

## Pierre FERMAT

Né à Beaumont-de-Lomagne dans la première décennie du 17<sup>e</sup> siècle; son père était un marchand aisé. Etudes de droit. Fréquente les cercles savants de Bordeaux. Premiers travaux mathématiques.

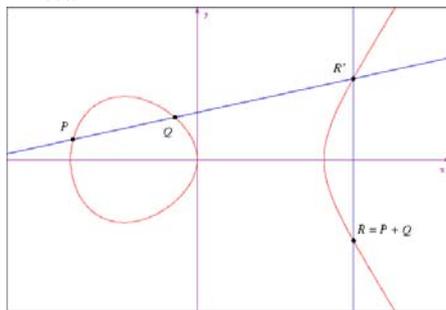
1631. Achète un office de conseiller au parlement de Toulouse. Il gravira tous les échelons d'une carrière de magistrat et sera aussi délégué à plusieurs reprises à la chambre de l'Edit à Castres, chambre chargée de régler les différends entre protestants et catholiques.



## LE GRAND THEOREME DE FERMAT

« Il n'est pas possible de décomposer un cube en somme de deux cubes, une puissance quatrième en somme de deux puissances quatrièmes et généralement aucune puissance d'exposant supérieur à 2 en deux puissances de même exposant. »

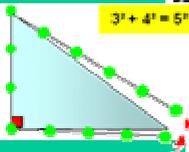
Cette courte annotation d'un magistrat français, Pierre Fermat, écrite en marge d'un livre de mathématiques dans la première moitié du 17<sup>e</sup> siècle, est devenue peu à peu un des théorèmes les plus célèbres des mathématiques : une preuve n'en fut en effet achevée qu'en... 1995, par Andrew Wiles de l'université de Princeton.



1670: Réédition par Samuel de Fermat, fils aîné de Fermat, des Arithmétiques de Diophante, intégrant les notes que son père aurait inscrites en marge sur son exemplaire, maintenant perdu. Parmi elles, la seule mention du cas général du Grand Théorème de Fermat, et la preuve par descente infinie du cas des puissances quatrièmes. Un supplément de Jacques de Billy fondé sur des lettres de Fermat explique une méthode algébrique pour trouver les solutions en nombres fractionnaires de certains problèmes de Diophante.

1679: *Varia Opera* de Fermat (publication posthume de lettres et opuscules, par son fils Samuel)

Avec une ficelle comportant treize nœuds équidistants, il est possible de se passer d'une équerre pour tracer un angle droit



1636. Entre en contact épistolaire avec le cercle mathématique parisien de Marin Mersenne. Echange informations, problèmes, manuscrits, avec Roberval, Descartes, les Pascal, Mersenne et bien d'autres...

c. 1637. Circulation à Paris du manuscrit de Fermat *Ad locos planos et solidos isagoge* qui annonce une voie générale pour résoudre certains problèmes géométriques en leur associant une équation algébrique. Fermat y donne les équations correspondant à la droite, au cercle, à la parabole, etc.

1638. Première mention dans la correspondance des premiers cas (cubes et puissances quatrièmes) du Grand Théorème de Fermat.

1654. Echange de lettres avec Blaise Pascal sur le calcul des chances, en particulier la répartition équitable de gains entre les joueurs lorsqu'une partie est interrompue avant que le nombre des points convenus pour gagner soit atteint. Sont mises en avant la quantité fondamentale qu'est la 'valeur' d'une partie (autrement dit, l'espérance) et l'idée de probabilité conditionnelle.

1657-8. Défis lancés par Fermat aux mathématiciens européens (incluant la détermination des solutions en nombres entiers de l'équation dite de Pell-Fermat).

1659. Lettre-bilan sur ses travaux arithmétiques. Fermat explicite sa méthode de la descente infinie et donne une liste de problèmes sur les entiers qu'elle peut résoudre (dont les premiers cas du Grand Théorème).

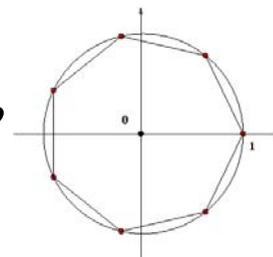
c. 1660. Controverse avec les épigones de Descartes sur la loi de la réfraction: partant du principe que 'la nature agit toujours par les voies les plus courtes et les plus simples' 'ou en tout cas par le temps le plus court', Fermat ramène la réfraction à une question géométrique d'extremum, qu'il résout par voie algébrique (retrouvant à sa grande surprise la loi cartésienne!).

Mort à Castres en 1665.

Pour généraliser les travaux de Gauss sur la loi de réciprocité quadratique, Kummer conçut l'arithmétique des nombres  $a + \zeta b$ , avec  $a$  et  $b$  entiers et  $\zeta$  un nombre complexe vérifiant  $\zeta^n = 1$ . Kummer découvrit des difficultés majeures pour généraliser l'arithmétique usuelle: il n'existe pas par exemple de décomposition unique en facteurs premiers pour ces nombres. Il parvint cependant, en inventant une nouvelle sorte de nombres, à récupérer à leur niveau une arithmétique adéquate et à démontrer certaines lois de réciprocité. Au passage, il appliqua ces idées au problème de Fermat. On peut en effet factoriser l'équation

$$a^n + b^n = (a+b)(a+\zeta b)\dots(a+\zeta^{n-1}b)$$

et, en utilisant son arithmétique, Kummer démontra le théorème de Fermat pour toute une famille d'exposants, en particulier pour tous les exposants plus petits que 100 (sauf trois d'entre eux qui furent étudiés un peu plus tard).



Les nombres complexes tels que  $\zeta^n = 1$

La démonstration de Wiles repose sur une réinterprétation géométrique. Dès les années 70, Yves Hellegouarch (université de Caen) avait relié l'équation de Fermat à celle de la courbe

$$y^2 = x(x-a^n)(x+b^n).$$

On remarquera qu'ici l'équation de Fermat n'est pas interprétée directement comme celle d'une courbe: chaque solution éventuelle de l'équation de Fermat définit les coefficients d'une courbe particulière, qu'on appelle courbe elliptique.

Au milieu des années 80, il fut montré que si le théorème de Fermat était faux, c'est-à-dire s'il existait une courbe elliptique avec les coefficients comme ci-dessus, elle contredirait une conjecture très importante en mathématiques, la conjecture de Shimura-Taniyama-Weil. Cette conjecture établit un dictionnaire entre les courbes elliptiques et des fonctions dites « modulaires »; ces dernières ressemblent un peu aux fonctions cosinus et sinus, en particulier elles vérifient certaines propriétés de périodicité.

Le lien entre la conjecture Shimura-Taniyama-Weil et le théorème de Fermat n'est pas du tout facile; Ken Ribet, qui l'a établi en 1986, a d'ailleurs reçu pour cela... le prix Fermat. Et c'est un cas particulier, suffisant pour le théorème de Fermat, qu'a obtenu Andrew Wiles, avec l'aide de Richard Taylor. La théorie développée pour cela a beaucoup d'intérêt en elle-même et donne l'espoir de mieux comprendre les relations profondes entre des objets issus de la géométrie (algébrique) et d'autres issus de l'analyse (fonctions modulaires).