$ avec $1 \leq q_1 < n$, et soit $q_1$ est premier, soit $q_1 = p_2 q_2$ avec $1 \leq q_2 < q_1$.

  Donc $n = p_1 p_2 q_2$ avec $1 \leq q_2 < q_1 < n$.

  On itère ce raisonnement, on obtient une suite strictement décroissante d'entiers naturels :

  $1 \leq q_i < \dots < q_2 < q_1 < n$

  Cette suite est nécessairement finie d'où l'écriture $n = p_1 p_2 \dots p_i$.

  Comme les $p_j$ ne sont pas tous nécessairement distincts, on écrit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

- Unicité : cf paragraphe suivant.

2) Une conséquence du théorème de Gauss

*Théorème* : un nombre premier divise un produit de facteurs si et seulement si il divise un de ces facteurs.

*Démonstration* :

On suppose que le nombre premier *p* divise le produit *bc*.

- On rappelle le théorème de Gauss : si *a* et *b* sont premiers entre eux et si *a* divise *bc*, alors *a* divise *c*.

  D'où, si *p* divise *bc* :

  - soit *p* et *b* ne sont pas premiers entre eux, ils ont donc un diviseur commun, et alors *p* divise *b*, car les seuls diviseurs de *p* sont1 et *p*, et $p \wedge b \neq 1$ ;
  - soit *p* et *b* sont premiers entre eux et *p* divise *c* d'après Gauss.
- La réciproque est triviale.

*Conséquences* :

- ① : Si un nombre *p* premier divise $a^k$, alors on a *p* divise $\underbrace{a \times a \times \dots \times a}_{k \text{ fois}}$, donc *p* divise *a* puis *p* divise $a^k$.
- ② : Si un nombre premier divise le produit de facteurs premiers $p_1 p_2 \dots p_n$, alors *p* est l'un des $p_i$.

*Preuve de l'unicité de la décomposition en facteurs premiers* :

- D'après ce qui précède ②, les seuls nombres premiers divisant $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sont les nombres premiers $p_i$ : on n'a pas le choix de ces nombres premiers dans la décomposition de *n*.
- D'après ①, $p_i^{\alpha_i} \mid n$, mais $p_i^{\alpha_i + 1} \mid n$ : on n'a pas le choix des puissances $\alpha_i$.
- Donc la décomposition est unique à l'ordre près.

*Exemple* : $16758 = 2 \times 3^2 \times 7^2 \times 19$

3) Applications aux diviseurs, pgcd, ppcm

*Théorème* : soit *n* un entier naturel non nul, on pose $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, avec $p_1, p_2, \dots, p_k$ premiers et $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{N}$. Alors les diviseurs positifs de *n* sont tous les nombres de la forme $n = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, où $\forall i \in \mathbb{N}, \quad 1 \leq i \leq k, \quad 0 \leq \beta_i \leq \alpha_i$.

*Applications* :

- $21300 = 2^2 \times 3 \times 5^2 \times 71$ et $45440 = 2^7 \times 5 \times 71$.
  Alors $\text{pgcd}(21300, 45440) = 2^2 \times 5 \times 71$ et $\text{ppcm}(21300, 45440) = 2^7 \times 3 \times 5^2 \times 71$ .
- Les diviseurs de 21300 sont de la forme $2^{\beta_1} \times 3^{\beta_2} \times 5^{\beta_3} \times 71^{\beta_4}$ , où $\underbrace{0 \le \beta_1 \le 2}_{\text{3 possibilités}}, \underbrace{0 \le \beta_2 \le 1}_{\text{2 possibilités}}, \underbrace{0 \le \beta_3 \le 2}_{\text{3 possibilités}}, \underbrace{0 \le \beta_4 \le 1}_{\text{2 possibilités}}$ . Donc 21300 admet $3 \times 2 \times 3 \times 2 = 36$ diviseurs distincts.
- Généraliser le raisonnement précédent à un nombre *n* tel que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, qui admet donc diviseurs distincts.
- On verra (éventuellement) en exercice comment calculer la somme de ces diviseurs, avec un raisonnement assez élégant.
- Déterminer *b* tel que $\text{ppcm}(28, b) = 140$.

  On doit avoir $b \mid 140$ et $b \nmid 28$. Or $28 = 2^2 \times 7$ et $140 = 2^2 \times 5 \times 7$, d'où par exemple $b = 5$. Y-a-t-il d'autres solutions ?

## Le petit théorème de Fermat

*Théorème* : Soit *p* un nombre premier et *a* un entier naturel premier avec *p*. Alors $a^{p-1} \equiv 1 [p]$ .

*Remarques* :

- Ceci équivaut à : $a^{p-1} - 1$ est divisible par *p* ;
- Ceci équivaut à : $a^p - a$ est divisible par *p* ;
  En effet $a^p - a = a(a^{p-1} - 1)$. Comme *a* et *p* sont premiers entre eux, on en déduit d'après Gauss que *p* divise $a^p - a$ si et seulement si *p* divise $a^{p-1} - 1$.
- Ce théorème n'a aucune utilité pour trouver des nombres premiers. En effet la condition $a^{p-1} \equiv 1 [p]$ est nécessaire pour que *p* soit premier mais non suffisante ; lisez bien le théorème… et comprenez bien la différence nécessaire/suffisant.
- Les démonstrations de ce théorème sont nombreuses, élégantes et formatrices. En voici trois, à comprendre.

*Démonstration 1* :

On considère les $p-1$ nombres $a, 2a, 3a, \dots, (p-1)a$ et leur reste respectif $r_1, r_2, r_3, \dots, r_{p-1}$ dans la division euclidienne par *p*.

- *p* ne divise aucun des nombres $a, 2a, 3a, \dots, (p-1)a$. En effet supposons que *p* divise un des nombres *ka* avec $1 \le k \le p-1$. Comme $a \wedge p = 1$, d'après Gauss *p* divise *k*. Or $k < p$ : c'est absurde.
- Donc tous les restes $r_1, r_2, r_3, \dots, r_{p-1}$ sont non nuls : $\forall k \in \mathbb{N},\ 1 \le k \le p-1 \quad r_k \ne 0$.

  Les restes $r_k$ sont strictement positifs et strictement inférieurs à *p*, ils sont tous dans l'ensemble $\{1, 2, 3, \dots, p-1\}$.
- Montrons que ces restes sont tous distincts.
  On remarque que pour $1 \le k < k' \le p-1$ on a $1 \le k' - k \le p-1$, donc *p* ne divise pas , et comme *a* et *p* ne sont pas premiers entre eux, *p* ne divise pas $(k'-k)a$.

  Ceci équivaut à $(k'-k)a \not\equiv 0 [p] \Leftrightarrow k'a \not\equiv ka [p] \Leftrightarrow r_{k'} \not\equiv r_k [p]$ : les restes sont deux à deux distincts.
- Il en découle que $\{r_1, r_2, r_3, \dots, r_{p-1}\} = \{1, 2, 3, \dots, p-1\}$.

  *Attention* : ceci ne signifie pas que $r_1 = 1, r_2 = 2, \dots$ , mais que l'ensemble des restes $r_1, r_2, r_3, \dots, r_{p-1}$ parcourt l'ensemble des nombres de 1 à *p* – 1. En effet il n'y a pas d'ordre dans les ensembles.

- On en déduit que $r_1 r_2 r_3 \ldots r_{p-1} = 1\times 2\times 3\times \ldots \times (p-1) = (p-1)!$ ①

  Or par définition : $a \equiv r_1 [p]$

  $2a \equiv r_2 [p]$

  $3a \equiv r_3 [p]$

  …

  $(p-1)a \equiv r_{p-1} [p]$

  On multiplie ces inégalités terme à terme, on obtient :

  $a\times 2a\times 3a\times \ldots \times (p-1)a \equiv r\times_1 r\times_2 r\times_3 \ldots \times r_{p-1} [p]$

  Soit d'après ① :

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

  $\Leftrightarrow (p-1)!(a^{p-1}-1) \equiv 0 [p]$

  Et comme $p$ est premier, $p$ ne divise pas le produit de facteurs $(p-1)!$ ; il faudrait pour cela que $p$ divise un des facteurs 1 , 2 , 3 , … , $p$ – 1 ce qui est impossible)

  Donc $p$ divise $a^{p-1}-1$ : on a montré que $a^{p-1}-1 \equiv 0 [p]$ ■

*Démonstration 2* : en faisant un coloriage (il n'y a pas d'âge pour ça).

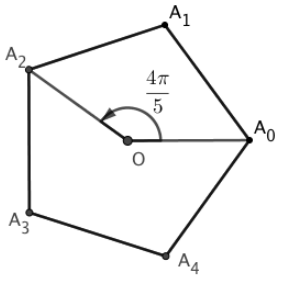
On considère un polygone régulier $A_0 A_1 \ldots A_{p-1}$ ayant $p$ sommets, où $p$ est un nombre premier. On colorie chacun des sommets, avec une couleur parmi $a$ disponibles.

Il y a au total $a^p$ coloriages possibles : $a$ choix pour le premier sommet que multiplie $a$ choix pour le deuxième sommet etc. jusqu'à $a$ choix pour le dernier sommet. Parmi ces coloriages, $a$ sont unicolores : tous les sommets sont soit de la couleur numéro 1, soit de la couleur numéro 2, etc. jusqu'à la couleur numéro $a$.

On veut montrer que le nombre de coloriages multicolores, qui est donc égal à $a^p - a$, est multiple de $p$.

On remarque qu'étant donné un coloriage, on peut en déterminer $p-1$ par des rotations $r_k$ d'angles respectifs $\frac{2k\pi}{p}$, où $1 \le k \le p-1$.

Dans l'exemple ci-contre, $p = 5$ et on considère la rotation $r_2$ d'angle $\frac{4\pi}{5}$.




$$\text{Alors} \begin{cases} r_2(A_0) = A_2 \\ r_2(A_1) = A_3 \\ r_2(A_2) = A_4 \\ r_2(A_3) = A_0 \\ r_2(A_4) = A_1 \end{cases}$$

On remarque sur cet exemple qu'un coloriage initial va donner 4 coloriages supplémentaires par les rotations correspondantes, donc qu'il y aura 5 coloriages associés.

En généralisant, un coloriage initial $(c_0, c_1, \ldots, c_{p-1})$ donne le coloriage $(c'_0, c'_1, \ldots, c'_{p-1})$ par la rotation $r_k$ d'angle $\frac{2k\pi}{p}$, avec $c_i \overset{r_k}{\mapsto} c'_i = c_{(i+k)[\mathrm{mod}\, p]}$. Le coloriage initial et les $p-1$ coloriages obtenus par les rotations $r_k$ donnent un total de $p$ coloriages. L'idée fondamentale de la démonstration est de montrer

que ces coloriages, obtenus par rotation à partir d'un coloriage non unicolore, sont tous distincts. Ainsi, on aura regroupé les coloriages par groupes de *p*, donc leur nombre total (égal à $a^p - a$) sera divisible par *p*.
On va raisonner par l'absurde.
Si un coloriage $\left(c_0, c_1, \ldots, c_{p-1}\right)$ non unicolore est invariant par une rotation $r_k$ fixée, alors en particulier :

$$c'_0 = c_0 = c_{k[p]}$$

On applique plusieurs fois la rotation $r_k$ :

$c_0 = c_{2k[p]}$ en appliquant deux fois la rotation

$c_0 = c_{3k[p]}$ en appliquant trois fois la rotation

…

$c_0 = c_{nk[p]}$ en appliquant *n* fois la rotation

…

$c_0 = c_{(p-1)k[p]}$ en appliquant $p-1$ fois la rotation

Comme *p* est premier, on montre que, exactement comme dans la démonstration 1 (partie « montrons que ces restes sont tous distincts ») :
toutes les valeurs des nombres $nk\left[p\right]$, où $0 \le n \le p-1$ sont tous les nombres de 0 à $p-1$
Cela signifie que l'on parcourt tous les sommets $A_n$ à partir du sommet $A_0$ de couleur $c_0$ lorsque l'on applique plusieurs fois la rotation $r_k$ fixée : tous les sommets ont donc la même couleur $c_0$. C'est en contradiction avec le fait que le coloriage n'est pas unicolore.
On a donc montré que les seuls coloriages invariants par rotation sont unicolores, et par conséquent que les coloriages multicolores peuvent être groupés par paquets de *p* coloriages. Chaque paquet est obtenu à partir d'un coloriage initial, et les autres coloriages du paquet sont obtenus à partir de ce coloriage par les $p-1$ rotations $r_k$ (d'où, au total et au risque de se répéter, un ensemble de *p* coloriages). Donc le nombre total de coloriages multicolores, égal à $a^p - a$ est divisible par $p$ : $\dfrac{a^p - a}{p}$ est entier. Si de plus $a \wedge p = 1$, on en déduit alors d'après Gauss que $a^{p-1} - 1 \equiv 0\left[p\right]$. ■

*Démonstration 3* : avec la formule du binôme
On rappelle que $\left(b+1\right)^p = b^p + 1 + \sum_{i=1}^{p-1} \begin{pmatrix} p \\ i \end{pmatrix} b^i$ ① où $\begin{pmatrix} p \\ i \end{pmatrix} = \dfrac{p\left(p-1\right)\ldots\left(p-i+1\right)}{i \times \left(i-1\right) \times \ldots \times 2 \times 1}$.

*Remarquez* la manière dont on a écrit la formule du binôme, ainsi que l'écriture simplifiée du coefficient binômial.
On peut écrire $\begin{pmatrix} p \\ i \end{pmatrix} = p \times \dfrac{\left(p-1\right)\ldots\left(p-i+1\right)}{i \times \left(i-1\right) \times \ldots \times 2 \times 1}$.

Comme *p* est premier et $i < p$ , alors aucun des nombres 2, 3, … , *i* ne divise *p*. Comme les coefficients binômiaux sont entiers, on en déduit que $i \times \left(i-1\right) \times \ldots \times 2 \times 1$ divise $\left(p-1\right)\ldots\left(p-i+1\right)$. Finalement $\begin{pmatrix} p \\ i \end{pmatrix} = p \times N$ , c'est-à-dire que *p* divise $\begin{pmatrix} p \\ i \end{pmatrix}$.

On obtient alors avec ① $\left(b+1\right)^p \equiv b^p + 1\left[p\right]$ .

Posons $a = b+1$ dans la formule précédente : $a^p \equiv (a-1)^p + 1[p]$ ②

On utilise à nouveau $(b+1)^p \equiv b^p + 1[p]$ en posant $b+1 = a-1 \Leftrightarrow b = a-2$ .

① devient $(a-1)^p \equiv (a-2)^p + 1[p]$

En substituant dans ② : $a^p \equiv (a-1)^p + 1[p]$ devient $a^p \equiv (a-2)^p + 1 + 1[p]$

On continue de proche en proche (une rédaction rigoureuse exigerait une récurrence) :

$a^p \equiv (a-3)^p + 1 + 1 + 1[p]$

…

$a^p \equiv (a-a)^p + \underbrace{1+\ldots+1}_{a \text{ fois}}[p]$

Soit $a^p \equiv a[p]$ . Comme à la démonstration 2, rajouter la condition $a$ et $p$ premiers entre eux donne alors $a^{p-1} - 1 \equiv 0[p]$ . ■