De Conjecture en conjecture

LES MATHS EN ACTION.

Pierre de Fermat
1601 - 1665

Michel DARCHE - Orléans

Vous connaissez tous les travaux de l'avocat toulousain Pierre de Fermat (1601-1665) en optique mais surtout en mathématique. Outre ses apports en géométrie analytique et en probabilités, poursuivant les travaux des grecs et particulièrement de Diophante (3è siècle ap. JC), il fonda véritablement la théorie des Nombres dont on parle beaucoup ces dernières années.

Deux aspects de ce travail ont aujourd'hui une place de tout premier ordre dans la cité mathématique.

Le "premier" concerne la primalité. Les fidèles lecteurs du PLOT (n° 23) connaissent sûrement les nombres de Fermat ($2^{2^n}+1$) dont il conjecturait, dans une lettre à Pascal (23 août 1654) qu'ils étaient tous premiers. Déjà en 1640, dans une lettre à Frén icle, Fermat écrivait :

Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers comme 3, 5, 17, 257, 65 537, 4 294 967 297, et le suivant de 20 lettres 18 446 774 073 709 551 617, etc.....

Je n'en ai pas la démonstration exacte, mais j'ai exclu à grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurais peine à me dédire".

Hélas, un siècle plus tard, Euler (1707-1783) montrait que pour n = 5 ce nombre était divisible par 641. Depuis on a montré que, pour n compris entre 5 et 16, ces nombres étaient composés mais on ignore actuellement la nature du 17è. (On sait par contre que $286243-1$ est premier "depuis" janvier 1983 grâce à D.Slowinski qui détient ainsi le dernier record dans les nombres de Mersenne (le 27è). A vos PLOT n° 23. Autre apport sur les nombres premiers toujours d'actualité: "Le petit théorème de Fermat".

Dans une lettre à Frénicle (18 octobre 1640), Fermat affirme que pour p premier $a^{p-1}-1$ est divisible par p (pour tout $a \geqslant 2$).

Tout nombre premier mesure infailliblement une des puissances -1 de quelques progressions que ce soit et l'exposante de la dite puissance est sous-multiple du nombre premier -1".

Cette conjecture est bien un théorème démontrable avec des connaissances de niveau Bac + 1. Elle est d'une grande actualité et d'une utilité évidente en cryptographie (l'étude des codes secrets) sur laquelle nous reviendrons dans un prochain numéro.

Le second aspect du travail de Fermat concerne un certain type d'équations diophantiennes et motive cet article.

* Conjecture : "Enoncé que les mathématiciens présentent comme vrai mais qu'ils n'arrivent pas à démontrer. (M.Arvonny, in :"Le Monde" 18.6.83).

* Théorème : "Vérité qui devient évidente au moyen d'un raisonnement appelé démonstration" (Legendre 1

Dans la marge d'une traduction en latin avec commentaires des livres arithmétiques de Diophante faite par Bachet de Meziriac (1581-1638) parue en 1621 Fermat affirma :

"il est impossible d'écrire un cube comme somme de deux cubes, une puissance quatrième comme somme de deux puissances quatrième et ainsi de suite, excepté pour la puissance de 2.

J'ai trouvé une démonstration mais la marge de ce livre est trop petite pour qu'elle puisse y aller".

"Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

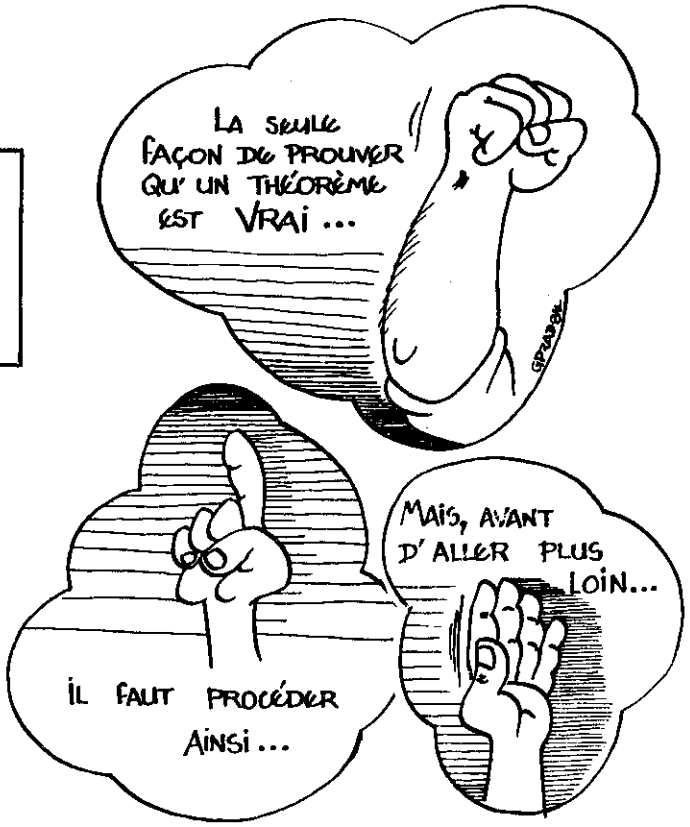
On sait, grâce à Pythagore, que l'équation $x^2+y^2= z^2$ a une infinité de solutions entières, la "première" étant le triplet pythagoricien (2,3,4). Mais le "théorème" de Fermat stipule que, pour n supérieur ou égal à 3, l'équation $x^n+y^n=z^n$ n'a pas de solution entière. A ce jour on n'en connaît pas la démonstration complète !

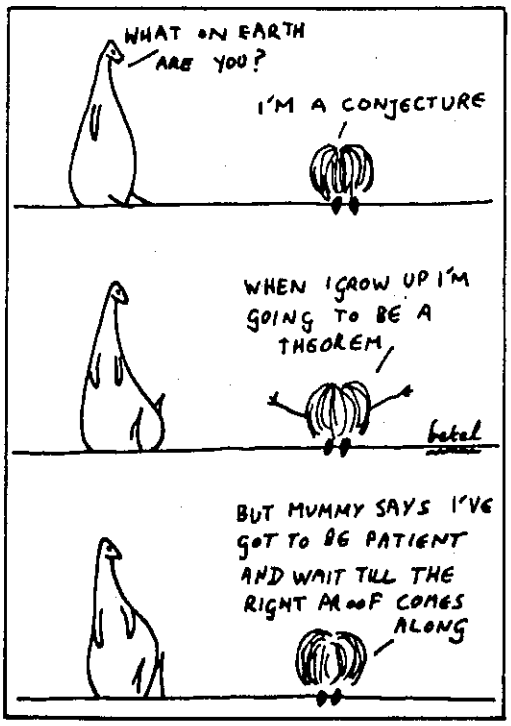
Ceux qui ont vu dernièrement l'exposition "Horizons Mathématiques" savent par contre que l'équation

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

a des solutions pour n 3 par exemple $3^3+4^3+5^3=6^3$. *Y en a-t-il d'autres ? Essayez de trouver des solutions pour d'autres puissances.*

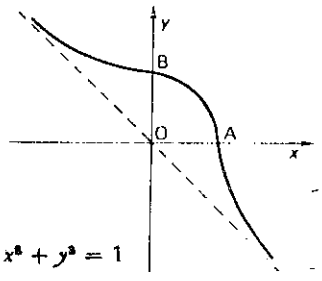
Fermat crut et affirma en avoir trouvé une mais à ce jour on ne connaît et reconnaît que sa justification pour n=4 et les mathématiciens actuels pensent avoir reconstitué ses arguments pour les autres cas et montrent qu'ils sont faux.





- *Qu'est-ce que vous êtes sur la Terre ?*
- *Je suis une conjecture.*

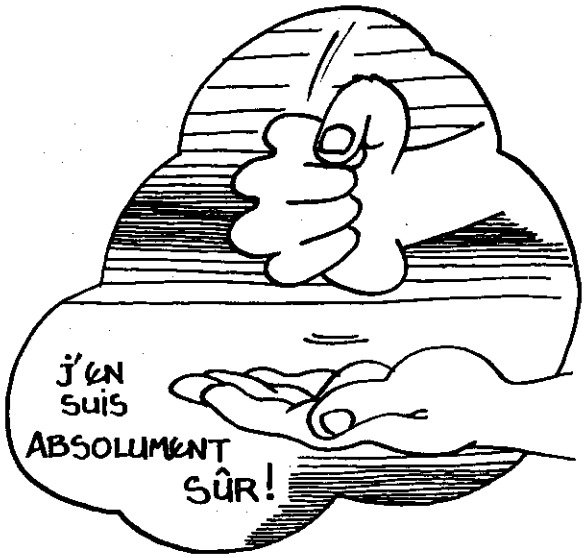
- *Quand je serai grand je deviendrai un théorème.*



- *mais maman m'a dit d'être patient et d'attendre que la preuve arrive.*

Depuis, la démonstration a progressé "n à n" : Euler crut la trouver pour n=3 mais se trompa une première fois avant d'y arriver ainsi que Gauss. Dirichlet (1805-1859) et Legendre (1752-1833) en trouvèrent une pour n=5. Lamé (1795-1870) crut, à partir d'une démonstration pour n=7, le généraliser à tout n mais se trompa... pour les mêmes raisons qu'Euler. (Il pensait que l'unicité de la décomposition de nombres complexes en nombres premiers allait de soi et ne nécessitait pas de justification). De nouveaux outils furent ainsi créés : la notion d'idéal et de nombre cyclotomique qui permirent à Kummer (1810-1893) de vérifier la conjecture pour tout n < 100 (sauf pour 37, 59, 67).

En 1908 est créé le prix Wolfskehl d'une valeur de 100 000 marks (1908 !).



"Dans son testament, Dr. Wolfskehl à fait remarquer que Fermat affirmait, mutatis mutandis, que l'équation $x^n+y^n=z^n$ n'avait pas de solution en entiers pour tout entier premier impair. Ce théorème doit être démontré, soit en suivant les idées de Fermat, soit en complétant les recherches de Kummer".

L'ordinateur, depuis, a permis d'aller plus loin. En 1980 Wagstaff a montré qu'il n'y avait pas de solutions inférieures à 25000 pour n < 125 000 ! Peut-on alors considérer la conjecture comme vraie ? vraisemblable ? quel intérêt apporterait la réponse pour n > 125 000 ?

Conjecture, démonstrations partielles, échecs nombreux (et révélateurs), introduction de nouvelles notions (sans parler de l'ordinateur !) Fermat n'avait pas fini de nous émerveiller.

1983, coup de tonnerre dans la cité mathématique et qui apparemment ne touche pas cette conjecture :

Un mathématicien allemand Gerd Faldings (29 ans) démontre une autre conjecture avancée par l'anglais Mordell en 1922 : "Toute courbe algébrique*, à l'exception des plus simples comme la droite ou le cercle, ne passe que par un nombre fini de points ayant des coordonnées entières (ou rationnelles)".

Jusqu'à présent le doute était total sur le "grand théorème de Fermat". On savait que les preuves apportées par Kummer laissaient en "conjecture" une infinité de nombres pour lesquels sa méthode ne s'appliquait pas.

La conjecture de Mordell et sa démonstration par Faldings permettent maintenant d'affirmer que, quelque soit n, l'équation de Fermat, si elle a des solutions, n'en a qu'un nombre .... fini !

---

* Une courbe algébrique est une courbe représentative d'une fonction polynômiale ou quotient de polynomes (cf. PLOT-Matériel, dossier sur les traceurs de courbes et le théorème de Lebesgue).

Le théorème de Faldings,

Théorème du siècle ? sur ce sujet on ne peut, comme le fait "The Mathematical Intelligencer" de décembre 1983, que faire des .... conjectures et attendre, peut être, une dizaine d'années pour voir quelles utilisations seront faites du théorème et de sa méthode. Ainsi en a-t-il été du théorème du siècle passé énoncé en 1882 par un autre jeune mathématicien allemand Ferdinand Lindemann (1852-1939) sur la transcendance de π (fidèles lecteurs à votre PLOT n° 21) reprenant le travail du français Charles HERMITE (1882-1901) sur la transcendance de e (1873) *et dont les travaux furent repris et simplifiés les années suivantes par Weierstrass, Hilbert, Hurwitz et Gordan.*

Alors de conjecture en conjecture, dans 10 ans... le PLOT en sera aux numéros .... 67,68 !!!!

> "Savoir c'est connaître par le moyen de la démonstration"
>
> In : La science et la démonstration d'Aristote (4è siècle av. JC).

Gerd Faldings a présenté ses travaux au séminaire Bourbaki en décembre 1983 (sans dire un mot du "Théorème" de Fermat).

Bibliographie :

- Imre Lakatos : Proofs and refutations Cambridge Press University, 1976.
- Hendrik Lenstra : Eucledean Number Fields, in : "The mathematical Intelligencer" 1979, Vol.2, n°1.
- Fragments d'histoire des mathématiques Brochure APMEP n° 41, 1981.
- Sciences et Avenir (Avril 84) ;
- De nombreux articles dans les publications scientifques.

Affaire à suivre (même en France) en lisant la presse scientifique.

Le grand théorème de Fermat est aussi appelé le "dernier" théorème de Fermat, dernier à n'être pas encore totalement démontré comme on vient de le voir.

Pour les cas démontrés, A. Bouvier et M. George en donnent une interprétation graphique et numérique intéressante.

Excepté les points A(1,0) et B(0,1), aucun autre point de la courbe d'équation $x^n + y^n = 1$ n'a ses coordonnées toutes deux rationnelles. La courbe se "faufile" à travers l'ensemble partout dense des points rationnels.

Ces illustrations sont extraites (ou reprises) des dessins humoristiques qui émaillent une revue anglaise sur les mathématiques pleine d'intérêt : "Manifold" éditée par Ian Stewart (connu par ses B.D. sur les catastrophes, les groupes éditées chez Belin) et John Jaworski de l'Open University.

Une preuve, en pratique, est rarement une suite de déductions logiques comme le disent les livres. La vie est plus courte ! l'important est d'être convaincant. Il y a plusieurs façons pour présenter un argument avec conviction. En voici une bien populaire.