Le théorème de Fermat : huit ans de solitude

Matthieu Romagny, Université Pierre et Marie Curie (Paris 6)

Conférence donnée pour la Fête de la Science, le 22 novembre 2008

Cet exposé a pour fil conducteur un théorème dont l'énoncé a été formulé par Pierre de Fermat (1601-1665), juriste français qui a vécu au dix-septième siècle, et dont la démonstration a été achevée en 1994 par Andrew Wiles (1953-), mathématicien anglais du vingtième siècle (et aussi du vingt-et-unième !). Ce théorème avait pris une telle place dans le paysage mathématique, et sa démonstration a constitué un tel événement dans la communauté scientifique, que les différents rapports qui en ont été faits ont été la plupart du temps très centrés sur la démonstration elle-même, sa stratégie, ses différents ingrédients. Je vais quant à moi prendre plutôt ce théorème pour prétexte pour faire un peu d'histoire, de sociologie et d'épistémologie (ce sont de bien grands mots !) sur les mathématiques et les mathématiciens. J'espère qu'il n'y a pas trop de gens dans l'assistance qui sont venus en se disant « chouette, je vais enfin comprendre le théorème de Fermat et je repartirai en sachant le démontrer ». Ceux-là seraient déçus ! Et je dois vous avouer tout de suite que je n'ai pas lu toute la démonstration du Grand Théorème (c'est comme cela qu'on l'appelle), et même, qu'il me faudrait vraisemblablement plusieurs mois de travail pour la lire et la comprendre entièrement.

Après cette petite introduction, vous pourriez avoir envie de vous indigner : qui c'est ce type qui vient nous parler du Grand Théorème de Fermat sans avoir lu sa démonstration ? Et pire encore, qui se prétend mathématicien et qui avoue qu'il lui faudrait plusieurs mois pour la comprendre ? Vous pourriez être titillés par certains détails : Fermat, juriste ?!? Il y en a même peut-être parmi vous qui se demandent ce que ce théorème a de si terrible pour qu'on fasse tant de bruit autour. C'est pour répondre à ces questions, éclairer certains points qui ne sont pas toujours bien mis en valeur, et tordre le cou à quelques idées fausses, que je vous raconte cette histoire. Pour que l'honneur soit sauf, nous ferons un peu de mathématiques, mais « à dose régime ». Quand on fait des maths, c'est comme partout ailleurs : lorsque c'est simple on y arrive, on est content ; quand cela se complique un peu, on s'accroche, d'autant plus quand on trouve la question jolie ; et puis, chacun à un moment différent, on décroche... Mais souvent on est tout de même pris par l'aspect esthétique et ludique du problème, et on voudrait connaître la solution ! Peut-être passerez-vous pendant l'exposé par ces différentes phases, ce qui voudra dire que vous aurez fait des maths.

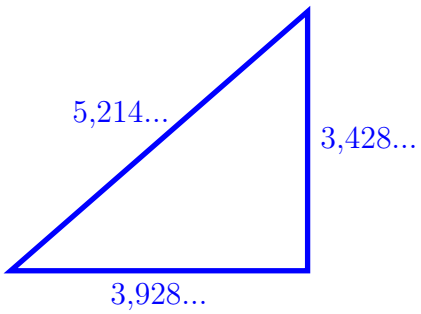
$\therefore$

Ainsi donc, pour apporter la dernière pierre à cette démonstration, nous avons un mathématicien – évidemment – alors que la personne qui a formulé l'énoncé était juriste ! C'est qu'au dix-septième siècle, faire des mathématiques, cela ne faisait pas forcément gagner sa vie, et il y avait peu de mathématiciens professionnels. Et de fait, Fermat était mathématicien amateur, ce qui ne l'empêchait pas de communiquer avec les scientifiques en poste dans les plus grandes universités européennes. À partir du dix-neuvième et surtout du vingtième siècle, les nations les plus riches ont eu (ou, se sont donné) les moyens d'employer un plus grand nombre de personnes au service du développement de la science. Ceci a un prix, mais je crois que c'est un sage investissement sur l'avenir, tant qu'on donne la possibilité aux citoyens de comprendre ce que peut faire la science et ce qu'elle ne peut pas faire, et de décider de l'opportunité d'utiliser ses découvertes. Le résultat est que la quantité de travaux mathématiques produits après 1950 est égale à la quantité de travaux produits dans toute l'histoire de l'Humanité jusqu'à cette date ! On compte aujourd'hui 1500 revues dans le monde, publiant 250000 articles par an dans 100 langues. Alors que l'une des questions les plus souvent posées à un mathématicien concerne le fait qu'il n'y aurait plus rien à trouver en maths... Eh bien oui, l'activité mathématique explose, et chaque réponse apportée pose dix questions nouvelles.

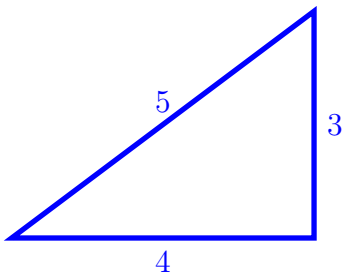
Pierre de Fermat

$\therefore$

Ce mathématicien amateur, Pierre de Fermat, dispose d'une traduction en latin d'un ouvrage qui s'appelle l'*Arithmétique* de Diophante (né aux alentours de 207, mort aux alentours de 291). Diophante y parle du théorème de Pythagore (né aux alentours de -569, mort aux alentours de -494), dont vous vous rappelez sûrement. Allez, farfouillez dans vos souvenirs... la somme des carrés des deux côtés de l'angle droit est égale au carré de l'hypoténuse.

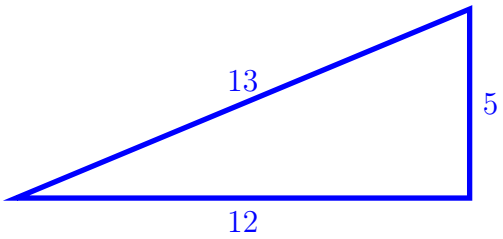


Sur cet exemple, le théorème de Pythagore dit que $(3,428...)^2+(3,928...)^2 = (5,214...)^2$. Ce qui intéressait Pythagore, c'est surtout les nombres entiers : 1, 2, 3, ... Il se trouve qu'il existe des triangles rectangles dont les trois côtés ont une longueur entière. Voici le plus connu :



$$3^2 + 4^2 = 5^2$$

En voici un autre :



$$5^2 + 12^2 = 13^2$$

Dans son *Arithmétique*, Diophante explique comment trouver *tous* les triangles rectangles dont les trois côtés ont une longueur entière. Ce n'est pas très difficile, et nous allons le faire ensemble (après, vous pourrez dire : « je l'ai fait ! »). Si on dispose d'un tel triangle, appelons x et y les longueurs des côtés de l'angle droit et z la longueur de l'hypoténuse. Ce sont des nombres entiers qui vérifient

$$x^2 + y^2 = z^2 \ .$$

Commençons par le cas plus simple où x, y, z ne sont pas divisibles tous les trois par un même entier $d > 1$ (on dit que leur *plus grand commun diviseur*, en abrégé pgcd, est 1). Alors x et y ne peuvent pas être pairs tous les deux, car sinon $x^2 + y^2$ serait pair, donc z^2 aussi, ce qui n'est possible que si z est pair, or on est dans un cas où x, y, z ne sont pas divisibles tous les trois par 2. Par un raisonnement qui ressemble, on peut montrer que x et y ne peuvent pas être impairs tous les deux. Donc l'un est pair et l'autre pair.

Disons que x est pair, y est impair, et alors z n'a plus le choix : il est impair. Si l'on réécrit l'équation comme cela :

$$x^2 = z^2 - y^2 = (z+y)(z-y) \ ,$$

on voit que $z-y$ et $z+y$, somme et différence de deux nombres impairs, sont pairs. Notons $z+y = 2a$, $z-y = 2b$, $x = 2c$. On se retrouve avec la nouvelle équation

$$c^2 = ab \ .$$

Comme le pgcd de x, y, z est 1, on peut voir qu'il en est de même pour a, b, c. Un petit raisonnement que nous admettrons permet de voir que comme $ab = c^2$ est un carré, a et b eux-mêmes doivent être des carrés. Ainsi,

$$a = i^2 \quad , \quad b = j^2 \quad \text{et} \quad c = ij$$

et en fait $i = \text{pgcd}(a, c)$ et $j = \text{pgcd}(b, c)$. En repassant aux inconnues x, y, z il vient :

$$x = 2ij \quad , \quad y = i^2 - j^2 \quad \text{et} \quad z = i^2 + j^2 \ .$$

Voilà pour le cas où le pgcd de x, y, z est 1. Maintenant, si le pgcd de x, y et z est un nombre $d > 1$, on peut écrire $x = dx'$, $y = dy'$, $z = dz'$ et on peut appliquer le raisonnement qui précède à x', y', z'. On obtient la forme générale d'une solution de l'équation qui nous intéresse, et on considère qu'on a résolu notre problème au sens où :

pour tout choix de d, i et j on obtient un triangle rectangle de côtés entiers

$$x = 2dij,\ y = d(i^2 - j^2),\ z = d(i^2 + j^2),$$

et de plus on obtient ainsi tous les triangles rectangles à côtés entiers.

Voilà ; si certains d'entre vous se sont accrochés et sont arrivés à ce moment où l'on décroche, vous pouvez raccrocher. Les parties les plus coriaces de l'exposé sont derrière nous, et la suite sera plus simple.

On peut s'amuser à essayer quelques exemples, cela permet aussi de vérifier qu'on ne s'est pas trompé. Lorsque j'ai préparé cette conférence, j'ai essayé les valeurs $d = 1$, $i = 29$ et $j = 12$. J'ai trouvé :

$$x = 696 \quad , \quad y = 697 \quad , \quad z = 985 \ .$$

Évidemment, on peut vérifier à la calculatrice que $696^2 + 697^2 = 985^2$. Le hasard a voulu que je tombe sur une solution dans laquelle x et y sont presque égaux... On peut se demander s'il existe des triangles rectangles à côtés entiers avec deux côtés vraiment égaux (pas seulement presque). Mais Pythagore – encore lui ! – a démontré qu'il n'en existe pas... Alors on peut se demander s'il y a beaucoup de triangles rectangles tels que les côtés de l'angle droit sont égaux à une unité près. Ceci mène à l'équation $d(i^2 - j^2) = 2dij + 1$. On peut aussi fixer un nombre entier e qu'on appelle un *écart*, et se demander s'il y a

beaucoup de triangles rectangles tels que les côtés de l'angle droit ont un écart égal à e. Ceci mène à l'équation $d(i^2 - j^2) = 2dij + e$. Je n'ai pas cherché plus loin... La curiosité de Fermat est allée dans une autre direction. Mais vous voyez : on résout un problème, et on en a dix nouveaux qui se posent naturellement.

$\therefore$

Fermat, donc, lit tout cela dans Diophante, et il a la curiosité de s'intéresser à l'équation proche $x^3 + y^3 = z^3$. Avec un peu d'astuce et de patience, on peut trouver des nombres x, y, z qui donnent presque une solution, par exemple $6^3 + 8^3$ est égal à 9^3... moins 1. Mais Fermat affirme, lui, que ni l'équation $x^3 + y^3 = z^3$, ni l'équation $x^4 + y^4 = z^4$, ni même l'équation $x^n + y^n = z^n$ pour un entier n supérieur, n'admet de solution en nombres entiers. En images :

Timbre du théorème de Fermat

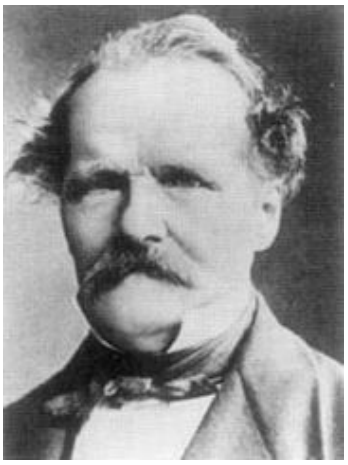
C'est ce qu'on appelle le Grand Théorème de Fermat (Fermat's Last Theorem en anglais), bien que ce ne soit devenu un théorème au sens strict du mot qu'en 1994. Et dans la marge de son exemplaire de l'*Arithmétique* de Diophante, Fermat écrit :

J'ai une démonstration véritablement merveilleuse de cette proposition,

que cette marge est trop étroite pour contenir.

Malheureusement pour nous, Fermat publiait très peu ses résultats. Pire encore, bien souvent il tenait cachées ses démonstrations, mettant ses interlocuteurs au défi de les retrouver ! On n'a jamais su si Fermat possédait en effet une preuve de son théorème.

De la démonstration, on n'a retrouvé que le cas $n = 4$, qu'il a établi aux alentours de 1637. Les progrès suivants sur la preuve du théorème concernent les petites valeurs de l'exposant n, et viennent assez lentement : Euler (1707-1783) en 1753 pour le cas $n = 3$, Dirichlet (1805-1859) et Legendre (1752-1833) en 1825 pour $n = 5$, Lamé (1795-1870) en



Ernst Kummer

Leonhard Euler

Carl Gustav Jacobi

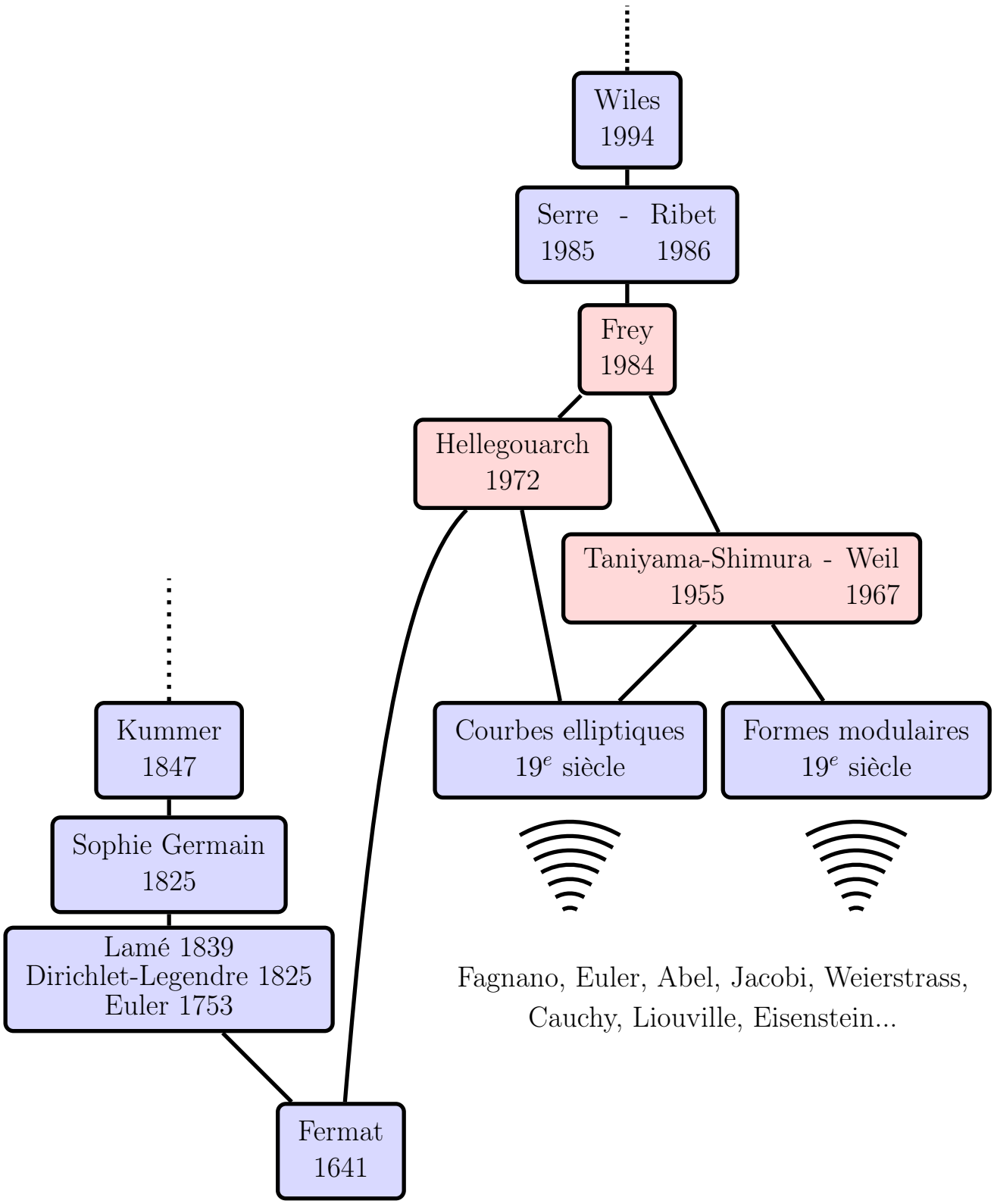
1839 pour $n = 7$. On peut avoir l'impression que le cas $n = 6$ est laissé en route. En fait, il découle du cas $n = 3$, car s'il existait des entiers tels que $x^6 + y^6 = z^6$, alors $X = x^2$, $Y = y^2$, $Z = z^2$ vérifieraient $X^3 + Y^3 = Z^3$. Par un argument semblable, il est suffisant de s'intéresser à l'équation de Fermat avec n un nombre premier.

Il faut attendre les travaux de Sophie Germain (1776-1831), puis surtout de Kummer (1810-1893) pour voir se développer des méthodes pour traiter des exposants n arbitraires, c'est-à-dire autres que les cas particuliers correspondants aux petites valeurs. Les spectaculaires résultats de Kummer ont établi le théorème de Fermat pour tous les exposants $n \leq 100$. Mais ce qui est sans doute encore plus important pour les mathématiciens, c'est qu'ils ont ouvert de nouvelles branches de recherche en algèbre et en théorie des nombres. Je ne veux pas parler trop de Kummer aujourd'hui, alors je signale juste qu'il existe un très bon livre qui décrit ses travaux (c'est un livre de niveau avancé ; voir les références en fin d'exposé). Ce livre a été écrit par H. Edwards en 1977, date à laquelle, sur le théorème de Fermat, on n'était pas beaucoup plus avancé que Kummer...

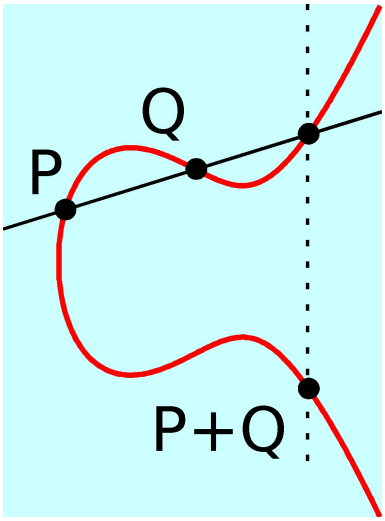
$\therefore$

Dans la fin de l'exposé, nous allons parler un peu du chemin qui a mené à la démonstration du théorème de Fermat, culminant avec le travail d'Andrew Wiles. Comme je vous ai promis que les efforts mathématiques étaient derrière nous, nous n'entrerons pas trop dans les détails. Nous dirons juste ce qu'il faut pour commenter le schéma de la page suivante, qui relie entre eux les différents contributeurs.

La démonstration du théorème de Fermat s'appuie sur une toute autre stratégie que celles envisagées jusqu'en 1986. Elle utilise des théories mathématiques développées essentiellement au dix-neuvième et au vingtième siècle, et en particulier les mathématiques les plus modernes de la fin du vingtième, incluant les travaux de cinq lauréats de la médaille Fields. Nous allons nous contenter de nommer deux des personnages centraux de la preuve de Wiles.

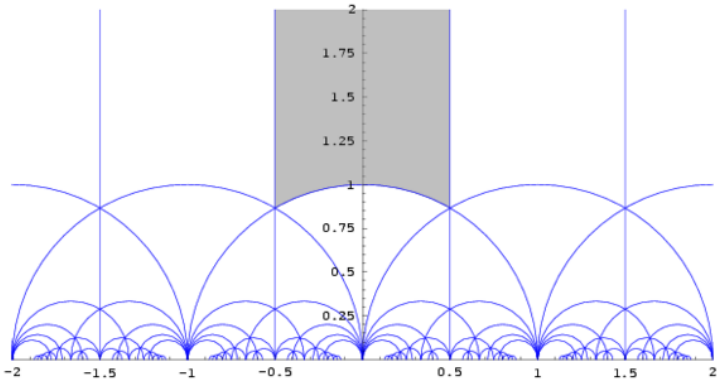

Wiles
1994
Serre - Ribet
1985 1986
Frey
1984
Hellegouarch
1972
Taniyama-Shimura - Weil
1955 1967
Courbes elliptiques
19e siècle
Formes modulaires
19e siècle
Fagnano, Euler, Abel, Jacobi, Weierstrass,
Cauchy, Liouville, Eisenstein...
Kummer
1847
Sophie Germain
1825
Lamé 1839
Dirichlet-Legendre 1825
Euler 1753
Fermat
1641

Le premier personnage est la famille des *courbes elliptiques*. Très brièvement, les courbes elliptiques sont des courbes planes définies par une équation polynomiale et dont on peut « additionner » les points par une loi d'addition qui s'interprète de manière très géométrique. Une courbe elliptique possède toujours un axe de symétrie, qui est horizontal sur le dessin ci-contre. Pour additionner deux points P et Q, tracez la droite qui les joint. Cette droite recoupe la courbe en un troisième point, dont le symétrique par rapport à l'axe de symétrie est le point $P + Q$ recherché. L'apparition des courbes elliptiques repose sur des travaux précurseurs de Fagnano (1682-1766) et Euler (1707-1783). Puis Abel (1802-1829) démontre qu'il est possible d'additionner les points par une construction géométrique simple. La théorie est ensuite complétée par Jacobi (1804-1851), Weierstrass (1825-1897), Cauchy (1789-1857), Liouville (1809-1882), Eisenstein (1823-1852)...



Addition des points d'une courbe elliptique

L'autre personnage important s'appelle la famille des *formes modulaires*. Les formes modulaires sont des fonctions définies sur le plan des nombres complexes, et qui possèdent des propriétés de symétrie remarquables. Les premières formes modulaires se trouvent semble-t-il dans des travaux de Bernoulli (1654-1705), Euler, Jacobi, puis Klein (1849-1925) les étudie de manière plus systématique. Mais elles apparaissent aussi dans des travaux de Gauss (1777-1855), Abel, Hermite (1822-1901)... Le dessin suivant ne prétend pas véritablement vous aider à imaginer ce qu'est une forme modulaire, mais il vous montre que c'est un objet compliqué, qui possède de nombreuses symétries.



Symétries d'une forme modulaire

Courbes elliptiques et formes modulaires sont situées au carrefour de l'algèbre, de la géométrie, de l'analyse et de la théorie des nombres. Comme on l'a vu, leur naissance a été un long processus qui a mis en jeu le travail de nombreux des plus grands mathématiciens de l'époque. Sur le schéma récapitulatif, les vaguelettes indiquent que cette naissance s'est faite par une lente maturation, une diffusion d'idées qui peu à peu se sont organisées pour former une théorie cohérente.

Bien sûr, il y a des liens entre courbes elliptiques et formes modulaires, ce qui explique d'ailleurs que l'on trouve les noms de certaines personnes qui se sont intéressées à l'un et à l'autre des sujets. Cependant, le lien précis qui est le point de départ de la preuve de Wiles n'a été suggéré qu'en 1955 par le japonais Yutaka Taniyama (1927-1958). Il a été ensuite reformulé par son collègue japonais Goro Shimura (1930-) puis étayé et complété par le français André Weil (1906-1998), ce qui explique son appellation de *conjecture de Taniyama-Shimura-Weil* (TSW). En mathématiques, une conjecture est un énoncé que l'on croit vrai, sur la base d'intuitions ou de constatations empiriques, mais qui attend d'être démontré. Une conjecture peut d'ailleurs être fausse, tant qu'elle n'a pas été démontrée, comme c'était le cas de l'affirmation de Fermat avant 1994. De manière outrageusement simplificatrice, la conjecture TSW dit la chose suivante. Partant d'une courbe elliptique, pour chaque nombre entier $n \geq 1$ on peut considérer le nombre a_n de points de la courbe qui sont « à coordonnées entières » en un certain sens, et fabriquer une fonction $f(q) = \sum_{n=1}^{\infty} a_n q^n$. La conjecture dit que cette fonction f est une forme modulaire.

Ensuite, dans sa thèse en 1972, le français Yves Hellegouarch établit un pont encore fragile entre le théorème de Fermat et les courbes elliptiques. En supposant qu'il existe une solution (a, b, c) de l'équation de Fermat (ce que l'on suppose être faux, naturellement), il associe à cette solution une courbe elliptique que nous noterons $E_{a,b,c}$ et constate que cette courbe possède des propriétés très particulières. Notez que, dans cette situation, il est extrêmement intéressant d'étudier un objet alors même qu'on suppose qu'il n'existe pas...

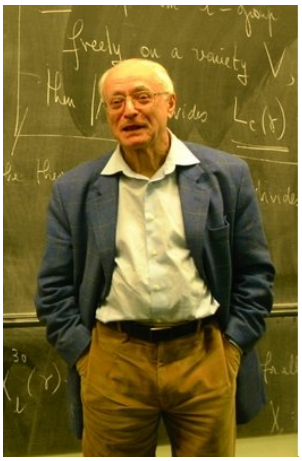
Un pas décisif est franchi en 1984 lorsque l'allemand Gerhard Frey (1944-) suggère que les propriétés de la courbe $E_{a,b,c}$ sont si particulières que son existence est incompatible avec la conjecture de Taniyama-Shimura-Weil. Dit autrement, si l'on parvient à démontrer la conjecture TSW, alors l'existence de $E_{a,b,c}$ est impossible, donc l'existence d'une solution (a, b, c) est elle-même impossible, et le théorème de Fermat est démontré. Cette idée de Frey a redonné beaucoup de foi en l'espoir d'une preuve du théorème de Fermat, car elle l'a relié à une branche de la théorie des nombres sur laquelle beaucoup de monde travaillait.


Gerhard Frey

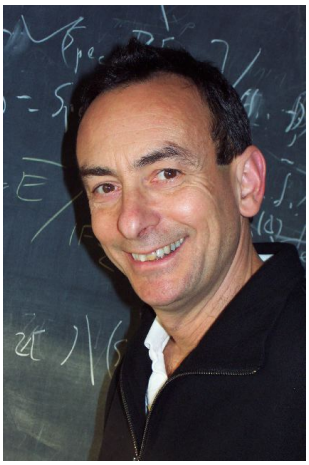
Dans le schéma récapitulatif, les cases colorées en rose indiquent un moment où un (ou des) mathématicien(s) a deviné un lien caché entre divers objets, sur la base de constatations empiriques, d'analogies, de calculs et d'exemples, et bien souvent, d'une

grande intuition. Ces moments sont décisifs pour la suite des événements, car ils donnent à leur découvreur et à toute la communauté des mathématiciens un problème sur lequel travailler : comment démontrer que ce lien existe bel et bien ? Il faut souligner que la personne qui a cette intuition *ne* démontre *pas* un résultat, et pourtant ce moment est tout à fait crucial dans le processus de recherche.

Les choses s'accélèrent, car l'année suivante, en 1985, le français Jean-Pierre Serre (1926-) formule des conjectures plus précises que l'affirmation de Frey, et en 1986 ces conjectures sont démontrées par l'américain Ken Ribet (1948-). On sait dès lors que si la conjecture TSW est vraie, alors l'équation de Fermat n'a pas de solution. Le défi reste immense, car personne à cette date-là n'a d'idée pour s'attaquer à la conjecture TSW. Andrew Wiles n'a sans doute lui-même que des idées éparses sur la question, mais il voit qu'il est plus proche que jamais de son rêve d'enfant de démontrer le Grand Théorème de Fermat. Il décide donc de dévouer désormais tout son temps à la conjecture TSW.

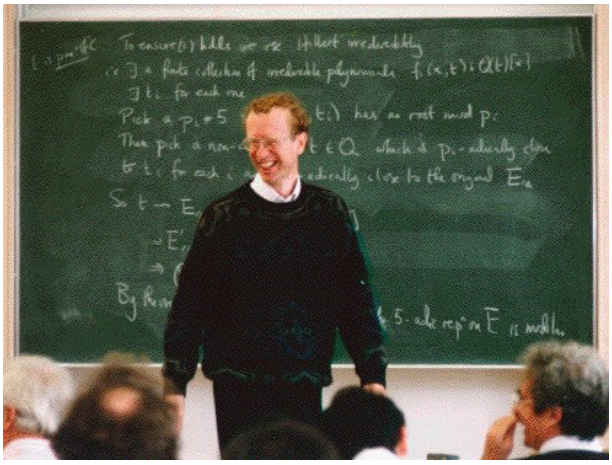


Jean-Pierre Serre



Ken Ribet

Nous sommes arrivés au point qui explique le titre de l'exposé, car il faudra huit ans de travail à Wiles, dans un isolement quasi-total, pour arriver à son but. L'effort nécessaire s'annonce énorme, mais la première difficulté était en fait de croire en la possibilité d'arriver à une démonstration là où tant d'autres ont échoué. Wiles fait le choix, sage mais difficile, de ne parler de son travail à personne, pour se soustraire à la pression qui viendrait de la communauté mathématique, curieuse de tout progrès en la matière. Ses progrès ont une trajectoire sinueuse, caractéristique du travail de recherche : essais inspirés mais infructueux, combinaison de différentes idées, apports personnels et intervention de l'actualité mathématique, alternance de moments d'espoir et de découragement. Le dernier de ces rebondissements est aussi le plus spectaculaire : en 1993, lors d'une conférence à Cambridge, Wiles annonce avoir démontré la conjecture TSW dans un cas suffisant pour établir le théorème de Fermat.



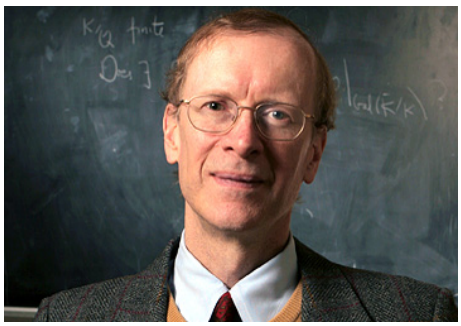
Andrew Wiles à la fin de sa conférence de Cambridge en 1993

Mais à l'automne, l'une des personnes qui effectue une vérification détaillée des manuscrits de Wiles découvre une erreur subtile. Wiles ne veut pas succomber à l'abattement et se replonge dans le travail, mais maintenant la communauté mathématique tout entière « écoute à la porte »... Il tente de s'isoler de nouveau, et pendant plusieurs mois, toutes les rumeurs circulent. En décembre 1993, il se prononce par un message électronique qui circule dans la communauté, pour confirmer qu'il y a un problème :

```
Subject :  Fermat Status
Date :  4 Dec 93  01:36:50  GMT

            In view of the speculation on the status of my work on the
Taniyama-Shimura conjecture and Fermat's Last Theorem I will give a brief
account of the situation.  During the review process a number of problems
emerged, most of which have been resolved, but one in particular I have
not yet settled.  The key reduction of (most cases of) the Taniyama-Shimura
conjecture to the calculation of the Selmer group is correct.  However
the final calculation of a precise uppper bound for the Selmer group in
the semistable case (of the symmetric square representation associated to
a modular form) is not yet complete as it stands.  I believe that I will
be able to finish this in the near future using the ideas explained in my
Cambridge lectures.

            The fact that a lot of work remains to be done on the manuscript
makes it still unsuitable for release as a preprint.  In my course in
Princeton beginning in February I will give a full account of this work.

Andrew Wiles.
```

Au début de l'année 1994, il décide de continuer à travailler en demandant à l'un de ses anciens étudiants, Richard Taylor, de venir l'aider. Au cours de l'été suivant, les deux hommes commencent à perdre confiance et se préparent à admettre l'échec... Mais à l'automne 1994, Wiles a une nouvelle idée qui vient mettre un point final à la preuve. L'article comportant l'essentiel de son travail pour démontrer le Grand Théorème de

Fermat est paru en 1995 sous le titre *Modular elliptic curves and Fermat's Last Theorem* dans la revue Annals of Mathematics. C'est un article de 109 pages, qui s'appuie sur des centaines et des centaines de pages de travaux d'autres mathématiciens... La première page de cet article est reproduite à la fin de ces notes.



Andrew Wiles

La démonstration mise au point par Wiles est un travail énorme, qui utilise de nombreuses idées extrêmement ingénieuses et novatrices. Cette démonstration, autant et même plus que ce qu'elle démontre, a redynamisé une branche entière des mathématiques. On demande souvent aux mathématiciens, plus encore qu'aux autres scientifiques, l'intérêt des questions qu'ils se posent. La réponse est parfois malaisée, car les mathématiciens ont souvent des motivations essentiellement esthétiques. Mais l'histoire du théorème de Fermat et de sa preuve sont tout de même extrêmement riches en enseignements. Si l'on se cantonne à la question de l'intérêt interne du théorème dans le champ des mathématiques, il faut signaler que la conjecture de Taniyama-Shimura-Weil était un point central d'intérêt en théorie des nombres. Elle a été prouvée par Wiles dans le but de démontrer le théorème de Fermat. L'histoire que nous avons décrite ici montre qu'un ingrédient essentiel pour réaliser des projets d'une grande envergure est d'avoir la foi que l'on peut déplacer une montagne, et l'énergie pour le faire. Quoi de mieux qu'un rêve d'enfant, un problème qui s'énonce aussi simplement que le théorème de Fermat, pour donner cette énergie !

Le dernier mot de ce texte est pour dire que, sur le schéma récapitulatif, les pointillés qui partent de la case de Wiles (et de celle de Kummer) indiquent qu'il y a encore beaucoup de pistes de travail pour poursuivre l'aventure. Car l'histoire du théorème de Fermat ne déroge pas à la règle que vous connaissez : chaque réponse apportée pose dix questions nouvelles...

$\therefore$

Voici une courte sélection de documents sur le théorème de Fermat et la preuve de Wiles.

Ouvrages et documentaire grand public

- *Le dernier théorème de Fermat* par Simon Singh. Ce livre est paru aux éditions JC Lattès (1998) et est maintenant aussi disponible en format poche aux éditions Hachette, dans la collection Pluriel (1998). La première version comporte des photos que ne comporte pas la deuxième.

- *Fermat's Last Theorem*, par Simon Singh, documentaire de la BBC tourné pour la série Horizon (1996). Ce documentaire réalisé à l'attention du grand public est difficile à se procurer pour l'achat mais est très facile à trouver sur internet, sur les sites d'hébergement de vidéos usuels. Il comporte des interviews de nombreux mathématiciens impliqués dans la preuve du théorème (y compris Wiles lui-même bien sûr), est très vivant, et je vous le recommande très vivement.

- *The Fermat Diary*, par C. J. Mozzochi (2000), éditions A.M.S. (American Mathematical Society). Ce livre en anglais est un récit, destiné aux non-mathématiciens, des événements de la fin de la preuve, de 1993 à 1995. Il est intéressant notamment car il comporte de très nombreuses photos de mathématiciens, prises par l'auteur.

Ouvrages plus spécialisés

- *Invitation aux mathématiques de Fermat-Wiles*, par Yves Hellegouarch, éditions Masson (1997). Ce livre, issu d'un cours de maîtrise donné par l'auteur à l'Université de Cæn, présente une introduction aux courbes elliptiques et aux formes modulaires qui permet d'arriver aux énoncés des théorèmes les plus difficiles sur la question (qui ne sont pas démontrés). Le style est très agréable, et l'approche historique du théorème de Fermat et de tous les thèmes présents dans le livre est très intéressante.

- *Fermat's Last Theorem*, Harold M. Edwards, Springer (1977), numéro 50 dans la collection Graduate Texts in Mathematics. Ce livre présente la théorie algébrique des nombres en prenant le théorème de Fermat pour fil conducteur.

Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By ANDREW WILES*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, 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.

Pierre de Fermat

Introduction

An elliptic curve over $\mathbf{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over $\mathbf{Q}$ with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over $\mathbf{Q}$ is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

*The work on this paper was supported by an NSF grant.