Séminaire de philosophie et mathématiques

Paulo Ribenboim

# Les records des nombres premiers

*Séminaire de Philosophie et Mathématiques*, 1987, fascicule 8
« Les records des nombres premiers », , p. 1-25

<http://www.numdam.org/item?id=SPHM_1987___8_A1_0>

# LES RECORDS DES NOMBRES PREMIERS

**par**

**PAULO RIBENBOIM**

Tout le monde aime les records. Ils exercent une fascination et excitent l'imagination. Le célèbre *Livre Guinness de Records*, qui a eu une quantité surprenante d'éditions, est rempli d'informations et faits des plus curieux et intéressants.

Saviez-vous que la plus longue course en vélo a été réalisée par CARLOS VIEIRA, de Leiria, Portugal? Il a pédalé pendant 91 heures, sans arrêt, en couvrant la distance de 2407 km., du 8 au 16 juin 1983?

**Le saviez-vous? La plus grande pierre rétirée d'un corps humain, pesait 6,290 kg.; le sujet était une dame de 80 ans, à Londres en 1952.**

**Et ceci, que nous intéresse de plus près:**

**HIDEAKI TOMOYOKI, né à Yokohama, en 1932, a récité de mémoire 40000** décimales de $\pi$ ; il a pris 17 heures et 20 minutes pour son exploit, avec des interruptions totalisant 4 heures.

Si l'on parcourt le *Livre Guinness de Records* on se rend compte qu'il contient très peu de records scientifiques, encore moins sur les nombres.

Vous savez peut-être que j'ai écrit un livre intitulé *Le Livre des Records des Nombres Premiers*, qui a pour but de traiter les records et les exploits des mathématiciens dans ce domaine délaissé par le

Guinness.

L'histoire autour de ce livre vaut d'être racontée. Ayant suggeré à mon université la création d'une série de leçons spéciales pour des élèves des premiers cycles d'études, je devais leur faire une conférence sur un sujet à la fois accessible, et très attirant. L'idée m'était venue de parler des records des nombres premiers, ce qui dans leur esprit s'approchait des exploits athlétiques, sexuels et d'autres.

L'intérêt montré par les étudiants, a été bien supérieur à mon expectative. J'ai décidé d'écrire un texte basé sur mon exposé. D'abord court, ensuite, de plus en plus long, au fur et à mesure que j'apprenais des nouveaux faits et records. Les suggestions nombreuses et utiles de mes collègues m'ont permis de compléter mon ouvrage, dont vous pouvez connaître une version abregée, traduite en français et publiée par les Presses Universitaires de France.

Je dois avouer tout de suite que, au moment de mon exposé pour les étudiants, je ne connaissais que peu de théorèmes et de records de nombres premiers. Pour moi, ces faits, intéressants comme ils l'étaient, ne se trouvaient pas réliés les uns aux autres et apparaissaient comme des Théorèmes isolés. Il n'était pas clair comment ils faisaient partie d'une théorie.

Si je devais écrire un livre, ma première tâche serait d'organiser ce que j'aurais à présenter en une théorie cohérente.

On sait que, en peu de mots, la méthode scientifique consiste en deux processus:

1) l'observation, l'expérimentation - c'est *l'analyse.*

2) la formulation des lois et théorèmes et l'organisation des connaissances - c'est la *synthèse.*

Ma tâche pouvait être ainsi précisée: la *synthèse des faits connus sur les nombres premiers, avec un accent sur les records.*

L'originalité de mon travail serait, sans doute, l'exploration systématique de l'interface calcul-théorie.

Il n'y avait pas un besoin de justifier cette étude, nul n'ignorant le rôle des nombres premiers en théorie des nombres. Le théorème fondamental de l'arithmétique dit, en effet, que tout entier $n > 1$ s'écrit de façon unique (à l'ordre des facteurs près) comme produit de nombres premiers. Ceux-ci sont donc, comme les pierres de base, sur lesquelles s'appuie l'édifice de l'arithmétique.

*Comment organiser la th*éorie des nombres premiers?

Je précise cette question par des questions naturelles et bien définies, qui s'imposent tour à tour.

I) Combien y a-t-il des nombres premiers?

II) Comment produire des nombres premiers?

III) Comment reconnaître si un nombre donné est premier?

IV) Où trouver les nombres premiers?

D'autres chapitres de la théorie doivent être dédiés aux études suivantes:

V) Les types spéciaux de nombres premiers.

VI) Expérimentation et heuristique.

En ce qui concerne (I), je dirai qu'il existe une infinité de nombres premiers, et j'indiquerai des démonstrations. A cause de leur nature indirecte, subsiste le problème de production ou engendrement des nombres premiers, que je discuterai à la partie (II).

Une des questions plus en vogue aujourd'hui concerne la reconnaissance des nombres qui sont premiers. C'est l'objet de la partie (III).

C'est à la partie (IV), dédiée à la distribution des nombres premiers parmi les entiers, que l'on rencontre les théorè*mes* les plus profonds de la théorie.

Je ne m'allongerai guère sur les parties (V) et (VI), qui mériteraient beaucoup d'attention et rendraient cet exposé démesuré.

## PARTIE (I)

## COMBIEN Y A-T-IL DES NOMBRES PREMIERS

Comme on le sait, EUCLIDE a donné dans ses *Elément*s la démonstration de l'existence d'une infinité de nombres premiers. Voici comment.

Si $p$ était le plus grand premier, soit

$$p\# + 1 = \left( \prod_{q \le p} q \right) + 1$$

(produit des premiers $q \le p$ , plus 1)

Deux cas sont possibles.

a) Ou bien $p\# + 1$ est premier, et alors il existerait un premier

plus grand que $p$ .

b) Ou bien, $p\# + 1$ n'est pas premier.

Dans ce cas, un diviseur premier de $p\# + 1$ ne pourrait pas être égal à

aucun des nombres premiers $q \leq p$ , donc il serait plus grand que $p$ .

Dans les deux cas, l'hypothèse que $p$ soit le plus grand premier mène à une conclusion absurde. Ceci montre qu'il existe nécessairement une infinité de nombres premiers.

Il faut remarquer que cette démonstration indirecte ne permet pas de déduire une méthode d'engendrement des nombres premiers. En effet, la question suivante s'impose naturellement:

Est-ce qu'il existe une infinité de premiers $p$ tels que $p\# + 1$ soit premier?

Beaucoup de calculs par beaucoup de mathématiciens ont été dédiés à cette question.

**RECORD**

Le plus grand premier $p$ connu, tel que $p\# + 1$ soit premier, est $p = 13649$ ; $p\# + 1$ a 5862 chiffres. Ceci a été accomplie par H. DUBNER en 1987.

Il y a bien d'autres démonstrations de l'existence d'une infinité de nombres premiers; chacune révèle un aspect intéteressant sur l'ensemble des nombres premiers.

EULER a montré:

$$\sum \frac{1}{p} = \infty$$

(somme des inverses de tous les nombres premiers). Donc, il ne pourrait

pas exister seulement un nombre fini de nombres premiers.

Cette démonstration se trouve dans beaucoup de livres élémentaires de théorie des nombres ou d'analyse réelle.

Voici un commentaire intéressant. Pour tout $\varepsilon > 0$, aussi petit qu'on veut, on a

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+\varepsilon}} < \infty .$$

En quelque sorte, ceci pourrait s'interpréter en disant que les nombres premiers sont disposés plus proches les uns des autres, ou de façon moins clairsemée, que les nombres de la forme $n^{1+\varepsilon}$. (par exemple, les nombres $\frac{1}{n^2}$, dont la somme, calculée par Euler, est $\frac{\pi^2}{6}$ ) .

PÓLYA a aussi donné une démonstration très simple et élégante de l'existence d'une infinité de nombres premiers.

Il suffit de trouver une suite infinie de nombres naturels, deux à deux relativement premiers, évidemment, sans faire appel à l'existence d'une infinité de nombres premiers - fait qu'on veut justement établir.

La suite des nombres de FERMAT $F_n = 2^{2^n} + 1$ (pour $n = 0,1,2...$) jouit de cette proprieté, comme il est facile de vérifier. Donc, si $p_n$ est un nombre premier quelconque qui divise $F_n$, alors les nombres premiers $p_n$ sont deux à deux distincts.

Je considérerai à la partie (III) les nombres de FERMAT avec plus d'attention.

# PARTIE (II)

## LA PRODUCTION DES NOMBRES PREMIERS

Le problème est de trouver une "bonne" fonction $f : \mathbb{N} \to \{premiers\}$. On veut que cette fonction $f$ soit autant que possible facile à calculer, et qu'elle s'exprime de préférence au moyen de fonctions déjà bien connues.

On doit aussi imposer des conditions sur cette fonction. Par exemple:

*Condition* (a): $f(n)$ est égal au $n^{ième}$ nombre premier (en ordre croissant); ceci donnera une "formule" pour le $n^{ième}$ nombre premier.

*Condition* (b): si $n \neq m$ alors $f(n) \neq f(m)$ ; ceci donnera une fonction engendrant des nombres premiers, mais pas nécessairement tous les nombres premiers.

*Condition* (c): l'ensemble des nombres premiers coïncide avec l'ensemble des valeurs positives de la fonction; ceci est une exigence beaucoup moins stricte, et qui sera possible de satisfaire, d'une façon surprenante comme je l'indiquerai plus tard.

Pour commencer, je discute les formules pour le $n^{ième}$ nombre premier. Il y en a beaucoup! En fait, plusieurs parmi nous, à notre jeunesse, ont essayé quelquefois avec succès d'obtenir une formule pour le $n^{ième}$ nombre premier. Malheureusement, toutes ces formules ont un aspect en commun: elles expriment le $n^{ième}$ premier en utilisant des

fonctions des nombres premiers précédents qui sont difficiles à calculer. Donc, ces formules n'ont pas été utiles pour dériver des propriétés des nombres premiers.

Je veux tout de même citer, à titre d'illustration, une de ces formules. Elle est due à J.M. GANDI (1971), mathématicien prématurement disparu et qui a aussi travaillé sur le dernier théorème de Fermat - je le fais comme hommage à sa mémoire. La voici:

$$p_n = \left[ 1 - \log \log \left( \frac{1}{2} + S_n \right) \right] , \quad \text{où}$$

$$S_n = \sum_{r=1}^{n} \frac{(-1)^r}{p_{i_1} \cdots p_{i_r} - 1}$$

et $1 \leq i_1 < i_2 < \ldots < i_r \leq n - 1$ , $p_1 = 2$ , $p_2 = 3$ , ... étant la suite des nombres premiers (écrits en ordre croissant).

On voit comment il serait malaisé de calculer $p_n$ .

J'indiquerai maintenant une fonction génératrice de nombres premiers. E.M. WRIGHT (co-auteur avec G.H. HARDY du célèbre livre sur la théorie des nombres) a montré:

Si $\omega = 1.9287800...$ alors

$$f(n) = \left[ 2^{2^{\cdot^{\cdot^{\cdot^{\omega}}}}} \right] \quad \text{(avec n "deux")}$$

est égal, pour tout $n \geq 1$ , à un nombre premier. Ainsi $f(1) = 3$ , $f(2) = 13$ , $f13) = 16381$ , tandis que $f(4)$ serait très difficile à calculer et aurait plus de 5000 chiffres décimaux. Par ailleurs, la détermination exacte de $\omega$ dépend en dernière analyse de la connaissance des nombres premiers, ce que fait que cette formule soit dépourvue d'intérêt.

On pourrait se demander s'il n'existe pas de fonctions génératrices de premiers qui soient beaucoup plus simples. Pourquoi pas des polynômes?

Parce que on a le résultat négatif suivant:

Si $f \in \mathbb{Z}[X_1, \ldots, X_m]$, il existe une infinité de m-tuples d'entiers $(n_1, \ldots, n_m)$ tels que $|f(n_1, n_2, \ldots, n_m)|$ soit un nombre composé.

Il y a bien d'autres résultats négatifs du genre.

Par contre, on peut demander s'il y a des polynômes, même à une indéterminée ayant beaucoup de valeurs successives qui soient des nombres premiers.

Je précise.

Soit $q$ un nombre premier. Il faudra trouver un polynôme de degré 1, c.à.d. $f_q(X) = d\,X + q$, tel que ses valeurs en $0, 1, \ldots, q-1$ soient des nombres premiers - ceci produit une suite de $q$ premiers en progression arithmétique, avec différence $d$ et ayant terme initial $q$.

Pour des petites valeurs de $q$, c'est très facile:

| q | d | VALEURS |
|---|---|---|
| 2 | 1 | 2 3 |
| 3 | 2 | 3 5 7 |
| 5 | 6 | 5 11 17 23 29 |
| 7 | 150 | 7 157 307 ... 907 |

On ne sait pas démontrer que ceci est possible pour chaque nombre premier $q$.

Voici les records sur cette question:

**RECORD**

En 1986, G. LÖH a donné les plus petites valeurs de $d$, lorsque $q = 11, 13$:

$q = 11$ donne $d = 1536160080$ ;

$q = 13$ donne $d = 9918821194590$ .

On peut aussi envisager la question analogue d'existence de longues suites de nombres premiers en progression arithmétique.

**RECORD**

La plus longue suite connue de premiers en progression arithmétique consiste de 20 termes, le premier est

$a = 214861583621$ et la différence est

$d = 18846497670$. Découverts par J. YOUNG & J. FRY en 1987.

EULER a découvert des polynômes quadratiques ayant beáucoup de valeurs nombres premiers. Précisement, il a observé que si $q$ est un nombre premier, à savoir, $q = 2, 3, 5, 11, 17$ ou $41$, alors le polynôme $f_q(X) = X^2 + X + q$ est tel que $f_q(0)$, $f_q(1)$, ..., $f_q(q-2)$ sont des nombres premiers (évidemment $f_q(q-1) = q^2$ n'étant pas premier, la suite de valeurs premières successives est la meilleure qu'on puisse espérer). Ainsi, on obtient 40 nombres premiers lorsque $q = 41$ : 41, 43, 47, 53,..., 1447, 1523. 1601 .

Peut-on trouver des nombres premiers $q > 41$ avec la propriété indiquée? C'est une question très naturelle. L'existence d'une

infinité de tels premiers q permettrait d'engendrer des suites arbitrairement longues de nombres premiers.

Mais, le théorème suivant dit justement que ceci n'est pas le cas:

THEOREME. Soit q un nombre premier.

1) RABINOVITCH a montré en 1912 que les entiers $f_q(0)$ , $f_q(1)$ ,..., $f_q(q-2)$ sont tous premiers si et seulement si le corps quadratique imaginaire $\mathbb{Q}\left(\sqrt{1-4q}\right)$ a nombre de classes égal à 1.

2) En 1966 BAKER et STARK ont déterminé, indépendemment et sans ombre du doute (qui planait sur le travail de HEEGNER en 1952), tous les corps quadratiques imaginaires ayant nombre de classes égal à 1. Il en résulte que le nombre de classes de $\mathbb{Q}\left(\sqrt{1-4q}\right)$ est 1 si et seulement si $4q-1 = 7, 11, 19, 43, 67, 163$, c'est-à-dire, $q = 2, 3, 5, 11, 17, 41$ .

Ainsi, on arrive au *record absolu* (qui ne pourra jamais être dépassé!) suivant:

**RECORD**

$q = 41$ est le plus grand nombre premier tel que $f_q(0)$ , $f_q(1)$ , ... $f_q(q-2)$ sont des nombres premiers.

Il faut remarquer ici qu'un problème plutôt à l'allure innocente comme celui-ci ait eu besoin, pour sa résolution, de faire appel à des théories très sophistiquées. Je donne des détails dans mon article intitulé *Euler's famous prime generating polynomial and the class number of imaginary quadratic fields* (L'Enseignement Mathématique 34 (1988), 23-42).

Maintenant je tourne mon attention vers les polynômes dont les valeurs positives constituent l'ensemble des nombres premiers. Leur

existence, très surprenante, a été découverte par Yu. V. MATIJASEVIČ en 1971, en liaison avec le 10e problème de HILBERT. En explicitant la démonstration de MATIJASEVIČ, des tels polynômes ont pu être indiqués concrètement. Voici les records, qui dépendent à la fois du nombre d'indéterminées n et du degré d .

**RECORD**

| n | d | Année | |
|---|---|---|---|
| 26 | 25 | 1976 | J.P. JONES, D. SATO H. WADA et D. WIENS |
| 42 | 5 (Minimum) | 1976 | (Non explicite) |
| 10 (Minimum) | $1,6 \times 10^{48}$ | 1977 | Yu. V. MATIJASEVIČ (Non-explicite) |

## PARTIE (III)

## LA RECONNAISSANCE DES NOMBRES PREMIERS

Il faut le dire tout de suite: donné un nombre natural N quelconque, il est possible de reconnaître, en effectuant un nombre fini d'opérations, si le nombre N est premier. En effet, il suffit de diviser successivement N par chacun des nombres d , $1 < d < N$ - d'ailleurs on peut se borner à le faire par les nombres premiers d tels que $d^2 < N$ . Si chaque fois on obtient un reste non nul, alors N est premier. Le problème avec cette méthode est que le nombre d'opérations est considérable dès que N est grand.

Il s'agit alors de chercher un algorithme A, dont le nombre d'opérations effectuées sur les chiffres de $N$ reste borné par une fonction $f_A$ qui ne croit pas trop vite avec $N$ ; soit, $f_A(N)$ est bornée par un polynôme dans le nombre de chiffres $1 + [\log_{10} N]$ de $N$.

Ce problème reste toujours ouvert, c'est-à-dire, on ne sait toujours pas si un tel algorithme à temps polynomial peut exister, car on n'a pas encore démontré l'impossibilité, mais d'autre part, un tel algorithme (s'il existe) reste à découvrir.

Les efforts dans cette direction ont amené à plusieurs types d'algorithmes

{ Algorithmes pour des nombres arbitraires.
{ Algorithmes pour des nombres de forme spéciale.

{ Algorithmes justifiés.
{ Algorithmes basés sur des conjectures.

{ Algorithmes déterministes.
{ Algorithmes probabilistes.

J'explique maintenant ces termes, en les illustrant par des exemples.

Parmi les algorithmes applicables à des nombres arbitraires, je cite d'abord l'algorithme de MILLER (1975), dont la justification requiert l'hypothèse généralisée de Riemann. Pour cet algorithme, $f_A(N) \leq C\ (\log N)^5$ (où $C > 0$ est une constante); c'est donc un algorithme non-justifié à temps polynomial.

L'algorithme de ADLEMAN, POMERANCE & RUMELY (1983) est complètement justifié et le nombre d'opérations sur les chiffres est borné par

$$(\log N)^{C \log\log\log N} . \qquad \text{(C constante)}$$

Il n'est pas loin, en pratique, d'être à temps polynomial et il s'applique à des nombres arbitraires.

Les deux algorithmes précédents sont déterministes, au contraire de ceux que je vais considérer maintenant.

Il faut pour ceci considérer les nombres pseudo-premiers.

Soit a un entier, $a > 1$ . Si p est un nombre premier, alors par le petit théorème de FERMAT, $a^{p-1} \equiv 1 \pmod{p}$ . Par contre, un nombre $N > 1$ tel que $a^{N-1} \equiv 1 \pmod{N}$ peut fort bien être composé - et dans ce cas N s'appelle un *pseudo-premier en base* a (noté psp(a)). Par exemple, 341 est le plus petit psp(2).

A vrai dire, il existe une infinité de nombres pseudo-premiers en base $a > 1$ .

Parmi les nombres pseudo-premiers en base a il y en a ceux, appelée *fortement pseudo-premiers en base* a, qui vérifient une propriété supplémentaire; il en existe aussi une infinité.

Un algorithme A est dit *probabiliste* (ou un test probabiliste de primalité) lorsque l'application de A au nombre N indiquera soit que N est composé, soit que, avec une forte probabilité, N est premier.

Parmi les tests de ce type, je mentionne ceux de BAILLIE & WAGSIAFF, de SOLOVAY & STRASSEN, et de RABIN. Le premier, à l'image des autres, fait appel à des nombres "témoins". Soit $k > 1$ (par exemple $k = 30$) , Soient $a_1 = 2$, $a_2 = 3, \ldots$ $a_k$ des entiers, qui servent de témoins. S'il existe un témoin $a_i$ tel que N ne satisfait pas la congruence $a_i^{N-1} \equiv 1 \pmod{N}$ alors N est composé. Si aucun témoin

reconnait N comme étant composé. c.à.d. , si $a_j^{N-1} \equiv 1 \pmod N$ par $j = 1,2,\ldots, k$ , alors, avec une forte probabilité, N est premier.

Le test de RABIN est basé sur la même idée, les k nombres $a_i$ témoignement si N satisfait les congruences définissant les nombres fortement pseudo-premiers en base $a_i$ . Dans ce test, la conclusion est que soit N est composé, soit N est premier avec probabilité $1 - \frac{1}{4^k}$ ; si $k = 30$ , le test est incorrect seulement en un nombre parmi 100 000 000 de nombres.

Evidemment ces tests sont très faciles à appliquer.

Maintenant je tourne mon attention vers des tests de primalité qui s'appliquent à des nombres de la forme $N \pm 1$ , où l'on connait tous, ou beaucoup de facteurs premiers de N .

Les tests pour les nombres $N + 1$ sont basés sur des réciproques faibles du petit théorème de FERMAT. Ceux qui s'appliquent aux nombres $N - 1$ utilisent les suite de LUCAS.

Pour les nombres de FERMAT $F_n = 2^{2^n} + 1$ , PEPIN a montré en 1877:

$F_n$ est un nombre premier si et seulement si

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n} .$$

La recherche de la primalité des nombres $F_n$ a mené aux records suivants.

**RECORD**

$F_4$ est le plus grand nombre de FERMAT premier connu.

Le plus grand nombre de FERMAT, dont on connait la factorisation

en nombres premiers, est $F_{11}$ (BRENT & MORAIN, 1988). Le dernier (en date) nombre de FERMAT dont on a déterminé les facteurs premiers, est $F_9$ (A.K. LENSTRA & M. MANASSE, 1990).

$F_{23471}$ est le plus grand nombre de FERMAT dont on sait qu'il est composé; il a le facteur $5 \times 2^{23473} + 1$ (W. KELLER, 1983).

$F_{22}$ est le plus petit nombre de FERMAT dont on ne sait pas s'il est premier ou composé.

Je passe aux nombres de MERSENNE $M_q = 2^q - 1$ (où $q$ est premier).

Pour ces nombres on applique le test de LUCAS (1878).

Soit $S_0 = 4$ , $S_{k+1} = S_k^2 - 2$ (pour $k \geq 0$) . Alors:

$M_q$ est un nombre premier si et seulement si $M_q$ divise $S_{q-2}$ .

Ce test a permis de découvrir des très grands nombres premiers.

**RECORD**

On connait à présent 31 nombres de MERSENNE premiers, le plus grand étant $M_q$ , avec $q = 216091$ , qui a été découvert par D. SLOWINSKI en 1985; ce nombre a 65050 chiffres et évidemment on ne saurait pas tester la primalité d'un nombre aussi grand, s'il n'était pas d'une forme spéciale.

Le dernier (en date) nombre de MERSENNE reconnu comme premier fut $M_q$ , avec $q = 110503$ (par W.N. COLQUITT & L. WELSCH, JR., EN 1988).

Le plus grand nombre de MERSENNE composé connu est $M_q$ , avec $q = 39051 \times 2^{6001} - 1$ (découvert par W. KELLER, 1987).

Pendant longtemps (depuis 1876) lorsque E. LUCAS a montré que

$M_{127}$ est premier, le titre de "plus grand nombre premier connu" est toujours revenu à un nombre de MERSENNE.

Mais cela n'est plus vrai!

**RECORD**

Le plus grand nombre premier connu aujourd'hui est

$$391581 \times 2^{216193} - 1 .$$

Sa découverte en 1989 est due à six mathématiciens, dont le premier en ordre anti-alphabétique (pourquoi pas?) est S. ZARANTONELLO. Les cinq autres sont J. SMITH, G. SMITH, B. PARADY, L.C. NOLL et J. BROWN.

## PARTIE (IV)

## LA DISTRIBUTION DES NOMBRES PREMIERS

A présent, nous savons:

1) Il existe une infinité de nombre premiers.
2) Il n'y a pas de formule raisonnablement simple pour les nombres premiers.
3) On peut reconnaître si un nombre pas excessivement grand est premier.

Mais que peut-on dire sur la manière dont les nombres premiers se distribuent parmi les nombres naturels? A ce propos, j'ai dit quelque chose de vague après la démonstration d'EULER d'existence d'une infinité de nombres premiers - ils forment un ensemble plus clairsemé que celui des carrés (par exemple).

Une idée très simple pour aborder la distribution des nombres premiers consiste à compter le nombre des nombres premiers inférieurs à un nombre donné. Pour tout nombre réel $x > 0$ , on désigne par

$$\pi(x) = \#\{p \text{ premier} \mid p \leq x\} ;$$

$\pi(x)$ est *la fonction qui compte les nombres premiers.* On étudie le comportement de $\pi(x)$ , qui est assez irrégulière, en la comparant avec des fonctions plus simples. Cette étude mène à des résultats de nature asymptotique.

Déjà à l'âge de 15 ans, par l'observation des tables de nombres premiers, C.F. GAUSS a suggéré que

$$\pi(x) \sim \frac{x}{\log x} ,$$

c.à,d. , la limite (lorsque $x$ tend vers l'infini) de $\frac{\pi(x)}{x/\log x}$ existe et est égale à $1$ .

Une formulation équivalente est la suivante:

$$\pi(x) \sim \int_1^x \frac{dt}{\log t}$$

(cette dernière fonction s'appelle *l'intégrale logarithmique* et se note $Li(x)$ ) .

L'affirmation de GAUSS a été démontrée par J. HADAMARD et C DE LA VALLÉE POUSSIN; auparavant P.L. TSCHEBYCHEFF avait montré que si la limite existe, elle est nécessairement égale à 1 .

On peut dire sans risque qu'il s'agit du théorème le plus important de la théorie des nombres premiers - pour cette raison, il est d'habitude appelé *le théorème des nombres premiers.*

Evidemment, ce théorème ne dit rien sur la valeur exacte de $\pi(x)$ . A ce propos, il existe une formule, dûe à E.D.F. MEISSEL,

célèbre astronome, qui a donné, en 1871, la valeur exacte de $\pi(x)$ , en termes des valeurs $\pi(y)$ pour tout $y \leq x^{2/3}$ , et des nombres premiers $p \leq x^{1/2}$ .

**RECORD**

Le plus grand entier $N$ pour lequel $\pi(N)$ a été calculé exactement est $N = 4 \times 10^{16}$ . J.C. LAGARIAS, V.S. MILLER & A. ODLYZKO (1985) ont trouvé

$$\pi(4 \times 10^{16}) = 1\ 075\ 292\ 778\ 753\ 150 \ .$$

Les différences $\left| \pi(x) - \frac{x}{\log x} \right|$ et $| \pi(x) - \mathrm{Li}(x) |$ ne restent pas bornées, lorsque $x$ tend vers l'infini. L'évaluation aussi exacte que possible, de ces termes d'erreur, est d'importance capitale dans les applications du théorème des nombres premiers.

D'abord, il a été suggéré par les tables, et ensuite démontré par J.B. ROSSER & L. SCHOENFELD en 1962, que $\frac{x}{\log x} \leq \pi(x)$ pour tout $x \geq 17$ .

L'histoire est plus intéressante en ce qui concerne la différence $\mathrm{Li}(x) - \pi(x)$ ; d'après J.E. LITTLEWOOD cette différence change de signes une infinité de fois.

**RECORD**

En 1955, S. SKEWES a montré que la différence $\mathrm{Li}(x) - \pi(x)$ est négative pour un $x_0$ tel que

$$x_0 < e^{e^{e^{7.7}}} \ .$$

Le plus petit $x_o$ connu, tel que $\mathrm{Li}(x_o) \leq \pi(x_0)$ est déjà tel que $x_o \leq 669 \times 10^{370}$ , comme il a été démontré par H.J.J. TE RIELE (1986).

Sans ombre de doute la fonction la plus importante dans l'étude de la distribution des nombres premiers, est la *fonction zeta* de RIEMANN.

Pour tout nombre complexe $s$, tel que $\mathrm{Re}(s) > 1$, la série

$$\sum_{n=1}^{\infty} \frac{1}{n^s}$$

est absolument convergente; elle est aussi uniformément convergente dans chaque domaine $\{ s \mid \mathrm{Re}(s) > 1 + \varepsilon \}$ (où $\varepsilon > 0$ est arbitrairement donné). La fonction $\zeta(s)$ ainsi définie admet un prolongement analytique à une fonction méromorphe, définie sur tout le plan complexe, ayant un seul pôle en $s = 1$, qui est d'ordre $1$, avec résidu égal à $1$. L'étude des propriétés de cette fonction a permis éventuellement de démontrer le théorème des nombres premiers.

$\zeta(s)$ a les zeros $-2, -4, -6, \ldots$, que l'on peut découvrir sans difficulté par l'équation fonctionnelle. Tous les autres zéros de $\zeta(s)$ sont des nombres complexes $\sigma + it$ ($\sigma, t$ réels), avec $0 < \sigma < 1$.

*L'hypothèse de RIEMANN* (qui est en fait une conjecture pas encore démontré) s'ennonce:

Les zéros non-triviaux de la fonction zeta de RIEMANN se trouvent sur la *droite critique*, des points $\frac{1}{2} + it$ ($t$ réel).

Sans rentrer dans le détail, il y a beaucoup de théorèmes sur la distribution des nombres premiers qui peuvent se démontrer en supposant l'hypothèse de RIEMANN. Il est donc capitale de déterminer les zéros non-triviaux de $\zeta(s)$ ; par symétrie, il suffit de considérer ceux pour lesquels $t > 0$.

On peut numéroter ces zéros comme suit: le $n^{\text{ième}}$ zéro se note $\sigma_n + it_n$, de sorte que $t_n \leq t_{n+1}$ et si $t_n = t_{n+1}$ alors $\sigma_n < \sigma_{n+1}$ (il faut remarquer qu'il y a tout au plus un nombre fini de zéros avec une valeur donnée de $t$ ) .

RECORD

Pour $n \leq 1\ 500\ 000\ 001$ les zéros $\sigma_n + it_n$ de la fonction zeta de RIEMANN se trouvent sur la droite critique, c.à.d. $\sigma_n = \frac{1}{2}$ . Ces calculs one été faits par J.J.H. TE RIELE, J. VAN DE LUNE & D.T. WINTER, jusqu'à 1986.

Une autre approche à ce problème a été developée par N. LEVINSON.

RECORD

B. CONREY a montré en 1989 que au moins 2/5 des zéros de la fonction zeta de RIEMANN se trouvent sur la droite critique.

Les considérations précédentes se rapportaient au comportement asymptotique de la fonction $\pi(x)$ et à la fonction $\zeta(s)$ qui est de toute importance dans l'estimation du terme d'erreur. On peut dire qu'il s'agit du comportement de $\pi(x)$ "à l'infini".

Maintenant j'aborde le comportement *local* de $\pi(x)$ , soit l'étude des lacunes entre nombres premiers.

Voici la question principale:

Si on connait le $n^{\text{ième}}$ nombre premier $p_n$ , où se trouve-t-il le nombre premier suivant? Il s'agit donc d'étudier le différence

$$d_n = p_{n+1} - p_n \ .$$

Il est facile de montrer que

$$\limsup\ d_n = \infty \ ,$$

c'est-à dire, il existe des blocs de nombres composés successifs arbitrairement grands. En voici un:

(N+1) ! + 2 , (N+1) ! + 3 ,..., (N+1) ! + (N+1) sont (pour tout N) des nombres composés.

Il est inéressant de trouver des grands blocs de nombres composés successifs, mais beaucoup plus petits.

**RECORD**

En 1989, J. YOUNG & A. POTLER ont trouvé la lacune suivante:

$P_n$ = 90 874 329 411 493 , avec

$d_n = 804$ .

Que peut-on dire sur la limite inférieure de la suite des différences $d_n$ ?

On dit que les nombres premiers $p < p'$ sont *jumeaux* si $p' - p = 2$ .

On ne sait pas encore s'il existe une infinité de nombres premiers jumeaux. Ceci se dit aussi: on ne sait pas si $\liminf d_n = 2$ .

La question est délicate. En 1919, V. BRUN a montré:

$$\sum \left( \frac{1}{p} + \frac{1}{r+2} \right) = B < \infty$$

(somme pour tous les couples de nombres premiers jumeaux).

Donc s'il y a une infinité de nombres premiers jumeaux (comme on le pense), ils forment un ensemble bien clairsemé.

En 1976, R.P. BRENT a calculé la constante de BRUN avec beaucoup de soin:

B = 1.90216054...

**RECORD**

Le plus grand couple connu de nombres premiers jumeaux a été découvert en 1989 par B.K. PARADY, J.F. SMITH, S. ZARANTONELLO, du groupe des "SIX de AMDAHL" (les mêmes qui détiennent à présent le record du plus grand nombre premier. C'est le couple $1706595 \times 2^{11235} \pm 1$ .

L'intérêt de déterminer grandes lacunes entre des nombres premiers pas trop grands, peut être précisé. Il faut étudier la suite $\frac{d_n}{p_n}$ qui indique les lacunes relatives.

Déjà en 1845, J. BERTRAND avait conclut, en observant les tables, qu'il existe toujours un nombre premier entre $p_n$ et $2p_n$ (pour tout $n \geq 1$ ) . Ce fut TSCHEBYCHEFF qui le premier a démontré ce résultat, qui s'écrit aussi $p_{n+1} < 2\, p_n$ , ou bien $\frac{d_n}{p_n} < 1$ .

C'est un résultat joli, mais bien plus faible que ce qu'on peut déduire du théorème des nombres premiers:

$$\lim \frac{d_n}{p_n} = 0 \ .$$

La théorie des lacunes entre nombres premiers a mené à la formulation de la conjecture:

Pour tout $\varepsilon > 0$ on a $p_{n+1} < p_n^{\frac{1}{2}+\varepsilon}$ , dès que $n$ est suffisamment grand.

**RECORD**

En poursuivant dans la lignée de nombreux prédécesseurs, le record est détenu en ce moment par MOZZOCHI (1986):

$$p_{n+1} < p_n^{\frac{1}{2} + \frac{1}{20} - \frac{1}{384}}$$

pour n suffisamment grand.

Cet exposé devenant trop long, je suis forcé à passer sous silence beaucoup de questions de grand intérêt. Ainsi, je ne dirai rien sur les nombres premiers en progression arithmétique, ni sur le problème de GOLDBACH. Heureusement qu'il existe maintenant un livre où ces faits, et bien d'autres, sont consignés et expliqués de façon détaillée. Ce livre n'attend que d'être lu!

Je terminerai par quelques curiosités, qui pourront être raccontées à vos amis à un cocktail (mais pas après quelques verres!).

Un nombre qui s'écrit Rn = 111...1 (n chiffres décimaux égaux à 1) est une *repunité*.

On ne sait pas s'il en existe une infinité qui soient des nombres premiers.

**RECORD**

H.C. WILLILAMS & H. DUBNER ont montré en 1986, que R1031 est un nombre premier.

Les seules autres repunités dont on sait que ce sont des nombres premiers, sont:

R2 , R19 , R23 , R317 .

Voici, enfin, un autre record curieux.

**RECORD**

Le plus grand nombre premier connu dont tous les chiffres sont des nombres premiers est

$$7532 \times \frac{10^{1104} - 1}{10^{4} - 1} + 1 \ .$$

Si vous voulez savoir pourquoi et comment on le trouve, il faudra le demander à H. DUBNER, qui l'a signalé en 1988.

**CONCLUSION**

Les matières qui appartiendraient aux parties (V) et (VI) (nombres premiers spéciaux et heuristique, expérimentation) n'ont pas du tout été évoquées ici.

Comme je viens de le dire, ceci et beaucoup d'autres faits se trouvent réunis sous une cape jaune.

L'observation et l'étude des nombres premiers, sous l'angle de cette présentation, s'avère une méthode très féconde, et d'ailleurs plaisante. Les mathématiciens en dérivent beaucoup de plaisir, et ceci en vaut la peine.

Il faut, comme moi, penser que les nombres sont des amis... des amis qui nous donnent des problêmes!

## REFÉRENCES.

**Paulo Ribenboim**, The Book of Prime Number Records (3rd. edition), Springer-Verlag, New York, 1991.

**Paulo Ribenboim**, Selections du Livre des Records de Nombres Premiers, Presses Universitaires de France, Paris, 1991.

Adresse de l'auteur:

Prof. Paulo Ribenboim
Department of Mathematics
Queen's University
Kingston, Ontario
K7L 3N6
Canada