Bermudes

Reste de savoir

Nouveau roi des nombres mégapremiers

12 août 2019

Table des matières

Ce jeudi 7 janvier 2016, un tout nouveau nombre premier a été découvert. Quel est-il ? Comment a-t-il été découvert ? Pourquoi cherche-t-on des nombres de plus en plus gros ?

Nous allons tenter, dans cet article, de répondre dans la mesure du possible à ces questions. On va commencer par se rappeler ce qu'est un nombre premier (pour les plus rouillés), et on va ensuite explorer la technique qui a mené à la découverte du dernier nombre premier en date. Le mot de la fin sera consacré à l'état de l'art en terme de recherche de nombres premiers aujourd'hui.

1. Rappels et résultats élémentaires sur les nombres premiers

1.1. Définitions

Un bon point pour commencer cet article est de se rappeler de ce qu'**est** une nombre premier.

Définition : Un nombre premier est un nombre naturel (donc entier strictement positif) ayant exactement deux diviseurs, à savoir **1** et lui-même.

On sait donc que **-4** n'est pas premier car il est négatif et donc pas naturel, **1** n'**est pas** premier car il n'a qu'un seul diviseur, **6** n'est pas un nombre premier car ses diviseurs sont au nombre

de 4 (**1**, **2**, **3**, et **6**), et finalement **17** est un nombre premier car il est naturel et a exactement deux diviseurs (**1** et **17**).

En fonction du nombre de chiffres nécessaires à l'écriture (en base **10**) d'un nombre premier, on l'associe à différentes *familles*. Ces *familles* ne sont nullement rigoureuses d'un point de vue mathématique. C'est juste un nom qui permet de situer le nombre premier. Voici ces familles :

nombre minimum de chiffres	**nom de la *famille***
mille ($1000 = 10^3$)	nombres premiers titanesques (*titanic primes*)
dix mille ($10\,000 = 10^4$)	nombres premiers gigantesques (*gigantic primes*)
un million ($1\,000\,000 = 10^6$)	nombres mégapremiers (*megaprimes*)

À l'aide du titre, vous pouvez déjà avoir une idée de ce dont il va être question ici !

1.2. Leur utilité

Les nombres premiers fascinent une partie des mathématiciens, mais pourquoi donc ? On pourrait être amenés à se dire qu'un nombre ne pouvant pas être divisé ne sert pas à grand chose. Cependant, *que nenni* ! Les nombres premiers sont au centre du théorème fondamental de l'arithmétique[1] qui dit que tout nombre entier (donc positif ou négatif) peut être écrit comme un produit **unique** de nombres premiers. Je vous laisse vous en convaincre sur des exemples, la preuve est un peu technique et n'apporte pas grand chose.

De plus, pour les informaticiens, les nombres premiers sont **essentiels**. En effet, toute la théorie de cryptographie du système RSA que vous pouvez retrouver dans le cours de Vayel et Dominus sur ZdS ici est basée sur l'arithmétique modulaire des nombres premiers.

Il faut donc comprendre par cela que les nombres premiers sont précieux. De plus, en informatique, plus le nombre premier est grand, plus il est intéressant (tout cela est **très bien** expliqué dans le cours lié ci-dessus). On peut donc en comprendre la volonté (voire la nécessité ?) d'en chercher encore et encore.

1.3. La quantité de nombres premiers

Question en substance également plus qu'importante : *jusqu'où peut-on chercher des nombres premiers ?* Ou encore : *Combien de nombres premiers existe-t-il ?* La réponse est évidente pour certains, étrange pour d'autres mais elle est sûre : il existe une infinité de nombres premiers.

Pour faire un peu d'histoire (qu'on ne me dise plus que je vous noie dans les mathématiques !), il est important de préciser que c'est à Euclide que l'on doit les débuts de la recherche sur les nombres premiers. Euclide était un grec ayant vécu quelque part dans les alentours de 300 avant J.C. À l'époque, les mathématiques n'étaient pas telles qu'on les connaît aujourd'hui : les mathématiques grecques se limitaient à la géométrie. D'ailleurs, la définition de nombre

1. Il faut savoir que lorsque les mathématiciens ont une branche importante (calcul différentiel et intégral, algèbre, arithmétique, etc), ils aiment bien y appliquer un théorème central qu'ils appellent **fondamental** pour se souvenir qu'il est important.

premier que je vous ai donnée ci-dessus ne vient pas d'Euclide car lui définissait un nombre premier comme *un nombre ne pouvant être* ***mesuré*** *qu'à l'aide de l'unité*. Donc pour Euclide, les nombres étaient *mesurables* car ce qu'il connaissait en mathématique venait directement de la géométrie.

C'est également Euclide qui a *prouvé* qu'il existe une infinité de nombres premiers. La preuve en est relativement simple, c'est une preuve par l'absurde[2].

Preuve : Supposons qu'il existe un nombre fini n de nombres premiers que l'on appelle $p_1, p_2, \ldots, p_n$. Soit le nombre P défini par $P = 1 + p_1 \times p_2 \times \cdots \times p_n$. P a au moins un diviseur premier D différent de **1** (possiblement $P = D$). De plus, on sait qu'aucun des n nombres premiers ne le divise. Il y a une contradiction car D est un nombre premier n'étant pas répertorié dans l'ensemble fini des nombres premiers, ce qui implique qu'il n'existe pas un nombre fini de nombres premiers mais bien un nombre infini.

Le fait qu'il existe une infinité de tels nombres veut-il dire que nous chercherons des nombres plus grands encore et encore ? Fort probablement, oui : je vous l'ai subtilement gardé, mais les nombres que l'on trouve aujourd'hui ne sont pas réellement applicables avec l'informatique d'aujourd'hui.

1.4. Le fameux nouveau record

Afin de laisser un brin de suspens, je me suis bien gardé de vous dévoiler ce nombre dont il est question. Je ne peux malheureusement pas vous l'écrire ici... La raison en est simple : ça va être looooooooooong ! En effet, ce nombre premier fait plus de 22 millions de chiffres !

La seule manière que j'ai de vous le donner est le suivant : $P = 2^{74\,207\,281} - 1$. Pour les amis du binaire, cela veut dire qu'en base **2**, ce nombre s'écrit par une succession de 74 millions, 207 mille et 281 fois le symbole **1**, et donc qu'il faut 74 millions de bits pour le stocker ($\simeq$ 10 Mo).

Comment sait-on qu'il est premier, comment l'a-t-on trouvé, sommes-nous sûrs à 100% que ce nombre est premier ? Ces questions concernent la section suivante. Elle risque d'être légèrement plus technique, mais le but n'est pas d'en faire une succession brutale de formules et de démonstrations, ne vous inquiétez pas.

2. Trouver de nouveaux nombres premiers

2.1. Crible d'Ératosthène

Une méthode que l'on doit à Ératosthène (2^{e} siècle avant J.C.) pour trouver les nombres premiers inférieurs à un nombre arbitraire n est appelée le *crible d'Ératosthène*. L'idée est de se faire un

2. Le principe est de supposer quelque chose de faux (dans notre cas : il existe un nombre **fini** de nombres premiers et de n'utiliser que des raisonnements logiques afin d'arriver à une contradiction qui indique que la supposition (l'*hypothèse*) est fausse.

tableau avec tous les nombres de **1** (non-compris car on sait qu'il n'est pas premier) à n, et sur chaque case, on laisse la place pour un marquage. Ensuite :

- on prend le premier nombre non-marqué (en l'occurrence, **2**) ;
- on l'ajoute à la liste des nombres premiers et on marque tous ses multiples dans le tableau ;
- on prend le premier nombre non-marqué (en l'occurrence **3** car **2** est déjà marqué) ;
- on l'ajoute à la liste des nombres premiers et on marque tous ses multiples dans le tableau ;
- on prend le premier nombre non-marqué (en l'occurrence **5** car **2**, **3** et **4** sont déjà marqués) ;
- on l'ajoute à la liste des nombres premiers et on marque tous ses multiples dans le tableau ;
- etc...

En répétant cela tant que le premier nombre marqué est inférieur ou égal à n, on obtient tous les nombres premiers inférieurs où égaux à n.

Cette méthode est une des plus connues car **très** efficace pour générer tous les nombres premiers inférieurs à un nombre **relativement** petit. Cependant, vous vous doutez bien, qu'il est compliqué de se faire un tableau de $2^{74\,207\,281}$ nombres entiers, ce qui ne tiendrait ni sur une feuille, ni dans une mémoire d'ordinateur. Il faut donc trouver d'autres méthodes.

!(https ://jsfiddle.net/rvujwmwv/17/)

2.2. Méthode brute

Il y a la méthode brute qui permet de tester un seul nombre à la fois (sans devoir gérer tout un tableau). Le principe est d'avoir le nombre en question (appelons le p) et de regarder pour tous les entiers d inférieurs ou égaux à $\sqrt{p}$ si d divise p. On peut y voir un avantage car il n'y a qu'un seul nombre à placer en mémoire, cependant, le problème ici est que tenter $2^{37\,000\,000} \simeq \sqrt{2^{74\,207\,281}}$ diviseurs distincts risque d'être plutôt long.

Il faut donc trouver des méthodes nous donnant des nombres premiers avec une plus haute probabilité que simplement prendre un nombre impair au hasard (obligatoirement impair car le seul nombre pair et premier est **2**) ou alors une méthode permettant d'affirmer plus facilement la primalité d'un nombre.

2.3. Les nombres de Mersenne

Les nombres dits *de Mersenne* sont des nombres sous la forme $2^n - 1$. Ils doivent leur nom au moine français (si si !) Marin Mersenne (17^{e} siècle) que l'on peut voir sur l'image suivante :

FIGURE 2. – Marin Mersenne

Cet homme s'était tout de même rendu compte qu'en faisant une suite de nombres sous la forme $2^p - 1$ où p est premier, il obtenait une plus grande proportion de nombres premiers.

Le tout nouveau nombre premier est un nombre de Mersenne. De plus, ces nombres ont pour habitude d'être noté M_n où n est la puissance de **2** utilisée. La notation de ce nouveau nombre premier est donc $M_{74\,207\,281}$.

Avec les nombres de Mersenne, on sait que si n n'est pas premier, alors M_n n'est pas premier non plus. Cependant le fait que n soit premier n'implique pas que M_n le soit également. Par exemple, on sait que **11** est un nombre premier, or $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier.

Les nombres de Mersenne nous donnent une séquence qui a l'air de générer des nombres premiers. Cependant, il faut toujours pouvoir être capable de déterminer si oui ou non le nombre est **effectivement** premier. Dans le cas d'un nombre de 22 millions de chiffres, c'est toujours aussi compliqué de tester tous ses diviseurs potentiels. On utilise donc des résultats importants d'arithmétique modulaire tels que le petit théorème de Fermat.

Il y a certains résultats permettant de savoir si un nombre **n'est pas** premier comme énoncé ci-dessus. En effet, si on prend un naturel n non premier car il est divisible par un autre naturel m (différent de **1**), alors on sait que le nombre de Mersenne M_m divise M_n et donc M_n n'est pas premier.

Contenu masqué n°1

2.4. Test de Lucas-Lehmer

Le résultat précédent nous permet de ne pas tester de nombres inutiles car il y a un moyen d'être sûr que le nombre n'est pas premier. Cependant, savoir qu'un nombre n'est pas premier n'est pas suffisant dans la quête des nombres premiers. Il faut effectivement un moyen de savoir si le nombre **est** effectivement premier. Et comme dit plus haut, tester tous les diviseurs potentiels peut être possible pour de petits nombres, viables pour des nombres moyens, mais totalement impensable pour des nombres de l'ampleur des nombres premiers trouvés à ce jour.

Un des tests utilisés aujourd'hui est appelé « test de Lucas-Lehmer » et doit son nom aux mathématiciens Édouard Lucas (français du 19e siècle) et Derrick Henry Lehmer (américain du 20e), illustrés ci-dessous.

FIGURE 2. – Édouard Lucas (à gauche) - Derrick Lehmer (à droite)

2.4.1. Suites et récurrences

Avant de pouvoir expliquer le fonctionnement du test, il est nécessaire de savoir ce qu'est une suite. Faisons donc un court rappel.

Définition : Une suite (dans un ensemble $\mathbb{E}$) est une *liste* infinie de valeurs $x_i \in \mathbb{E}$ indicées par $i \in \mathbb{N}$. On la note (x_i) ou plus explicitement $(x_i)_{i\in\mathbb{N}}$.

Pour les intéressés, je ne m'attarderai pas ici sur le fonctionnement ou sur les utilisations des suites. Je redirige donc vers le cours de Mewtow, Holosmos et Vayel en parlant.

Une suite peut-être définie de manière directe afin de trouver directement l'élément indicé n de la suite. Par exemple :

$$x_n = 3\log_2(n) - 1.$$

De là, il est possible de trouver $x_1 = -1$, $x_4 = 5$, mais également x_n pour tout n, il *suffit* de remplacer n dans la formule afin d'obtenir le résultat.

D'autres suites sont définies autrement. On parle de définition par récurrence. Le principe est de définir l'élément indicé n par l'élément indicé $n-1$. Par exemple :

$$\begin{cases} x_n = x_{n-1} + x_{n-2} \\ x_0 = 0, x_1 = 1 \end{cases}$$

Je suppose que la plupart d'entre vous reconnaîtra la célèbre *suite de Fibonacci*. Maintenant, parlons du rapport entre les suites et la recherche de primalité d'un nombre.

2.4.2. Suite de Lucas-Lehmer

Il existe une suite portant le même nom que le test : la suite de Lucas-Lehmer. Cette suite (que nous allons noter (L_n) avec L pour Lucas, ou Lehmer, au choix) est définie par récurrence comme suit :

$$\begin{cases} L_0 = 4 \\ L_n = (L_{n-1})^2 - 2 \end{cases}$$

Ce qui veut dire, globalement que pour déterminer les éléments de cette suite, on procède comme suit : on commence avec le nombre **4**. Ensuite, on le met au carré et on retire **2** ce qui fait **14** (**16** - **2**). Après, on prend ce même nombre, et on le met au carré et on y retire **2** ce qui fait **194** (**14** au carré donne **196**). On réitère ce procédé jusqu'au nombre voulu.

Vous remarquerez que cette suite croit très vite car on met à chaque fois le nombre au carré. Le nombre de chiffres composant le nombre L_n est donc (approximativement !) le double du nombre de chiffres dans L_{n-1}.

Cette suite qui peut sembler sans grande importance a une propriété étonnante qui est que pour déterminer si un nombre $M_n = 2^n - 1$ est premier, il faut et il suffit que L_{n-2} soit un multiple de M_n. Par exemple, on sait que $M_5 = 31$ est un nombre premier. Trouvons donc le 3e nombre de la suite de Lucas-Lehmer :

$$L_3 = L_2^2 - 2 = 194^2 - 2 = 37634 = 1214 \times 31.$$

Donc effectivement M_5 est un nombre premier. Malheureusement, le nombre L_3 est déjà un nombre à **5** chiffres. Donc les éléments de la suite (L_n) sont beaucoup plus grands que ceux de la suite (M_n). Donc ça ne nous arrange pas beaucoup : pour déterminer si un nombre déjà très grand est premier, il faut en plus passer par un nombre bien plus grand et tester s'il en est un diviseur. Ça n'aide pas. Pourtant, je vous ai dit que le test de Lucas-Lehmer est un test qui est massivement utilisé aujourd'hui. C'est donc qu'il y a une astuce. Et effectivement, astuce il y a !

Une manière équivalente pour dire que M_n divise L_{n-2} est de dire que le reste de la division de L_{n-2} par M_n vaut **0**. Cette remarque va nous permettre de **largement** réduire les calculs. En effet, en transformant notre suite de Lucas-Lehmer ainsi :

$$\begin{cases} L_0 = 4 \\ L_n = (L_{n-1}^2 - 2) \mod M_n \end{cases}$$

Dès lors, si L_{n-2} vaut **0**, c'est que le reste de la division de L_{n-2} par M_n vaut **0**, ou encore que L_{n-2} est un multiple de M_n. C'est (à quelques optimisations près) la méthode utilisée pour tester la primalité des nombres de Mersenne.

2.5. Nombres de Fermat

Si les nombres de Mersenne sont nommés par rapport à Marin Mersenne, les nombres de Fermat sont nommés par rapport à... Pierre de Fermat ! C'est bien, je vois qu'il y en a encore deux/trois qui suivent.

Tout comme Mersenne, Fermat était un mathématicien français du 17e siècle. Il a **énormément** travaillé sur la théorie des nombres et on lui doit certains résultats très importants (dont le petit théorème **de Fermat** et le dernier théorème **de Fermat**)[3]. Il a, entre autres, travaillé sur les nombres premiers, tout comme Mersenne.

3. Ce n'est pas ma faute si les mathématiciens ne sont pas très originaux sur les noms qu'ils donnent aux résultats...

FIGURE 2. – Pierre de Fermat

Mersenne s'était tout particulièrement intéressé aux nombres sous la forme $2^n - 1$, et Fermat s'était plutôt intéressé aux nombres sous la forme $2^n + 1$. Ça semble léger comme différence... et pourtant !

Un résultat montre que si un nombre sous la forme $2^n + 1$ est premier, il faut que n n'ait pas de facteur premier impair et donc soit une puissance de deux.

Contenu masqué n°2

Les nombres de Fermat sont donc notés F_n et sont sous la forme $2^{(2^n)} + 1$. C'est Fermat qui a commencé à y chercher des nombres premiers, et il en a trouvé : la suite donne : $F_0 = 3$ qui est premier, $F_1 = 5$ qui est premier également, $F_2 = 17$ qui est toujours premier, $F_3 = 257$ qui est effectivement premier, $F_4 = 65\,537$ qui est... long... Et premier ! Fermat s'est arrêté là car au 17e siècle, trouver la valeur de $F_5 = 2^{32} + 1$, c'est long et embêtant, il n'y avait pas GMP ou Python à l'époque ! Fermat était donc tout content de lui et a conjecturé[4] que tous les nombres de la suite (F_n) sont premiers.

Malheureusement, c'est beau de conjecturer, mais le nombre F_5 n'est pas premier. En réalité, nous n'avons pas réussi à trouver un seul autre nombre premier de Fermat que ceux trouvés par Fermat ! Il n'y a cependant pas de preuve que ce sont les seuls, et il est actuellement conjecturé que les seuls nombres premiers de Fermat sont les nombres F_0 à F_4.

3. Les méthodes de recherche aujourd'hui

Dans la section précédente, j'ai tenté de vous expliquer brièvement par quelles techniques on pouvait déterminer *efficacement* si un nombre est premier ou non, et comment faire pour avoir plus de chances de tomber sur un nombre premier. Cependant, aujourd'hui, qui les cherche ces fameux nombres ?

3.1. Détenteur du record

Comme dit dans le titre, la découverte du nouveau nombre premier le plus grand est bien un **record**. Et ce record a été attribué à quelqu'un : le Dr. Curtis Cooper de l'université du Missouri

4. En mathématique, une conjecture est une affirmation (au même titre qu'un lemme, un théorème ou une proposition) n'étant pas démontré mais que l'on a de bonnes raisons de croire vraie. Certaines conjectures se voient démontrées avec le temps (la conjecture de Poincaré par exemple), d'autres se voient réfutées (la conjecture d'Euler par exemple), et d'autres sont toujours en cours (la conjecture de Riemann par exemple).

(dans le... Missouri). C'est également lui qui avait le dernier record (en 2013). C'est même son 4e record de nombre premier ! On peut tout de même se demander comment il a fait.

3.1.1. La recherche informatique

Vous vous doutez que ce n'est pas le Dr. Cooper qui a calculé la suite de Lucas-Lehmer jusqu'au 74 millionième terme mais bien qu'il a utilisé un ordinateur. Il en a même utilisé plusieurs ! Pour faire court, ce professeur a eu l'autorisation par son université d'utiliser plus ou moins 800 ordinateurs des labos quand ils ne sont pas utilisés. Mais comment ces ordinateurs communiquent entre eux pour se répartir le travail ?

3.1.2. GIMPS

Le programme utilisé pour déterminer ce nombre de Mersenne (et plus généralement les 10 plus grands nombres premiers connus !) est appelé GIMPS. C'est un acronyme signifiant *Great Internet Mersenne Prime Search*, ce qui peut se traduire en « Grande recherche de nombres premiers de Mersenne par internet ». Ce programme est en téléchargement libre et gratuit sur le site officiel www.mersenne.org afin que tout le monde puisse participer à la recherche chez soi ! Il a débuté en 1996, ce qui lui donne tout de même une vingtaine d'années et ce qui en fait , selon cette page un des premiers systèmes distribués sur internet.

Ce programme doit être lancé, puis une fois connecté et identifié, le programme récupère de l'information à traiter par internet, ensuite l'ordinateur la traite (globalement il calcule les éléments de la suite de Lucas-Lehmer) puis renvoie la donnée au serveur une fois l'opération terminée.

3.1.3. Alternatives à GIMPS

Bien que GIMPS soit en quelque sorte le chercheur de nombres premiers le plus connu car c'est lui qui a permis de trouver les 10 plus grands, il n'est pas le seul. Il existe par exemple Prime95 qui cherche également les nombres de Mersenne avec la suite de Lucas-Lehmer.

On peut également citer PrimeGrid, un des nombreux sous-programmes de BOINC, le système distribué de Berkley. PrimeGrid diffère un brin de GIMPS car il ne recherche pas les mêmes nombres premiers : PrimeGrid ne cherche pas des nombres de Mersenne mais des nombres de Cullen (sous la forme $C_n = n2^n + 1$) ou des nombres premiers factoriels (sous la forme $P_n = n! \pm 1$), etc.

Nous avons donc vu comment les nombres premiers sont trouvés. J'espère que cet article vous a un peu éclairé et que vous l'avez trouvé intéressant. Retenons que les nombres premiers, c'est bien ! C'est utile ! Mais que les derniers trouvés ne nous serviront pas de si tôt !

4. Pour aller plus loin, liens et sources

Pour ceux qui seraient intéressés par les nombres de Mersenne :

- quelques informations globales ;
- des infos sur Lucas-Lehmer : *Sur les bonnes valeurs initiales de la suite de Lucas–Lehmer*, Deschamps Bruno ;
- La référence de GIMPS ;
- une preuve sur le fonctionnement de Lucas-Lehmer : *A Really Trivial Proof of the Lucas-Lehmer Test*, J. W. Bruce.

Concernant le record :

- Une interview de Curtis Cooper par Matt Parker ;
- quelques records .

Et une retranscription (en anglais) de l'œuvre d'Euclide (*Éléments*) peut se trouver ici .

Pourquoi chercher de tels nombres ? À lire ici .

Contenu masqué

Contenu masqué n°1

Cela peut se montrer en un développement (en supposant $n = mt$) :

$$= \sum_{k=0}^{t-1} (2^m - 1)\,(2^m)^k = (2^m - 1) \sum_{k=0}^{t-1} 2^{mk} = M_m \sum_{k=0}^{t-1} 2^{mk}$$

Où, par la formule de la somme d'une suite géométrique, on a :

avec $u_k = u_0 q^k$.

On a un produit de deux nombres entiers différents de M_n, on en conclut que M_n n'est pas premier. Retourner au texte.

Contenu masqué

Contenu masqué n°2

Prenons un nombre n qui n'est pas une puissance de deux, et qui a donc au moins un facteur impair $s \neq 1$ tel que $n = st$. Alors :

$$= 2^t \sum_{i=1}^{s} 2^{t(i-1)}(-1)^{s-i} - \sum_{i=0}^{s-1} 2^{ti}(-1)^{s-i} = 2^t \sum_{i=0}^{s-1} 2^{ti}(-1)^{s-1-i} + (-1) \sum_{i=0}^{s-1} 2^{ti}(-1)^{s-i} = 2^t \sum_{i=0}^{s-1} 2^{ti}(-1)^{s-1-i} + \sum_{i=0}^{s-1}$$

où $(-1)^{s-i+1} = (-1)^{s-i-1} \times (-1)^2 = (-1)^{s-i-1}$. En mettant la somme en évidence, on obtient :

On a un produit de deux nombres naturels donnant $2^n + 1$, on en déduit qu'il n'est pas premier.
Retourner au texte.