a été calculée avec une bonne précision, elle vaut : 1,3063778838630806904686144926025712916784585156713644368053759966434...

Pour $n = 1$, on obtient 2 ; pour $n = 2$, 11 ; pour $n = 3$, 1361 ; pour $n = 4$, 2521008887, nombres qui sont premiers, comme on le vérifie sans peine. Hélas, la formule $[A^{3^n}]$, amusante et curieuse, est sans intérêt pratique, car pour l'utiliser il faut connaître A avec une grande précision, ce qu'aujourd'hui on ne sait obtenir qu'en calculant... les nombres premiers eux-mêmes. Il paraît improbable qu'on puisse calculer cette constante autrement qu'à partir des nombres premiers, mais il serait merveilleux d'y parvenir. Cette formule ne donne les nombres premiers que parce que l'information sur les nombres premiers est cachée dans la constante A... Dans la même veine, un résultat étrange a été démontré par G. Wright en 1951. Il existe une constante w telle que la formule : $f(n) = [2^{2^{2^{\cdot^{\cdot^{\cdot^{w}}}}}}]$, avec n exposants, fournit un nombre premier pour tout n supérieur ou égal à 1. La constante w, dénommée bien sûr constante de Wright, vaut 1,9287800...

La formule suivante – un peu plus compliquée – va faire comprendre pourquoi ni la formule de Mills ni celle de Wright ne sont autre chose que des curiosités : il existe une constante L (appelée parfois constante de Liouville-Erdös) telle que la formule : $[L \times 10^{n^2}] - [L \times 10^{(n-1)^2}]10^{2n-1}$ donne le n-ième nombre premier pour tout $n \geq 1$: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, etc. Cette formule non seulement ne donne que des nombres premiers (comme les deux précédentes), mais elle les donne tous dans l'ordre. L'escroquerie apparaît quand on voit la constante L :

L = 0,2003000050000007000000011000000000001300..., le n-ième nombre premier est placé en position n^2. Le détail du mécanisme de calcul est expliqué en figure 1.

PLUS DE TRICHE!

Ce type de formules étant une forme de tricherie, interdisons-nous d'utiliser des nombres réels qui peuvent cacher une infinité d'informations dans leurs décimales, infinité où l'on peut loger insidieusement tous les nombres premiers !

Peut-on, en respectant cette nouvelle contrainte, trouver une formule qui donne tous les nombres premiers ? Si on ne peut pas les obtenir tous dans l'ordre, on se contenterait de les avoir dans le désordre, avec des répétitions, ou même d'en avoir une infinité.

Ce qu'on a vu au début montre qu'on ne réussira qu'avec un symbolisme un peu plus riche que celui des polynômes. Proposons d'accepter le symbolisme naturel suivant considéré comme banal en algèbre et en arithmétique :

– [x] partie entière de x, définie comme l'arrondi à l'entier inférieur de x (déjà utilisée plus haut) ;

– $\sum$, pour la somme généralisée ; exemple $\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + ... + n^2$

– !, la notation factorielle définie par $n! = n(n-1)(n-2)...4.3.2.1$;

– | | la valeur absolue, définie par $|n| = n$ si $n \geq 0$ et $|n| = -n$ si $n \leq 0$.

Il est maintenant possible de trouver des formules qui ne «trichent pas». Le premier exemple est une formule qui donne tous les nombres premiers et qui pourtant comporte 37 symboles :

$$t(n) = 2 + n[1/(1 + \sum_{p=2}^{n+1} [(n+2)/p - [(n+1)/p]])] \qquad n \geq 0$$

Le fonctionnement de cette formule, due à Roland Yélé-hada, s'explique en quelques mots. Si $n + 2$ est un multiple de p, alors $(n + 2)/p$ est un entier q, et donc $(n + 1)/p = q - 1/p$. Il en résulte que $[(n + 1)/p] = q - 1$ et que $[(n + 2)/p - [(n + 1)/p]]$ est égal à 1. En revanche, si $n + 2$ n'est pas un multiple de p,

2. JUSTIFICATION D'UNE FORMULE POUR P_n

$P(i) = [((i-1)! + 1) / i - [(i - 1)! / i]]$; $P(i)$ vaut 1 si i est premier.

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0

$P_i(m) = \sum_{i=1}^{m} P(i)$; $P_i(m)$ est le nombre de nombres premiers ≤ m

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	7	7

$P_i(m) / n$

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	7	7
2	0,5	1	1	1,5	1,5	2	2	2	2	2,5	2,5	3	3	3	3	3,5	3,5
3	0,33	0,66	0,66	1	1	1,33	1,33	1,33	1,33	1,66	1,66	2	2	2	2	2,33	2,33
4	0,25	0,5	0,5	0,75	0,75	1	1	9	1	1,25	1,25	1,5	1,5	1,5	1,5	1,75	1,75
5	0,2	0,4	0,4	0,6	0,6	0,8	0,8	0,8	0,8	1	1	1,2	1,2	1,2	1,2	1,4	1,4
6	0,16	0,33	0,33	0,5	0,5	0,66	0,66	0,66	0,66	0,83	0,83	1	1	1	1	1,16	1,16

$[P_i(m) / n]$; [a] donne la valeur entière du nombre a

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	2	2	3	3	4	4	4	4	5	5	6	6	6	6	7	7
2	0	1	1	1	1	2	2	2	2	2	2	3	3	3	3	3	3
3	0	0	0	1	1	1	1	1	1	1	1	2	2	2	2	2	2
4	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
5	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1

min $([P_i(m)/n], 1) = g(n, m)$; min $(x,y) = (x + y - |x - y|)/ 2$
min donne le minimum des nombres entre ( ).

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1
5	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1

$g(n, m-1)$.

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	0	0	0	0	1	1	1	1	1	1	1	1	1	1	**1**	1	1
4	0	0	0	0	0	0	1	1	1	1	1	1	1	1	**1**	1	1
5	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1

$g(n, m) - g(n, m-1)$.

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	**1**	0	0	0	0	0

$m(g(n, m) - g(n, m-1))$. $\quad p_n = \sum_{m=2}^{n^2+1} m(g(n, m) - g(n, m-1))$.

m / n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**2**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	**3**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	**5**	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	**7**	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	**11**	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	**13**	0	0	0	0	0

3. UNE FORMULE POUR LES NOMBRES PREMIERS JUMEAUX

Les nombres premiers jumeaux sont les paires de nombres premiers dont la différence est 2, comme 11 – 13 ou 17 – 19. On ne sait toujours pas s'il existe une infinité de paires de nombres premiers jumeaux. En revanche, on sait que n est le premier élément d'une paire de nombres premiers jumeaux si et seulement si :

$$4((n-1)!+1) + n \text{ est un multiple de } n(n+2).$$

D'où l'on tire que $n + 3$ est le premier élément d'une paire de nombres premiers jumeaux si et seulement si :

$$4(n+2)! + n + 7 \text{ est un multiple de } (n+3)(n+5).$$

Il en résulte que la formule assez simple suivante engendre tous les nombres premiers jumeaux (sur le principe de la formule de Minac) :

$$j(n) = 3 + n\,[(4(n+2)! + n + 7)/(n+3)(n+5) - [(4(n+2)! + n + 6)/(n+3)(n+5)]].$$

Cette formule est amusante, car, bien qu'elle soit assez simple, personne ne sait si elle prend au total un nombre fini ou infini de valeurs différentes.

alors $[(n+2)/p - [(n+1)/p]]$ vaut 0. Autrement dit le sigma dans la formule compte le nombre de diviseurs de $n + 2$ compris entre 2 et $n + 1$.

De deux choses l'une :

– $n + 2$ est premier, alors le nombre de diviseurs de $n + 2$ entre 2 et $n + 1$ est 0, donc le crochet derrière $2 + n$ est [1/1], c'est-à-dire 1, et l'on a $t(n) = n + 2$, qui est bien un nombre premier.

– $n + 2$ n'est pas premier, alors le nombre de diviseurs de $n + 2$ entre 2 et $n + 1$ est supérieur à 1, donc le crochet derrière $2 + n$ vaut 0 et donc $t(n) = 2$, qui est bien un nombre premier.

La formule ne donne que des nombres premiers, les donne tous, mais très lentement et en répétant 2 trop souvent :
$t(0) = 2$, $t(1) = 3$, $t(2) = 2$, $t(3) = 5$, $t(4) = 2$, $t(5) = 7$, $t(6) = 2$, $t(7) = 2$, $t(8) = 2$, $t(9) = 11$, $t(10) = 2$, $t(11) = 13$, $t(12) = 2$, $t(13) = 2$, etc.

Le théorème de John Wilson (1741-1793), publié en 1770 par Waring, indique que $(p-1)! + 1$ est un multiple de p si et seulement si p est premier. Cela a conduit Minác à simplifier grandement la formule de Yéléhada, laquelle devient : $t(n) = 2 + n\,[((n+1)!+1)/(n+2) - [(n+1)!/(n+2)]]$.

Ce qu'on a gagné (seulement 36 symboles pour tous les nombres premiers et la disparition de l'utilisation de la notation sigma) est malheureusement compensé par une rapidité bien inférieure : la nouvelle formule passe par des factorielles dont le calcul est long.

D'autres formules n'ont pas les défauts des formules de Yéléhada et de Minác, qui ne fournissent pas les nombres premiers dans l'ordre. Les mathématiciens Minác et Willans ont imaginé une remarquable formule dont l'explication est nettement moins simple, mais qui cette fois donne tous les nombres premiers dans l'ordre et sans répétition. Cette formule de 52 symboles repose, elle aussi, sur le théorème de Wilson.

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, etc.

$$p_n = 1 + \sum_{m=1}^{2^n} [[n/(1 + \sum_{j=2}^{m} [((j-1)! + 1)/j - [(j-1)!/j]])]^{1/n}] \quad n \geq 1$$

La formule est merveilleuse : peu de gens imaginaient avant qu'elle soit publiée en 1995 qu'une telle formule pouvait exister. Est-elle utile ? Non, d'un point de vue pratique. En effet, si l'on utilise cette formule pour programmer une méthode de calcul des nombres premiers, on obtient un programme d'une rare inefficacité. J'ai tenté l'expérience : la formule fonctionne comme prévu par la théorie, mais, bien qu'utilisant un logiciel puissant et calculant avec un grand nombre de chiffres exacts, je n'ai pas pu aller au-delà de p_6. La figure 2 explicite en détail une formule légèrement plus complexe pour p_n, mais plus transparente et plus efficace.

Sur un plan théorique, ces formules sont cependant intéressantes, car elles montrent que l'ensemble des nombres premiers n'est pas compliqué : peu de symboles permettent de le représenter entièrement et dans l'ordre. Cette conclusion n'est pas une surprise pour les informaticiens, qui utilisent pour écrire leurs programmes des langages plus riches que ceux utilisés habituellement en algèbre et en arithmétique. Écrire une formule ou un programme n'est pas très différent : d'ailleurs le nom du langage Fortran qui fut l'un des premiers langages de l'informatique scientifique, est la forme contractée de *Formula Translation,* car il était considéré simplement comme un moyen d'écrire des formules mathématiques.

Si l'on réfléchit au problème des formules pour p_n, il faut admettre que finalement ce sont les informaticiens qui ont raison : il vaut mieux enrichir un peu le vocabulaire qu'on se donne : cela permet d'écrire des formules pour les nombres premiers (ou pour d'autres choses) qui ne sont pas seulement des exercices de virtuosité d'un intérêt incertain, mais qui retranscrivent fidèlement et sans détour des procédés de calcul ou des idées naturelles. La logique mathématique a depuis longtemps compris cela et propose un système de notation qui permet des définitions de p_n par des formules à la fois courtes, claires et efficaces.

Voici, dans le langage Maple (utilisé aujourd'hui dans les classes préparatoires scientifiques aux Grandes Écoles et dans les premiers cycles des universités), une formule de 165 caractères donnant à nouveau le n-ième nombre premier p_n. Ce programme est fondé uniquement sur la fonction a mod b, qui donne le reste de la division de l'entier a par l'entier b (la fonction «mod», offerte dans tous les langages de programmation actuels peut se définir par $a \bmod b = a - b\,[a/b]$).

```
premier := proc(n)
local p,k,d;
 if n=1 then 2
 else
  p:= 1; k:= 1;
  while k<>n do
   p:= p+2; d:= 2;
   while (d*d<=p) and
        (p mod d <>  0) do d:=d+1;od;
```

4. AUTRES FORMULES ÉTONNANTES

Voici quelques formules déconcertantes concernant les nombres premiers.

(A) Formules de Willans (1964) du nombre de nombres premiers inférieurs à m :

$$Pi(m) = \sum_{j=2}^{m} \sin^2(\pi((j-1)!)^2/j)/\sin^2(\pi/j).$$

$$Pi(m) = -1 + \sum_{j=1}^{m} [\cos^2(\pi((j-1)!+1)/j)].$$

(B) Formule due à G. Hardy, qui soutenait que les mathématiques n'ont pas à être utiles, mais seulement belles (c'est bien le cas de cette formule) :

$$\lim_{r\to\infty} \lim_{m\to\infty} \lim_{n\to\infty} \sum_{i=1}^{m} (1-(\cos((i!)^r \pi/N))^{2n})$$

est le plus grand facteur premier de l'entier N.

(C) Formule donnant le plus grand commun diviseur des entiers n et m, trouvée en 1997 par Marcelo Polezzi :

$$\text{pgcd}(m,n) = 2\sum_{i=1}^{m-1} [in/m] + (m+n) - mn.$$