QUELQUES EXEMPLES DE RECHERCHE EN THÉORIE DES NOMBRES...

par Jean-Louis NICOLAS, Université de LIMOGES

(conférence du 15/10/1976 devant la Régionale de Limoges)

Pour savoir ce qui se passe dans la tête d'un chercheur. Pour comprendre la genèse de la pensée mathématique, demandons quelques illustrations à l'un d'entre eux.

La théorie des nombres a toujours posé des problèmes aux énoncés simples, mais très difficiles à résoudre. Pour les étudier, il a souvent fallu développer de façon considérable des secteurs importants des mathématiques qui n'avaient rien à voir au départ, avec l'arithmétique

La plupart des résultats exposés ici sont tirés des trois livres :

-[HW] : Hardy and Wright, an introduction to the theory of numbers, Oxford at the Clarendon Press, 4th édition 1960

en anglais, mais très attrayant et tout à fait abordable (la moitié du livre est accessible à un élève de terminale C)

-[BC]: Borevitch et Chafarevitch , théorie des nombres, Gauthiers Villars 1967

-[MC]: Mathématics of computation vol.29, 1975

Ce numéro spécial de la revue Mathematics of computation rassemble plusieurs articles qui montrent à quoi peut servir un ordinateur dans la recherche en théorie des nombres.

1) - le théorème de Fermat

Soit n un entier ≥ 3. Il n'existe pas trois entiers x, y, z non nuls, tels que :

$$x^n + y^n = z^n$$

Sur son exemplaire des oeuvres de Diophante, Pierre de Fermat posait ce problème en 1637 et écrivait qu'il en connaissait une solution, mais que la marge était trop petite pour la contenir. De nos jours, ce problème n'est toujours pas complètement résolu, bien que de nombreux mathématiciens l'aient abordé.

Le cas n = 2 était connu de Diophante :

Si l'on a : $x^2 + y^2 = z^2$ avec

$x > 0$, $y > 0$, $z > 0$, $(x,y) = 1$, x pair.

(l'un des deux nombres x ou y doit être pair, pour des raisons de congruence modulo 4).

Alors $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$
où a et b sont des entiers de parité opposée, avec :

$$(a,b) = 1 \quad \text{et} \quad a > b > 0.$$

Il y a une bijection entre les paramètres a et b et la solution x,y,z.

On trouvera dans [HW] , ch.XIII, la démonstration de ce théorème. Exemples :

$a = 2$, $b = 1$ donne $3^2 + 4^2 = 5^2$

$a = 3$, $b = 2$ donne $5^2 + 12^2 = 13^2$

Si le théorème de Fermat est vrai pour n, il est vrai a fortiori pour un multiple de n puisque :

$$x^{an} + y^{an} = z^{an}$$

s'écrit aussi

$$(x^a)^n + (y^a)^n = (z^a)^n$$

Il suffit donc de démontrer le théorème de Fermat pour n = 4 et lorsque n est un nombre premier impair.

Fermat résolvait le cas n = 4 en démontrant que l'équation $x^4 + y^4 = z^2$ n'a pas de solutions non nulles.

Le cas n = 3 fut résolu par Euler qui a démontré que l'équation $\xi^3 + \eta^3 + \zeta^3 = 0$ n'a pas de solutions dans l'anneau $\mathbb{Z} + j\mathbb{Z}$ ou $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ est une racine cubique de l'unité.

Dans cet anneau, il y a des nombres premiers et une décomposition unique en facteurs premiers. Cette dernière propriété n'est malheureusement pas générale, puisque dans l'anneau $\mathbb{Z} + \mathbb{Z}\sqrt{10}$, les nombres 2, 3, $4 + \sqrt{10}$, $4 - \sqrt{10}$ sont premiers et que $6 = 2.3 = (4 + \sqrt{10})(4 - \sqrt{10})$ a deux décompositions.

Pour pallier à cet inconvénient, Kummer en 1850 inventa la théorie des nombres idéaux pour lesquels il y a unicité de la décomposition en facteurs premiers. Il démontra ainsi que pour tout nombre premier p régulier, le théorème de Fermat est vrai.

Les nombres de Bernouilli B_n sont définis comme les coefficients du développement en série entière de $\frac{x}{e^x - 1}$

$$\frac{x}{e^x - 1} = 1 + \sum_{n=1}^{\infty} \frac{B_n}{n!} x^n = 1 - \frac{x}{2} + \frac{B_2}{2} x^2 + \frac{B_4}{4!} x^4 + \dots$$

On peut calculer B_n en faisant le quotient des développements limités de x par $e^x - 1$, ou par la relation :

$$1 + \sum_{k=1}^{m-1} \binom{m}{k} B_k = 0 \quad \text{avec} \binom{m}{k} = \frac{m!}{k!(m-k)!}$$

On trouve $B_1 = -\frac{1}{2}$; $B_2 = \frac{1}{6}$; $B_4 = -\frac{1}{30}$; $B_6 = \frac{1}{42}$;

$B_8 = -\frac{1}{30}$; $B_{10} = \frac{5}{66}$; $B_{12} = \frac{-691}{2730}$; $B_{14} = \frac{7}{6}$; etc...

Tous les Bn, pour n impairs sont nuls à l'exception de B_1.

Ces nombres servent à développer tgx et cotgx en série entière :

$$tgx = \sum_{n=1}^{\infty} Tn \frac{x^{2n-1}}{(2n-1)!} \quad \text{avec } Tn = 2^{2n}(2^{2n}-1)\frac{|B_{2n}|}{2n}$$

(Tn est un nombre entier)

$$Cotgx = \frac{1}{x} - \sum_{n=1}^{\infty} \frac{|B_{2n}|}{(2n)!} 2^{2n} x^{2n-1}$$

On peut également exprimer en fonction des B_n la somme des séries $\sum_{k=1}^{\infty} \frac{1}{n^{2k}}$ pour k entier : on a :

$$\frac{|B_{2k}|}{2k!} = \frac{2}{(2\pi)^{2k}}\left(\sum_{n=1}^{\infty} \frac{1}{n^{2k}}\right)$$

On a en particulier : $\sum_{n\neq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ et $\sum_{n\neq 1} \frac{1}{n^4} = \frac{\pi^4}{90}$

Cette dernière formule donne l'ordre de grandeur des B_{2k}, car $\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}}$ est une suite décroissante de k, dont la limite est 1.

Un nombre premier p impair est dit régulier, s'il ne divise aucun numérateur des nombres de Bernouilli

$$B_2, B_4, \ldots\ldots B_{p-3}$$

Le plus petit nombre irrégulier est p = 37 qui divise B_{32}. On trouvera une table des nombres premiers irréguliers dans [BS].

Kummer devait bien penser être près du but en donnant son critère : pour p régulier, le théorème de Fermat est vrai. Malheureusement, l'étude des nombres premiers réguliers s'avérait très difficile. On ne sait pas encore s'il existe une infinité de tels nombres. On sait cependant qu'il y a une infinité de nombres premiers irréguliers.

Depuis Kummer, des critères numériques ont été donnés pour démontrer que le théorème de Fermat était vrai lorsque p est irrégulier (cf [MC]). On a ainsi pu démontrer le théorème de Fermat jusqu'à n = 30 000 (cf [MC]) et depuis Wagstaff a poursuivi les calculs jusqu'à 100 000 à l'Université de l'Illinois à Urbana. D'autres problèmes sont soulevés par ces calculs : la répartition des nombres premiers réguliers : On conjecture que le quotient $\frac{\pi_r(x)}{\pi(x)}$ du nombre de nombres premiers réguliers $\leq x$ sur le nombre total de nombres premiers $\leq x$ tend vers $\sqrt{e} = 0{,}61$ lorsque x tend vers l'infini. On étudie aussi l'index d'un nombre premier irrégulier : c'est le nombre de nombres de Bernouilli qu'il divise. Ainsi 491 qui divise B_{292}, B_{336}, et B_{338} pour index 3.

Cas simplifié

On a pu démontrer que l'équation $x^p + y^p = z^p$ n'avait pas de solution x,y,z telle que p ne divise pas x,y,z sauf si :

$$2^{p-1} \equiv 1 \bmod p^2$$

Le petit théorème de Fermat affirme que $2^{p-1} \equiv 1 \bmod p$ Modulo p^2, c'est vrai pour p = 1093. Là encore c'est un problème bien difficile que d'étudier cette congruence.

Conjecture d'Euler

Après avoir résolu $x^3+y^3=z^3$, c'est-à-dire montré qu'un cube ne pouvait être une somme de 2 cubes, Euler avait conjecturé qu'une puissance $n^{ième}$ ne pouvait être la somme de (n-1) puissances $n^{ième}$.

L'ordinateur a mis fin à cette conjecture en donnant :

$$144^5 = 27^5 + 84^5 + 110^5 + 133^5$$

Mais est-ce le seul contre exemple ? et sinon, comment sont distribués les autres contre exemples ?

Le théorème des nombres premiers et l'hypothèse de Riemann

Euclide a démontré qu'il existait une infinité de nombres premiers, par la démonstration encore utilisée de nos jours. S'il n'y en avait qu'un nombre fini $p_1, p_2, \ldots\ldots p_k$, on considère $N = p_1 p_2 \ldots p_k + 1$; ou bien N est premier et plus grand que p_k, ou bien N a un facteur premier plus grand que p_k.

En 1808, Legendre écrivait : "Quoique la suite des nombres premiers soit extrêmement irrégulière, on peut cependant trouver avec une précision très satisfaisante, combien il y a de ces nombres depuis 1 jusqu'à une limite donnée x. La formule qui résout la question est :

$$y = \frac{x}{\log x - 1{,}08366}$$

log x étant un logarithme hyperbolique".

Legendre avait basé cette conjecture sur l'étude des tables de nombres premiers.

Dirichlet a démontré que dans toute progression arithmétique an + b, avec a et b premiers entre eux, il y a une infinité de nombres premiers. Le raisonnement d'Euclide s'adapte à certaines progressions comme 4n + 3 ou 6n + 5 (cf. [HW], ch.2), mais pas à toutes et le théorème de Dirichlet est plus profond.

On note habituellement $\pi(x)$ le nombre de nombres premiers $\leq x$. Tchebychev démontra qu'il existait deux réels A et B vérifiant $0 < A < 1 < B$ tels que :

$$\frac{Ax}{\log x} < \pi(x) < \frac{Bx}{\log x}$$

Pour obtenir la majoration, il considère le coefficient du binôme $M = \frac{(2m+1)!}{m!(m+1)!}$. Comme M intervient deux fois dans le développement de

$$(1+1)^{2m+1}, \text{ on a } M < 2^{2m}$$

Maintenant soit $q_1 \ldots\ldots q_k$ les nombres premiers appartenant à $]m+1, 2m+1]$. On a $k = \pi(2m+1) - \pi(m+1)$.

D'autre part le produit $q_1 \ldots\ldots q_k$ divise M et on a : $(m+1)^k < q_1 q_2 \ldots\ldots q_k < 2^{2m}$ d'où l'on tire

$$\pi(2m+1) - \pi(m+1) < \frac{2m \log 2}{\log(m+1)}$$

On démontre alors par récurrence sur n, la formule $\pi(n) < \frac{Bn}{\log n}$.

En utilisant des combinaisons plus compliquées :

$$\frac{x!\,(x/30)!}{(x/2)!(x/3)!(x/5)!}$$

pour x multiple de 30, Tchebychev resserrait autour de 1 les constantes A et B et démontrait que pour $x > x_0$ on avait :

$$\frac{ax}{\log x} < \pi(x) < \frac{6}{5}\,a\,\frac{x}{\log x}$$

avec $a = \log \frac{2^{1/2}\,3^{1/3}\,5^{1/5}}{30^{1/30}} = 0{,}92129$. En améliorant ces techniques, il pensait bien arriver à montrer que $\pi(x) \sim \frac{x}{\log x}$. Malheureusement ce n'était pas possible.

Tchebychev démontra le postulat de Bertrand : pour tout x réel > 1, il y a un nombre premier entre x et 2 x.

Riemann introduisit la fameuse fonction ζ définie par :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{pour } s \in \mathbb{C},\ \mathrm{Re}(s) > 1.$$

Cette fonction est liée aux nombres premiers par la formule :

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - \frac{1}{p^s}} \quad \text{pour } \mathrm{Re}(s) > 1$$

Cette formule montre qu'il y a une infinité de nombres premiers : en effet, pour s = 2, s'il y en avait un nombre fini, le produit π serait fini et $\zeta(2)$ serait rationnel. Or, on a vu que $\zeta(2) = \frac{\pi^2}{6}$ qui n'est pas rationnel.

On peut donner un sens à $\zeta(s)$ pour $0 < \mathrm{Re}(s) < 1$.

La série $f(s) = \sum_{n \geq 1} \frac{(-1)^n}{n^s}$ est convergente pour s réel > 0 par le critère des séries alternées et pour s complexe, $\mathrm{Re}(s) > 0$ par le théorème d'Abel. Dans la somme $\zeta(s) + f(s)$ les termes pairs s'ajoutent, les termes impairs s'en vont et l'on a :

$$\zeta(s) + f(s) = 2 \sum_{k=1}^{\infty} \frac{1}{(2k)^s} = \frac{2}{2^s}\,\zeta(s)$$

d'où pour $s \neq 1$, $\quad \zeta(s) = f(s) \Big/ \left(\frac{1}{2^{s-1}} - 1\right)$

On a $\lim_{s \to 1} \zeta(s) = \infty$

Hadamard et De La Vallée Poussin démontrait simultanément en 1896 le théorème des nombres premiers (i-e $\lim_{x \to \infty} \frac{\pi(x)\,\log x}{x} = 1$). Ils montraient d'abord qu'il était équivalent à : $\forall t \in \mathbb{R}^*\ \ \zeta(1 + it) \neq 0$ puis démontraient ce dernier résultat.

L'étude des "zéros" de la fonction ζ est donc importante. On peut montrer que dans la bande $0 < \mathrm{Re}(s) < 1$, ils sont placés symétriquement par rapport à la droite $x = \frac{1}{2}$. L'hypothèse de Riemann dit qu'ils sont

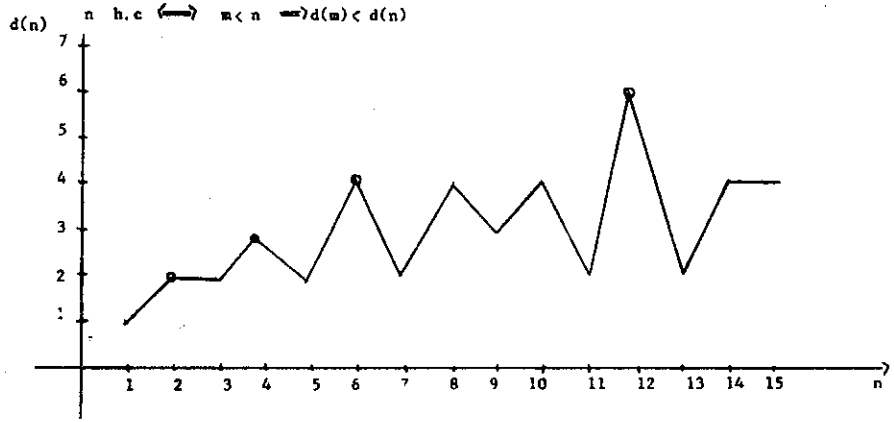
tous localisés sur cette droite. Ils sont aussi placés symétriquement par rapport à l'axe réel ($\zeta(\bar{s}) = \overline{\zeta(s)}$). Le premier zéro est $\frac{1}{2} + 14{,}1\ldots i$. On a calculé (cf. [MC]) les zéros de $\zeta(s)$ dont la partie imaginaire est inférieure à 1 894 438. Il y en a plus de 3 millions et demi, tous situés sur la droite $x = \frac{1}{2}$.

En 1950, Erdos et Selberg donnait une autre démonstration du théorème des nombres premiers, dite élémentaire, c'est-à-dire n'utilisant pas la théorie des variables complexes.

Nombres hautement composés

Un entier n est dit hautement composé (h.c) s'il a plus de diviseurs que tous les nombres qui le précèdent. Soit d (n) le nombre de diviseurs de n, on a :

n h.c $\Longleftrightarrow$ $m < n \Longrightarrow d(m) < d(n)$



Les nombres h.c sont les nombres qui ont une vue imprenable sur $-\infty$: 2, 4, 6, 12.

Si n a pour décomposition en facteurs premiers

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Un diviseur d de n s'écrira $d = p_1^{\beta_1} \ldots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$

Il y a donc $(\alpha_1 + 1)$ choix possibles pour $\beta_1, \ldots (\alpha_1 + 1)$ choix possibles pour β_i et on a donc :

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1)$$

L'étude des nombres hautement composés est liée à l'étude de : $\max_{n \leq a} d(n)$. Ce dernier problème se met sous la forme d'un problème d'optimisation en nombres entiers :

Trouver des entiers $x_i \geq 0$ tels que :

$$x_1 \log 2 + x_2 \log 3 + \ldots + x_k \log p_k + \ldots \leq \log a$$

$$\max \left[\log(x_1 + 1) + \log(x_2 + 1) + \ldots + \log(x_k + 1) + \ldots\right]$$

où p_k désigne le k ième nombre premier.

Les problèmes d'optimisation en nombres entiers interviennent en Recherche Opérationnelle à des fins militaires ou commerciales. Et, j'ai eu la surprise de voir que les méthodes d'études des nombres h.c, que je croyais enfermés dans un domaine abstrait et inutile, pouvaient servir à résoudre des problèmes très concrets.

Voici quelques conclusions que l'on peut dégager de ces exemples :

- un problème n'est jamais complètement résolu,
- en théorie des nombres, il a toujours été utile de faire des calculs, de construire des tables pour en déduire des conjectures. Les ordinateurs facilitent et amplifient cette méthode.
- quand on ne sait pas résoudre un problème, on tourne autour en le généralisant ou en le restreignant, en le modifiant pour tenter de l'abattre.
- les discussions sur un problème sont très utiles d'où la nécessité des congrés, des rencontres, de l'enseignement de niveau 3ème cycle.
- il peut paraître sécurisant de penser que des gens s'intéressent au théorème de Fermat. Mais l'expérience a montré (éventuellement à long terme) que ce genre de travail pouvait développer la recherche scientifique dans bien d'autres secteurs,
- dans un récent article (13 octobre 1976) sur la Recherche Scientifique en France, "Le Monde" mentionnait : "Le chercheur est un être un peu à part qui s'amuse de choses qui n'amusent pas les autres".

Il me reste à souhaiter que les professeurs que nous sommes sachent communiquer à leurs élèves le goût de s'amuser avec les mathématiques.