FASCINANTS ET ÉNIGMATIQUES NOMBRES PREMIERS

André Paternottre

[ndlr] *Math-Jeunes, Junior* est une des deux revues de nos collègues de la Société Belge des Professeurs de Mathématique d'expression française, destinées aux collégiens. On y trouve de nombreux articles, propositions d'activités, problèmes ... s'adressant à un public jeune, pour lui permettre d'aborder des thèmes mathématiques dans un langage accessible.
Rédiger des articles de mathématiques lisibles par une majorité d'élèves de 12 à 15 ans n'est pas chose aisée. Il faut maintenir la rigueur scientifique nécessaire tout en adoptant un langage simple, direct et incitant le lecteur à entrer dans la problématique traitée. C'est le pari des auteurs de *Math-Jeunes Juniors*. Les lecteurs de *Math-Ecole* pourront en juger eux-mêmes à la lecture de cet article et, par la même occasion, ils se rappelleront quelques connaissances fondamentales sur les nombres premiers.
Nous remercions A. Paternottre de nous autoriser à reprendre son texte et de faire découvrir à de nombreux collègues de Suisse romande son excellente revue *Math-Jeunes, Junior*. (Pour de plus amples renseignements, sur la SBPMef et ses revues, voir le site http://www.sbpm.be).]

Dans l'ensemble des nombres naturels, s'il est un sous-ensemble qui, depuis toujours, a fasciné les mathématiciens, c'est bien celui des nombres premiers.
A leur propos, il existe bien sûr des certitudes c'est-à-dire des propriétés démontrées. Mais il existe aussi pas mal d'incertitudes constituant autant d'énigmes qu'on tente toujours de tirer au clair de nos jours. Je vous propose donc un double mini-voyage dans l'univers des nombres premiers. Dans la première partie de cet article nous nous intéresserons aux certitudes et dans la seconde, aux incertitudes.

Et tout d'abord qu'est-ce qu'un nombre premier ?

Un nombre naturel est premier <=> il ne possède que deux diviseurs naturels distincts: lui-même et 1

Sur la base de cette définition, justifie que :

1°) Parmi les nombres premiers, le seul qui soit pair est 2.

2°) 0 et 1 ne sont pas des nombres premiers.

3°) Tout nombre premier d'au moins 2 chiffres possède 1, 3, 7 ou 9 comme chiffre des unités.

Rappelons aussi que plusieurs nombres naturels sont « *premiers entre eux* » si et seulement si leur seul diviseur naturel et commun est 1. Ainsi 4, 6, 15, 21 sont quatre nombres premiers entre eux.
Un ensemble de n nombres premiers distincts constitue-t-il aussi un ensemble de n nombres premiers entre eux ? La réciproque de cette affirmation est-elle vraie ou fausse ?

Quelques théorèmes relatifs aux nombres premiers :

Le théorème fondamental de l'arithmétique:

Tout nombre naturel non premier et supérieur à 1 peut s'écrire d'une seule manière sous la forme d'un produit de nombres premiers (non nécessairement distincts).

Ainsi : $231 = 3 \times 7 \times 11$;
$343 = 7 \times 7 \times 7 = 7^3$;
$27720 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 7 \times 11 =$
$2^3 \times 3^2 \times 5 \times 7 \times 11$

Peut-être as-tu utilisé ces « factorisations » lors de la recherche du PGCD (plus grand commun diviseur) et/ou du PPCM (plus grand commun multiple) de plusieurs nombres naturels.

A propos de factorisation, celle du produit des naturels *consécutifs* 714 et 715 est assez curieuse.
Observe : $714 = 2 \times 3 \times 7 \times 17$
et $715 = 5 \times 11 \times 13$
Donc $714 \times 715 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17$
c'est-à-dire le produit des 7 premiers nombres premiers.
D'autre part $2 + 3 + 7 + 17 = 5 + 11 + 13 = 29$ (nombre premier)

Combien y a-t-il de nombres premiers ?

Il existe une infinité de nombres premiers.

C'est le célèbre mathématicien grec **Euclide** (≈ 300 av J-C) qui, dans ses « Eléments », donne une démonstration élégante et convaincante de cette propriété. La voici :

Supposons que la suite des nombres premiers ne soit pas infinie. Cela revient à supposer, dit Euclide, qu'il existe un nombre naturel p qui soit le plus grand des nombres premiers. Envisageons alors le produit P de tous les nombres premiers, du plus petit (2)au supposé plus grand p:

$$P = 2 \times 3 \times 5 \times 7 \times \ldots p$$

P est évidemment divisible par chacun des facteurs premiers qui le compose.
Intéressons-nous au nombre naturel $P + 1$.
De toute évidence, on a : $P + 1 > p$. Mais alors $P + 1$ n'est pas premier puisque p est réputé être le plus grand des nombres premiers. Dès lors $P + 1$ est divisible par au moins un des facteurs premiers (notons-le q) figurant dans le produit P.
Conclusion : le nombre premier q divisant P et $P+1$ divise aussi la différence $(P + 1) - P = 1$, ce qui est absurde. Il n'y a donc pas un nombre premier p plus grand que tous les autres. Chapeau Euclide !

Deux théorèmes démontrés par Pierre de Fermat (Français ; 1601-1665)

Si p est un nombre premier qui ne divise pas le naturel n, alors $n^{p-1} - 1$ est divisible par p.

Ainsi 7 est premier et ne divise pas 4 $\Rightarrow 4^{7-1} - 1$ ou encore $4^6 - 1$ est divisible par 7.
Peut-on aussi affirmer que $4^7 - 4$, $10^{106} - 10^{100}, 14^6 - 1$ sont aussi divisibles par 7 ?

Ce théorème, appelé « petit théorème de Fermat », trouve une application pratique intéressante dans une méthode de décryptage d'un message codé.

Si p est un nombre premier de la forme $4n + 1$ alors p est d'une manière unique égal à $a^2 + b^2$. (n, a et b sont des nombres naturels non nuls). La réciproque n'est pas vraie.

Ainsi $(4 \times 7) + 1 = 29$ (nombre premier) $\Rightarrow$ $29 = 2^2 + 5^2$.
Par contre $10^2 + 11^2 = 221$ et $221 = 4 \times 55 + 1$. Cependant $221 = 13 \times 17$ n'est pas premier !

Un théorème démontré d'abord par Tchebytchev (Russe ; 1821-1894) puis par Erdös (Hongrois ;1913-1996)

Si n est un naturel > 1, alors il existe au moins un nombre premier entre n et 2n.

Il peut sans doute paraître évident qu'entre 25 et 50 par exemple, il existe au moins un nombre premier. Mais peut-on être certain qu'il en est de même entre 25^{70} et 2×25^{70} ? Ce théorème l'affirme.
Notons qu'en 1845, un théorème connu sous la dénomination « Postulat de Bertrand » existait déjà.
Il était proche mais un peu plus restrictif que le théorème précédent.

Un théorème démontré par Dirichlet (Allemand ; 1805-1859)

> ***Toute suite arithmétique infinie a,a+r,a+2r,a+3r,... dans laquelle le premier terme a et la raison r sont premiers entre eux, renferme une infinité de nombres premiers.***

Ainsi parmi les termes de la progression arithmétique 9, 20, 31,...de premier terme 9 et de raison 11
(9 et 11 sont premiers entre eux) , il y a une infinité de nombres premiers.
Invente d'autres suites arithmétiques renfermant une infinité de nombres premiers.

Comment obtenir tous les nombres premiers inférieurs à nombre naturel n donné ?

Si tu te réfères à l'article de *S.* Trompler du n°105 de MJJ, tu liras comment Eratosthène (-276,-194) filtrait une suite de nombres naturels consécutifs pour qu'il n'y subsiste que des nombres premiers. C'est une méthode simple, sûre et efficace mais qui exige pas mal d'écritures et de concentration. On l'appelle ***« crible d' Eratosthène »***.
Ce crible est une source d'inspiration pour découvrir un *algorithme* (c'est-à-dire une suite de consignes à suivre) débouchant finalement sur un programme d'ordinateur capable d'écrire tous les nombres premiers inférieurs à un nombre naturel donné. L'article de N. Vandenabeele qui suit le présent article est consacré à ce sujet. Il y sera aussi question d'un algorithme permettant de reconnaître si un nombre naturel donné est ou non premier.

Un petit clin d'œil pour terminer
(cette première partie[1])

Parmi les nombres naturels de 3 chiffres, 131 est assez sympathique. En effet 131, en plus d'être premier et palindrome (il se lit aussi bien de gauche à droite que de droite à gauche) possède aussi les qualités suivantes : La permutation de ses chiffres donnent les naturels 113 et 311 qui sont aussi premiers . De plus $1 \times 3 \times 1$, $1 + 3 + 1$, $1^2+3^2+1^2$, $1^3+3^3+1^3$, $1^4+3^4+1^4$ sont tous premiers.
Hélas cela s'arrête là !
....
(Deuxième partie[2])

Nous venons d'examiner quelques propriétés connues et démontrées des nombres premiers. Il faut cependant savoir que pas mal de zones d'ombre subsistent en ce qui les concerne. Si les mathématiciens soupçonnent certaines propositions d'être vraies, ils n'en sont pas moins réduits, faute de pouvoir les démontrer, à se contenter de les énoncer, de les vérifier sur de nombreux exemples et de tenter de les prendre en défaut.
Tant qu'une propriété n'est ni démontrée ni invalidée, on dit qu'elle est au stade de la ***conjecture***.
Voici quelques conjectures et incertitudes, toujours actuelles, qui concernent les nombres premiers:

Existe-t-il une expression algébrique capable d'engendrer tous les nombres premiers ?

A ce jour, la réponse est clairement « non ».
Pourtant plusieurs grands noms des mathématiques ont bien tenté de découvrir une telle expression :

Euler (Suisse ; 1707-1783) proposa l'expression $n^2 + n + 41$ qui, pour $n =$ 0,1, 2, 3, ... , 39 n'engendre que des nombres premiers. Hélas pour $n = 40$ cette expression vaut $40^2 + 40 + 41 = 40(40+1) + 41 = 41^2$ qui n'est évidemment pas un nombre premier . Cependant, en continuant à donner à n les valeurs 42, 43, 44...,un puissant ordinateur a cal-

1 L'article a été publié en deux parties dans *Maths-jeunes Junior*. no 112 et 113 (novembre 2005 et janvier 2006)

2 Voir note précédente

culé que l'expression d'Euler engendrait des nombres premiers inférieurs à 10^7 dans 47,5 % des cas, ce qui est quand même assez remarquable.

Mersenne (Français ; 1588-1648) pensait que l'expression $2^n - 1$ engendrait un nombre premier lorsque n est aussi un nombre premier. Il avait raison pour n = 2, 3, 5, 7. Mais il dut déjà déchanter pour $n = 11$. En effet $2^{11} - 1 = 2047 = 23 \times 89$.
Il prouva cependant qu'il avait raison pour n = 13,17 et 19.
Il est donc incorrect d'affirmer que si n est premier alors $2^n - 1$ l'est aussi.
Par contre il est correct d'affirmer que si $2^n - 1$ est premier alors n l'est aussi. En effet si n n'est pas premier, on peut poser $n = pq$ et on sait que $2^{pq} - 1$ est divisible par $2^p - 1$ et par $2^q - 1$.
Ainsi $2^n - 1 = 8191$ (nombre premier - vérifie-le) => n est premier. Que vaut n ?

La chasse aux nombres premiers de Mersenne pour des valeurs de n de plus en plus grandes débuta dès le 17e siècle :

En 1640, Fermat prouve que $2^{23} - 1$ n'est pas premier car divisible par 47. (vérifie-le sur une calculatrice).
En 1738, Euler montre que $2^{29} - 1$ n'est pas non plus premier car divisible par 233. Le même Euler, dans la foulée, montre par contre que $2^{31} - 1$ est un nombre premier.
Pendant une longue période, $2^{31} - 1$ restera le plus grand nombre premier de Mersenne connu.
En 1951, $2^{127} - 1$, un nombre de 39 chiffres, constituait le dernier record obtenu « à la main ».
De nos jours, les ordinateurs ont sensiblement accéléré la course aux grands nombres premiers.
En 2000, le plus grand nombre premier connu était $2^{6\,972\,593} - 1$, soit un nombre de 2 098 960 chiffres ! Il a fallu 12 600 ordinateurs reliés entre eux par internet pour pouvoir obtenir ce dernier résultat !

« C'est de la folie ! A quoi cela peut-il bien servir ? », me direz-vous. J'ai trouvé un début de réponse à cette question dans le n°120 de « Math-Jeunes » (janvier 2005). Voici ce qu'il y est dit : « l'utilisation du système de codage de messages secrets appelé *cryptosystème RSA* nécessite le choix par le destinataire du message de *deux grands nombres premiers distincts*. » Et l'auteur de l'article (Françoise Valette) d'ajouter : « *c'est-à-dire d'au moins 150 chiffres* » !
Pourquoi de si grands nombres premiers ? Parce que le codage des messages secrets doit être très fiable si on veut que la sécurité soit maximale dans une opération telle que le paiement d'une facture via une carte de crédit ou via internet. Alors ?...pas si fous qu'on ne pense ces matheux !

La conjecture de Goldbach (Allemand ; 1690 - 1764)

La somme de deux nombres premiers supérieurs à 2 est évidemment toujours un nombre pair. Pourquoi ?
Goldbach s'est posé la question de savoir si la réciproque était vraie. Faute de pouvoir la démontrer,(et elle n'est toujours pas démontrée aujourd'hui), il a proposé la conjecture suivante :

Tout naturel pair (>2)est la somme de deux nombres premiers.

Ainsi $4 = 2 + 2$; $6 = 3 + 3$; $8 = 3 + 5$; $10 = 3 + 7 = 5 + 5$; $12 = 5 + 7$; $34 = 3 + 31 = 5 + 29 = 11 + 23 = 17 + 17$; $60 = \ldots$; $96 = \ldots$
Certains nombres pairs ont donc plus de 2 décompositions en une somme de deux nombres premiers.
Un ordinateur peut vérifier que si p est un nombre **pair** et d le nombre de ses décompositions en une somme de deux nombres premiers alors :
$14 \leq p \leq 32 \Rightarrow d \geq 2$;
$34 \leq p \leq 74 \Rightarrow d \geq 3$ (sauf 68);
$76 \leq p \leq 200 \Rightarrow d \geq 4$ (sauf 98) ;
$200 \leq p \leq 500 \Rightarrow d \geq 6$;
$500 \leq p \leq 1000 \Rightarrow d \geq 10$;
$1000 \leq p \leq 2000 \Rightarrow d \geq 16$ ... etc.

Pour les nombres impairs, il existe aussi une conjecture analogue à celle de Goldbach :

Tout naturel impair (>1) est la somme d'au plus trois nombres premiers.

Ainsi : $3 = 3$; $5 = 3 + 2$; ... ; $25 = 23 + 2 = 19 + 3 + 3 = 17 + 5 + 3 = 13 + 7 + 5 = 11 + 7 + 7$.
Recherche d'autres décompositions.
Des recherches récentes (1989) ont démontré que cette conjecture est vraie lorsque le nombre impair est $< 10^{43000}$. Hélas cela ne suffit pas pour affirmer qu'elle est vraie quel que soit le nombre impair $> 10^{43000}$!

Répartition des nombres premiers dans l'ensemble des nombres naturels.

Si tu examines la suite des 625 premiers nombres premiers[3] tu peux en conclure qu'ils appartiennent tous à l'intervalle [1, 4637].
Avec de la patience, tu peux observer dans cette même suite que : l'intervalle [1, 100] comprend exactement 25 nombres premiers,

l'intervalle	[100,200]	en comprend	21
"	[200,300]	"	16
"	[300,400]	"	16
"	[400,500]	"	17

Tu l'auras compris, dans des intervalles de même « longueur », le nombre de nombres premiers est loin d'être le même. La répartition des nombres premiers dans l'ensemble des nombres naturels est donc assez chaotique. A ce jour, il n'existe pas de règle permettant de calculer la « distance » qui sépare un nombre premier de son suivant.
A la fin du 18e siècle, le grand mathématicien allemand C-F GAUSS (1777-1855) avait pressenti que les nombres premiers se raréfient au fur et à mesure qu'on progresse vers les très grands naturels. Il a même conjecturé le « Théorème des nombres premiers » qui ne sera démontré qu'un siècle plus tard et séparément par J. HADAMARD (Français ; 1865-1963) et C. de la VALLEE-POUSSIN (Belge ; 1866-1962). En 1949, P. ERDÖS (Hongrois ; 1913-1996) et A. SELBERG (Norvégien ; 1917-) en donnèrent une preuve élémentaire.
Pour appliquer ce théorème, il faut connaître la notion de *« logarithme népérien d'un nombre x (x > 0) qu'on note ln x »*. Tu n'aborderas cette notion qu'en 6e année. Sache seulement que ta calculatrice, grâce a sa touche « ln » donne directement la valeur de ln x. Par exemple ln 254 = 5,537. Voici l'énoncé du « Théorème des nombres premiers » :

Une valeur *approximative* du nombre de nombres premiers inférieurs à *x* est $\frac{x}{\ln x}$
et l'approximation est d'autant meilleure que *x* est grand.

Ainsi une valeur approximative du nombre de nombres premiers inférieurs à 4637 vaut $\frac{4637}{\ln 4637} \approx \frac{4637}{8,44} \approx 550$. Or on lit dans la liste des nombres premiers que 4637 est le 625e nombre premier. Le pourcentage d'erreur est donc de $\frac{100(630-550)}{550} = 14,5\,\%$.
De même une valeur approchée du nombre de nombres premiers inférieurs à 10^6 vaut $\frac{10^6}{\ln 10^6} \approx 72382$.

Or on sait (grâce aux ordinateurs) que le nombre exact de nombres premiers inférieurs à 10^6 est 78498.
Cette fois le pourcentage d'erreur n'est plus que 8,4 %.

Un deuxième préalable avant d'aller plus loin : la notion (facile) de « factorielle ».
Par définition : $n ! = 1 \times 2 \times 3 \times 4 \times \ldots \times n =$ produit des n premiers nombres naturels.
La notation « $n !$ » se lit « factorielle (de) n ».
Ainsi $5 ! = 1 \times 2 \times 3 \times 4 \times 5 = 120$.
Calcule la valeur de 10 !
$n !$ est donc divisible par 1, 2, 3, 4, 5, ... $(n - 1)$, n ainsi que par tout produit de 2, 3,... n facteurs choisis parmi les précédents.

3 Cette suite est donnée dans *Maths-Jeunes Junior* no 112. Elle n'est pas reproduite ici mais le lecteur pourra vérifier dans une table de nombres premiers.

Cela étant, *Il est possible de créer des intervalles de nombres naturels arbitrairement longs et ne comprenant aucun nombre premier. Observe l'intervalle suivant :*
[100! + 2 , 100! + 3 , 100! + 4, ... , 100! + 100].
Cet intervalle comprend exactement 99 naturels consécutifs. Aucun d'eux n'est premier.
En effet :
2 divise 2 ainsi que 100 !
Donc 2 divise 100! + 2 et dès lors
100 ! + 2 n'est pas premier.
3 divise 3 ainsi que 100 !
Donc 3 divise 100! + 3 et dès lors
100 ! + 3 n'est pas premier.
....etc
100 divise 100 ainsi que 100 ! .
Donc 100 divise 100 ! + 100 et dès lors
100 ! + 100 n'est pas premier.
Conclusion : l'intervalle écrit ci-dessus comprend 99 naturels consécutifs dont aucun n'est premier.

Si on avait pris $n = 5000$, on aurait obtenu un intervalle de 4999 naturels consécutifs et non premiers.
Il est donc possible, en prenant n assez grand, de créer de très longs intervalles de naturels consécutifs ne comprenant aucun nombre premier.

Une dernière incertitude.

Deux nombres premiers sont dits « jumeaux » si leur différence vaut 2. Ainsi 3 et 5, 5 et 7, 11 et 13 , 4517 et 4519 sont des paires de nombres premiers jumeaux.
On pense qu'il existe une infinité de telles paires mais on ne l'a jamais démontré !

Au royaume des nombres premiers, tout est donc loin d'être connu. C'est sans doute pour cela que, depuis l'Antiquité, les nombres premiers ont toujours fasciné les mathématiciens. Si, d'une part, leurs recherches ont été souvent fructueuses, ils sont conscients, d'autre part, qu'ils ont encore un long chemin à parcourir. Croisons donc les doigts !
Que les nombres premiers ne t'empêchent quand même pas de dormir !

4 Cet article est suivi d'un complément biographique, de Simone Trompler, qui, sur deux pages, donne une biographie de huit mathématiciens particulièrements liés au théorème des nombres premiers : Selberg, Erdös, Hadamard, Goldbach, Mersenne, La Vallée-Poussin, Euler, Gauss.

Cryptarithmes

Nous remercions M. Bernard Lamirel, qui nous envoie régulièrement ses cryptarithmes. Parmi ceux-ci, nous retenons les suivants, sur les thèmes actuels de la « bonne bouffe » et des méfaits des drogues dites légères.

a)		b)		c)	
MANGER		REPAS		TABAC	
+MANGER		+REPOS		+ALCOOL	
GROSSIR		SANTE		CANCER	

Le a), facile, vient du *Kangourou* ; le b) et le c), de plus en plus difficiles, sont des créations de M. Lamirel.
Les règles de ces opérations arithmétiques à reconstituer, sont toujours les mêmes :
- chaque chiffre est représenté par une même lettre,
- deux lettres différentes représentent deux chiffres différents,
- aucun nombre ne commence par le chiffre 0.

Solutions sur notre site http://www.math-ecole.ch