

# Une formule pour des nombres premiers

Simon Plouffe

En 1947, W. H. Mills publiait un article montrant une formule qui peut donner un nombre arbitraire de nombres premiers. Si  $A = 1.3063778838630806904686144926\dots$  alors  $\lfloor A^{3^n} \rfloor$  donne une suite arbitraire de nombres tous premiers. Ici  $\lfloor x \rfloor$  est le plancher de  $x$ . Plus tard en 1951, E. M. Wright en proposait une autre, si  $g_0 = \alpha = 1.9287800\dots$  et  $g_{n+1} = 2^{g_n}$  alors

$$\lfloor g_n \rfloor = \lfloor 2^{\dots 2^{2^\alpha}} \rfloor \text{ est toujours premier.}$$

Les premiers consécutifs sont uniquement représentés par  $\alpha$ . La suite de premiers est 3, 13, 16381,...

Le taux de croissance de ces 2 fonctions est assez élevé puisque le 4<sup>ème</sup> terme de la suite de Wright a 4932 chiffres décimaux. La croissance de celle de Mills est moins élevée, le 8<sup>ème</sup> terme a quand même une taille de 762 chiffres. Une série de formules est présentée ici qui minimise le taux de croissance et qui possède les mêmes propriétés de fournir une suite de premiers de longueur arbitraire. Si  $a_0 = 43.8046877158\dots$  et  $a_{n+1} = (a_n^{\frac{5}{4}})^n$  alors la suite  $S(n) = \{ a_n \}$  : l'arrondi de  $a_n$ , est une suite de premiers de longueur arbitraire. Ici l'exposant  $\frac{5}{4}$  peut être abaissé à  $\frac{11}{10}$ , ou même  $\frac{101}{100}$ . Si  $a_0$  est bien choisi il est conjecturé que l'exposant peut être aussi près de 1 que l'on veut. Lorsque l'exposant est  $\frac{3}{2}$  il est conjecturé que tous les nombres premiers peuvent être générés par une série d'arbres.

## Introduction

Y a-t-il une formule pour les nombres premiers ?

La réponse est oui et non. Tout d'abord qu'est-ce qu'on entend par formule ? Par exemple, une formule dite close comme celle trouvée par Euler en 1772,

$$p(n) = n^2 + n + 41$$

Pour  $n$  entre 0 et 39 produit 40 nombres premiers d'affilée : 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523 et 1601.

Elle est élégante et simple. François Dress et Bernard Landreau en ont trouvé une meilleure en 2010

$$\frac{n^6}{72} - \frac{5n^5}{24} - \frac{1493n^4}{72} + \frac{1027n^3}{8} + \frac{100471n^2}{18} - \frac{11971n}{6} - 57347$$

Qui est premier pour  $n = -42$  à 15. Il faut aussi mentionner que la recherche de ce polynôme a tout de même demandé 6 mois d'efforts avec une batterie d'ordinateurs.

Mais ?, est-ce donc si difficile de produire une formule qui en donne un bon paquet ? La réponse à cette question a été clouée une bonne fois pour toute avec la formule de Mills.

Il écrit en 1947, si  $\vartheta = 1.306377\dots$  alors la suite

$$\lfloor \vartheta^{3^n} \rfloor$$

produit une suite de premiers de longueur arbitraire, elle débute ainsi :

2, 11, 1361, 2521008887, ... . On prend ici la valeur plancher de  $\vartheta^{3^n}$ . Mais il faut dire également que le 20<sup>ème</sup> terme de la suite est de bonne taille : environ 6 milliards de chiffres.

E.M. Wright en 1951, réitère en en produisant une autre, si  $g_0 = \alpha = 1.9287800$  et  $g_{n+1} = 2^{g_n}$  alors

$$\lfloor g_n \rfloor = \lfloor 2^{\dots 2^{2^\alpha}} \rfloor$$

Donnera une suite de premiers aussi infinie, 3, 13, 16381, ... le 4<sup>ème</sup> terme fait plus de 4932 chiffres et personne n'a osé calculer le 5<sup>ème</sup>.

Donc, ces 2 suites produisent une infinité de nombres premiers mais bien sûr le taux de croissance décourage les plus téméraires.

Voici un petit tableau de chasse des formules et procédés pour les nombres premiers.

Auteur (s)	Année	Commentaire	Efficacité	Nombres de termes calculés
Erathosthène	-276 à -194	Crible d'exclusion	Pratique	Infini calculable
Mersenne	1536	Nombres premiers de la forme $2^p-1$ .	Pratique, exact	51
Fermat	1640	Petit théorème de Fermat	Produit des premiers probables faibles	Infini calculable
Euler	1772	Polynôme du second degré	Pratique	40
Mills	1947	Double exponentielle	Pratique	Moins de 10 termes
Wright	1951	Super exponentielle	Pratique	Moins de 5 termes
Wilson	Circa 1780	Formule qui utilise $p!$	Théorique	Très peu
Jones, Sato, Wada, Wiens	1976	Polynôme de degré 25 à 26 variables	Théorique	Très peu
John H. Conway	1987	FRACSTRAN	Théorique	Très peu
Rowland	2008	Récurrence	Théorique	Très peu
Dress, Landreau	2010	Polynôme de degré 6	Pratique	58
Benoit Perichon (et al).	2010	26 premiers en progression arithmétique	Pratique	26
Tomás Oliveira e Silva et al.	2019	Programme Primesieve, crible d'Érathosthène optimisé. Le plus rapide connu	Pratique	Infini calculable

On entend ici par infini calculable que le calcul ou procédé peut être fait jusqu'à ce que les ressources soient insuffisantes. Par exemple, le programme Primesieve est le plus rapide qui existe. Il peut produire tous les nombres premiers jusqu'à 1000 milliards enregistrés sur disque en 52 minutes sur un ordinateur moyen. Dans sa version courante la liste peut aller jusqu'à  $2^{64}$ , soit  $1,844 \times 10^{19}$  mais qui demande 4.1 exaotets d'espace pour être stocké. L'infini calculable en l'an 200 av J.C. est bien sûr une limite manuelle, la même chose s'applique à la limite calculable pour le petit théorème de Fermat.

Les nombres premiers produits par le petit théorème de Fermat sont probables et faibles. Si  $p$  est très grand, à toute fin pratique c'est un test probabiliste.

Les nombres de Mersenne sont limités par la taille de  $n$ , pour tester un seul exposant dans la liste des candidats on a besoin d'un ou 2 mois de calcul intensif sur un ordinateur puissant. La croissance de la fonction de Wright est supérieure à la double exponentielle puisque le 5<sup>ème</sup> terme est difficilement calculable même avec Mathematica installé sur un ordinateur puissant.

## Première approche

Le premier type à considérer est de construire une suite basée sur la représentation en base 10 avec par exemple,  $a_{n+1} = 10 a(n)$  avec  $a_0 = 7.3327334517988679$  on obtient 7, 73, 733, 7333, 73327, 733273... est une suite de premiers mais qui s'arrête faute de premiers de cette forme qui soient plus grands. C'est l'une des quelques unes connues et la plus étendue [10]. Si on utilise une autre base beaucoup plus grande mais de taille fixe elle est forcément prise à défaut éventuellement à cause de l'espace entre les nombres premiers qui s'agrandit.

Si on utilise une fonction qui croit plus rapidement comme  $n^n$  on obtient de meilleurs résultats, par exemple avec  $c = 0.26558837294314339089712945366546...$  et  $a_n = \lfloor cn^n \rfloor$ . Elle s'arrête au bout de 19 termes, ici  $a_3$  à  $a_{22}$ . C'est la meilleure qui a été trouvée à l'aide d'une méthode que nous expliquerons plus loin.

$a_n = 7, 67, 829, 12391, 218723, 4455833, 102894377, 2655883729, 75775462379, 2368012611049,$   
 $80440106764817, 2951219812933057, 116299525867995629$   
 $4899240744635092571, 219705395187452015923, 10449948501874965563651,$   
 $525445257345556693801913, 27848959374722952425334841,$   
 $1551723179991864497606172809$

Encore une fois pour les mêmes raisons, le procédé ne marche plus au bout d'un moment, cet exemple est le meilleur qui a été trouvé. La méthode utilisée est basée sur une programme maison à la Monte-Carlo qui utilise le principe du recuit (Simulated Annealing). Si une fonction croit trop lentement alors l'écart entre chaque nombre premier finit par avoir raison sur la formule.

La prochaine étape consiste alors à considérer des formules du type Mills ou Wright, celle de Wright a été écartée parce qu'elle croit trop vite. La question alors est y a-t-il un moyen d'obtenir une fonction qui croit juste assez pour produire une suite de premiers de longueur arbitraire ?

Considérons alors la récurrence  $a_{n+1} = a_n^2 - a_n + 1$ , dite de Sylvester, elle apparait dans le développement en fraction égyptienne du nombre 1. C'est la suite A000058 du catalogue OEIS et commence comme suit :  $a_0 = 2, a_n = 2, 3, 7, 43, 1807, 3263443, 10650056950807, \dots$   
 La suite a la propriété que

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{43} + \frac{1}{1807} + \frac{1}{3263443} + \dots$$

L'extension naturelle de cette formule est de se demander, si  $a_0$  est un réel, peut-on en trouver un qui produise des premiers ? Il suffirait d'utiliser la fonction plancher  $\lfloor x \rfloor$ . La réponse est oui, si  $a(0) = 1.6181418093242092$  alors

$$a(n) = 2, 3, 7, 43, 1811, 3277913, 10744710357637, \dots$$

La suite est intéressante en ceci qu'elle a une croissance bien moins élevée que la formule de Mills et encore plus que celle de Wright. Chaque terme a environ 2 fois la taille du précédent.

### Une famille de formules pour les nombres premiers

Peut-on choisir l'exposant dans la formule précédente de sorte que la croissance soit moins grande ? Ici, la longueur qui double à chaque terme nous donne que  $a(14) = 9.838 \dots \times 10^{1667}$ .

En remettant au four le procédé et en choisissant un exposant petit comme  $5/4$  on trouve assez rapidement : Si  $a_0 = 43.80468771580293481 \dots$  et en utilisant  $\{ x \}$ , l'arrondi de  $x$  on obtient  $S(n) = \{ a_n \}$  et

$$a_{n+1} = a_n^{\frac{5}{4}}$$

C'est maintenant la suite A323176 du catalogue OEIS,  $S_n = 113, 367, 1607, 10177, 102217, \dots$

Maintenant que ça semble fonctionner, ne peut-on pas prendre un exposant plus petit ? Si on choisit soigneusement  $a_0$  et un exposant plus petit, ça marcherait aussi ? Par exemple, si

$$a_{n+1} = a_n^{\frac{11}{10}}$$

Et  $a_0 = 1000000000000000000000000000000049.31221074776345 \dots$  on obtient la suite de premiers

10000000000000000000000000000000049  
 158489319246111348520210137339236753  
 524807460249772597364312157022725894401  
 3908408957924020300919472370957356345933709  
 70990461585528724931289825118059422005340095813  
 3438111840350699188044461057631015443312900908952333  
 489724690004200094265557071425023036671550364178496540501  
 ...

Et si on choisit l'exposant  $3/2$  et  $a(0) = 2.038239154782 \dots$  on obtient la suite de premiers



## Description de l'algorithme et méthode

Il y a 3 étapes.

- 1) On choisit la valeur de départ et l'exposant, préférablement une fraction simple.
- 2) On utilise Monte-Carlo et le recuit simulé, en français ça signifie qu'on ne garde que les valeurs qui sont des nombres et on ignore le reste. Une fois 4-5 valeurs trouvées c'est suffisant pour l'étape 3.
- 3) On utilise une formule qui permet soit d'aller vers l'avant ou l'arrière.

Vers l'avant : le plus petit nombre premier après  $\{ a(n)^\alpha \}$ .

Le nombre premier est facile à trouver même s'il a des milliers de chiffres. Maple permet d'avoir un premier très probable jusqu'à 10000 chiffres et PFGW permet d'avoir une taille allant jusqu'à 1 million de chiffres en quelques minutes.

Vers l'arrière : (pour vérifier que la formule fonctionne).

Nombre premier précédent = résoudre pour  $x$  avec  $x^\alpha - S(n+1)$ . Ici  $S(n+1)$  est le prochain nombre premier candidat, c'est ici que si  $\alpha$  est rationnel est plus aisé pour le calcul.

## Conclusions

Tous ces calculs sont empiriques. En terme pratique on arrive à générer un nombre arbitraire de nombres premiers et qui a une croissance minimale. Les formules sont bien plus économes que celles Mills et Wright. À un nombre premier donné on peut remonter jusqu'à 2 et à partir de 2 on peut obtenir une famille de suites infinies de premiers. Avec l'exposant 101/100 (voir appendice), on peut arriver à produire une suite de 100 nombres premiers, battant ainsi le record de 58 (polynôme) ou de 26 (premiers en progression arithmétique). La suite de 100 nombres premiers peut être étendue jusqu'à 1000000 de chiffres si on utilise PFGW (moyennant un certain temps de calcul). Les premiers sont tous des premiers probables lorsque la taille dépasse 20 chiffres.





018398322694298351939147983130015136908252323673866239520792574613411868677642235073704177013092547\  
469988942740792286178287439751171740781473269073892222500856819101508763905159436890713516706806073\  
230340709775247109962639304731268726673513194358760146498716630917326127104834470990855699126724423\  
364563400627298922622307293846063438117272268793768275879962254097799354158085762961064123057607966\  
160601776755818203159773936124656112065523115090064101111495353498206258795439413673812037278296733\  
645267287644097356076684710114796664999936120575287724837293697351493924409500224966132968519714416\  
842453707637954130055549264002324165047468473929271485946165503217356837601629639419879469016702185\  
282884953955978837040813769790737964024765936560132201947329589020684688103783508207953909226973353\  
311673228475465554368940907592962420614466784994981282960825721578943945413044348721413359994322887\  
267908768807338482433090925796834068237180403901988798369730955930342861808229822928384548983053573\  
536591973775077187971574678905969616118381414141776504673183500635532110860928139441058326506259628\  
5149447865883142706706104362406568168733890352436821318127

La liste complète des nombres premiers se trouve ici :

<http://plouffe.fr/Record%20100%20primes%20sequence.txt>

## Bibliographie

- [1] Encyclopedia of Integer Sequences, N.J.A. Sloane, Simon Plouffe, Academic Press , San Diego 1995.
- [2] Mills, W. H. (1947), *A prime-representing function*, *Bulletin of the American Mathematical Society* 53 (6): 604, doi:10.1090/S0002-9904-1947-08849-2.
- [3] E. M. Wright (1951). *A prime-representing function*. *American Mathematical Monthly*. 58 (9): 616–618. doi:10.2307/2306356. JSTOR 2306356.
- [4] The OEIS, Online Encyclopedia of Integer Sequences, sequences : sequences A051021, A051254, A016104 and A323176.
- [5] Wikipedia : formulas for primes (effective and non-effective formulas).  
[https://en.wikipedia.org/wiki/Formula\\_for\\_primes](https://en.wikipedia.org/wiki/Formula_for_primes)
- [6] Baillie Robert, The Wright's fourth prime:  
<https://arxiv.org/pdf/1705.09741.pdf>
- [7] Wikipedia : Le recuit simulé : [https://fr.wikipedia.org/wiki/Recuit\\_simul%C3%A9](https://fr.wikipedia.org/wiki/Recuit_simul%C3%A9)
- [8] Wikipedia : Simulated Annealing : [https://en.wikipedia.org/wiki/Simulated\\_annealing](https://en.wikipedia.org/wiki/Simulated_annealing)
- [9] László Tóth, A Variation on Mills-Like Prime-Representing Functions, ArXiv :  
<https://arxiv.org/pdf/1801.08014.pdf>
- [10] Makoto Kamada Prime numbers of the form  $7, 73$ , <https://stdkmd.net/nrr/7/73333.htm#prime>