Le dernier théorème de Fermat

Paul Milan

12 janvier 2004

Table des matières

1 Pierre de Fermat (20 août 1601 - 1665).

Pierre de Fermat fit son éducation chez les franciscains puis à l'université de Toulouse. En 1631, il est nommé conseiller à la Chambre des Requêtes au parlement de Toulouse (3 ans après la nomination de Richelieu à la tête du gouvernement). Il est un fonctionnaire efficace et courtois mais s'acquitte de ses tâches sans se distinguer. Il frôle la mort en contractant la peste en 1652. En Europe, à l'époque, seule l'université d'Oxford avait une chaire de géométrie. En France, les mathématiques se font à l'intérieur d'une petite communauté surtout à Paris. Fermat est ainsi isolé de la communauté des mathématiciens (Pascal, Gassendi, Roberval, Beaugrand, et l'abbé Marin de Mersenne). Fermat travaille seul. Le culte du secret remontait aux cossistes italiens du XVIéme siècle. " *Cossiste* " vient de " *cosa* " la " *chose* " en italien, un peu comme x représente l'inconnue. Tartaglia se fâche ainsi avec Cardan qui publia ses travaux sur les équations du 3ème degré. Mersenne combattit cette conspiration du silence en proposant des rencontres régulières par exemple à l'Académie des Sciences. Ainsi Mersenne est en correspondance avec Descartes. Il rend visite à Fermat à chaque déplacement en province. On doit à Fermat de nombreux travaux en arithmétique, cependant il ne publia jamais ses preuves laissant aux autres le soin de les retrouver. Ce qui fit dire à Descartes que Fermat était un " *vantard* ". Pascal et Fermat correspondaient sur une nouvelle branche des mathématiques : les probabilités. Résolution de problèmes tels que : soit 23 convives, quelle est la probabilité que deux d'entre eux aient la même date d'anniversaire ? 10%, 30%, 50% ou 70% ? Avec 30 convives : 10%, 30%, 50% ou 70% ?

Fermat est aussi associé à la création du calcul différentiel (dérivée). On pensa pendant des siècles que Newton avait découvert le calcul différentiel sans connaître le travail de Fermat, mais en 1934, on découvrit une note de Newton contenant la mention " la méthode de Fermat de tracer des tangentes "

2 Ensembles

$\mathbb{N}$: Les entiers naturels,
$\mathbb{Z}$: les entiers relatifs,
$\mathbb{Q}$: Les nombres rationnels (fractions),
$\mathbb{R}$: les nombre réels (rationnels et irrationnels),
$\mathbb{C}$: Les nombres complexes (réels et imaginaires)

3 Triplets pythagoriciens

Combinaison de trois nombres entiers x, y , z tels que :

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

Tout le monde connaît le triplet $(3, 4, 5)$, mais les pythagoriciens en recherchèrent d'autres par exemple $(5, 12, 13)$, (99, 4 900, 4 901). Leur nombre est infini (démontré par Euclide).

4 Le dernier théorème de Fermat (1637).

En s'inspirant des triplets de Pythagore, Fermat eut l'idée de changer la puissance des trois entiers. Ne trouvant ni de solution au cube ni à la puissance 4, il arriva à la conclusion qu'il n'y en avait pas. Il posa alors la conjecture suivante :

il n'existe pas de triplets d'entiers (non nuls) vérifiant :

$$x^n + y^n = z^n \quad \text{pour} \quad n > 2$$

Bien que Fermat ait écrit ce commentaire qui allait hanter des générations de mathématiciens "j'ai une démonstration véritablement merveilleuse de cette proposition, que cette marge est trop petite pour contenir ", il n'en proposa la preuve que pour $n = 3$ (dans les grandes lignes) et $n = 4$ (méthode de la décroissance infinie, spirale de Fermat). Ce théorème a résisté 358 ans aux mathématiciens !

5 Diophante

Le mathématicien qui a fait pour les nombres ce qu'Euclide fit pour la géométrie fut Diophante d'Alexandrie, le dernier héros de la tradition grecque. Son lieu de naissance est inconnu et son arrivée à Alexandrie peut se situé dans une marge de temps de 5 siècles. Il vécut après 150 av. JC et avant 364 ap. JC. On admet qu'il vécut vers 250 ap. JC. Sa spécialité résidait dans les problèmes dont les solutions sont des nombres entiers. Par exemple les équations du type :

$$ax + by = c$$

6 Théorème et conjecture.

Les mathématiciens se servent de théorèmes comme des jalons sur la route de nouveaux résultats ; il est donc essentiel que chacun des théorèmes soit démontré. Ce n'est pas parce que Fermat disait qu'il avait fait la démonstration d'un théorème qu'on devait le croire sur parole. Avant qu'on puisse l'utiliser, chaque théorème doit être démontré avec une imparable rigueur, sans quoi les conséquences risquent d'être désastreuses car d'autres théorèmes peuvent en dépendre. C'est un château de cartes et si une erreur surgit tout le bel édifice s'effondre. Les hypothèses qui ne sont pas vérifiées ont beaucoup moins de valeur et sont désignées sous le nom de conjectures. Toute logique qui se fonde sur une conjecture est elle-même une conjecture.

7 Léonhard Euler (1707 à Bâle, 1783).

Par le recours à la spirale de Fermat, Euler démontra la conjecture pour $n = 3$ et $n = 4$ en recourant aux nombres complexes. C'était la première fois depuis cent ans que quelqu'un relevait le défi. C'était une méthode prodigieuse mais qui ne s'appliquait pas pour d'autres valeurs de n. Bien que les mathématiciens ne fissent que des progrès lents, la situation s'était un peu améliorée. En effet lorsque n n'est pas un nombre premier, si n par exemple est un multiple d'un nombre premier p et si le théorème de Fermat est vrai pour la valeur p, il le sera de même pour n. Il ne restait qu'à démontrer le théorème pour les nombres premiers. Malheureusement, il y a une infinité de nombres premiers (prouvé par Euclide). Le théorème fut vérifié au début du $19^{\text{ème}}$ siècle pour les exposants 5 (Dirichlet) et 7 (Lamé). Mais il en restait toujours une infinité à démontrer.

8 Sophie Germain (1776-1831).

Démontré dans les années 1810, le théorème de Sophie Germain affirme que si p et $2p + 1$ sont des nombres premiers (exemple 5 et 11, 11 et 23) alors le théorème de Fermat

est vérifié pour l'exposant p. Elle montre d'abord que si l'équation de Fermat est vérifiée, il n'y a qu'un nombre fini de solutions possibles. Elle démontre ensuite qu'aucune de ces solutions ne vérifie l'équation de Fermat.

9 Ernst Eduard Kummer (1810 - 1893)

Critère de Kummer : p est un nombre premier régulier si et seulement si p^2 ne divise aucune des sommes

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \quad \text{avec} \quad k = 2,\ 4,\ 6, \ldots,\ p-3$$

Kummer fit faire un grand pas en montrant que si p est un nombre premier régulier alors le théorème de Fermat est vérifié. Dans les entiers inférieurs à 100, il n'y a que 3 nombres premiers irréguliers (37, 59 et 67). Il utilisait pour sa démonstration des nombres " cyclotomiques " $\xi^n = 1$. Mais malheureusement, il existe une infinité de nombres premiers irréguliers et Kummer affirma qu'on ne pouvait les traiter d'un seul coup mais au cas par cas. Cela fut fait pour les trois premiers (37, 59 et 67). Mais il en restait toujours une infinité. Au cours du 19$^{\text{ème}}$ siècle la renommé du théorème de Fermat se développa. C'est d'ailleurs vrai de la théorie des nombres dans son ensemble. Son charme particulier, écrivait Gauss, vient de la simplicité des énoncés jointe à la difficulté des preuves : une réflexion qui semble faite tout exprès pour le théorème de Fermat. Le problème fut donc souvent choisi jusqu'à notre époque comme exemple dans la vulgarisation des mathématiques où dans les ouvrages d'enseignements et Andrew Wiles dit d'ailleurs que c'est ainsi qu'il s'est intéressé aux mathématiques lorsqu'il était enfant.

10 Le prix Wolfskehl (1908).

Paul Wolfskelh, qui devait la vie indirectement au théorème de Fermat l'ayant absorbé alors qu'il s'apprêtait à se suicider, légua à sa mort (1908) 100 000 marks (soit 1,5 millions d'euros) à qui démontrerait le théorème de Fermat. Peu de semaines après s'ensuivit une avalanche de candidatures. Malheureusement toutes les solutions sont d'un niveau très élémentaire. Le docteur Schlichting, qui était chargé des textes dans les années 70 dit même "*j'ai confié quelques manuscrits à des médecins qui ont diagnostiqué une schizophrénie aiguë*". Comme le rapporte Schlichting, les candidats ne se limitaient pas à adresser leurs solutions à l'académie. Tous les départements de mathématiques ont probablement des placards pleins de prétendues démonstrations d'amateurs. Par contre la grande majorité des professionnels a continué d'ignorer le problème.

11 Kurt Gôdel (1906 -1978)

En 1931, Göddel a montré qu'il était impossible de créer un système mathématique complet et cohérent. Ses idées peuvent être résumées en deux points :

1. Si la théorie d'une série d'axiomes est cohérente, il existe des théorèmes qui ne peuvent être ni confirmés, ni infirmés.
2. Il n'existe pas de procédure constructive qui prouvera qu'une théorie axiomatique est cohérente.

Le premier théorème signifie que quelle que soit la série d'axiomes qu'on utilisera, il se posera des questions auxquelles les mathématiques ne pourront pas répondre, la complétude ne sera jamais atteinte.

Plusieurs années plus tard, le grand théoricien des nombres André Weil déclara : "*Dieu existe parce que les mathématiques sont cohérentes, et le Diable existe, puisque nous ne pouvons pas le prouver* ".

Le premier théorème de Gödel peut-être illustré par une autre analogie logique qu'on doit à Épiménide et qui est connue sous le nom de paradoxe crétois ou paradoxe du menteur. Epiménide est un crétois qui déclare :"*je suis un menteur*". Admettons que cette déclaration soit vraie. Or si Épiménide dit la vérité, il n'est donc pas un menteur et nous nous trouvons en présence d'une contradiction. Admettons ensuite qu'elle soit fausse. Or, si Épiménide ment, il n'est donc pas un menteur, et nous nous trouvons en présence d'une autre contradiction. Cette déclaration n'est donc ni vraie, ni fausse. Cette déclaration est donc improuvable.

Quatre ans avant que Gödel publie ses travaux sur l'indécidabilité, le physicien allemand Werner Heisenberg avait découvert le principe d'indétermination : il existe une limite fondamentale à celles des propriétés que les physiciens peuvent mesurer. Parce que pour mesurer la position par exemple d'un photon, il faudrait l'éclairer avec des photons qui perturberaient la vitesse du dit photon. On ne peut mesurer la vitesse et la position d'un photon au-delà d'une certaine précision.

En 1963, Paul Cohen, mathématicien de 29 ans prouva que l'hypothèse du continu (il n'existe pas d'ensemble intermédiaire entre le cardinal des entiers et celui des réels) est indécidable. Si la théorie des ensembles de Zermano-Fraenkel est non contradictoire, on peut ajouter à ses axiomes l'hypothèse du continu ou sa négation.

Peut-être que le théorème de Fermat était-il indécidable ? Sa démonstration en serait alors impossible. Paradoxalement si le théorème de Fermat se révélait indémontrable, il devait être vrai. Car si le théorème de Fermat était faux, on pourrait trouver un contre exemple. Donc, il serait alors décidable.

Le travail de Gödel sur l'indécidabilité avait introduit un doute sur la possibilité de résoudre le problème, mais ce n'était pas assez pour décourager le fanatique de Fermat : Andrew Wiles. Dans les années trentes, les mathématiciens avaient épuisé toutes leurs techniques et ils disposaient de bien peu d'autres recours. Un nouvel outil leur faisait défaut.

12 L'ordinateur.

En 1944, John von Neumann fit paraître un livre sur la théorie de jeux et du comportement économique. Il commença par étudier les échecs et le poker, puis aborda le modèle des jeux plus complexes, tel que l'économie. Après la Seconde Guerre mondiale, la Rand Corporation l'engagea pour l'appliquer au développement des stratégies de la guerre froide. Une illustration : le truel.

Un truel est un duel à trois. Un matin, M. Noir, M. Gris et M. Blanc décident de régler une querelle au pistolet jusqu'à ce qu'il ne reste qu'un seul survivant. M. Noir est le plus mauvais tireur, n'atteignant sa cible qu'une fois sur trois, M. Gris est un meilleur tireur, atteignant sa cible une fois sur deux et M. Blanc est le meilleur des trois, mettant dans le mille à tous les coups. Pour égaliser les chances, M. Noir est autorisé à tirer le premier, puis ce sera le tour de M. Gris, s'il est encore vivant, suivi de M. Blanc, s'il est également encore en vie et le tour reprendra jusqu'à ce qu'il n'y en reste plus qu'un. Quelle stratégie M. Noir doit-il adopter pour son premier tir ?

Pendant la Seconde Guerre mondiale, Alan Turing fut attaché au service de cryptographie (en Angleterre) dont le but était le décodage des messages ennemis. Turing dirigea une équipe de mathématiciens, appliqua ses abstractions (machines fictives abstraites décrivant symboliquement les opérations de la logique, formalisant la notion d'algorithme) d'avant-guerre à la réalisation d'une machine qui pouvaient théoriquement examiner toutes les grilles d'Egnima (système allemand) jusqu'à ce que le code fût percé. Mais en dépit de leur vitesse, il était impossible à ces machines de passer en revue les cents cinquante millions de millions d'arrangement possibles. Turing recourait alors à l'intuition essayant de deviner un mot clé dans les messages. Quand les mathématiciens se heurtaient à un mur, la British Cypher School, prétend-on, utilisait une stratégie : elle demandait à la Royal Air Force de miner un port allemand donné. Immédiatement, le commandant du port envoyait un message codé, où devait se trouver les mots "*mine*", " *éviter* " et " *référence cartographique* ". Turing pouvait alors percer la grille d'Egnima. À la fin de la guerre, Turing a contribué à la construction de Colossus : l'ordinateur était né.

L'avènement de l'ordinateur signifia que les aspects difficiles du théorème de Fermat pouvaient être expédiés rapidement et, après la Seconde Guerre mondiale, des équipes d'informaticiens et de mathématiciens démontrèrent le Dernier théorème de Fermat pour toutes les valeurs de n jusqu'à 500, puis 1 000 et enfin jusqu'à 10 000. Dans les années 80, Samuel S. Wagstaff, porta la limite à 25 000 et plus récemment, des mathématiciens ont démontré que le théorème était valide pour des valeurs allant jusqu'à 4 000 000.

Mais cela n'étaient que des faux-semblants car il restait toujours une infinité de nombres n à démontrer. L'infini n'est pas accessible par la force brute du broyage informatique des chiffres. Tout ce que les ordinateurs pouvaient offrir était une évidence en faveur du théorème. Pour l'amateur, cette évidence pourrait sembler écrasante, mais aucune évidence ne saurait satisfaire les mathématiciens qui n'acceptent que la preuve absolue. Un petit exemple pour montrer qu'une conjecture peut être vraie jusqu'à un certain nombre et s'avérer fausse ensuite. Les nombre suivant : 31, 331, 3 331, 33 331, 333 331, 3 333 331 et 33 333 331 sont tous premiers. On pourrait donc avancer la conjecture que les nombres formés uniquement du chiffre 3 avec le chiffre 1 comme unité sont tous premiers. Malheureusement le nombre $333\,333\,331 = 17 \times 19\,607\,843$ n'est pas premier.

Un autre exemple, Euler avait déclaré qu'il n'y avait pas de solution à une équation qui n'est pas très différente de celle de Fermat :

$$x^4 + y^4 + z^4 = w^4$$

Pendant deux cents ans personne ne pouvait non plus l'infirmer à l'aide d'un contre-exemple. Les premières tentatives de vérification manuelle, puis avec des ordinateurs ne parvinrent pas à offrir de solution. L'absence de contre-exemple plaidait fortement en faveur de la conjecture. Mais en 1988, Noam Elkies, de l'université de Harvard, découvrit la solution suivante :

$$26\,824\,404^4 + 153\,656\,394^4 + 187\,967\,604^4 = 206\,156\,734^4$$

La conjecture d'Euler était donc fausse. Il n'y avait alors aucune raison pour laquelle le théorème de Fermat ne se révélât pas aussi cruellement décevant que la conjecture d'Euler.

13 Les courbes elliptiques.

Courbe définie par une équation à coefficients rationnels qui n'admet ni point double (la courbe ne passe pas deux fois par le même point), ni point de rebroussement (la courbe

ne rebrousse pas chemin) dans $\mathbb{R}$. Dans un repère convenablement choisi, son équation se met sous la forme :

$$y^2 = x^3 + ax^2 + bx + c \quad \text{où } a, b \text{ et } c \text{ appartiennent à } \mathbb{Q}$$

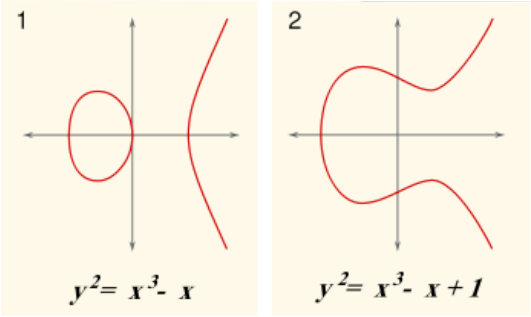

FIG. 1 – Deux formes de courbes elliptiques

Ces courbes sont utilisées pour le calcul de la longueur d'une ellipse ainsi qu'en cryptographie. Mais leur propriété la plus remarquable tient au fait qu'à l'aide de construction de sécantes et de tangentes, on peut définir une opération qui a les mêmes propriétés que l'addition des nombres entiers.

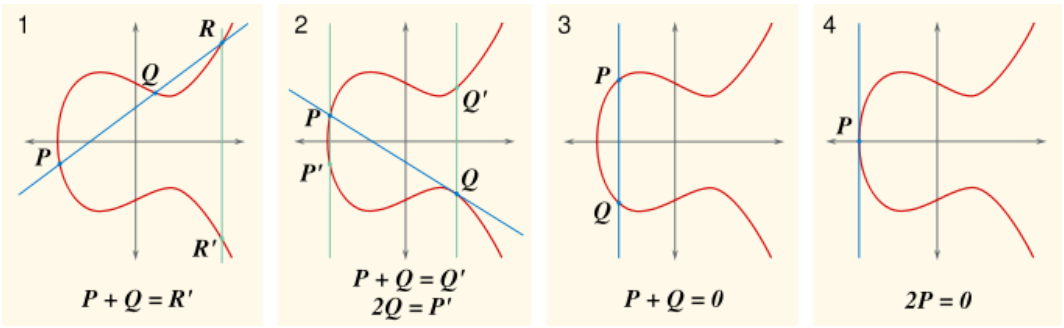

FIG. 2 – Opérations avec une courbe elliptique : $y^2 = x^3 - x + 1$ avec x et y réels

Le défi avec les courbes elliptiques est de déterminer si elles ont des solutions formulables en nombres entiers et, si c'est le cas, combien de solutions. Les courbes elliptiques avaient été à l'origine étudiées par les mathématiciens grecs, y compris Diophante, qui avait consacré une bonne partie de son Arithmética à en explorer les possibilités. Probablement inspiré par Diophante, Fermat releva la gageure des courbes elliptiques et, parce qu'elles avaient été étudiées par son héros, Andrew Wiles fut content au début de sa vie professionnelle de les approfondir. Même après deux mille ans, les courbes elliptiques posent des problèmes énormes. Même les questions que Fermat avaient considérées restent encore aujourd'hui sans solution.

Étant donné que les mathématiciens ne peuvent pas savoir combien de solutions existent, pour certaines équations elliptiques, dans l'espace des nombres normaux[1] (N), qui s'étend jusqu'à l'infini, on étudie les solutions dans des espaces de nombres plus petits (congrus à 2 puis 3, 4, 5, 6, 7, 8 etc...). Ces séries de solutions (série E) dans ces espaces plus petits définissent ainsi ces courbes, et par analogie avec la biologie, une série E est

[1]En mathématiques, un nombre normal est un nombre réel qui a ses chiffres equi-distribués dans son développement décimal, ceux-ci apparaissant tous à la même fréquence. Les " chiffres " font référence aux chiffres avant la virgule (la partie entière) et la suite infinie de chiffres après la virgule (la partie fractionnaire)

à une courbe elliptique ce qu'une molécule d'ADN est à un organisme vivant. Personne ne s'en rendait compte, mais les mathématiciens du japon de l'après-guerre allaient déclencher une réaction en chaîne qui devait inextricablement lier les courbes elliptiques au Dernier théorème de Fermat.

14 Les formes modulaires

La définition des fonctions dites modulaires, est malheureusement beaucoup trop technique pour en donner une définition. On peut seulement dire que ces fonctions ressemblent un peu aux fonctions cosinus et sinus, en particulier, elles vérifient certaines propriétés de périodicité.

Il est impossible de dessiner une fonction modulaire, car étant une fonction de C dans C, sa représentation nécessite un espace avec quatre dimensions dit hyperbolique. Sa dimension supplémentaire lui assure son immense symétrie. Le graveur Maurits Escher, qui était fasciné par les idées mathématiques, a tenté de représenter ces fonctions, en reflétant en partie la symétrie des fonctions modulaires.

Ces " formes " modulaire de l'espace hyperbolique ont des formes et des dimensions variées, mais elles sont constituées des mêmes éléments. Ce qui différentie ces formes est le nombre d'éléments qu'elles contiennent. Cette description de la construction d'une fonction modulaire peut être résumée dans une série dite modulaire (série M), liste des éléments et le nombre requis de chacun d'eux.

De même que la série E est l'ADN des courbes elliptiques, la série M est l'ADN des fonctions modulaires. Les fonctions modulaires sont tout à fait autonomes en mathématique. Elles étaient sans rapport avec les courbes elliptiques. Les fonctions modulaires sont surtout étudiées en raison de leur symétrie et elles n'ont été découvertes qu'au 19"" siècle, alors que les courbes elliptiques remontent aux Grecs.

15 Conjecture de Taniyama - Shimura.

En septembre 1955, au cours d'un symposium international à Tokyo, Yutaka Taniyama soutenu par Goro Shimura, après avoir examiné quelques fonctions modulaires avec des courbes elliptiques, émis la conjecture suivante : chaque fonction modulaire possède le même ADN qu'une courbe elliptique.

La proposition était tellement extraordinaire que ceux qui examinaient la question ne la considéraient que comme une curiosité. Après le symposium, les deux jeunes gens travaillèrent à développer cette hypothèse. Malheureusement cette collaboration s'interrompit brutalement après le suicide de Taniyama en 1958. Après sa mort, Shimura concentra tous ses efforts sur la compréhension de la relation exacte entre les courbes elliptiques et les fonctions modulaires. Il se convainquit que toute courbe elliptique doit être liée à une fonction modulaire. Mais Shimura ne pouvait pas le prouver.

Ce fut André Weil qui adopta la conjecture et la fit connaître en occident. Il trouva de nouvelles preuves en sa faveur. Cette conjecture prit alors le nom de conjecture de Shimura - Taniyama - Weil (STW).

Cette conjecture établit un lien entre un objet géométrique et l'arithmétique. Ces deux branches des mathématiques ont été étudiées de manières intensives mais séparément. C'était merveilleux, les mathématiciens adorent construire des ponts. La valeur des ponts en mathématique est considérable car ils permettent à des groupes de mathématiciens vivant sur des îles éloignées d'échanger des idées et d'explorer les créations des autres. Ces îles se comptent par douzaines et chacune à son propre langage, incompréhensible aux

habitants des autres. Le grand potentiel de la conjecture (STW) était de relier deux îles et de permettre ainsi à leurs habitants de se parler pour la première fois. Barry Mazur la compare même à la pierre de Rosette, qui permit de déchiffrer les hiéroglyphes égyptiens, qui étaient gravée en démotique égyptien, en grec et en hiéroglyphes. Le mathématicien Robert Langland rêvait de voit aboutir grâce à ces ponts de grandes mathématiques unifiées. Cette conjecture permettait de traiter des courbes elliptiques qui étaient restées sans solution pendant des siècles, en les abordant sous l'angle modulaire. Malheureusement la preuve de cette conjecture semblait hors de portée.

16 Théorème de Ken Ribet

Démontré en 1986, il affirme que la conjecture STW entraîne la conjecture de Fermat. La démarche utilisée par Ribet consiste à raisonner par l'absurde. On suppose que l'équation de Fermat : $x^n + y^n = z^n$ pour $n > 2$ admet une solution non nulle (a, b, c) , on montre alors que l'équation de Fermat engendre la courbe d'équation :

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

qui est une courbe elliptique semi-stable, qui contredit alors la conjecture STW.

Le Dernier théorème de Fermat était désormais inextricablement lié à la conjecture STW. Si quelqu'un pouvait démonter que toute courbe elliptique est modulaire, cela signifierait que l'équation de Fermat n'avait pas de solution. Un casse-tête d'une énorme importance historique et émotionnelle était ainsi lié à une conjecture qui pouvait bouleverser les mathématiques modernes. Il y avait un espoir. Cependant même Ribet, qui avait pourtant réussi une percée majeure était pessimiste "*je faisais partie de la vaste majorité de ceux qui estimaient que la conjecture STW était hermétique* ".

17 Andrew Wiles.

À peine connu, le théorème de Ribet, Wiles abandonna tout travail qui n'intéressait pas directement le théorème de Fermat et cessa d'assister à l'incessante noria de conférences et de colloques. Il continua à donner ses cours et à guider le travail de ses étudiants à Princeton. II prit la décision surprenante de travailler seul dans l'isolement et le secret complets. C'est probablement le seul cas où quelqu'un ait travaillé aussi longtemps sans en parler à personne. Il fallait donc démontrer la conjecture STW. Ce qu'on pourrait naïvement être tenté de faire, c'était de compter les courbes elliptiques et les fonctions modulaires. Mais on ne compte pas l'infini. Comme beaucoup de théorèmes dans la théorie des nombres un ordinateur n'eut été d'aucun secours.

Au bout d'une année de contemplation, Wiles décida d'adopter la stratégie connue sous le nom d'induction ou encore le raisonnement par récurrence. On démontre que la conjecture est vérifiée à l'ordre 1 (initialisation) puis en admettant qu'elle soit vraie à l'ordre n on la démontre à l'ordre $n + 1$ (hérédité). Ce raisonnement peut être comparé à une rangée infinie de dominos. Si les dominos sont correctement disposés, la chute du premier entraînera la chute de tous les autres.

Pour démontrer l'initialisation, Wiles eut recours aux travaux d'un génie français du 19éme siècle : Évariste Galois. Au coeur des idées de Galois se trouvait un concept connu sous le nom de théorie des groupes. Un groupe est une série d'éléments qui peuvent être combinés par une opération telle qu'une addition ou une multiplication et qui satisfont à certaines conditions : deux éléments combinés doivent former un élément qui appartient

à la série (opération interne). Cette opération doit être associative, posséder un élément neutre et chaque élément doit posséder un symétrique. De plus si l'opération est commutative, on parle de groupe commutatif ou abélien. Si le groupe des entiers N est un groupe abélien, il existe des petits groupes constitués, d'un nombre fini d'éléments, soigneusement composés qui possèdent leurs richesses. Par exemple le groupe des solutions d'une équation elliptique. L'approche de Wiles fut d'apparier un élément de toutes les série E et M puis de passer à l'élément suivant. En d'autres termes, chaque ADN comportant une liste infinie d'éléments, les " *gènes* " individuels qui constitue l'ADN, Wiles voulait démontrer que chaque premier gène de chaque série E pouvait être apparié à chaque premier gène de chaque série M. Même si l'approche de Wiles ne supprimait pas l'infini, elle avait l'avantage de créer un ordre et ainsi de pouvoir raisonner par récurrence.

Grâce à Galois, Wiles avait réussi à faire tomber le premier domino (initialisation). Il lui avait fallu deux ans pour arriver à ce résultat.

Le 8 mars 1988, Wiles fut consterné de lire dans les journaux que le Dernier théorème de Fermat avait été résolu par le japonais Yochi Miyaoka, grâce à la géométrie différentielle et aux travaux de Falting. Gerd Falting de Princeton, en 1983, démontra que l'équation de Fermat a au plus un nombre fini de solutions primitives. Les formes correspondantes à chacune des équations sont toutes différentes, mais elles présentent un trait commun : elles comportent toutes des trous, les formes sont quadridimensinnelles (un peu comme les fonctions modulaires). Falting put prouver qu'étant donné que ces formes ont toujours plus d'un trou, l'équation de Fermat associée ne pouvait avoir qu'un nombre fini de trous correspondant à une solution en nombres entiers. Il n'avait pas démontré le théorème de Fermat mais, il avait montré que si l'équation admettait des solutions, le nombre de solutions serait fini. Miyaoka annonçait qu'il avait montré que ce nombre fini de solution était égal à zéro. Malheureusement pour Miyaoka le détail de son manuscrit montra une faille dans le parallélisme qu'il faisait entre la géométrie différentielle et la théorie des nombres. Deux mois après la proclamation initiale la démonstration originale avait fait chou blanc.

Wiles poussa un soupir de soulagement. En 1990 Wiles travailla sur une technique dite théorie d'Iwasawa. : méthode d'analyse des courbes elliptiques. Il espérait pouvoir la modifier et la transformer en un instrument assez efficace pour engendrer un effet domino. Mais en 1991, Wiles constata que la théorie d'Iwasawa ne lui offrait pas la sécurité recherchée pour son effet domino. Wiles se trouvait ainsi dans une impasse après déjà 5 ans de travaux. À l'occasion d'une conférence, Wiles réalisa, qu'il pouvait s'appuyer sur une nouvelle méthode sur les courbes elliptiques : la méthode Kolyvagin - Flach. Pendant plusieurs mois Wiles se familiarisa avec cette méthode puis l'adapta afin de la mettre en oeuvre. Et bientôt pour une courbe elliptique donnée, il réussit à faire fonctionner la méthode inductive, et se trouva en mesure de renverser tous les dominos. Au bout de 6 ans, Wiles voyait enfin le bout du tunnel. Il décida de mettre Nick Katz dans la confidence, afin de vérifier son travail. Il choisit alors comme subterfuge une série de cours appelée : Calculs sur les courbes elliptiques.

Au bout de 7 ans de dur labeur, Wiles décida de mettre la communauté mathématique au courant de sa démonstration, lors d'une série de conférences au Isaac Newton Institute en juin 1993. Tous les mathématiciens présents avaient alors le sentiment d'assister à un moment historique. Barry Mazur dit "*je n'ai jamais assisté à une aussi splendide conférence, aussi pleine d'idées lumineuses, avec une telle tension dramatique* ". Ken Ribet " *c'était un événement tout à fait remarquable, ce n'est qu'une fois dans une vie que l'on a une conférence où quelqu'un déclare avoir résolu un problème vieux de 350 ans* ".

18 Un petit problème.

Wiles soumis son manuscrit à Burry Mazur, président des jurés. Pour simplifier la tâche, les 200 pages de démonstration furent divisées en 6 sections et chacun des six jurés se vit attribuer la responsabilité d'un chapitre. Le chapitre 3 revint à Nick Katz. Le 23 août, il adressa un courrier à Wiles lui demandant quelques explications sur un point du chapitre 3 traitant de la méthode Kolyvagin - Flach. En résumé, le problème était qu'il n'y avait pas de garantie que la méthode Kolyvagin - Flach fonctionnât comme Wiles l'avait projeté.

Au début Wiles pensait rectifier l'erreur rapidement, puis petit à petit il prit conscience de la nature de la faille. Moins de 6 mois après la conférence, la démonstration de Wiles était en ruine. En janvier, Wiles épaulé par Taylor (un de ses anciens élèves), explorait toujours la méthode Kolyvagin - Flach essayant de trouver une issue à l'impasse. Passons sur un poisson d'avril de 1994 qui affirma que le théorème de Fermat était faux pour un n très grand (de l'ordre de 1020), qui donna encore des frissons à Wiles. En août, Wiles est près d'abandonner, lorsque Taylor, qui disposait encore d'un mois, lui proposa un mois supplémentaire avant d'abandonner. Et c'est alors que Wiles en essayant de comprendre son échec, compris, que même si la méthode Kolyvagin -Flach ne marchait pas complètement, c'était tout ce dont avait besoin pour faire marcher la théorie Iwasawa. La théorie Iwasawa en tant que telle avait été inadéquate. Et la théorie de Kolyvagin - Flach aussi. Mais elles se complétaient. Ce fut un moment d'inspiration que Wiles ne devait pas oublier. " *C'était indescriptiblement beau, c'était si simple et élégant* ". Les quatorze mois écoulés avaient été les plus douloureux, les plus humiliants et les plus déprimants de sa carrière mathématique. Mais une seule intuition brillante avait mis fin à ses souffrances. Cette fois il n'y avait plus de doute sur la preuve.

En terme mathématique, cette preuve finale est l'équivalent de la fission de l'atome ou de la découverte de l'ADN déclara John Coates, l'ancien professeur d'Andrew Wiles. " *Pour moi, le charme et la beauté du travail d'Andrew Wiles résident dans ce qu'il constitue un pas de géant pour la théorie des nombres* ".

Durant huit ans Wiles avait pratiquement réuni toutes des découvertes du siècle dans la théorie des nombres et les avaient fondues en une démonstration suprême.

Le 17 juin 1995, la démonstration de Wiles est entérinée à Paris par la Société mathématique de France et Bourbaki. Le prix Fermat, créé en 1850 par l'Académie des sciences françaises, fut remis à Wiles le 27 octobre 1995 à Toulouse. Le 27 juin 1997, Wiles reçut le prix Wolfskehl d'une valeur de 50 000 dollars (beaucoup moins qu'en 1908 car le crack boursier de 1929 était passé par-là).