LES 350 ANS DU "GRAND THÉORÈME DE FERMAT"

(SUITE)

Norbert SCHAPPACHER

Dans une série de trois conférences à l'Institut Isaac Newton (Cambridge) en juin 1993, Andrew Wiles de l'Université de Princeton annonçait une preuve du "Grand théorème de Fermat". Au moment d'écrire cette introduction à la suite du précédent article (*'L'Ouvert'* n° 73) en ce mois d'avril 1994, il n'y a pas encore de manuscrit de Wiles disponible. En fait, Wiles a rencontré quelques difficultés inattendues en rédigeant les détails techniques du noyau central de son argumentation. Il semble difficile de dire si oui, et quand, la preuve complète éventuelle sera achevée et acceptée par la communauté mathématique. Toutefois, la partie de la preuve de Wiles qui fonctionne avec certitude, représente déjà des progrès considérables dans l'histoire du problème. Cela justifie, nous l'espérons, la publication de la suite de cet article.

2.– Kummer et la création de la théorie des nombres algébriques (1844-1855)

Ernst Eduard Kummer (1810-1893) était un scientifique, plus précisément un professeur de l'Université de Berlin, plus ou moins tel que nous imaginons un professeur aujourd'hui : il était payé autant pour enseigner que pour faire de la recherche en mathématiques. Il a publié dans des journaux scientifiques réputés, notamment le Journal de Crelle. La théorie des nombres n'était pas son seul domaine de recherche active, mais faisait officiellement partie de son travail de professeur. Tout cela montre combien la situation de la science pure et particulièrement celle de la théorie des nombres avait évolué depuis Fermat, lorsque Kummer a commencé à produire son immense contribution au Grand théorème de Fermat et à l'histoire des mathématiques (12). Au moment où la situation sociologique des mathématiques était très proche de ce à quoi nous sommes habitués aujourd'hui, ses mathématiques ne sont déjà plus aussi faciles à expliquer que celles de Fermat, bien que les résultats principaux que nous allons étudier maintenant ont environ 150 ans. La théorie que Kummer a commencé à créer est enseignée dans les cours universitaires de niveau licence. Et quelques unes de ses découvertes sont encore réservées à des cours plus avancés.

Le point de départ est facile à expliquer. Nous avons déjà réduit l'étude des équations de Fermat aux exposants $n = p$ qui sont des nombres premiers impairs,

(12) Voir C. Goldstein "Le métier des nombres aux XVII^{e} et XIX^{e} siècles", in : Eléments d'Histoire des Sciences (M. Serres, éd.), Paris (Bordas) 1989, 275-295.

au moins égaux à 5. Réécrivons l'égalité en question sous la forme

$$a^p = c^p - b^p = \prod_{i=0}^{p-1}(c - \zeta_p^i b)$$

où ζ_p est une racine p$^{\text{ième}}$ de l'unité avec $\zeta_p = 1$ et $\zeta_p \neq 1$. En considérant que ζ_p est complexe on peut prendre $\zeta_p = e^{2i\pi/p}$ pour fixer les idées.

Le gain stratégique de cette décomposition est que nous pouvons espérer jouer avec les propriétés arithmétiques des produits p-uples qui apparaissent maintenant des deux côtés de l'équation. La difficulté est que l'arithmétique de ce nouvel anneau que nous étudions maintenant, l'anneau

$$\mathbb{Z}[\zeta_p] = \{\sum_{i=0}^{p-1} a_i \zeta_p^i | a_i \in \mathbb{Z}\}$$

des entiers algébriques en les racines $p^{\text{ième}}$ de l'unité, par opposition à l'anneau usuel $\mathbb{Z}$ des entiers relatifs, est moins facilement accessible parce que la factorisation unique en nombres premiers n'est pas vraie en général dans $\mathbb{Z}[\zeta_p]$. Pour expliquer aussi simplement que possible ce qui arrive, observons un exemple d'anneau où la factorisation unique est mise en défaut, qui n'est pas de la forme $\mathbb{Z}[\zeta_p]$ mais plutôt $\mathbb{Z}[\alpha]$, où α est un complexe racine carrée de -5, $\alpha^2 = -5$. Dans cet anneau nous avons les trois façons suivantes, essentiellement différentes, pour factoriser 21 en éléments de l'anneau qui ne peuvent être factorisés davantage :

$$21 = 3 \times 7 = (1 + 2\alpha)(1 - 2\alpha) = (4 + \alpha)(4 - \alpha).$$

L'idée de Kummer pour traiter cet imbroglio de factorisations différentes est de supposer seulement quatre "nombres premiers idéaux" déterminés de façon **unique**, non nécessairement éléments de l'anneau lui-même, qui opèrent comme le plus grand commun diviseur de différents éléments irréductibles; par exemple:

$$\wp_1 = (3, 1 + \alpha); \wp_2 = (3, 1 - \alpha); \wp_3 = (7, \alpha + 3); \wp_4 = (7, \alpha - 3).$$

Alors les trois différentes décompositions de 21 sont expliquées par l'unique factorisation du même nombre en "premiers idéaux" :

$$21 = \wp_1\wp_2\wp_3\wp_4; 3 = \wp_1\wp_2; 7 = \wp_3\wp_4; 1 + 2\alpha = \wp_2\wp_4;$$
$$1 - 2\alpha = \wp_1\wp_3; 4 + \alpha = \wp_1\wp_4; 4 - \alpha = \wp_2\wp_3.$$

Il est bien sûr aisé de postuler l'existence d'une telle décomposition "idéale", mais cela ne crée pas une théorie mathématique effective. Cependant Kummer pouvait utiliser la structure spécifique des anneaux $\mathbb{Z}[\zeta_p]$ qu'il étudiait afin de donner un critère entièrement rigoureux et aussi efficace pour qu'un élément de $\mathbb{Z}[\zeta_p]$ soit

divisible par un nombre premier idéal $\wp$, spécifique. (En termes actuels, le point fondamental est qu'on peut "voir" le corps fini qui sera la réduction de $\mathbb{Z}[\zeta_p]$ modulo un quelconque $\wp$, parce que les corps finis sont formés à partir de racines de l'unité...) Nous ne donnons pas les formules ici, mais nous recommandons la lecture des articles de Kummer écrits durant la période indiquée dans le titre de ce paragraphe (13).

Afin d'établir les résultats en lien avec le Grand théorème de Fermat, nous allons introduire le nombre de classes h_p de l'anneau $\mathbb{Z}[\zeta_p]$. Cet invariant compte les nombres idéaux que nous devons ajouter aux éléments actuels de l'anneau, afin d'obtenir un domaine idéal où la factorisation unique est valable. Il est calibré de telle façon que si, comme c'est le cas pour $p = 3$, il arrive que $\mathbb{Z}[\zeta_p]$ soit factoriel, alors $h_p = 1$ et nous n'avons besoin que de la classe des éléments de l'anneau actuel pour obtenir une factorisation unique.

D'autre part, en ajoutant un nombre idéal premier $\wp$, nous ajoutons la classe de tous les éléments de l'anneau multipliés par $\wp$ à notre domaine d'opération. Kummer savait dans tous les cas que la factorisation unique idéale peut être réalisée dans un domaine formé d'un nombre fini de telles classes, précisément h_p classes.

Le théorème de Kummer. *Si p ne divise pas le nombre de classes h_p, alors l'assertion du Grand Théorème de Fermat est vraie pour l'exposant $n = p$.*

En fait, Kummer n'a pas seulement prouvé ce résultat, mais il a donné en même temps un critère efficace pour qu'un nombre premier p satisfasse à l'hypothèse $p \not| \ h_p$ c'est-à-dire, comme il l'exprimait, un critère pour vérifier que p est un nombre premier régulier.

Le critère de Kummer. *Le nombre premier p est régulier si et seulement si pour tout $k = 2, 4, 6, \ldots p-3$, le nombre premier p ne divise pas le numérateur du nombre de Bernoulli B_k.*

Rappelons que les nombres de Bernoulli peuvent être définis par la série entière

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

de telle façon que $B_0 = 1, B_1 = -1/2, B_2 = 1, B_3 = 0$ et en général $B_{2n+1} = 0$ pour tout $n \geq 1$; alors que $B_4 = 1/30; B_6 = 1/42; B_8 = -1/39; B_{10} = 5/66; B_{12} = -691/2730$.

D'après le critère de Kummer, la dernière valeur signifie que $p = 691$ n'est pas un nombre premier régulier. Incidemment, la liste des nombres premiers irréguliers commence avec 37, 59, 67, 101, 103, 131, 149, 157.

(13) Voir Kummer's Collected Papers (Springer Verlag) avec la préface instructive d'A. Weil. Il existe également un livre très détaillé sur la théorie de Kummer : H.E. Edwards, "Fermat's last Theorem". A Genetic Introduction to Algebraic Number Theory, GTM 50 (Springer Verlag) 1977.

Nous n'entrerons pas dans des détails techniques ici. Mais il sera évident que la théorie de Kummer a représenté un grand pas en avant dans l'histoire du Grand théorème de Fermat. D'un autre côté, on peut également penser que ce n'était pas le début d'une preuve complète de la conjecture de Fermat. En fait, nous savons aujourd'hui qu'il y a une infinité de nombres premiers irréguliers, mais nous ne pouvons pas encore prouver qu'il y a une infinité de nombres premiers réguliers. Kummer lui-même, et beaucoup de mathématiciens après lui ont bien entendu affiné ces résultats. En conséquence, aujourd'hui, pour chaque nombre premier à l'intérieur d'un intervalle confortable de calcul et même s'il est irrégulier, il y aura quelque critère raffiné permettant de conclure (essentiellement à la façon de Kummer) que le Grand théorème de Fermat est valable pour ce nombre premier. Mais en même temps, il semble assez désespéré de développer cette approche en une véritable théorie générale qui fournirait éventuellement une chance d'établir la conjecture pour **chaque** nombre premier.

Néanmoins cet état de la situation, non seulement ne diminue en rien l'exploit de Kummer, mais il nous en fait voir plus clairement l'impact le plus important que la recherche de Kummer a eu dans l'histoire de l'arithmétique. Cet impact est double.

D'abord les générations qui ont suivi immédiatement Kummer ont généralisé son travail aux anneaux d'entiers de toute extension algébrique finie du corps $\mathbb{Q}$ des rationnels, et pas seulement les corps cyclotomiques $\mathbb{Q}[\zeta_p]$ (et leurs extensions obtenues par adjonction des racines $p^{\text{ième}}$ des éléments de $\mathbb{Q}[\zeta_p]$, que Kummer avait aussi étudiées). Cette théorie générale est connue aujourd'hui comme **la théorie des entiers algébriques**. Elle a été établie dans ses bases de manière indépendante par Richard Dedekind (1831-1916) qui n'a pas seulement traduit les "nombres idéaux" de Kummer en idéaux de l'anneau en question (comme nous faisons encore aujourd'hui : au lieu de travailler avec la quantité $\wp$ de Kummer, d'une manière quelque peu incertaine, nous étudions le sous ensemble de tous les éléments de l'anneau divisibles par $\wp$) il a introduit également beaucoup de concepts et de méthodes d'algèbre moderne (14) caractérisée par sa perspective structurelle. Ainsi, pratiquement toute l'algèbre moderne, autant que les développements profonds de la théorie des nombres algébriques de la première moitié du 20$^{\text{e}}$ siècle tels la théorie du corps de classes, se situent dans la continuité historique évidente du travail de Kummer.

Mais il y a un autre aspect qui est presque comme la face cachée de la même pièce. Inévitablement, quand on généralise une théorie profonde, comme le fit Dedekind si fructueusement avec la théorie arithmétique des corps cyclotomiques de Kummer, alors il faut aussi sacrifier certains caractères spéciaux – ceux en rapport avec le cas cyclotomique, et qui tout simplement n'existent pas pour un corps de nombres arbitraire.

(14) Cette utilisation particulière du mot "moderne" date des années 1920 ou 1930.

En 1897 David Hilbert publia son œuvre capitale le **Zahlbericht** (15) qui représente pour l'époque un compte rendu d'ensemble de l'état de la théorie des nombres algébriques, utilisant le point de vue de Dedekind (16) et incorporant aussi la propre recherche de Hilbert sur l'arithmétique des extensions de Galois des corps de nombres, dans la partie III. Suivant cette partie III (qui traite de la théorie des corps quadratiques et dont une grande partie renvoie aux travaux de Gauss et Dirichlet, avant Kummer) le **Zahlbericht** s'attaque spécifiquement à la théorie cyclotomique de Kummer (parties IV et V) et en fait la seconde moitié de ce volumineux rapport. Eh bien, contrairement à la première partie, Hilbert est visiblement non satisfait avec le fait qu'il doive suivre de près les pas de Kummer. Les deux générations entre Kummer et Hilbert ont tout simplement échoué à produire des avancées conceptuelles dans la partie de la théorie où la virtuosité cyclotomique de Kummer avait atteint son sommet (17). Ne pouvant se contenter de répéter fondamentalement Kummer, mais aussi, incapable de produire une présentation véritablement nouvelle de la théorie, Hilbert signale du moins (dans le chapitre 35) la possibilité de prouver les théorèmes et les lemmes de Kummer dans un ordre différent : voir les remarques de Hilbert, en particulier les §166, 170 et 171.

Aujourd'hui nous sommes dans une meilleure situation grâce à la théorie commencée dans les années 1950 par Kenkichi Iwasawa qui fournit un nouveau cadre et en fait un prolongement très profond de la théorie cyclotomique la plus avancée de Kummer. C'est autant que nous puissions le dire aujourd'hui, l'autre ligne de développement qui avait démarré avec l'arithmétique de Kummer. Elle est toujours au premier rang des recherches courantes en théorie des nombres comme l'atteste par exemple le fait que deux des plus importants titres à la renommée d'Andrew Wiles avant l'annonce de sa preuve du Grand théorème de Fermat étaient des démonstrations (reconnues) de ce que l'on appelle la **conjecture principale de la théorie d'Iwasawa** (18).

3. La géométrie arithmétique des courbes de Fermat (1901-1983)

Les développements dont je veux traiter maintenant appartiennent à notre siècle. Ils ont été rendus possibles grâce aux progrès de la géométrie algébrique réalisés aux cours du 19^{e} siècle, en particulier pendant sa seconde moitié. L'année 1901 mentionnée dans le titre de cette section renvoie à un écrit remarquable d'Henri

(15) Jahresbericht der D.M.V.4 175-546.

(16) La plus grande partie de I du Zahlbericht est écrite dans la veine de Dedekind. Pour une exception bien connue (Satz 7, le théorème fondamental de décomposition des idéaux) voir H.E. Edwards, "The Genesis of Ideal Theory", Archive Hist. Ex. Sc. 23 1980, 321-378, en particulier p. 349. Cf. la bibliographie sur cette question dans les références d'Edwards, Neumann, Purkert, Archive Hist. Ex. Sc. 27 1983, 49-85. Plus récemment, on trouve la thèse (Göttingen 1993) sur Dedekind, ainsi qu'une prépublication sur l'émergence de la théorie des nombres algébriques, par le jeune Ralph Haubrich.

(17) Pour citer un exemple, le calcul formel de Kummer des "dérivées logarithmiques" d'unités cyclotomiques.

(18) Travail conjoint avec Mazur en 1984 pour le cas abélien; et Wiles par lui-même en 1991 pour l'ensemble des extensions de $\mathbb{Q}$.

Poincaré (1854-1912) qui parut cette année là : *Sur les propriétés arithmétiques des courbes algébriques* (19).

Dans cet écrit, le but de Poincaré est d'appliquer les notions développées par la géométrie algébrique du 19^e siècle – en particulier, l'idée d'invariance birationnelle – pour classer les problèmes diophantiens. Avant de décrire plus nettement ce que cela signifie, je vais essayer d'expliquer la motivation de Poincaré (incidemment, ceci est aussi en accord avec la remarque que je faisais au début, quant au fait que "le Grand théorème de Fermat" est lui-même sans intérêt...)

Ce qui rend le domaine de l'Analyse diophantienne (20) si peu attrayant pour un mathématicien (à l'esprit théorique) (21) c'est son caractère morcelé. En regardant par exemple dans l'**Histoire de la Théorie des nombres** de Dickson – dont je ne mets pas en doute la valeur comme source de références historiques détaillées pour des problèmes spécifiques! – le lecteur est frappé par le manque apparent d'organisation intrinsèque pour les différents problèmes diophantiens examinés. La forme extérieure des équations semble être le principal critère déterminant l'ordre des chapitres. Mais tout le monde sait que les équations peuvent être rendues tout à fait différentes par certaines substitutions, sans modification du problème. Ansi la compilation de Dickson illustre le manque traditionnel d'invariants théoriques dans l'Analyse diophantienne. C'est à ces desiderata fondamentaux que Poincaré souhaitait remédier.

Nous allons maintenant expliquer la disposition d'ensemble de l'article de Poincaré, en donnant les équations du "Grand théorème de Fermat" comme un exemple.

Chercher des solutions entières de l'équation $X^n + Y^n = Z^n$ équivaut à chercher les points rationnels de la courbe $x^n + y^n = 1$. Plus précisément, les solutions entières (X, Y, Z) de la première équation, avec $Z \neq 0$, correspondent aux points rationnels $(x, y) = (\frac{X}{Z}, \frac{Y}{Z})$ sur la courbe d'équation $x^n + y^n = 1$. Maintenant, dans le cas des équations de Fermat, les solutions restantes : (X, Y, Z) avec $Z = 0$, sont facilement identifiables (et n'apportent pas de contradiction à la validité du "Grand théorème de Fermat"). Cependant elles doivent être prises en compte géométriquement et la méthode commune pour les traiter est de considérer les trois variables X, Y, Z symétriquement, c'est-à-dire de ne pas en particulariser une qui soit ou ne soit pas nulle. La courbe projective $x^n + y^n = 1$ a comme points rationnels tous les triplets d'entiers (X, Y, Z) tels que $XYZ \neq 0$; mais deux tels triplets $(X_1, Y_1, Z_1), (X_2, Y_2, Z_2)$ définissent le même point dans le plan projectif sur le corps des rationnels, si et seulement si il existe un nombre rationnel non nul λ tel que $X_2 = \lambda X_1, Y_2 = \lambda Y_1, Z_2 = \lambda Z_1$. La condition pour qu'un tel point

(19) Journal de Mathématiques, 5^e série, t. 7 fasc. III 1991, 161-233 (= Oeuvres V, 483-550).
(20) C'est-à-dire la branche des mathématiques qui s'occupe de la résolution concrète d'équations la plupart du temps polynômes à plusieurs variables ayant des coefficients entiers, résolution en nombres entiers ou rationnels.
(21) Ce qui est décrit ici comme un défaut en Analyse diophantienne est **"défaut"** uniquement sous l'hypothèse qu'il faut avoir des objectifs théoriques. Des problèmes diophantiens non systématiques sont bien sûr totalement acceptables dans un autre contexte, tel les mathématiques récréatives...

projectif appartienne à la courbe $X^n + Y^n = Z^n$ est bien définie indépendamment du triplet choisi pour représenter le point puisque l'équation est homogène : $(\lambda X_1)^n + (\lambda Y_1)^n - (\lambda Z_1)^n = \lambda^n (X_1^n + Y_1^n - Z_1^n)$. Notons que de cette manière, pour $Z \neq 0$, nous devons retrouver les points rationnels de $x^n + y^n = 1$ traités ci-dessus car les fractions peuvent être simplifiées : $\frac{\lambda X}{\lambda Z} = \frac{X}{Z}$.

Cela étant dit, à partir de maintenant toutes les courbes seront considérées comme des courbes projectives mais seront notées sous la forme affine : $x^n + y^n = 1$. Cet abus de notation est habituel dans ce domaine des mathématiques.

Il est un premier invariant qui se présente de lui-même quand on étudie la famille des courbes de Fermat : le degré n de la courbe $F_n : x^n + y^n = 1$. C'est plus ou moins l'invariant de base que Poincaré utilise dans sa discussion – exception faite que le degré peut bien sûr changer sous des transformations. Par exemple, si on substitue $x = u, y = uv$ dans la courbe F_3, l'équation devient $u^3 + u^3 v^3 = 1$, qui a un degré total égal à 6. La raison pour laquelle ceci "ne doit pas compter" est que la substitution introduit une singularité. Plus précisément, nous obtenons une singularité à l'infini. En effet : écrivons la courbe transformée projectivement en $F(U, V, W) = 0$, où

$$F = U^3 W^3 + U^3 V^3 - W^6.$$

Ainsi nous ajoutons la puissance minimale de W à chaque monôme pour rendre toute l'équation homogène. Il y a alors sur cette courbe deux points projectifs qui sont de la forme $(U, V, 0)$; ils peuvent être représentés par les triplets d'entiers $(1, 0, 0)$ et $(0, 1, 0)$. Notons que ces points sont "à l'infini" dans le sens qu'ils ne peuvent être trouvés dans les termes de l'équation affine $u^3 + u^3 v^3 = 1$ de variables u et v. En ces deux points, les dérivées partielles $\frac{\partial F}{\partial U}, \frac{\partial F}{\partial V}, \frac{\partial F}{\partial W}$ s'annulent toutes trois. Cela signifie, par définition, que ce sont des points singuliers. L'équation d'origine : $x^n + y^n = 1$ n'a pas de points singuliers ni dans le plan affine (x, y), ni à l'infini.

Aujourd'hui, il est acquis que le degré est un invariant de toutes les équations non singulières définissant la même courbe. Pour démontrer ceci, on utilise un invariant fondamental des courbes algébriques qui fut introduit par Bernhard Riemann (1822-1866) : le genre. – Et c'est le genre que Poincaré emploie pour la première classification des problèmes diophantiens liés aux courbes algébriques.

Cet invariant peut être défini de plusieurs manières substantiellement distinctes. Topologiquement, par exemple, examinons sur l'ensemble des nombres complexes les points de notre courbe algébrique (qui forment une surface de Riemann car $\mathbb{C}$ est de dimension 2 sur $\mathbb{R}$), le genre compte le nombre de "trous" : la sphère est de genre 0, le tore de genre 1, la surface d'un bretzel de genre 2, etc ...

Dans notre contexte nous avons cette formule : si la courbe algébrique est donnée par une équation non singulière de degré n, alors son genre est égal à

$$g = \frac{(n-1)(n-2)}{2}.$$

Ainsi la classification des courbes de Fermat selon leur genre donne ceci :

Premier cas : genre $g = 0$, degré $n = 2$.

Il s'agit alors de la courbe de Fermat F_2 : $x^2 + y^2 = 1$, qui est le cas exclu de l'énoncé du "Grand théorème de Fermat". Nous pouvons donner maintenant la raison géométrique qui fait que la conjecture ne peut être retenue pour $n = 2$. La courbe est naturellement un cercle (si nous la considérons sur $\mathbb{R}$) ou une sphère (sur $\mathbb{C}$), et elle a au moins un point rationnel, disons (0,1). Puis nous pouvons utiliser la méthode de projection stéréographique (qui convient pour toutes les coniques, c'est-à-dire toutes les courbes données par une équation quadratique non singulière ayant au moins un point rationnel) en paramétrant **tous** les points rationnels qui lui appartiennent en traçant toutes les droites de pente rationnelle passant par le point fixe (0,1). Une droite (étant donnée par une équation de degré 1) rencontre la courbe (qui est donnée par une équation de degré 2) en deux points (en comptant avec les multiplicités et, en général, en admettant tous les points projectifs comme intersections) : l'un d'eux est le point fixe, l'autre variera et se positionnera sur tous les autres points de la courbe, comme cela peut être facilement prouvé par un examen des équations algébriques concernées.

Ainsi nous voyons qu'une conique non singulière qui admet un point rationnel a une infinité de points rationnels. Dans le cas particulier de F_2 cela explique la paramétrisation des triplets pythagoriciens utilisée dans l'appendice.

En fait, le point de vue de Poincaré avait déjà été appliqué dans les problèmes diophantiens liés aux courbes de genre 0 par Hilbert et Hurwitz (22).

Deuxième cas : genre $g = 1$, degré $n = 3$.

Les courbes algébriques non singulières de genre 1 qui admettent un point rationnel sont appelées courbes elliptiques. Cette terminologie est un peu malheureuse car l'ellipse – qui est bien sûr une conique et ainsi de genre 0 – n'est pas une courbe elliptique (23). La raison en est historique : l'intégrale mesurant la longueur d'un arc d'ellipse nécessite l'intégration d'une expression de la forme $\frac{dx}{y}$ avec x et y liés par une équation cubique non singulière, c'est-à-dire une équation de genre 1.

Le cas du "Grand théorème de Fermat" pour lequel on a F_n de genre 1 est $n = 3$ qui a été démontré par Euler, comme nous l'avons mentionné (dans l'article précédent). Contrairement au cas de genre 0 cette courbe de Fermat a donc par conséquent seulement un nombre fini de points rationnels – à savoir les points triviaux, ayant au moins une coordonnée projective nulle.

Ceci n'est pas vrai de façon générale pour toutes les courbes elliptiques. En fait certaines courbes elliptiques ont un grand nombre fini de points rationnels, certaines en ont un nombre infini. Et la question de savoir quel cas s'applique à

(22) D. Hilbert et A. Hurwitz, Über die diophantischen Gleichungen vom Geschlecht Null, Acta Mathematica 14 (1890) 217-224 = Hilbert, "Gesammelte Abhandlungen " II, 258-263 = Hurwitz, "Math. Werke" II, 116-121.

(23) Dans le dictionnaire français "Le Petit Larousse", on trouve la magnifique erreur : 'ELLIPTIQUE' : adj. math. Qui est en ellipse : Courbe elliptique.

une courbe elliptique donnée est intimement liée à l'une des grandes conjectures des mathématiques contemporaines : la conjecture de Birch et Swinnerton-Dyer (24).

Mais ce qui distingue vraiment le cas elliptique de tous les autres n'est pas tant cette gamme du nombre possible des solutions. C'est plutôt la structure supplémentaire présente sur les courbes elliptiques qui permet une théorie arithmétique riche qui n'existe pas pour les courbes de genre 0 ou supérieur à 1. Pour comprendre au moins le début de cela, utilisons le fait qu'une courbe elliptique peut être donnée par une équation cubique. Alors une droite rencontrant la courbe E en deux points rationnels (comptant toujours avec les multiplicités) la rencontrera de nouveau en un troisième. L'opération binaire résultante (appelée communément **processus de tangente et sécante**)

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow E(\mathbb{Q})$$

n'est pas en général une loi de groupe (25), mais peut être transformée en loi de groupe abélien, essentiellement par le choix d'une origine (26).

Le premier grand résultat fondamental de l'arithmétique des courbes elliptiques – pour lequel il n'est pas tout à fait clair si Poincaré en fit la conjecture dans son article ou simplement ne réussit pas à prévoir la possibilité que celui-ci soit faux – est que **pour une courbe elliptique E sur $\mathbb{Q}$, le groupe abélien $E(\mathbb{Q})$ a un nombre de générateurs fini**. Ceci fut prouvé par J.-L. Mordell (1888-1972) à Cambridge en 1922. La preuve peut être interprétée joliment comme une version généralisée et théorique de la descente de Fermat mais nous ne l'introduisons pas ici.

Troisième cas : genre $g \geq 2$, degré $n > 3$.

Tout à la fin de son écrit de 1922, Mordell conjectura que toutes les courbes de genre au moins égal à 2 n'avaient qu'un nombre fini de points rationnels. Cette conjecture fut démontrée par Gerd Faltings (alors à Wuppertal) en 1983, une réussite qui lui valut la médaille Fields. Ainsi on peut dire de façon imagée que, lorsque les courbes deviennent trop compliquées, il n'y a en général pas de structure naturelle sur l'ensemble des points rationnels ; mais cet ensemble est fini.

Quand j'essayai d'expliquer le théorème de Faltings à ma mère (qui n'est pas une mathématicienne) en 1983, je choisis, comme je le fais ici, la famille des courbes F_n de Fermat pour illustrer le résultat, parlai et expliquai pendant près d'une

(24) cf. N. Schappacher, Neuere Forschungsergebnisse in der Arithmetik elliptischer Kurven, Didaktik der Mathematik 17 (1989), 149-158.

(25) Dans le cas spécifique de la 3^e courbe de Fermat, il y a déjà une loi de groupe, simplement parce qu'il y a si peu de points rationnels. La structure obtenue ainsi sur l'ensemble des solutions triviales de $x^3 + y^3 = 1$ (y compris le point à l'infini) est celle de 4-groupe de Klein, i.e. le groupe non cyclique d'ordre 4.

(26) cf. N. Schappacher, Développement de la loi de groupe sur une cubique, Séminaire de Théorie des Nombres Paris 1988-89, Progress in Mathematics 91 (Birkhäuser) 1991, 159-184.

demi-heure, et puis j'entendis ma mère remarquer plutôt sèchement qu'après tout Fermat restait non démontré.

Ma mère avait bien sûr raison : le "Grand théorème de Fermat" ne permet pas de bien apprécier l'importance du théorème de Faltings. Même aujourd'hui il n'existe pas de variante efficace de la conjecture de Mordell qui puisse faire tomber la conjecture de Fermat. Les propriétés de la famille des courbes F_n sont justement très particulières. D'un autre côté le théorème de Faltings couvre toutes les courbes de genre au moins égal à 2, et qui plus est, pendant qu'il prouvait la conjecture de Mordell, en réalité Faltings établissait deux autres conjectures techniques (de Tate et de Safarevic) qui à elles seules suffisent à expliquer la grande réputation de son travail parmi les experts.

4.– Le lien avec l'Arithmétique des courbes elliptiques (1984-1993)

Ce fut un an et demi après le théorème de Faltings, en décembre 1984, que Gerhard Frey (de Saarbrück, à ce moment là) envoya une note de deux pages et demi à ses amis intimes dans laquelle il indiquait une stratégie de démonstration pour le fait que la conjecture de Taniyama-Shimura (voir plus loin) impliquerait le "Grand théorème de Fermat". Puisque le document était confidentiel, la nouvelle se répandit rapidement – et on découvrit aussi vite que la démonstration de Frey sur cette implication n'était pas complète. Mais l'idée avait été lancée et en 1986/87 Ken Ribet arriva à résoudre la question par une démonstration (très compliquée mais maintenant entièrement acceptée).

Voici l'idée de Frey dans une coquille de noix : supposons que le "Grand théorème de Fermat" soit faux. Alors il existerait un nombre premier $p \geq 5$ (en fait, p serait même beaucoup plus grand ...) et trois entiers non nuls a, b, c tels que $a^p + b^p = c^p$. Appelons $\mathcal{L} = (a, b, c)$ cette hypothétique solution de l'équation de Fermat pour l'exposant p. S'il existe un facteur commun divisant les trois composantes a, b, c nous pouvons l'enlever car l'équation est homogène. Ainsi nous supposons que $\text{pgcd}(a, b, c) = 1$. Ceci implique que parmi a et b l'un est pair, et l'autre impair.

Disons que b est pair; alors a et c sont impairs et par conséquent $\equiv \pm 1 \pmod 4$. Comme p est impair nous pouvons échanger a et c en les multipliant par -1. Alors nous pouvons supposer sans perte de généralité que c a pour reste 3 (et non 1) lorsqu'on le divise par 4. Avec ces normalisations, étant donnée une solution hypothétique $\mathcal{L}$ de l'équation de Fermat pour l'exposant p, nous écrivons l'équation suivante d'une courbe elliptique sur $\mathbb{Q}$:

$$E_{\mathcal{L}} : y^2 = x(x - b^p)(x - c^p).$$

Notons que nous avons bien là une courbe elliptique : l'équation est de degré 3, et elle n'est pas singulière car le polynôme en x du membre de droite a trois racines distinctes.

La courbe elliptique $E_{\mathcal{L}}$ monte vraiment sur scène comme un *deus ex machina*. Une telle écriture amène comme par magie la conjecture de Fermat à portée de la

théorie arithmétique des courbes elliptiques relativement bien développée – plutôt que de la laisser dans le domaine des courbes de genre supérieur, comme dans le paragraphe précédent. La courbe $E_{\mathcal{L}}$ se rencontre dans la littérature avant Frey (voir les articles référencés dans la note 2 de bas de page). Mais Frey fut apparemment le premier à envisager de démontrer la non existence de la courbe $E_{\mathcal{L}}$ de la manière qui suit.

Théorème de Ribet. La courbe $E_{\mathcal{L}}$ n'est pas une courbe elliptique modulaire.

Conjecture de Taniyama-Shimura. Toute courbe elliptique sur $\mathbb{Q}$ est modulaire.

Théorème annoncé par Wiles. Toute courbe elliptique semi-stable sur $\mathbb{Q}$ est modulaire.

Maintenant afin d'arriver à comprendre ces énoncés nous devons définir les notions de courbe modulaire et de courbe elliptique semi-stable. La courbe $E_{\mathcal{L}}$ se revèle être toujours semi stable, de sorte que le résultat annoncé par Wiles suffirait à déduire le "Grand théorème de Fermat".

Courbes elliptiques semi-stables

Pour définir ce qu'est une courbe elliptique semi-stable nous devons étudier la réduction d'une courbe elliptique (qui est définie sur $\mathbb{Q}$) modulo un nombre premier q. A première vue ceci est simple. Prenons par exemple l'équation définissant notre courbe $E_{\mathcal{L}} : y^2 = x(x - b^p)(x - c^p)$. Elle a des coefficients entiers que l'on peut considérer comme entiers modulo q, pour n'importe quel nombre premier q donné. La courbe algébrique projective résultante sur le corps fini $F_q = \mathbb{Z}/q\mathbb{Z}$ ayant q éléments est habituellement non singulière, et en conséquence une courbe elliptique – sur F_q. Plus précisément c'est le cas lorsque les trois racines $0, b^p, c^p$ du polynôme en x de droite sont (non seulement distinctes dans $\mathbb{Z}$, comme elles le sont, mais aussi) deux à deux non congrues modulo q.

Les mauvais premiers q, c'est-à-dire ceux pour lesquels l'équation réduite a une singularité, sont ceux qui divisent l'une des différences des trois racines $0, b^p, c^p$ – en d'autres termes ce sont les premiers q qui divisent le produit abc. Pour ces nombres q, la condition de réduction semi-stable à q signifie qu'il y a deux tangentes distinctes au point singulier de la courbe réduite. Pour notre équation particulière ceci équivaut à dire que les racines du polynôme en x de droite ne se réduisent pas toutes trois en un même élément de F_q – une condition qui est satisfaite car nous avons fait en sorte que $\mathrm{pgcd}(a, b, c) = 1$.

Jusqu'ici ça va, mais nous voulons vraiment une notion géométrique qui ne dépende pas de l'équation spécifique utilisée pour décrire notre courbe. Et en étudiant les réductions modulo les premiers $q = 2$ et $q = 3$, les équations de la forme $y^2 = P(x)$, où $P(x)$ est un polynôme de degré 3 en x, ne sont justement pas assez générales. Par exemple, une telle équation aura toujours une singularité avec une tangente unique (de multiplicité deux) quand elle est réduite modulo $q = 2$.

Un type d'équation qui convient pour tous les premiers q, appelé **modèle général de Weierstrass**, est une équation non singulière de la forme suivante :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Deux telles équations définissent la même courbe si et seulement si l'une peut être obtenue à partir de l'autre par un changement de coordonnées $x = A^2x' + B; y = A^3y' + Cx' + D$, avec $A, B, C, D \in \mathbb{Q}$, et une division ultérieure par A^6.

Définition. Une courbe elliptique E définie sur le corps $\mathbb{Q}$ des nombres rationnels est appelée semi-stable, si pour tout nombre premier q, il existe une équation définissant E, qui, lorsqu'elle est réduite modulo q, soit est non singulière soit admet une singularité avec deux tangentes de directions distinctes.

Exemples (27).
1. La courbe elliptique $y^2 = x(x+9)(x-16)$ est aussi donnée par $y^2+xy+y = x^3+x^2-10x-10$, et par conséquent semi-stable. Mais la courbe $y^2 = x(x-9)(x+16)$ n'est pas semi-stable pour le nombre premier $q = 2$.

2. Les courbes $E_{\mathcal{L}}$ de Frey admettent l'équation suivante (28) qui montre qu'elles sont semi-stables

$$v^2 + uv = u^3 - \frac{1 + b^p + c^p}{4}u^2 + \frac{b^pc^p}{16}u.$$

Courbes elliptiques modulaires

Soit $\mathcal{H}$ le demi-plan supérieur $\mathcal{H} = \{z = x + iy \in \mathbb{C} | y > 0\}$. Muni de la métrique $ds^2 = \frac{dx^2+dy^2}{y^2}$, c'est un des modèles courants de la géométrie hyperbolique non euclidienne. La métrique est invariante en ce qui concerne l'"action" suivante des matrices réelles 2×2 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ayant un déterminant positif :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longmapsto \frac{az + b}{cz + d}.$$

Nous allons utiliser le quotient de $\mathcal{H}$ sous l'action du sous-groupe suivant de matrices entières de déterminant 1, où N est un entier donné :

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) | c \equiv 0 (mod N)\}.$$

Ce quotient $\Gamma_0(N) \setminus \mathcal{H}$ est une surface de Riemann qui peut être compactifiée en ajoutant un nombre fini de pointes à savoir un point $i\infty$ à distance infinie dans la

(27) Le premier exemple est pris chez K. Rubin et A. Silverberg, Wiles prof of Fermat's Last Theorem; manuscrit de présentation non publié, accessible electroniquement par le réseau mathématique.
(28) Via $x = 4u, y = 8v + 4u$.

direction imaginaire positive, et ses translatés sous l'action de $\Gamma_0(N) \setminus SL_2(\mathbb{Z})$. La surface de Riemann compacte résultante est appelée la courbe modulaire $X_0(N)$.

Définition. Une courbe elliptique E qui est définie sur le corps $\mathbb{Q}$ des nombres rationnels est appelée une courbe elliptique modulaire s'il existe $N \geq 1$ et une application holomorphe surjective

$$\varphi : X_0(N) \longrightarrow E(\mathbb{C}).$$

Cette définition (29) ne rend pas évident le contenu arithmétique de la notion. En fait, il existe un certaion nombre de conditions de nature différente, dont chacune caractérise des courbes elliptiques modulaires. Mais il est clair au moins à partir de la définition donnée, que nous entamons une autre source géométrique de classification des courbes et variétés algébriques, différente de celle discutée dans la section 3 (programme de Poincaré).

Plutôt que de continuer à introduire des concepts et des méthodes prérequises pour l'attaque par Wiles du "Grand théorème de Fermat", permettez-moi de revenir à mon point de départ : la question de l'intérêt du "Grand théorème de Fermat". Du théorème annoncé par Wiles on peut aussi déduire que l'équation plus générale que celle de Fermat:

$$Ax^p + y^p = z^p$$

n'a pas de solutions entières non nulles, pourvu que la constante A soit de la forme l^n avec $n \geq 1$ et l l'un quelconque des nombres 3, 5, 7, 11, 13, 17, 19, 23, 29, 53 ou 59. (On pourrait pousser davantage la liste des A admissibles.....)

Ceci peut donner une idée du degré de généralité de la méthode en question.

(29) Voir B. Mazur, Number Theory as Gadfly, Amer. Math. Monthly 98 (1991), 593-610.