Les équations diophantiennes

La grande histoire du théorème de Fermat

Préambule Le texte qui suit suit est la version écrite d'une conférence donnée à la séance du 2 avril 2007 de l'Académie Montesquieu. L'ambition de l'exposé était de raconter l'histoire d'un problème qui a passionné les mathématiciens pendant 358 ans. Toutefois l'auteur demande un peu d'indulgence à son lecteur parce que les paragraphes 5.2. et 5.3. abordent l'aspect mathématique, ainsi les dits paragraphes pourront être bien ardus pour le lecteur qui a oublié ses mathématiques et bien superficiels pour celui qui a conservé une bonne connaissance en la matière.

0. Introduction

Cet exposé traite d'un peu d'histoire des équations diophantiennes, l'une des plus célèbres étant bien entendu l'équation de Fermat. Nous avons retenu trois moments marquants dans l'histoire des équations diophantiennes au XXème siècle : la structure du groupe des points rationnels d'une courbe elliptique par Mordell et Weil ([Mo],1922 ; [We], 1928), la démonstration de la conjecture de Mordell-Weil concernant les points rationnels des courbes de genre ≥ 2 , par Faltings ([Fa]) et enfin la démonstration par Wiles ([Wi]) du "dernier théorème de Fermat". L'essentiel de notre exposé est dédié à la stratégie qui a conduit à la première démonstration du "dernier théorème de Fermat" présentée à la communauté mathématique.

La solution de Wiles est vraiment une démonstration du XXème siècle et même une démonstration de la deuxième moitié du XXème. Les mots-clés sont formes modulaires, courbes elliptiques, cela est bien connu avant 1950, et ensuite géométrie arithmétique parfaitement maîtrisée depuis la théorie des schémas (1960) et enfin les représentations galoisiennes largement développées à partir des années 1980. Même si ce descriptif est schématique, il respecte assez bien la chronologie des bouillonnements mathématiques autour des moments qui nous concernent.

On rappelle que le "dernier théorème de Fermat" dit que si x, y, z sont des entiers, si $n \geq 3$, si $x^n + y^n = z^n$, alors $xyz = 0$; on dira que l'équation de Fermat n'admet que les solutions triviales. Il est bien connu que Fermat affirme avoir une démonstration merveilleuse de cet énoncé, et qu'on n'en a pas retrouvé trace.

En 1983 le théorème de **Faltings** a pour conséquence que l'équation de **Fermat** n'a (projectivement) qu'un nombre fini de solutions. Ainsi donc la fameuse équation n'a (projectivement) que les solutions triviales, plus quelques autres. On aurait dû s'arrêter là ; mais **Fermat** était trop fascinant, il fallait montrer que $x^n+y^n=z^n$ impliquait $xyz=0$.

Un lien inattendu entre une hypothétique solution non triviale à l'équation de **Fermat** d'exposant un nombre premier p et une courbe elliptique, i.e. une équation de degré 3 , remise à l'honneur par **G. Frey** ([Fr]) en 1985, a mis en évidence un moyen d'attaque au célèbre problème. Le premier coup de tonnerre est arrivé en 1986 quand **K. Ribet** ([R]) a montré que son résultat sur les représentations galoisiennes — conjecturé peu de temps auparavant par **J.-P. Serre** ([Se1]) — impliquerait le dernier théorème de **Fermat** si une vieille conjecture de **Shimura-Taniyama-Weil** ([Ta],1955), concernant la "modularité" des courbes elliptiques, était prouvée. C'est à ce moment que stimulé par ce résultat, le mathématicien **A. Wiles** s'attaque dans le plus grand secret à cet himalaya. En 1993 il annonce lors d'une conférence au **Isaac Newton Institute** la démonstration de la conjecture. Toutefois, quelques mois après, on apprend qu'il existe un trou dans la preuve. Après une année d'angoisse et de travail il rectifie sa démonstration et son travail est présenté le 14 octobre 1994 au célèbre journal **Annals of Mathematics** ([Wi]). Après 358 ans, la communauté mathématique dispose enfin d'une preuve (de 127 pages) du "dernier théorème de **Fermat**".

1. **Diophante** et les équations diophantiennes

Diophante né en 250 à 350 après J. C. , aurait vécu à Alexandrie ; il a écrit 13 livres d'Arithmétique (6 étaient connus à l'époque de **Fermat**, 4 ont été découverts depuis).

Qu'est-ce qu'une équation diophantienne ? Cela peut se décrire sous forme d'un problème, donnons quelques exemples.

Exemple 1. Trouver x et y entiers tels que $7\times x+3\times y=1$. Facilement on peut vérifier que $7\times(1)+3\times(-2)=1$, ainsi donc $x=1$ et $y=-2$ sont solutions du problème.

Exemple 2. De même, trouver x et y entiers tels que $1576\times x+113\times y=1$. Facilement on peut montrer que $1576\times(-19)+113\times(265)=1$ et aussi que $1576\times(-19+113)+113\times(265-1576)=1$, on a donc deux couples de solutions qui sont d'une part $(-19,265)$ et d'autre part $(-19+113,265-1576)$.

Exemple 3. (les triplets pythagoriciens) Trouver x,y,z des entiers tels que $x^2+y^2=z^2$. Les égyptiens savaient que le triplet $(3,4,5)$ convient. Essentiellement, on peut montrer que les solutions sont de la forme $x=2ab, y=a^2-b^2, z=a^2+b^2$ où a et b sont des entiers.

De façon un peu plus formalisée, on note $\mathbb{Z}$ l'ensemble des entiers, i.e. $0, \pm1, \pm2, \pm3, \ldots$. et on note $\mathbb{Q}$ l'ensemble des nombres rationnels, i.e. les fractions de nombres entiers. Ainsi une *équation diophantienne* est la donnée d'une famille $P_1, P_2, \ldots, P_s$ de polynômes à coefficients dans $\mathbb{Z}$ à plusieurs variables et l'objectif est de trouver les solutions des équations définies par ces polynômes, i.e. de trouver des n-uples $x:=(x_1, x_2, \ldots, x_n)$ à coefficients dans $\mathbb{Z}$ ou $\mathbb{Q}$ tels que $P_1(x)=P_2(x)=\ldots=P_s(x)=0$.

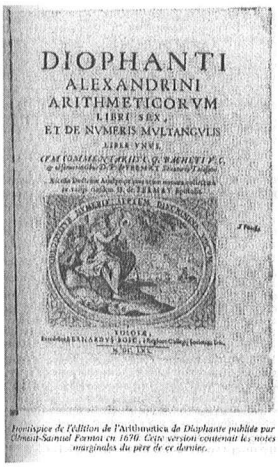
2. Fermat et l'équation de Fermat

Fermat né en 1601 à Beaumont de Lomagne, mort en 1665 à Castres, conseiller au parlement de Toulouse, Fermat est un mathématicien amateur, digne des grands professionnels.

Pierre de Fermat, en marge de son *Arithmetica*, à la suite du problème 8, nota ainsi son observation : *"Il est impossible pour un cube d'être décrit comme la somme de deux cubes ou pour une quatrième puissance d'être écrite comme la somme de deux quatrièmes puissances ou, en général, pour n'importe quel nombre égal à une puissance supérieure à deux d'être écrit comme la somme de deux puissances semblables"*,

et il ajoutait

"J'ai une démonstration véritablement merveilleuse de cette proposition, que cette marge est trop étroite pour contenir".



Frontispice de l'édition de l'Arithmetica de Diophante publiée par Claude-Samuel Fermat en 1670. Cette version contenait les notes marginales du père de ce dernier.

C'est donc cela qu'on a appelé le *"Dernier théorème de Fermat"* sans avoir jamais eu connaissance d'une démonstration de l'énoncé.

En d'autres termes, soit $n\geq 3$ un nombre entier, si le triplet d'entiers (x,y,z) (que l'on notera $(x,y,z)\in\mathbb{Z}^3$) est solution de l'équation diophantienne $X^n+Y^n-Z^n=0$, alors $xyz=0$. Là commence l'histoire du dernier théorème de Fermat qui a duré 358 ans.

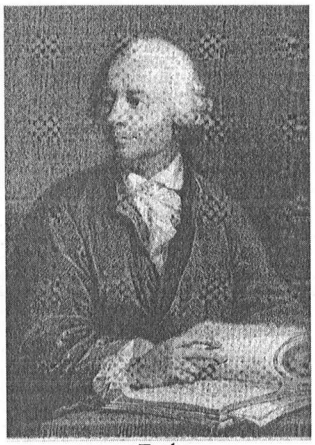
3. Les résultats des 17ème, 18ème, 19ème siècle.

A partir de l'expression explicite des solutions entières de l'équation $x^2+y^2=z^2$, on déduit par un procédé de "descente" que si $x^4=y^4+z^4$ avec $x,y,z\in\mathbb{Z}$, alors $xyz=0$, i.e. **Fermat** est vrai pour $n=4$. Il suit de cela que si **Fermat** est vrai pour un exposant qui est un nombre premier $p\geq 3$, i.e. $p=3,5,7,11,17,.....$ alors **Fermat** est vrai pour les multiples de p .

En effet l'égalité $x^{mp}+y^{mp}=z^{mp}$ implique $(x^m)^p+(y^m)^p=(z^m)^p$ et alors **Fermat** vrai pour p implique $x^m y^m z^m=0$, i.e. $xyz=0$.

Il suit de cela que si Fermat est vrai pour tous les nombres premiers, alors il sera vrai pour tout $n\geq 3$. Il suffit donc de considérer les équations de **Fermat** pour un exposant premier $p\geq 3$.

L'équation diophantienne $x^3+y^3=z^3$ a été traitée en 1753 par **Euler** (1707-1783).



Euler

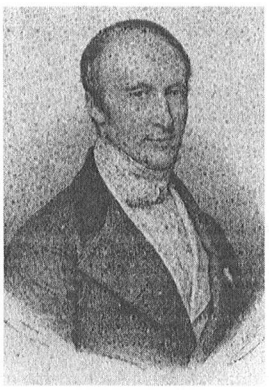
En 1804 **Sophie Germain** donne une solution partielle dans le cas où p et $2p+1$ sont premiers, par exemple 2 et 5 , 3 et 7 , 11 et 23 , mais 7 et 15 ne marchent pas.

Quatorze ans plus tard, en France encore, une autre percée fut accomplie. C'est **Gabriel Lamé** qui prouve le cas où $n=7$.

Après la percée réalisée par **Sophie Germain**, l'Académie des sciences créa une série de prix, y compris une médaille d'or et 3.000 francs, au mathématicien qui viendrait à bout du Dernier théorème de Fermat. Le prestige de la démonstration se doublerait donc d'une récompense matérielle appréciable. Les salons de Paris bruirent de rumeurs sur les stratégies qu'adopterait tel ou tel et sur l'imminence d'un succès. Puis, le 1er mars 1847, l'Académie tint la séance la plus dramatique qu'elle eût jamais connue. **Lamé** annonça qu'il était sur le point d'offrir une démonstration, **Cauchy** annonça aussi la même affirmation. Mais personne n'avait de preuve complète.

Sophie Germain

Gabriel Lamé



Cauchy

Le 24 mai, une annonce mit fin aux spéculations. Or, ce n'était ni **Lamé**, ni **Cauchy** qui s'adressaient à l'Académie, mais **Joseph Liouville**, qui frappa l'audience de stupeur en lisant une lettre du mathématicien allemand **Ernst Kummer**.

Le fait le plus marquant du XIXième siècle est sans nul doute le théorème de **Kummer** (1810-1893).

Kummer

Théorème (Kummer, 1847) *Soient* $p \geq 5$ *un nombre premier régulier,* $x, y, z \in \mathbb{Z}$ *tels que* $x^p + y^p + z^p = 0$, *alors* $x\,y\,z = 0$ *; en d'autres termes* **Fermat** *pour l'exposant* p *est satisfait.*

L'idée essentielle de Kummer était d'écrire l'équation $x^p + y^p + z^p = 0$ sous la forme $(x+y)(x+\zeta y)\ldots(x+\zeta^{p-1}y) = -z^p$ avec ζ qui est un nombre complexe racine d'ordre p de 1 et d'utiliser des propriétés arithmétiques de l'anneau engendré par $\mathbb{Z}$ et ζ ; c'est là la grande nouveauté. C'est l'avènement de la théorie algébrique des nombres.

Remarque Même si le résultat de **Kummer** est un progrès, il reste limité par le fait qu'on ne sait s'il existe une infinité de premiers réguliers.

Les prix pour **Fermat**

Paul Wolfkehl

Comme il a été dit précédemment, en 1816 et 1850 l'Académie des sciences de Paris offre une médaille d'or et un prix de 3.000 francs (les juges sont **Cauchy, Liouville, Lamé, Bertrand, Chasles**).

En 1908 est créé le **Wolfkehl** Prize (valable jusqu'en 2007) qui est de 100.000 DM en 1900 , et par suite de dévaluations, il tombe à 7.600 DM en 1974. C'est un prix issu d'une donation d'un riche industriel allemand de Darmstadt du nom de **Paul Wolfkehl**. Pour ce prix, 621 solutions sont arrivées en 1908 (toutes fausses).

Le théorème de Fermat se révèle être un fléau pour les sociétés savantes et les journaux mathématiques. Les mathématiciens professionnels sont vite découragés par l'avalanche de solutions fausses présentées par des amateurs ; aussi **Klein, Hilbert, Minkowski** utilisent une partie du prix pour inviter **Henri Poincaré.**

A ce propos l'Académie des sciences reçoit toujours des démonstrations (fausses) du théorème de **Fermat.** Localement le Journal de théorie des nombres de Bordeaux est assailli chaque année par 4 ou 5 preuves du théorème de **Fermat.**

A noter que Toulouse a créé un prix **Fermat,** financé par **Matra Marconi Space** aujourd'hui **Astrium.** Le prix est modeste 100.000 francs (15.000 euros) .

4. Les courbes et les équations diophantiennes, ou la voie de la géométrie arithmétique

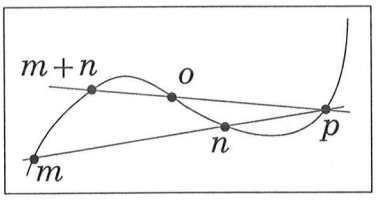
Qu'est-ce que l'équation de **Fermat** ? C'est l'équation $X^p+Y^p-1=0$.
Qu'est-ce que le problème de **Fermat** ? C'est trouver les solutions rationnelles de l'équation de **Fermat.**

4.1. Les courbes planes

Ici, une *courbe plane* C sera la donnée d'un polynôme irréductible à deux variables à coefficients dans $\mathbb{Z}$, on le note $F(X,Y)\in\mathbb{Z}[X,Y]$. L'ensemble des *points rationnels* de la courbe C sera noté $C(\mathbb{Q})$ et défini comme étant l'ensemble des couples (u,v) de nombres rationnels tels que $F(u,v)=0$. Si $\deg F=2$, la courbe est appelée *conique,* si $\deg F=3$, la courbe est appelée *cubique.*

4.2. Les courbes elliptiques

4.2.1. La définition



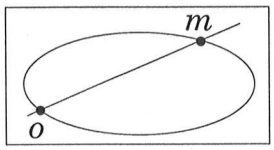
Un cas particulièrement intéressant est celui des courbes E , cubiques planes qui admettent un point rationnel $o=(\alpha,\beta)$ et qui sont non singulières. Alors l'ensemble $E(\mathbb{Q})$ peut être muni d'une structure de groupe commutatif où o est l'élément neutre de la façon qui suit. Si m,n sont des éléments de $E(\mathbb{Q})$, la droite passant par m et n coupe $E(\mathbb{Q})$ en un troisième point p . Ensuite la droite passant par p et o coupe $E(\mathbb{Q})$ en

un troisième point noté $m+n$. Alors l'application $(m,n)\mapsto m+n$ définit sur $E(\mathbb{Q})$ une loi de groupe commutatif (en fait cet énoncé est approximatif pour deux raisons, la première est qu'il faudrait considérer la cubique projective associée, la seconde est que le troisième point demande à être précisé si la droite passant par m et n est tangente à la courbe ; enfin le fait que la loi soit associative n'est pas évident).

4.2.2. Les beaux résultats.

Deux noms sont historiquement attachés aux courbes elliptiques, ce sont L. J. Mordell ([Mo],1922) et A. Weil ([We],1928). Leur résultat est que le groupe commutatif $E(\mathbb{Q})$ est de type fini , i.e. $E(\mathbb{Q}):=F\times\mathbb{Z}^{r_E}$ où F est un groupe commutatif fini, $r_E\geq 0$ est entier. En 1978, B. Mazur ([Ma1]) montre que le groupe F , i.e. le sous-groupe de torsion de $E(\mathbb{Q})$ est d'ordre borné indépendamment de E . Cependant tout est loin d'être connu, par exemple, on pense que r_E peut être aussi grand qu'on veut, mais on ne sait pas le montrer.

4.3. Les points rationnels d'une courbe



Si C est une courbe plane définie par le polynôme F (selon 4.1.), on note toujours $C(\mathbb{Q})$ l'ensemble des couples (u,v) de nombres rationnels tels que $F(u,v)=0$.

Facilement si C est une conique propre qui admet un point rationnel o , alors $C(\mathbb{Q})$ est infini, en effet $m\in C(\mathbb{Q})$ si et seulement si la pente de la droite passant par o et m est rationnelle. Si C est une courbe elliptique, alors le théorème de Mordell-Weil dit que $C(\mathbb{Q})$ est infini si et seulement si $r_E\geq 1$.

4.3.1. Le genre des courbes.

Quelles sont les autres courbes ? Une première classification passe par le genre. C'est une notion essentielle, mais difficile à définir. Nous donnerons ici deux exemples. Si C est la courbe définie par le polynôme $F(X,Y)=Y^2-(X-a_1)(X-a_2)\ldots(X-a_{2n+1})$, les a_i étant distincts, alors le genre de la courbe associée est n . Si $F(X,Y,Z)$ est un polynôme homogène de degré n et de plus non singulier, alors le genre de la courbe associé est $\frac{(n-1)(n-2)}{2}$; on trouvera donc que le genre d'une cubique non singulière est $1=\frac{(3-1)(3-2)}{2}$. En particulier la courbe de Fermat définie par le polynôme homogène $X^p+Y^p+Z^p$ est de genre $\frac{(p-1)(p-2)}{2}>2$ si $p\geq 5$.

4.3.2. La conjecture de Mordell-Weil, le théorème de Faltings ([Fa])

La conjecture de Mordell-Weil dit que si le genre de $C \geq 2$, alors $C(\mathbb{Q})$ est fini. On sera amusé par la remarque ci-après d'André Weil, datant environ de 1928 : "... *mon ambition avait été de prouver aussi que sur les courbes de genre* $g \geq 2$, *les points rationnels sont en nombre fini...* Je le dis à Hadamard. "*travaillez-y encore*" me dit-il "*vous ne devez pas publier un demi résultat*".

En effet ce n'est qu'en 1983 que G. Faltings démontre cette conjecture, ce qui lui valut de recevoir la médaille Fields.

En application de ce grand résultat, la courbe de Fermat a un nombre fini de solutions rationnelles ; immense progrès, mais ce n'est pas Fermat.

5. Le dernier épisode, la victoire de Mazur-Ribet-Wiles (Taylor), ou la voie des formes modulaires, de la géométrie arithmétique, des représentations galoisiennes

5.1. La chronologie abrégée de la démonstration

En 1969, lors des journées arithmétiques (Bordeaux), Y. Hellegouarch introduit la courbe elliptique $y^2 = x(x-a^p)(x+b^p)$ où $a^p+b^p+c^p=0$, $1=\text{pgcd}(a,b,c)$, $abc \neq 0$, i.e. une courbe elliptique définie à partir d'une hypothétique solution non triviale à l'équation de Fermat d'exposant p . Il laisse entendre que la courbe a des propriétés si belles qu'elle ne devrait pas exister. Il parle presque dans le désert. Il faut attendre 1985 ; G. Frey ([Fr]), lors d'une conférence à Oberwolfach (en forêt noire), reprend l'argument de façon plus convaincante et croit avoir fait le pont avec la conjecture de Taniyama-Shimura-Weil ([Ta]). On a beaucoup progressé sur les courbes elliptiques ; on y croit. Mais on s'aperçoit que la démonstration de G. Frey est insuffisante. En 1987, c'est le premier coup de tonnerre, un grand théorème sur les représentations galoisiennes de K. Ribet ([R]), précédé depuis quelques temps par un autre de B. Mazur ([Ma2]) implique comme cas particulier, qu'une conjecture dite de Taniyama-Shimura-Weil impliquera le dernier théorème de Fermat.

Taniyama

Shimura

En 1993-1994 après un faux pas, A. Wiles ([T,W],[Wi]) montre que la conjecture est vraie (pour les courbes elliptiques semi-stables). Le 14 octobre 1994 il présente au célèbre journal Annals of Mathematics un article intitulé "Modular elliptic curves and Fermat's Last Theorem" ; c'est un résultat très important qui en particulier donne une démonstration du dernier théorème de Fermat.

Wiles

5.2. Les objets mathématiques pour la démonstration de Fermat

1. Les formes modulaires paraboliques
2. Les fonctions L de courbes elliptiques
3. La représentation galoisienne associée à la torsion d'une courbe elliptique
4. La fameuse courbe elliptique de Hellegouarch-Frey : $y^2=x(x-a^p)(x+b^p)$ avec $a^p+b^p+c^p=0$, $1=\mathrm{pgcd}(a,b,c)$, $abc\neq 0$.
5. L'équation de Fermat $X^p+Y^p+Z^p=0$

5.2.1. Les formes modulaires paraboliques de poids 2, de niveau N

Ce sont les fonctions définies sur le demi-plan complexe supérieur, i.e. $\mathrm{Im}(\tau)>0$, par $f(\tau)=\sum_{n=1}^{\infty} a(n)\,e^{2i\pi n\tau}$. Si $\Gamma_0(N)$ désigne les matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ à coefficients entiers avec $ad-bc=1$ et $N \mid c$, alors on a la relation fonctionnelle $f(\frac{a\tau+b}{c\tau+d})=(c\tau+d)^2 f(\tau)$. De plus pour toute matrice $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\in S\ell_2(\mathbb{Z})$ (et non seulement $\Gamma_0(N)$) , la fonction $\tau\longmapsto(c\tau+d)^{-2}f(\frac{a\tau+b}{c\tau+d})$ admet un développement en série entière suivant les puissances de $q^{\frac{1}{N}}=e^{\frac{2i\pi\tau}{N}}$.

On note $S_2(\Gamma_0(N))$ l'espace vectoriel des formes modulaires paraboliques définies ci-dessus, alors la dimension g de $S_2(\Gamma_0(N))$ est donnée pour les premières valeurs de N par le tableau ci-après :

N	1	2	3	4	5	6	7	8	9	10	11	12	13
g	0	0	0	0	0	0	0	0	0	0	1	0	0

5.2.2. La fonction L d'une courbe elliptique

Soit la courbe elliptique (semi-stable) E d'équation minimale sur $\mathbb{Z}$ $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$. Cette équation modulo p définit une cubique qui s'appelle la réduction de E modulo p . Alors on associe à cette courbe elliptique une fonction définie par
$L_E(s)=\prod_{p|N}\frac{1}{1-a(p)p^{-s}}\prod_{p\nmid N}\frac{1}{1-a(p)p^{-s}+p^{1-2s}}$ lorsque $\mathrm{Re}(s)>\frac{3}{2}$ et où $a(p)$ est relié aux nombres de points de la courbe elliptique E regardée modulo $p\mathbb{Z}$. Facilement L_E admet aussi un développement sous la forme $L_E(s)=\sum_{n=1}^{\infty}a(n)\,n^{-s}$ où lorsque $n=p$, le $a(n)$ est le même que celui défini précédemment.

5.3. Les ponts qui aboutissent à la démonstration de Fermat

5.3.1. Le pont conjectural entre 5.2.1. et 5.2.2. , i.e. la conjecture de Taniyama-Shimura-Weil .

Soient E une courbe elliptique sur $\mathbb{Q}$ de conducteur N , $L_E(s)=\sum_{n\geq 1}a(n)\,n^{-s}$ sa série L associée selon 5.2.2. . La conjecture de Taniyama-Shimura-Weil, dit que la fonction f définie par $f(\tau)=\sum_{n\geq 1}a(n)\,e^{2i\pi n\tau}$ est une forme parabolique de poids 2, de niveau N au sens de 5.2.1. . Le fameux théorème de Wiles (14 octobre 1994) dit que le pont existe pour les courbes elliptiques semi-stables ; la conjecture de Taniyama-Shimura-Weil, devient un théorème.

5.3.2. Comment Fermat est une conséquence des théorèmes de Mazur, Ribet et Wiles.

Supposons qu'il existe un triplet (a,b,c) de nombres entiers, solution de l'équation de Fermat, i.e. $a^p+b^p+c^p=0$, $p\geq 5$ premier , $1=\mathrm{pgcd}(a,b,c)$, $abc\neq 0$. Soit E la courbe elliptique définie par l'équation $y^2=x(x-a^p)(x+b^p)$. Le théorème de Wiles dit que si $L_E(s)=\sum_{n\geq 1}a(n)\,n^{-s}$ est la fonction L associée à la courbe elliptique E selon 5.2.2. , alors $f(\tau):=\sum_{n\geq 1}a(n)\,e^{i2\pi n\tau}$ est une forme parabolique de poids 2 et de niveau N. Alors, par Mazur-Ribet (1989-90) on savait que l'on pouvait choisir $N=2$, pour le niveau de la forme parabolique f supposée non nulle, selon 5.2.1 . Ainsi

K. Ribet

donc $f \in S_2(\Gamma_0(2))$. Mais le tableau de 5.2.1. nous dit que $S_2(\Gamma_0(2)) = \{0\}$, ainsi la seule forme parabolique est la forme nulle. C'est donc là une contradiction. Par conséquent le triplet (a,b,c) avec $a^p + b^p + c^p = 0$ et $abc \neq 0$, ne peut exister et donc l'équation de Fermat $X^p + Y^p - Z^p = 0$ n'admet que les solutions triviales.

6. Questions et remarques inutiles

6.1. Fermat disposait-il d'une démonstration ?

On ne peut répondre à cette question. Pour ce faire il faudrait exhiber une preuve qui utilise les outils mathématiques de l'époque. Ils étaient essentiellement les propriétés arithmétiques de divisibilité des nombres entiers et la technique de descente, i.e. un processus qui fait passer d'une solution à une "solution plus petite". Au dire même de A. Wiles, sa démonstration de 1994 est une démonstration qui ne pouvait être imaginée au 17 ème siècle.

6.2. Le dernier théorème de Fermat est-il un théorème fondamental pour les mathématiques ?

Vite dit, l'équation de Fermat est une équation diophantienne comme les autres et le dernier théorème de Fermat semble sans conséquence sur le reste des mathématiques.

6.3. Le dernier théorème de Fermat a-t-il suscité un enthousiasme dans la communauté mathématique ?

Cette énigme a revêtu un caractère symbolique que l'on peut difficilement expliquer. C'est une vedette qui a tenu le monde mathématique en haleine pendant 358 ans.

6.4. L'énigme de Fermat a-t-elle contribué au développement des mathématiques ?

La réponse est indéniablement oui. Au XIX ème siècle, la recherche d'une solution à Fermat est à l'origine de la création des nombres algébriques et du développement de la théorie arithmétique des corps de nombres. Au XXème siècle, Y. Taniyama énonçait sa conjecture en 1950, elle fut résolue en 1994. Savoir qu'un résultat positif dans le sens de la conjecture conduirait à une démonstration du dernier théorème de Fermat a été un considérable stimulant. On peut aussi dire que le développement de la théorie des représentations galoisiennes a été dynamisé par ses conséquences sur le dernier théorème de Fermat.

7. Une bibliographie

[Fa] Faltings G. Endlichkeitzätze für abelsche Varietäten über Zahlkorpern ; Inv. Math. 73, 349-366 (1983)
[Fr] Frey G. Links between solutions of $A-B=C$ and elliptic curves, Lect. Notes in Math. 1380 (1989), 31-62
[He] Hellegouarch Y. Invitation aux mathématiques de Fermat-Willes, Masson, Paris 1997
[Li] Liu Algebraic geometry and arithmetic curves, Oxford university press, 2002
[Ma1] Mazur B. Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. 47 (1977) 33-186
[Ma2] Mazur B. Deforming Galois représentations in : Galois groups over $\mathbb{Q}$, Y. Ihara, K. Ribet, J.-P. Serre, edit, Springer-Verlag, 1989, 385-427
[Mo] Mordell L. J. On the rational solutions of the indeterminate equations of the 3rd an 4th degrees. Proc. Camb. Phil. Soc., 21 (1922), 179-192
[Oe1] Oesterlé J. Nouvelles approches du "théorème de Fermat" ; Sém. Bourbaki 1987-88, 165-186, S.M.F.
[Oe2]Oesterlé J. Travaux de Wiles (et Taylor, ..) partie II Sém. Bourbaki 1994-95 n° 804
[Ri]Ribenboin P. 13 Lectures on Fermat's Last Theorem ; Springer, Berlin 1979
[R]Ribet K.A. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms ; Inv. Math. 100 (1990), 431-416
[Se1]Serre J.-P. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; Duke Math. J. 54, 179-230 (1987)
[Se2]Serre J.-P. Travaux de Wiles (et Taylor, ...) partie I Séminaire Bourbaki 1994-95 n° 803
[Sh1]Shimura G. Correspondances modulaires et les fonctions ζ de courbes algébriques, J. Math. Soc. Japan 10 (1958), 1-28
[Sh2]Shimura G. Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan 11, Princeton Univ. Press, 1971
[Sil]Silverman J. H. The Arithmetic of Elliptic Curves ; Springer, 1986
[Si]Singh S. Le dernier théorème de Fermat, J.C. Lattès (1998)
[Ta]Taniyama Y. Problem 12, in "Some unsolved problems in mathematics", polycopié Tokyo-Nikko, 1955
[T,W]Taylor R. Wiles A. J. Ring-theoretic properties of certain Hecke algebras ; Annals of Math 142 (1995), 553-572
[We]Weil A. Sur un théorème de Mordell. Bull. Sci. Math., (2) 54 (1930) 182-191
[Wi]Wiles A. J. Modular elliptic curves and Fermat's Last Theorem ; Annals of Maths. 142 (1995), 443-551