Les nombres premiers

Sommaire

1. Qu'est-ce qu'un nombre premier ?

Si tu connais déjà la définition d'un nombre premier, tu peux aller directement ici.

Nous allons nous intéresser aux nombres entiers : $0, 1, 2, 3, 4, \ldots$. Tu connais peut-être aussi les nombres négatifs $-1, -2, -3, -4, \ldots$, qui sont aussi des nombres entiers, mais on n'en aura pas besoin. Les nombres entiers (aussi appelés entiers) peuvent sembler très simples : tu les connais depuis l'école primaire ! Cependant, l'étude de certaines de leurs propriétés peut s'avérer très compliquée. La branche des mathématiques qui étudie les entiers s'appelle l'**arithmétique**.

Comme tu le sais, on peut additionner et multiplier n'importe quels entiers, et le résultat sera encore un entier. On peut aussi soustraire deux entiers, et on obtiendra un entier (qui sera peut-être négatif, mais peu importe). Par contre, quand on divise deux entiers, ce n'est plus toujours le cas : par exemple, $1 \div 2 = 0,5$ qui n'est pas un entier. Il est donc assez naturel de se demander, étant donnés deux entiers, à quelle condition la division de l'un par l'autre sera aussi un entier. Cette notion s'appelle la **divisibilité**.

Définition 1.1 : On dit qu'un entier n est divisible par un entier k si la fraction $\frac{n}{k}$ est un entier.

Remarque 1.1 : Tu n'es peut-être pas familier avec le fait d'utiliser des lettres pour désigner des nombres. En fait, cela signifie juste que la lettre utilisée peut être remplacée par n'importe quel nombre. Par exemple, si on remplace n par 5 et k par 3 dans la définition ci-dessus, on obtient un cas particulier de la définition : 5 est divisible par 3 si la fraction $\frac{5}{3}$ est un entier. En l'occurrence, ce n'est pas le cas : 5 n'est pas divisible par 3.

Nous allons maintenant voir quelques exemples pour avoir une meilleure intuition de cette notion.

Exemple 1.1 :

1. 4 est-il divisible par 2 ?
2. 5 est-il divisible par 3 ?
3. 0 est-il divisible par 42 ?
4. 11 est-il divisible par 36 ?
5. 4580 est-il divisible par 10 ?
6. 456987958 est-il divisible par 2 ?
7. 456987958 est-il divisible par 5 ?
8. 456987958 est-il divisible par 1 ?
9. 456987958 est-il divisible par 456987958 ?

Solution :

1. Oui, parce que $\frac{4}{2} = 2$, qui est un entier.

2. Non, parce que $\frac{5}{3} = 1,6666...$, qui n'est pas un entier.
3. Oui, parce que $\frac{0}{42} = 0$, qui est un entier. En fait, 0 est divisible par n'importe quel nombre !
4. Non, parce que $11 < 36$, donc $\frac{11}{36} < 1$. Plus généralement, un entier ne peut pas être divisible par un entier strictement plus grand que lui (à part 0 qui est divisible par tous les entiers !).
5. Oui, parce que $\frac{4580}{10} = \frac{458 \times 10}{10} = 458$. En fait, les nombres divisibles par 10 sont ceux qui se terminent par au moins un zéro. Ils sont donc très facile à « détecter ».
6. Oui, parce que $\frac{456987958}{2} = \frac{45698795 \times 10 + 8}{2} = 45698795 \times \frac{10}{2} + \frac{8}{2} = 45698795 \times 5 + 4$, qui est un entier. Plus généralement, les nombres divisibles par 2 sont les nombres pairs, c'est-à-dire ceux qui se terminent par 0, 2, 4, 6 ou 8.
7. Non : les nombres divisibles par 5 sont ceux qui se terminent par 0 ou 5.
8. Oui, parce que $\frac{456987958}{1} = 456987958$, qui est un entier. Plus généralement, tous les entiers sont divisibles par 1 !
9. Oui, parce que $\frac{456987958}{456987958} = 1$, qui est un entier. Plus généralement, tous les entiers sont divisibles par eux-mêmes !

Pour aller plus loin (critères de divisibilité) :

On a vu qu'il est très facile de savoir si un nombre est divisible par 1, 2, 5 et 10.

On peut se demander s'il existe un moyen de savoir si un nombre est divisible, par exemple, par 3. La réponse est oui : pour savoir si un nombre est divisible par 3, on peut regarder la somme de ses chiffres. Si elle est divisible par 3, alors le nombre original l'est aussi. Par exemple, la somme des chiffres de 213 est $2 + 1 + 3 = 6$, qui est divisible par 3, donc 213 est divisible par 3. Ceci s'appelle un critère de divisibilité par 3.

Il existe des critères de divisibilité par d'autres nombres, qui sont parfois assez compliqués. Pour en savoir plus, voir cette page Wikipédia.

On va maintenant se demander, étant donné un nombre, combien il a de diviseurs (c'est-à-dire par combien de nombres il est divisible). Par exemple, 6 est divisible par 1, 2, 3 et 6, et par aucun autre nombre. Il a donc 4 diviseurs.

Voici un tableau qui donne le nombre de diviseurs de chacun des entiers compris entre 2 et 20.

Nombre	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Nombre de diviseurs	2	2	3	2	4	2	4	3	4	2	7	2	4	4	5	2	6	2	6

On remarque que certains nombres ont seulement 2 diviseurs : 2, 3, 5, 7, 11, 13, 17 et 19. Les deux diviseurs sont toujours 1 et le nombre lui-même. On va appeler ces nombres des **nombres premiers**.

Définition 1.2 : On dit qu'un nombre est premier s'il possède exactement 2 diviseurs : 1 et lui-même.

Voyons à nouveau quelques exemples :

Exemple 1.2: Les nombres suivants sont-ils premiers ?

1. 4
2. 5
3. 6
4. 500
5. 1
6. 57
7. 489846541

Solution:

1. Non, parce que 4 est divisible par 2 (en plus d'être divisible par 1 et 4).
2. Oui : 5 est seulement divisible par 1 et 5.
3. Non, parce que 6 est divisible par 2. Plus généralement, aucun nombre pair n'est premier, à part le nombre 2 lui-même.
4. Non, parce que 500 est divisible par 10.
5. Non, parce que 1 a seulement un diviseur (lui-même) et non pas deux. Tu trouves peut-être ça étrange qu'on ne considère pas que 1 est un nombre premier, alors qu'il a encore moins de diviseurs, alors qu'il est seulement divisible par 1 et lui-même. En fait, c'est juste une question de définition, et la raison de ce choix sera expliquée un peu plus tard.
6. Ici, c'est un peu plus compliqué, mais en cherchant un peu (ou en utilisant le critère de divisibilité par 3), tu peux trouver que 57 est divisible par 3 et par 13, donc il n'est pas premier.
7. Là, c'est franchement compliqué. Les critères de divisibilité par 2, 3, 5 et 10 que nous avons vu ne fonctionnent pas. De manière générale, quand on prend un grand nombre, il est souvent très difficile de déterminer s'il est premier. Et ceci est parfois très utile, comme on va le voir plus tard. En l'occurrence, pour savoir si 489846541 est premier, il n'y a à première vue pas de moyen franchement plus simple que de tester s'il est divisible par chacun des nombres $2, 3, 4, 5, \ldots, 489846540$. Si tu t'ennuies, tu sais ce qu'il te reste à faire.

Pour aller plus loin (tester si un nombre est premier):

En fait, pour savoir si un nombre n est premier, on peut tester s'il est divisible par chacun des nombres compris entre 2 et $\sqrt{n}$ (si tu ne sais pas ce qu'est une racine carrée, tu peux sauter cette partie). S'il est divisible par un de ces nombres, il n'est pas premier par définition, et s'il n'est divisible par aucun de ces nombres, il est premier. En effet, si n est divisible par un entier $d > \sqrt{n}$, alors il sera aussi divisible par $\frac{n}{d}$ (car $\frac{n}{d}$ est un entier et $\frac{n}{n/d} = d$ qui est un entier), et on a

$$\frac{n}{d} < \frac{n}{\sqrt{n}} = \frac{\sqrt{n} \times \sqrt{n}}{\sqrt{n}}$$

Du coup, si un n n'est divisible par aucun nombre compris entre 2 et $\sqrt{n}$, il est aussi divisible par aucun nombre compris entre $\sqrt{n} + 1$ et $n - 1$, donc il est premier.

Encore mieux : il suffit de regarder si n est divisible par chacun des nombres **premiers** inférieurs à $\sqrt{n}$. En effet, comme on le verra plus loin, un nombre non premier est toujours divisible par au moins un nombre premier.

Si n est « très grand », cette méthode est nettement plus rapide que de regarder s'il est divisible par tous les nombres inférieurs à n, mais ça reste très long.

La notion de nombre premier remonte au moins à l'Antiquité grecque. Le mathématicien Euclide démontre qu'il y a une infinité de nombres premiers vers 300 avant Jésus-Christ. Depuis, de nombreux mathématiciens s'y sont intéressés. Depuis 2018, le plus grand nombre premier connu est $2^{82589933} - 1$, qui est un nombre à plus de 24 millions de chiffres !

Nous allons maintenant voir une propriété dans laquelle interviennent les nombres premiers, parfois connue sous le nom de « théorème fondamental de l'arithmétique ». Commençons par un exemple.

Exemple 1.3: Prenons l'exemple du nombre 60. 60 n'est pas premier, puisqu'il est divisible par 2. Ceci signifie que $\frac{60}{2}$ est un entier, en l'occurrence 30. On a donc $60 = 2 \times 30$. 2 est premier, mais 30 ne l'est pas. On peut répéter la procédure : $30 = 2 \times 15$. 2 est premier, mais 15 ne l'est pas, et on a $15 = 3 \times 5$. Or, 3 et 5 sont premiers, donc on ne peut plus continuer. Si on récapitule, on a $60 = 2 \times 30 = 2 \times 2 \times 15 = 2 \times 2 \times 3 \times 5$. On a donc écrit 60 comme un produit de nombres premiers.

On peut faire cette procédure en partant de n'importe quel nombre. Par exemple, $75 = 3 \times 5 \times 5$ et $26 = 2 \times 13$. De plus, cette décomposition est unique : étant donné un nombre, il existe une et une seule manière de l'écrire comme un produit de nombres premiers (en ne tenant pas compte de l'ordre des facteurs : on considère bien sûr 2×13 et 13×2 comme la même décomposition). C'est précisément ce que dit le théorème fondamental de l'arithmétique :

Théorème 1.1 (fondamental de l'arithmétique): Tout nombre entier n supérieur à 1 s'écrit comme produit de nombres premiers, de manière unique à l'ordre près des facteurs.

De manière imagée, on peut voir les nombres premiers comme des briques de Lego élémentaires, qu'on peut assembler pour créer n'importe quel nombre.

Remarque 1.2: Le théorème est bien valable si n est un nombre premier : on a $n = n$, donc n s'écrit comme un produit d'un seul nombre premier.

Remarque 1.3: Le théorème est l'une des raisons pour lesquelles on considère que 1 n'est pas un nombre premier. En effet, si on considérait que 1 était premier, on pourrait par exemple écrire $26 = 2 \times 13 = 2 \times 13 \times 1$, donc la décomposition en produit de facteurs premiers ne serait plus unique.

Remarque 1.4: Un entier n est divisible par chacun des nombres de se décomposition en facteurs premiers. En particulier, n est toujours divisible par au moins un nombre premier. Cette propriété est utile pour le paragraphe ci-dessus, et aussi pour celui sur « tester si un nombre est premier ».

Pour aller plus loin (il existe une infinité de nombres premiers):

Ici, je vais essayer d'expliquer la preuve d'Euclide de l'infinité des nombres premiers. C'est un peu compliqué, mais c'est pas grave si tu ne comprends pas tout.

On va faire un **raisonnement par l'absurde**, c'est-à-dire qu'on va commencer par supposer qu'il existe un nombre fini de nombres premiers, et aboutir à une contradiction, à quelque chose d'absurde. On pourra alors conclure qu'il existe une infinité de nombres premiers.

Supposons donc qu'il existe un nombre fini de nombres premiers. On va les appeler $p_1, p_2, p_3, ..., p_n$. On considère maintenant le nombre $N = p_1 \times p_2 \times p_3 \times ... \times p_n + 1$. Ce nombre est divisible par un certain nombre premier p_k. Donc $\frac{N}{p_k}$ est un entier. Mais

$$\begin{aligned}\frac{N}{p_k} &= \frac{p_1 \times p_2 \times p_3 \times ... \times p_{k-1} \times p_k \times p_{k+1} \times ... \times p_n + 1}{p_k} \\ &= p_1 \times p_2 \times p_3 \times ... \times p_{k-1} \times p_{k+1} \times ... \times p_n + \frac{1}{p_k}\end{aligned}$$

et ce nombre n'est visiblement pas un entier, à cause du $+\frac{1}{p_k}$. On a à la fois démontré que $\frac{N}{p_k}$ est un entier, et que ce n'est pas un entier : c'est absurde !

On en déduit qu'il existe une infinité de nombre premiers.

2. Pourquoi les nombres premiers sont-ils utiles ?

Les nombres premiers sont une notion très théorique, tu penses donc peut-être qu'ils n'ont pas d'application dans la « vraie vie ». En fait, c'était un peu le cas il y a encore un siècle. Maintenant, il n'en est rien. Je vais parler un peu de l'exemple de la cryptographie, qui est un domaine dans lequel ils interviennent beaucoup.

La cryptographie consiste en gros à chiffrer des messages pour que seulement certaines personnes puissent les décoder.

Plus précisément, on va voir ici l'exemple du chiffrement RSA, qui est très utilisé pour l'échange des données personnes sur Internet.

Une personne, qu'on va appeler Alice, souhaite que des correspondants lui envoient des messages. Ces messages pourront être interceptés par des utilisateurs malveillants, ils doivent donc être chiffrés de manière à ce que seule Alice puisse les décoder.

Cela peut sembler à première vue très difficile, voir impossible à mettre en place. En fait, ce qui rend tout cela possible, c'est les nombres premiers. Alice va partir de deux très grands nombres premiers, et calculer leur produit, ce qui est très rapide avec un ordinateur. A partir de ce produit, elle va générer ce qu'on appelle une clé publique et une clé privée (je ne vais pas détailler comment, même si c'est relativement simple). Elle va communiquer la clé publique à tout le monde, et conserver le clé privée. Ensuite, chaque personne qui souhaite lui envoyer un message va coder ce message à l'aide de la clé publique (là encore, je ne vais pas détailler comment), et lui envoyer. Alice pourra décoder ce message très facilement grâce à sa clé privée, mais les autres n'y arriveront pas, essentiellement parce qu'il est presque impossible de retrouver les deux nombres premiers d'origine à partir de leur produit.

3. Pourquoi les nombres premiers sont-ils fascinants ?

Les nombres premiers sont une notion mathématique très simple : pour l'expliquer, on a besoin uniquement de connaître les opérations de base sur les nombres entiers. Normalement, j'ai réussi à te l'expliquer sans trop de problèmes. Peut-être que tu n'es pas encore très à l'aise avec, mais pour quelqu'un qui a un peu l'habitude des raisonnements abstraits, il n'y a vraiment rien de compliqué. Pourtant, les nombres premiers sont étonnamment riches et complexes. Les quelques propriétés que nous avons vues, comme la décomposition en facteurs premiers et l'infinité de nombres premiers, ne sont déjà pas si simples. En fait, les nombres premiers interviennent dans des sujets autrement plus complexes, et il existe même de nombreux problèmes non résolus à leur sujet ! C'est la raison pour laquelle, depuis l'Antiquité grecque, de nombreux mathématiciens les trouvent fascinants et passent leur vie à les étudier.

Je vais mentionner 4 problèmes encore non résolus (on les appelle des **conjectures**) au sujet des nombres premiers : les 4 problèmes de Landau, que le mathématicien Landau a présenté lors d'un congrès en 1912. Ces conjectures ont la particularité d'être très simples à énoncer, malgré leur difficulté. Il existe beaucoup d'autres conjectures sur les nombres premiers : si tu parles anglais, tu peux consulter cette page Wikipédia qui en liste une soixantaine !

- **La conjecture de Goldbach :** elle affirme que tout entier pair supérieur à 3 s'écrit comme la somme de deux nombres premiers.

  Par exemple : $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 3 + 7$, $12 = 5 + 7$, $14 = 3 + 11$, $16 = 3 + 13$, $18 = 7 + 11$, $20 = 7 + 13$…

  Elle a été conjecturée par Christian Goldbach en 1742. Il a envoyé une lettre à Leonhard Euler, le plus grand mathématicien de son temps, qui n'a lui non plus pas réussi à la démontrer.

  Aujourd'hui, la conjecture a été vérifiée par ordinateur pour tous les entiers pairs jusqu'à 4×10^{18}, mais n'a toujours pas été démontrée. Pourtant, l'énoncé est ridiculement simple !

- **La conjecture des nombres premiers jumeaux :** Deux nombres premiers sont dits jumeaux s'ils ont un écart de 2. Par exemple, les nombres premiers 3 et 5 sont jumeaux parce que $5 - 3 = 2$.

  La conjecture des nombres premiers jumeaux affirme tout simplement qu'il existe une infinité de nombres premiers jumeaux.

  Les origines de cette conjecture sont incertaines.

  En fait, pour tout entier n, il existe une conjecture similaire, il existe une infinité de nombres premiers dont l'écart est égal à n. Il y a donc une infinité de conjectures, et la conjecture des nombres premiers jumeaux correspond à $n = 2$. Pour chaque valeur de n, les mathématiciens pensent que la conjecture est vraie, mais personne n'a réussi à le démontrer.

  En 2009, le mathématicien Zhang Yitang a démontré qu'il existe au moins un entier n inférieur à 70000000 pour lequel la conjecture est vraie. En 2013 et 2014, le projet collaboratif Polymath a amélioré ce résultat en montrant qu'il existe au moins un entier n inférieur à 246 pour lequel la conjecture est vraie.

Les deux autres conjectures de Landau sont un peu moins connues et je vais juste donner leur énoncé.

- **La conjecture de Legendre :** elle affirme que pour tout entier n, il existe un nombre premier compris entre n^2 et $(n + 1)^2$.

- **La conjecture « $n^2 + 1$ » :** elle affirme qu'il existe une infinité de nombres premiers de la forme $n^2 + 1$, où n est un entier.

Pour aller plus loin (l'hypothèse de Riemann) :

L'hypothèse de Riemann est une autre conjecture en rapport avec les nombres premiers. Contrairement aux problèmes de Landau, je ne vais même pas pouvoir l'énoncer précisément, mais je vais essayer de t'en donner un petit aperçu.

En fait, l'hypothèse de Riemann, n'est pas directement un problème d'arithmétique, mais plutôt d'**analyse complexe**. De manière très très grossière, l'analyse, c'est la branche des mathématiques qui étudie les fonctions ; et les nombres complexes, c'est des nombres bizarres (il y a par exemple un nombre complexe i tel que $i^2 = -1$). L'analyse complexe, c'est donc l'étude des fonctions de variables complexes.

A priori, ceci n'a donc rien à voir avec l'arithmétique. Mais en fait, de manière tout à fait surprenante et fascinante, il y a un lien entre les deux : c'est une fonction, qui s'appelle la **fonction zêta de Riemann**, qui est une fonction complexe dont les points d'annulation ont un rapport avec les nombres premiers. Le problème, c'est qu'on ne sait pas quels sont ces points d'annulation. Et le fait de les connaître permettrait de bien mieux comprendre les nombres premiers.

Aujourd'hui, l'hypothèse de Riemann est une des conjectures les plus célèbres en mathématiques. Elle fait partie des **7 problèmes du millénaire**, ce qui signifie que si quelqu'un arrive à la démontrer, il recevra 1 million de dollars !

Pour aller plus loin (des ressources pour approfondir) :

- Une excellente vidéo de la chaîne YouTube ScienceEtonnante.
- La page Wikipédia sur les nombres premiers.
- Si tu es vraiment motivé, le site Mathraining propose des cours et des problèmes amusants d'arithmétique (et aussi sur plein d'autres sujets).

Pour aller plus loin (un petit défi à propos des nombres premiers) :

Pour tout entier n, on note $n! = 1 \times 2 \times \ldots \times n$ la **factorielle** de n. Par exemple, $4! = 1 \times 2 \times 3 \times 4 = 24$.

Le défi est de montrer que pour tout entier $n \geqslant 2$, il existe un nombre premier compris entre n et $n! + 1$. Tu peux peut-être t'inspirer de la preuve de l'infinité de nombres premiers…