Andrew Wiles reçoit le Prix Abel 2016

Le mathématicien anglais Sir Andrew Wiles a reçu le Prix Abel 2016 *pour avoir démontré de manière éclatante le dernier théorème de Fermat par le biais de la conjecture de modularité pour les courbes elliptiques semi-stables, ouvrant ainsi une nouvelle ère dans la théorie des nombres.*

Sir Andrew Wiles (1953–)

Créé en 2003, le Prix Abel est décerné par l'Académie norvégienne des Sciences et des Lettres pour récompenser l'œuvre de grands mathématiciens et se veut un analogue du Prix Nobel. Richement doté (environ 750 000 euros), il a depuis été remis à dix-sept mathématiciens, parmi lesquels trois Français : Jean-Pierre Serre (2002), Jacques Tits (2008) et Mikhaïl Gromov (2009).

Même si son travail mathématique ne se réduit pas à cela, Andrew Wiles est mondialement connu pour avoir démontré en 1995 un résultat énoncé plus de 350 ans plus tôt par le mathématicien Pierre de Fermat :

L'équation $x^n + y^n = z^n$ n'a pas de solution entière avec $x, y, z > 0$ et $n \geq 3$.

Cette démonstration a eu un retentissement considérable, parfaitement inhabituel pour le domaine, notamment dû à l'ancienneté et à l'histoire rocambolesque de ce problème. Cette célébrité est également méritée du point de vue mathématique, à la fois pour la tension entre l'aspect élémentaire du résultat et la sophistication de sa démonstration et pour la profondeur

et l'élégance des liens crées par la *conjecture de modularité* dont parle la citation du comité Abel.

Le but de cette note est de présenter très brièvement quelques aspects mathématiques du théorème de Fermat. Évidemment, on ne touchera que très superficiellement les apports d'Andrew Wiles lui-même, en indiquant toutefois quelques références pour le lecteur curieux.

On peut déjà citer le *best-seller* de Simon Singh, *Le Dernier Théorème de Fermat* ([Sin11]) et le documentaire qui l'accompagne, que l'on peut visionner en version française [1] (et qualité sonore médiocre) sur le site Dailymotion, qui rend bien mieux justice à l'histoire fascinante de ce résultat, depuis ses débuts légendaires dans la marge de l'exemplaire appartenant à Fermat de l'*Arithmétique* de Diophante jusqu'au travail solitaire d'Andrew Wiles dans les années 1990, qu'il ne serait possible de le faire ici.

A. Pythagore, Diophante et Fermat

Pierre de Fermat (date de naissance inconnue, peut-être 1607–1665) est un mathématicien amateur [2] dont l'œuvre concerne la géométrie, le calcul différentiel, les probabilités et la théorie des nombres. Dans ce domaine, son nom est notamment attaché à deux résultats classiques (voir par exemple [IR1990]).

Pierre de Fermat (1607 ?–1665)

Petit théorème de Fermat. Soit p un nombre premier et a un entier premier avec p. Alors [3] $a^{p-1} \equiv 1 \pmod{p}$.

Théorème des deux carrés. Un entier positif n s'écrit comme la somme de deux carrés parfaits si et seulement si sa décomposition en facteurs premiers $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ne fait intervenir que des exposants e_i pairs pour les nombres premiers p_i congrus à -1 modulo 4.

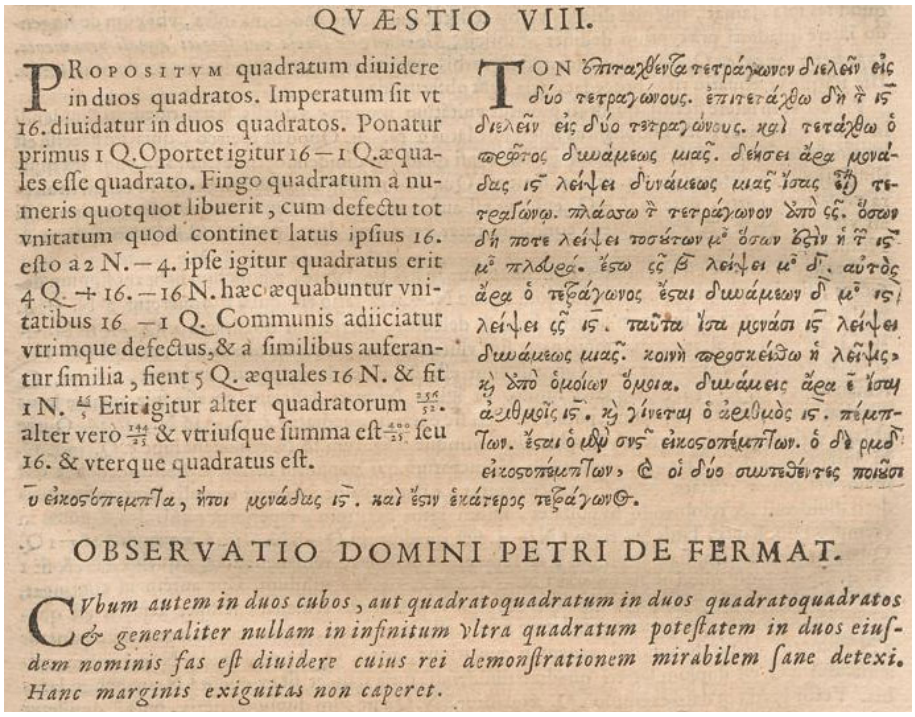
1. Il est également possible de le trouver en meilleure qualité et en V.O. en recherchant *Fermat's Last Theorem* dans un moteur de recherche.

2. « [...] mathématicien amateur devant qui les plus grands professionnels s'inclinaient. » selon [Hel09].

3. On rappelle que l'écriture $a \equiv b \pmod{c}$ signifie que a et b sont *congrus* modulo c, c'est-à-dire que c divise la différence $b - a$.

En particulier, le nombre premier 2017 est une somme de deux carrés[4], parce qu'il n'a qu'un seul facteur premier (lui-même !) et que celui-ci n'est pas congru à -1 modulo 4 (donc il satisfait tautologiquement la condition) alors que $2016 = 2^5 \times 3^2 \times 7$ n'en est pas une, à cause du premier 7 qui intervient dans sa décomposition avec une puissance impaire.

Cependant, le nom de Fermat reste surtout attaché à son *grand théorème* ou *dernier théorème* (surtout dans la littérature anglophone) affirmant que l'équation $x^n + y^n = z^n$ n'a pas de solution non triviale. L'énoncé de ce résultat se trouve dans les notes que Fermat inscrivait en marge de son exemplaire de l'*Arithmétique* de Diophante et qui furent publiées par son fils.



QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum ſit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales eſſe quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipſius 16. eſto a 2 N. − 4. ipſe igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à ſimilibus auferantur ſimilia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriuſque ſumma eſt $\frac{400}{25}$. ſeu 16. & vterque quadratus eſt.

ΤΟΝ ὁπταχθέντα τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτετάχθω δὴ τὸ ιϛ διελεῖν εἰς δύο τετραγώνους. καὶ τετάχθω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ιϛ λεῖψει δυνάμεως μιᾶς ἴσας ϛ̄ τετραγώνῳ. πλάσω τὸ τετράγωνον ἀπὸ ϛ̄. ὅσων δὴ ποτε λείψει τοσούτων μ̄ ὅσαν ὀξεῖαν ἡ τὸ ιϛ μ̄ πλευρά. ἔστω ϛ̄ β̄ λεῖψει μ̄ δ̄. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ̄ μ̄ ιϛ λεῖψει ϛ̄ ιϛ. ταῦτα ἴσα μονάσι ιϛ λεῖψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε̄ ἴσαι ἀριθμοῖς ιϛ. καὶ γίνεται ὁ ἀριθμὸς ιϛ̄. πέμπτων. ἔσται ὁ μβ̄ σνς̄ εἰκοσοπέμπτων. ὁ δὲ ρμδ̄ εἰκοσοπέμπτων. καὶ οἱ δύο συντεθέντες ποιοῦσι τὸν εἰκοσόπεμπτα, ἥτοι μονάδας ιϛ̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

L'édition de l'*Arithmétique* de Diophante avec les commentaires de Fermat.
Hang marginis exiguitas non caperet.

Notons que la manière employée par Fermat pour communiquer ses résultats consistait surtout en une correspondance avec ses amis et les grands mathématiciens de son époque (dont Pascal). Dans ces lettres, Fermat ne donnait en général que les énoncés des résultats dont il pensait avoir une preuve, ou pour lesquelles il connaissait une idée de preuve, même incomplète. À ce titre, il est probablement significatif de remarquer que Fermat ne fit jamais à ce résultat aujourd'hui célèbre la publicité qu'il accorda à d'autres, ce qui peut donner à penser qu'il réalisa assez tôt son erreur, et à relativiser la célébrité qu'acquit sa note marginale (publiée à titre posthume). Dans son ouvrage historique sur la théorie des nombres ([Wei83, page 104]), André Weil écrit d'ailleurs[5] :

> « Comment aurait-il pu deviner qu'il écrivait pour l'éternité ? Nous connaissons sa preuve pour les puissances quatrièmes ; il est possible qu'il ait construit une preuve pour les cubes semblables à celle découverte par Euler en 1753 ; il répéta fréquemment ces deux énoncés, mais pas le plus général. Brièvement peut-être, et peut-être dans sa jeunesse, il a dû se leurrer en croyant tenir le principe d'une preuve plus générale ; nous ne saurons jamais ce qu'il avait à l'esprit ce jour-là. »

4. Et, de fait, $2017 = 9^2 + 44^2$.
5. Traduction de M. B.

Comme le fait remarquer Weil, la preuve de l'absence de solution non triviale pour l'équation $x^4 + y^4 = z^4$ est une des seules preuves de Fermat qui nous soient parvenues. [6] Elle demande d'abord de revenir au cas $n = 2$, c'est-à-dire à la compréhension des triplets pythagoriciens.

On peut trouver facilement des démonstrations complètement arithmétiques de la classification des triplets pythagoriciens (cf. par exemple [Hin08, page 83]). Il n'est pourtant pas inintéressant d'en donner une présentation géométrique.

Définition. Un *triplet pythagoricien* est un triplet d'entiers tel que $x^2 + y^2 = z^2$. Il est dit *primitif* si $z > 0$ et que x, y et z sont premiers entre eux dans leur ensemble, c'est-à-dire qu'aucun entier $d \geq 2$ ne les divise simultanément.

L'intérêt de la notion de triplet primitif provient de la remarque selon laquelle tout triplet pythagoricien, comme par exemple $(3, 4, 5)$, donne naturellement naissance à une infinité d'autres, ses multiples, comme par exemple $(-3, -4, -5)$ ou $(12, 16, 20)$.

Remarquons toutefois que se restreindre aux triplets primitifs ne détruit pas toutes les symétries possibles, puisque, si (x, y, z) est un triplet primitif, il en va de même de (y, x, z) ou $(\pm x, \pm y, z)$. Nous avons simplement choisi une définition adaptée à notre démarche.

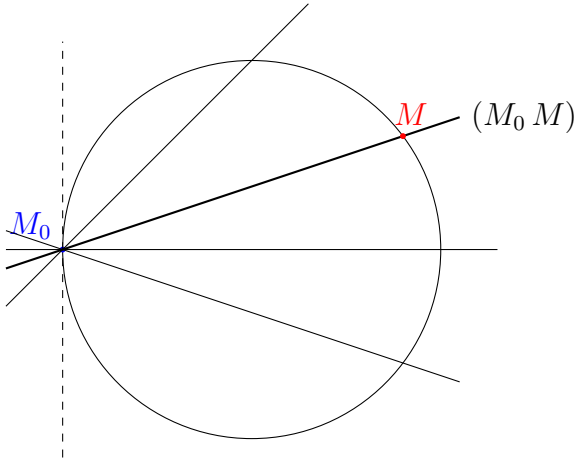
En divisant par z, on voit qu'un triplet pythagoricien (x, y, z) donne naissance à une solution $\left((X = \frac{x}{z}, Y = \frac{y}{z}\right)$ rationnelle de l'équation $X^2 + Y^2 = 1$, c'est-à-dire à un point (X, Y) à coordonnées rationnelles sur le cercle unité. Réciproquement, en réduisant au même dénominateur les coordonnées d'un tel point, on retrouve un triplet pythagoricien, que l'on peut même supposer primitif. L'identification des triplets pythagoriciens est donc équivalente à la question plus géométrique de la recherche des points à coordonnées rationnelles sur le cercle unité.

Le problème évident pour attaquer cette question est que, si l'on paramètre le cercle de la façon habituelle, par l'application $t \mapsto (\cos t, \sin t)$, il est très difficile de savoir si un t donné correspond à un point à coordonnées rationnelles. Nous allons donc utiliser une autre paramétrisation.

Pour cela, considérons un point rationnel de référence sur le cercle, par exemple $M_0 = \binom{-1}{0}$. On voit alors que tout point $M \neq M_0$ sur le cercle définit une droite $(M\,M_0)$ et que réciproquement, toute droite non verticale [7] passant par M_0 intersecte le cercle en un unique autre point $M \neq M_0$.

6. Pour bien d'autres résultats célèbres, il fallut attendre que d'autres mathématiciens démontrent les résultats annoncés par Fermat. C'est par exemple Euler qui publia les premières preuves du petit théorème de Fermat et du théorème des deux carrés. Toujours selon [Wei83], l'intérêt d'Euler pour la théorie des nombres fut d'ailleurs initié par une lettre de Goldbach citant le résultat selon lequel Fermat prétendait que les nombres $F_n = 2^{2^n} + 1$ étaient tous premiers, ce qui se vérifie pour $F_1 = 3$, $F_2 = 5$, $F_3 = 17$, $F_4 = 257$ et $F_5 = 65\,537$. Non seulement Euler montra que ce résultat tombait en défaut pour l'exemple suivant, en montrant que 641 divisait F_6, mais on ne connaît à l'heure actuelle aucun nombre de Fermat F_n premier pour $n > 5$!

7. À la limite, on peut remarquer que la droite verticale est tangente au cercle en M_0 et considérer que son point d'intersection avec le cercle « compte double », comme on considère que l'unique racine d'une équation du second degré de discriminant nul est une racine double. Dans ce cas, non seulement les points du cercle $\neq M_0$ correspondent aux droites non verticales, mais la correspondance est même parfaite puisqu'il semble raisonnable d'associer la droite verticale à M_0. Cela semble d'autant moins ridicule que plus une droite issue de M_0 s'approche de la verticale, plus son deuxième point d'intersection avec le cercle unité se rapproche de M_0.



On a en quelque sorte paramétré le cercle par les droites issues de M_0. Qu'a-t-on gagné ?

Les droites non verticales issues de M_0 ont une certaine pente [8] $p \in \mathbb{R}$ et il est clair que la pente de la droite reliant M_0 à $M = \binom{x}{y}$

$$p_M = \frac{y}{x+1}$$

est rationnelle dès que x et y le sont.

Mieux : la réciproque est vraie, c'est-à-dire que si la pente p_M de la droite $(M_0\,M)$ est rationnelle, les coordonnées de M le sont.

En effet, si $M = \binom{x}{y} \neq \binom{-1}{0}$ appartient à la fois à la droite passant par M_0 et de pente p et au cercle unité, on a

$$\left\{ \begin{array}{rcl} y & = & p(x+1) \\ x^2+y^2 & = & 1 \end{array} \right. \iff \left\{ \begin{array}{rcl} y & = & p(x+1) \\ (p^2+1)x^2+2p^2\,x+p^2-1 & = & 0. \end{array} \right.$$

Vu la signification géométrique des équations, on sait que $x = -1$ est une solution, ce qui permet de factoriser l'équation sous la forme

$$(x+1)\left((p^2+1)x+(p^2-1)\right) = 0$$

et donc de trouver les coordonnées de M :

$$M = \begin{pmatrix} \dfrac{1-p^2}{1+p^2} \\ \dfrac{2p}{1+p^2}. \end{pmatrix}$$

En particulier, ces coordonnées sont bien rationnelles si p l'est. Résumons ce que l'on vient de montrer sous la forme d'un théorème.

Théorème. Tout point du cercle unité différent [9] de $(-1,0)$ s'écrit de façon unique sous la forme $\left(\dfrac{1-p^2}{1+p^2}, \dfrac{2p}{1+p^2}\right)$, avec $p \in \mathbb{R}$. Ce point est à coordonnées rationnelles si et seulement si p l'est.

8. Encore une fois, on pourrait considérer que la droite verticale a une pente infinie et donc dire que les droites correspondent à tous les « nombres » $p \in \mathbb{R} \cup \{\infty\}$.

9. Encore et toujours, vu le comportement des fractions rationnelles $\frac{1-p^2}{1+p^2}$ et $\frac{2p}{1+p^2}$ quand $p \to \pm\infty$, il est tout à fait raisonnable de considérer que $p = \infty$ correspond au point $M_0 = \binom{-1}{0}$.

Remarques.

— Par exemple, la symétrie $(x, y) \mapsto (x, -y)$ correspond à la transformation $p \mapsto -p$. Quelle transformation correspond à la symétrie $(x, y) \mapsto (y, x)$?

— Les formules donnant les coordonnées en fonction de la pente p sont familières. En effet, il n'est pas très difficile de voir que si (x, y) est le point $(\cos\theta, \sin\theta)$, la pente p n'est rien d'autre que $p = \tan\left(\frac{\theta}{2}\right)$. On a ainsi retrouvé (et expliqué géométriquement) les changements de variables des fonctions sinus et cosinus en fonction de la tangente de l'arc moitié.

On peut maintenant revenir à notre tâche principale : déterminer les triplets pythagoriciens primitifs. On sait que ceux-ci correspondent aux points rationnels sur le cercle, et on vient de déterminer ceux-ci. Si $p = a/b$ est une expression irréductible de la fraction p, on obtient le point rationnel

$$\left(\frac{1-p^2}{1+p^2}, \frac{2p}{1+p^2}\right) = \left(\frac{1-(a/b)^2}{1+(a/b)^2}, \frac{2(a/b)}{1+(a/b)^2}\right) = \left(\frac{b^2-a^2}{a^2+b^2}, \frac{2ab}{a^2+b^2}\right),$$

et on obtient donc un triplet pythagoricien $(b^2 - a^2, 2ab, a^2 + b^2)$ pour tous nombres a et b premiers entre eux (le cas exceptionnel $p = \infty$ correspond à $a = 1$ et $b = 0$, c'est-à-dire au triplet $(-1, 0, 1)$).

Reste à savoir si ce triplet est primitif. Soit donc ℓ un nombre premier divisant les trois coordonnées. En particulier, ℓ divise $2ab$. Comme a et b sont premiers entre eux, cela implique $\ell = 2$ ou ℓ divise a ou ℓ divise b. Si ℓ divise a, il ne peut pas diviser b, ce qui entraîne qu'il ne divise pas $a^2 + b^2$. Le cas $\ell | b$ se traite de la même façon. Ainsi, la seule obstruction éventuelle pour que le triplet pythagoricien $(b^2 - a^2, 2ab, a^2 + b^2)$ soit primitif est que ses trois coordonnées soient paires. Comme la parité d'un nombre ne change pas quand on le transforme en son opposé ou qu'on l'élève au carré, on obtient que cette éventualité ne se produit que si a et b sont de même parité. Comme ils sont premiers entre eux, cela revient à dire qu'ils sont tous les deux impairs.

En résumé, l'unique triplet pythagoricien primitif correspondant à $p = a/b$ est

— $(b^2 - a^2, 2ab, a^2 + b^2)$ si a et b sont de parité différente ;

— $\left(\frac{b^2-a^2}{2}, ab, \frac{a^2+b^2}{2}\right)$ si a et b sont tous deux impairs.

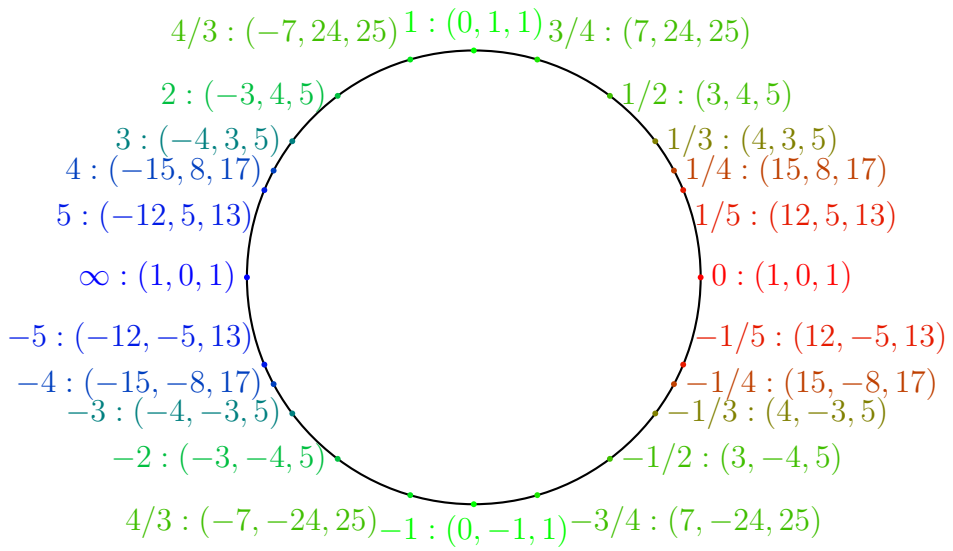
On remarque que dans ce deuxième cas, $b^2 - a^2 = (b-a)(b+a)$ est en fait multiple de 4, ce qui implique que la première coordonnée du triplet est paire. Cela éclaire notre distinction : les premiers triplets ont leur première coordonnée impaire et la deuxième paire, alors que c'est le contraire pour les seconds. On peut donc énoncer notre classification des triplets pythagoriciens primitifs sous la forme suivante, particulièrement agréable.

Théorème.

— Un triplet pythagoricien primitif (x, y, z) vérifie nécessairement que x et y sont de parités différentes.

— Si a et b sont deux nombres premiers entre eux de parités différentes, $(b^2 - a^2, 2ab, a^2 + b^2)$ est un triplet pythagoricien primitif, et tous les triplets pythagoriciens primitifs (x, y, z) avec y pair sont obtenus de cette façon.

Pour clore cette discussion, donnons quelques exemples de points rationnels du cercle, avec les pentes p et les triplets primitifs correspondants.



On peut maintenant passer au cas $n = 4$ du grand théorème de Fermat.

Théorème (Fermat). L'équation $x^4 + y^4 = z^2$ n'a pas de solution entière non triviale (c'est-à-dire une solution avec $x, y, z \neq 0$.

Preuve. Supposons le résultat faux. On peut alors choisir une solution (x, y, z) non triviale avec z^2 minimal. Quitte à changer leur signe, on suppose également $x, y, z > 0$.

D'après la classification des triplets pythagoriciens, quitte à échanger x et y, on peut trouver $0 < a < b$ premiers entre eux et de parités différentes tels que

$$x^2 = b^2 - a^2, \qquad y^2 = 2ab \qquad \text{et} \qquad z = a^2 + b^2.$$

La première de ces deux équations affirme que (x, a, b) est un triplet pythagoricien. Comme a et b sont de parités différentes, on sait que x est impair. Cela implique que a est pair et que l'on peut trouver $0 < u < v$ premiers entre eux et de parités différentes tels que $x = u^2 - v^2$, $a = 2uv$ et $b = u^2 + v^2$.

En particulier, on a alors $y^2 = 2ab = 4uv(u^2 + v^2)$. En observant la décomposition en facteurs premiers des nombres u, v et en utilisant le fait que u et v sont premiers entre eux, on montre que u, v et $u^2 + v^2$ sont des carrés parfaits. Cela entraîne que l'on peut trouver des entiers positifs X, Y tels que $u = X^2$, $v = Y^2$ et $u^2 + v^2 = Z^2$. Dans ces conditions, on a $X^4 + Y^4 = Z^2$.

Par ailleurs,

$$Z^2 = u^2 + v^2 = b < a^2 + b^2 = z < z^2,$$

donc la solution que l'on vient de trouver vérifie donc $Z^2 < z^2$. Elle ne peut pourtant pas être triviale : si $X = 0$ ou $Y = 0$, on voit que cela entraîne la nullité de u ou v, et donc $a = 0$, puis $y = 0$. On obtient donc une contradiction avec le fait que notre solution était minimale parmi les solutions non triviales.

On vient donc de démontrer par l'absurde que l'équation $x^4 + y^4 = z^2$ n'a pas de solution entière non triviale.

— On a ici rédigé la preuve par l'absurde, en partant d'un contre-exemple minimal. On parle traditionnellement de preuve par *descente infinie*, ce qui est une autre façon de regarder la même preuve : une solution non triviale donne naissance à une autre solution

plus petite, qui engendre à son tour une solution encore plus petite et ainsi de suite à l'infini. La contradiction vient alors du fait que l'on obtient une suite d'entiers strictement positifs (ici, les z^2), ce qui est absurde.

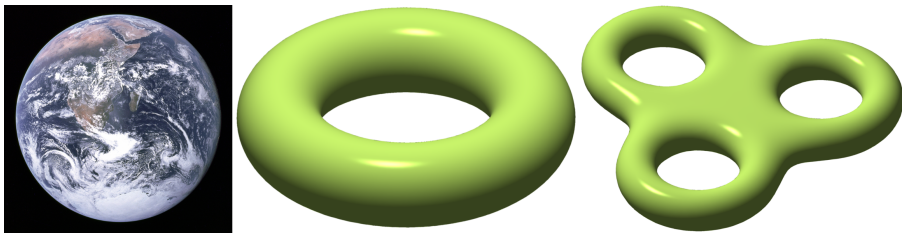
— On a dit que cette preuve était explicitement due à Fermat, contrairement à beaucoup de résultats qu'il a énoncés, mais dont il ne publia jamais les démonstrations. C'est en fait une approximation : le résultat démontré par Fermat est qu'un triangle rectangle dont les côtés sont entiers ne peut jamais avoir une aire valant un carré parfait. Autrement dit, il n'existe pas de triplet pythagoricien (x, y, z) tel que $xy/2$ soit un carré. La preuve que nous venons de donner, dans le même esprit que celle de ce dernier résultat quoiqu'un peu plus facile, était très probablement connue de Fermat (cf. [Wei83, page 79] et [Edw77, section 1.6]).

— Évidemment, le théorème que l'on vient de démontrer implique le cas $n = 4$ du grand théorème de Fermat. En effet, une solution non triviale de l'équation $x^4 + y^4 = z^4$ fournirait un contre-exemple $x^4 + y^4 = (z^2)^2$ au théorème ci-dessus. Ce genre de remarques montre d'ailleurs que le grand théorème de Fermat pour un certain exposant n entraîne le résultat pour les exposants multiples de n. Puisque le cas $n = 4$ est démontré, il « suffit » donc de le démontrer pour les nombres premiers impairs pour en obtenir le cas général : tout nombre $n \geq 3$ est divisible par un nombre premier impair ou par 4 !

Revenons un moment à l'étude des triplets pythagoriciens. Comme on l'a vu, déterminer les solutions entières de l'équation $x^2 + y^2 = z^2$ est intimement lié à l'étude des points rationnels (i.e. à coordonnées rationnelles) sur la courbe $x^2+y^2 = 1$ (qui est un cercle). Cela se généralise à un exposant quelconque : une forme équivalente du grand théorème de Fermat est l'affirmation selon laquelle la *courbe de Fermat* d'équation $x^n+y^n = 1$ ne possède que deux points rationnels quand $n \geq 3$: $(0, 1)$ et $(1, 0)$.

Un grand nombre de progrès en théorie des nombres au cours du vingtième siècle ont eu pour objet de rapprocher des problèmes arithmétiques (comme celui de déterminer les points rationnels de la courbe de Fermat) aux propriétés géométriques d'objets continus, comme ici l'ensemble des solutions **complexes** de l'équation $x^n + y^n = 1$. Notamment, un invariant extrêmement important d'une équation comme celle définissant la courbe de Fermat est son *genre* : si on cherche les solutions complexes de l'équation, on obtient une partie de $\mathbb{C}^2$ que l'on peut voir comme une surface.

Les surfaces fermées orientables sont classées, à équivalence près, par un entier $g \geq 3$, leur genre. La surface de genre 0 est la sphère, la surface de genre 1 est le tore, et les surfaces de genre $g \geq 2$ sont les « bouées à g anses » que l'on peut obtenir en recollant g tores.



Trois surfaces de genre 0, 1 et 3.

On peut alors montrer que les solutions complexes de l'équation $x^n + y^n = 1$ forment une surface de genre g à laquelle on aurait enlevé quelques points. Les propriétés arithmétiques de l'équation de Fermat dépendent alors de ce genre. Plus précisément, on distingue trois cas [10] :

10. C'est une constante des problèmes liés aux surfaces : les cas $g = 0$, $g = 1$ et $g \geq 2$ sont en général très différents. De même que les trois parts du gâteau découpé par Obélix dans *Astérix et Cléopâtre*, ces trois cas sont d'importance et de difficulté inégales, comme l'illustre entre autres le cas de la courbe de Fermat.

— Si $n = 2$, la courbe de Fermat est de genre 0 (ses solutions réelles forment un cercle, mais on peut voir que ces solutions complexes dessinent une figure équivalente à un cylindre, ou encore à une sphère à laquelle on aurait enlevé deux points). Dans ce cas, la courbe a une infinité de points rationnels, comme on l'a vu.
— Si $n = 3$, la courbe de Fermat est de genre 1. On dit alors que c'est une *courbe elliptique*. La théorie des courbes elliptiques est extrêmement développée : on sait par exemple que les points rationnels de la courbe forment un groupe abélien de type fini, sur lequel on possède beaucoup d'informations (assez par exemple pour démontrer le grand théorème de Fermat dans ce cas), mais sur lequel des questions importantes restent encore ouvertes. On pourra par exemple consulter l'article [Col05] de Pierre Colmez pour voir les liens entre un très vieux problème de théorie des nombres et des questions contemporaines sur les courbes elliptiques.
— Si $n \geq 4$, la courbe de Fermat est de genre ≥ 3. Un important et difficile théorème (connu auparavant sous le nom de *conjecture de Mordell* et démontré par Gerd Faltings en 1983-1984) affirme alors que la courbe ne peut posséder qu'un nombre fini de points rationnels.

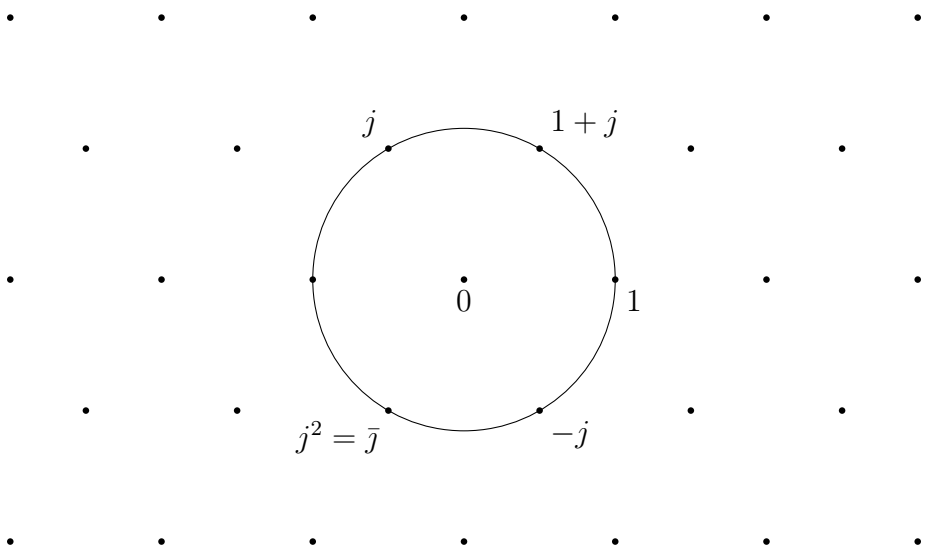
B. Gauss et Kummer

Comme le faisait remarquer Weil dans la citation ci-dessus, le cas $n = 3$ du grand théorème de Fermat fut démontré par Euler en 1753. D'autres preuves ont été données au fil du temps, notamment par Gauss dans une preuve publiée à titre posthume. Un des intérêts de cette preuve est qu'elle se déroule dans un ensemble de nombres qui ne sont pas tous rationnels, celui des *entiers d'Eisenstein.* Nous allons présenter dans cette section une partie de cette preuve. Le lecteur curieux pourra consulter la preuve complète aux pages 84 et 85 de l'excellent livre [Hin08] ou dans [Rib99, section I.5]

Un intérêt de cette preuve (ou même du petit cas particulier que nous présentons) est qu'elle illustre comment les propriétés algébriques de certains ensembles de nombres complexes peuvent éclairer les propriétés de telle ou telle équation diophantienne, une philosophie magnifiquement illustrée par les résultats de Kummer de 1850, qui démontra le grand théorème de Fermat pour une grande variété d'exposants premiers.

Carl Friedrich Gauss (1777–1855)

Les *entiers d'Eisenstein* sont les nombres de la forme $a + bj$ avec $a, b \in \mathbb{Z}$, où $j = e^{2i\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. On note $\mathbb{Z}[j]$ leur ensemble. Dessiné dans le plan complexe, il s'agit d'un réseau triangulaire.



La *norme* d'un entier d'Eisenstein est le carré de son module :

$$N(a + bj) = (a + bj)\overline{(a + bj)} = a^2 - ab + b^2.$$

Comme on le voit sur le dessin, le réseau formé par les entiers d'Eisenstein a pour maille des triangles équilatéraux de côté 1. En particulier, cela démontre que tout point du plan est à distance $\leq \frac{\sqrt{3}}{3}$ d'un entier d'Eisenstein. Si $a, b \in \mathbb{Z}[j]$ et que b est non nul, on peut en particulier trouver un point $q \in \mathbb{Z}[j]$ tel que $N\left(\frac{a}{b} - q\right) \leq \frac{\sqrt{3}}{3} < 1$. Autrement dit, il existe des entiers d'Eisenstein q et $r = a - bq$ tels que

$$a = bq + r \qquad \text{et} \qquad N(r) = N(b)\, N\left(\frac{a}{b} - q\right) < N(b).$$

Cette propriété, analogue à la division euclidienne dans $\mathbb{Z}$ permet de démontrer pour les entiers d'Eisenstein toutes les propriétés bien connues des entiers usuels, c'est-à-dire tout le cours de spécialité du cours de Terminale S : on peut définir la divisibilité comme dans $\mathbb{Z}$ et obtenir le théorème de Bézout, le lemme de Gauss, l'existence et l'unicité de la décomposition en nombres premiers en calquant les preuves usuelles.

Deux remarques sont importantes.

— Quand on travaille avec la relation de divisibilité dans $\mathbb{Z}$, il est courant de se restreindre aux entiers positifs pour éviter des circonlocutions liées au fait que les entiers n et $-n$ se divisent mutuellement. En fait, pour toutes les questions de divisibilité, le signe ne change rien et l'on travaille essentiellement « au signe près ». Cela provient fondamentalement du fait que 1 et -1 sont les seuls entiers dont l'inverse est aussi un entier (on dit que ce sont les *inversibles* ou les *unités* de $\mathbb{Z}$). Dans un ensemble de nombres plus général, comme celui des entiers d'Eisenstein, cette propriété peut être partagée par d'autres nombres. On voit facilement que les entiers d'Eisenstein inversibles sont ceux qui sont de module 1, c'est-à-dire ± 1, $\pm j$ et $\pm j^2$. Ainsi, dans toutes les questions de divisibilité, il est commode de traiter comme équivalents des nombres d'Eisenstein *associés*, c'est-à-dire deux nombres dont l'un est le produit de l'autre par un inversible.

— On a dit que l'existence d'une division euclidienne permettait de retrouver dans $\mathbb{Z}[j]$ toutes les propriétés habituelles de l'arithmétique. Il faut prendre cependant garde au fait qu'un nombre premier peut se décomposer dans $\mathbb{Z}[j]$ de manière non triviale. Utilisons deux mots différents pour souligner cette différence : on continuer à réserver l'appellation de *nombre premier* aux usuels 2, 3, 5, 7, 11… et on appellera *élément irréductible* de $\mathbb{Z}[j]$ tout élément x qui ne se décompose que trivialement, c'est-à-dire tout élément x tel que $x = yz$, avec $y, z \in \mathbb{Z}[j]$, entraîne que y ou z est inversible.
Notre remarque consiste à dire qu'un nombre premier n'a alors pas de raison d'être irréductible. Par exemple, on a la décomposition

$$3 = (1-j)(1-j^2) = (1+j)(1-j)^2.$$

Puisque $1+j$ est un irréductible de $\mathbb{Z}[j]$, on a démontré que 3 est associé au carré de l'élément $\lambda = 1-j$ qui va jouer un rôle important dans la suite de la discussion. On vient de dire que les éléments inversibles ne changeaient pas grand chose aux propriétés de divisibilité donc on peut retenir que le premier 3 est essentiellement devenu un carré dans $\mathbb{Z}[j]$ (on dit que 3 est *ramifié*). On peut en revanche montrer que λ est un élément irréductible de $\mathbb{Z}[j]$. En effet, si $\lambda = ab$, on a $3 = N(\lambda) = N(a)\,N(b)$. Comme $N(a)$ et $N(b)$ sont des entiers naturels et que 3 est premier, l'un des deux doit être égal à 1, ce qui entraîne que l'élément correspondant est inversible.

Nous allons pouvoir retourner à notre but principal, c'est-à-dire expliquer comment l'arithmétique dans $\mathbb{Z}[j]$ permet de démontrer le grand théorème de Fermat pour l'exposant 3, ou plutôt un cas particulier de celui-ci, connu sous le nom peu parlant de « premier cas ». (Même pour ce premier cas, il fallut attendre la preuve de Wiles pour une démonstration valable pour tout p).

Théorème (« Premier cas » du grand théorème de Fermat). Soit $p \geq 3$ un nombre premier. L'équation $x^p + y^p = z^p$ n'a pas de solution entière avec x, y et z non divisibles par p.

On verra qu'en fait notre preuve démontre en fait une version forte de ce premier cas pour l'exposant 3, à savoir l'absence de solutions dans $\mathbb{Z}[j]$.

Théorème (Gauss, premier cas). L'équation $x^3 + y^3 = z^3$ n'a pas de solution dans $\mathbb{Z}[j]$ avec x, y et z non divisibles par $\lambda = 1-j$.

Remarque. On a déjà dit que λ divise 3 dans $\mathbb{Z}[j]$ (et même que 3 est associé à λ^2). Ce dernier théorème entraîne donc bien le premier cas du grand théorème de Fermat pour l'exposant 3.

Preuve. Comme on l'a dit, il va essentiellement être question d'arithmétique dans $\mathbb{Z}[j]$, et plus précisément de congruences modulo λ (et ses puissances).

Lemme 1. Tout élément de $\mathbb{Z}[j]$ est congru à -1, 0 ou 1 modulo λ.

Preuve du lemme 1. On a déjà dit que 3 était un multiple de λ. Comme tout entier est congru à -1, 0 ou 1 modulo 3, il suffit de démontrer que tout élément de $\mathbb{Z}[j]$ est congru à un entier modulo λ. Or, puisque $\lambda = 1-j$, on a directement $j \equiv 1 \pmod{\lambda}$, donc tout élément $a+bj \in \mathbb{Z}[j]$ est congru à $a+b$ modulo λ.

Lemme 2. Soit $x \in \mathbb{Z}[j]$ un élément non divisible par λ. Alors $x^3 \equiv \pm 1 \pmod{\lambda^4}$.

Preuve du lemme 2. D'après le lemme précédent, si x n'est pas divisible par λ, il est congru à ± 1 modulo λ. Supposons dans un premier temps que $x \equiv 1 \pmod{\lambda}$, c'est-à-dire que l'on

peut trouver un élément $q \in \mathbb{Z}[j]$ tel que $x = 1 + \lambda q$. En utilisant la factorisation $X^3 - 1 = (X-1)(X-j)(X-j^2)$, on obtient donc

$$\begin{aligned} x^3 - 1 &= ((1+\lambda q) - 1)\,((1+\lambda q) - j)\,((1+\lambda q) - j^2) \\ &= \lambda q\,\lambda(q+1)\,\lambda(q+1+j) && \text{car } 1 - j^2 = \lambda(1+j) \\ &= \lambda^3 q\,(q+1)\,(q+1+j). \end{aligned}$$

Comme $1 + j \equiv -1 \pmod{\lambda}$, les trois nombres $q, q+1, q+1+j \in \mathbb{Z}[j]$ ne sont pas congrus deux à deux modulo λ. Comme on a vu qu'il n'y avait que trois possibilités modulo λ, l'un des trois est donc congru à 0 modulo λ, c'est-à-dire divisible par λ. Cela démontre bien que $x^3 - 1$ est divisible par λ^4 et donc $x^3 \equiv 1 \pmod{\lambda^4}$.

Si $x \equiv -1 \pmod{\lambda}$, il suffit d'appliquer ce que l'on vient de dire à $-x$ pour obtenir $x^3 \equiv -1 \pmod{\lambda^4}$ et conclure la preuve du lemme 2.

On peut maintenant conclure la preuve du théorème de Gauss. Si x, y et z n'étaient pas divisibles par λ et vérifiaient $x^3 + y^3 = z^3$, le lemme 2 entraînerait que

$$0 = x^3 + y^3 - z^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4}.$$

Or, cette dernière somme vaut ± 1 ou ± 3. Dans tous les cas, on obtiendrait que λ^4 divise l'entier 3. Mais on a vu que 3 est associé à λ^2, et n'est donc pas divisible par λ^4, et cette contradiction conclut la preuve.

La preuve que nous venons de donner a utilisé l'arithmétique de $\mathbb{Z}[j]$, et notamment les propriétés de $\lambda = 1 - j$ en tirant parti du fait que la théorie générale de la divisibilité dans cet ensemble fonctionnait essentiellement de la même façon que dans $\mathbb{Z}$: division euclidienne, existence et unicité de la décomposition en facteurs premiers...

Pour les exposants $p \geq 5$ du grand théorème de Fermat, la stratégie naturelle analogue consisterait à travailler dans l'ensemble des *entiers cyclotomiques*

$$\mathbb{Z}[\zeta_p] = \left\{ a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \;\middle|\; (a_0, \ldots, a_{p-2}) \in \mathbb{Z}^{p-1} \right\} \subset \mathbb{C},$$

où $\zeta_p = \exp\left(\frac{2i\pi}{p}\right)$. Le problème est que cet ensemble de nombres ne possède en général pas les mêmes propriétés arithmétiques. Le travail de Kummer au milieu du dix-neuvième siècle a permis de grandes avancées sur les liens entre l'arithmétique de $\mathbb{Z}[\zeta_p]$ et le grand théorème de Fermat.

À un nombre premier p, Kummer associe un entier $h_p \geq 1$, son *nombre de classes* qui « mesure » d'une certaine façon [11] l'écart entre les propriétés arithmétiques de $\mathbb{Z}[\zeta_p]$ et $\mathbb{Z}$. En particulier, $h_p = 1$ si et seulement si on dispose dans $\mathbb{Z}[\zeta_p]$ d'un théorème d'existence et d'unicité de la décomposition en nombres premiers. Le travail de Kummer montre en particulier que pour ces nombres premiers (qui sont en fait les nombres premiers $p \leq 19$), le grand théorème de Fermat est vrai.

Mais il y a mieux : Kummer a démontré [12] que le grand théorème de Fermat était valable pour tous les nombres premiers *réguliers*, c'est-à-dire ceux pour lesquels h_p n'était pas un multiple de p. Même si on ignore encore aujourd'hui s'il existe une infinité de nombres premiers réguliers,

11. voir par exemple [Hin08, III. 4] ou [IR1990, chapitre 12] pour une définition précise.

12. Le lecteur très savant pourra jeter un œil à la preuve reconstituée par K. Conrad sur sa page web. Comme pour le cas $p = 3$, le « deuxième cas » du théorème, c'est-à-dire celui où l'une des coordonnées peut être divisible par p, est significativement plus pénible que le premier cas.

on conjecture que c'est le cas (et même que la proportion de nombres premiers réguliers parmi les n premiers nombres premiers s'approche de $1/\sqrt{e} \approx 61\%$).

Les travaux de Kummer constituent une avancée majeure dans la *théorie algébrique des nombres*, c'est-à-dire l'étude de l'arithmétique des ensembles de nombres du même type que $\mathbb{Z}[j]$ ou $\mathbb{Z}[\zeta_p]$, dont la portée dépasse largement le cadre du grand théorème de Fermat.

C. Shimura, Taniyama et Wiles

La preuve de Wiles s'inscrit dans un programme de recherche toujours actif visant à connecter des objets « géométriques », typiquement des équations définissant des courbes, et des objets de nature plus analytiques, comme des fonctions spéciales.

Il est impossible de rendre compte honnêtement [13] des travaux de Wiles ou même de leur contexte dans une telle note. Il est cependant intéressant de remarquer que la preuve du théorème de Fermat est extrêmement indirecte.

Nous avons vu à la fin de la première section que les propriétés arithmétiques d'une courbe dépendaient de son degré, le cas intermédiaire étant celui des *courbes elliptiques*, c'est-à-dire des équations à coefficients rationnels que l'on peut mettre, par un changement de variables [14] sous la forme

$$y^2 = P(x),$$

où P est un polynôme de degré 3 dont les racines sont distinctes.

Des exemples de telles courbes sont les *courbes de Mordell* $y^2 = x^3 + n$, où n est un entier non nul. La courbe de Fermat pour l'exposant 3, d'équation $x^3 + y^3 = 1$ est d'ailleurs une courbe de ce type déguisée car le changement de variables $x = \frac{36-\eta}{6\xi}$, $y = \frac{36+\eta}{6\xi}$ met son équation sous la forme $\xi^3 = \eta^2 + 432$.

Comme on l'a fait remarquer, seule la courbe de Fermat d'exposant 3 est une courbe elliptique. Il semble donc *a priori* impensable que la théorie des courbes elliptiques puisse apporter des renseignements sur les autres cas du grand théorème de Fermat.

Pourtant, progressivement à partir des années 1970, des chercheurs (Hellegouarch, Frey, Serre, Ribet...) se sont rendu compte que s'il existait une solution non triviale $a^\ell + b^\ell = c^\ell$ à l'équation de Fermat pour un exposant premier $\ell \geq 5$, la courbe elliptique d'équation $y^2 = x(x - a^\ell)(x + b^\ell)$ (parfois appelée *courbe de Hellegouarch-Frey*) possèderait des propriétés qui semblaient aller à l'encontre de grands principes conjecturaux gouvernant le monde des courbes elliptiques. [15]

Notamment, en 1990, Kenneth Ribet démontra que, si elles existaient, les courbes de Hellegouarch-Frey infirmeraient une conjecture importante, dite de *Shimura-Taniyama*. [16]

13. Et, à vrai dire, l'auteur de cette note en serait incapable. Nous pouvons cependant conseiller au lecteur curieux et courageux, par complexité croissante, [Maz91, Hel09, Rib95].

14. On est ici volontairement un peu flou sur la forme autorisée pour les changements de variables.

15. Un de ces grands principes, sur lequel Wiles a travaillé au début de sa carrière, est la *conjecture de Birch et Swinnerton-Dyer*, toujours ouverte, qui décrit le comportement près du point 1 de la fonction L dont nous allons parler brièvement. C'est un des sept *problèmes du millénaire* de l'institut Clay, et à ce titre, sa résolution est mise à prix pour un million de dollars. On renvoie à [Col05] pour une présentation de cette conjecture et de son impact sur des problèmes classiques de théorie des nombres.

16. Cette conjecture a une histoire compliquée et porte des noms variés, en général à base de permutations et d'omissions parmi les noms des mathématiciens japonais Yutaka Taniyama et Goro Shimura et du mathématicien français André Weil. Parfois, elle est aussi appelée *conjecture de modularité*, comme dans la citation du comité Abel qui ouvre cette note.

Nous n'énoncerons pas la conjecture de Shimura-Taniyama précisément, mais pour donner une idée du genre de ponts que celle-ci crée entre géométrie et analyse, nous allons essayer de donner une image (impressioniste) d'un des objets qui peuvent servir à en donner une définition rigoureuse, la *fonction L*.

Pour cela, revenons à la courbe d'équation $x^2+y^2=1$ (qui n'est pas elliptique !). En plus de considérer ses points à coordonnée rationnelle, on peut chercher à considérer ses solutions dans d'autres corps, et notamment sur les corps finis $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, et en particulier à en déterminer le nombre N_p. En fait, même si l'intuition géométrique est plus difficile à capturer, la discussion de la première section reste encore valide et montre que les couples (x, y) d'éléments de $\mathbb{F}_p$ vérifiant cette équation sont paramétrés par les formules $x = \frac{1-t^2}{1+t^2}$ et $y = \frac{2t}{1+t^2}$. Ici comme dans $\mathbb{Q}$, t peut *a priori* parcourir toutes les valeurs possibles dans le corps et même $t = \infty$ (correspondant à $(x, y) = (-1, 0)$), à condition que le dénominateur ne s'annule pas (ce qui n'arrivait jamais dans $\mathbb{Q}$ pour des questions de signe). Si p est un nombre premier impair, on montre que $t^2 + 1 = 0$ a deux solutions dans $\mathbb{F}_p$ si $p \equiv 1 \pmod 4$ et aucune si $p \equiv 3 \pmod 4$. Ainsi, le nombre de solutions de notre équation dans $\mathbb{F}_p$ est $N_p = p - \chi(p)$, où l'on a noté χ la fonction qui associe à un nombre entier ± 1 s'il est congru à ± 1 modulo 4, et 0 dans les autres cas.

On peut alors utiliser ces nombres $\chi(p) = p - N_p$ (qui mesurent d'une certaine façon la fluctuation entre le nombre de points de la courbe et le nombre de points d'une droite) pour définir une fonction

$$L(s) = \prod_p \frac{1}{1 - \chi(p)\, p^{-s}},$$

où le produit porte sur les nombres premiers p (et où la variable s est un nombre complexe de partie réelle suffisamment grande).

Il est d'ailleurs possible de donner une autre expression de cette *fonction L*, cette fois-ci comme une somme infinie. [17]

$$L(s) = \sum_{n>0} \frac{\chi(n)}{n^s}.$$

Pour une courbe elliptique, on peut de la même façon définir une fonction L (la définition est légèrement différente, quoique tout à fait dans le même esprit, cf. [Col05, Hin08]), qui s'écrit à son tour comme une série

$$L(s) = \sum_{n>0} \frac{a_n}{n^s}.$$

La conjecture de modularité affirme que ces coefficients a_n sont les coefficients de Fourier d'une forme modulaire, c'est-à-dire que la fonction

$$\sum_{n>0} a_n e^{2i\pi nz}$$

est une fonction (d'une variable complexe z) pourvue de propriétés de périodicité remarquables. [18] Voir par exemple le cinquième chapitre de [Hel09].

À partir du moment où Ribet a démontré qu'elle impliquait le grand théorème de Fermat, Wiles s'est consacré à la démonstration de la conjecture de Shimura-Taniyama. Il y est finale-

17. Le passage de l'une à l'autre expression est une technique standard souvent connue sous le nom de produit eulérien, en hommage à la première de ces identités, démontrée par Euler : $\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n>0} \frac{1}{n^s}$. Voir par exemple [Hin08, théorèmes 3.4 et 4.11].

18. Dans le cas du cercle $x^2 + y^2 = 1$, qui n'est pas elliptique, on obtient ainsi (le double de) la fonction sécante $\sec(z) = \frac{1}{\cos z}$, qui est certes une fonction intéressante, mais pas une forme modulaire.

ment arrivé [19] en 1995, après une première annonce prématurée et avec l'aide de son étudiant Richard Taylor.

Pour résumer : Wiles démontre une conjecture liant deux objets classiques mais non élémentaires, les courbes elliptiques et les formes modulaires, pour démontrer un théorème à l'énoncé parfaitement élémentaire qui n'a *a priori* aucun rapport ni avec les courbes elliptiques, ni avec les formes modulaires. Pour encore compliquer la situation, il le fait en mettant en relation ces deux objets avec une troisième notion, beaucoup plus moderne et sophistiquée, celle de *représentation galoisienne...*

Parce qu'elle clôt l'histoire haute en couleur du grand théorème de Fermat, mais aussi parce qu'elle constitue un paradigme de la sophistication des méthodes employées en théorie des nombres à travers l'histoire, la preuve de Wiles est probablement l'une des preuves les plus marquantes des mathématiques du vingtième siècle (et elle fut sans aucun doute la preuve la plus médiatisée).

En guise de conclusion, citons Wiles lui-même, qui parle de son activité mathématique dans la scène d'introduction du documentaire de Singh que nous avons déjà cité (mais que nous recommandons à nouveau !), et la compare à la découverte d'un manoir dans le noir complet.

> *"One goes into the first room and it's dark, really dark. One stumbles around, bumping into the furniture. Gradually you learn where each piece of furniture is and finally after six months or so, you find a light switch, you turn it on and suddenly it's all illuminated, you can see exactly where you were."*[20]

Maxime Bourrigan
maxime.bourrigan@ens.fr
École Normale Supérieure
45, rue d'Ulm
75 230 Paris cedex 05

19. Techniquement, les travaux de Wiles et Taylor-Wiles ne démontrent la conjecture de Shimura-Taniyama que dans le cas particulier des courbes semistables, mais cela suffit à démontrer le théorème de Fermat. La conjecture générale fut démontrée en 2001 par Breuil, Conrad, Diamond et Taylor lui-même.

20. Traduction approximative : « *On entre dans la première salle et il fait noir, complètement noir. On tâtonne, on se cogne aux meubles. Progressivement, vous apprenez où est chaque meuble et après peut-être six mois, vous trouvez un interrupteur, vous appuyez dessus et soudainement tout est illuminé, vous voyez exactement où vous étiez.* ».

Références

[Col05] Pierre Colmez, *Le Problème des nombres congruents*, exposé donné à l'école polytechnique, 2005. Disponible à l'adresse `https://webusers.imj-prg.fr/~pierre.colmez/congruents.pdf`

[Edw77] Harold M. Edwards, *Fermat's Last Theorem — A Genetic Introduction to Algebraic Number Theory*, Graduate Texts in Mathematics **50**, Springer Verlag, 1977.

[Hel09] Yves Hellegouarch, *Invitation aux Mathématiques de Fermat-Wiles*, Dunod, 2009.

[Hin08] Marc Hindry, *Arithmétique*, Calvage et Mounet, 2008.

[IR1990] Kenneth Ireland et Michael Rosen, *A Classical Introduction to Modern Number Theory*, deuxième édition, Graduate Texts in Mathematics **84**, Springer Verlag, 1990.

[Maz91] Barry Mazur, *Number theory as gadfly*, Amer. Math. Monthly **98** (1991).

[Rib99] Paulo Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer Verlag, 1999.

[Rib95] Kenneth Ribet, *Galois representations and modular forms*, Bull. Amer. Math. Soc. **32** (1995).

[Sin11] Simon Singh, *Le Dernier Théorème de Fermat*, (trad. : G. Messadié) Fayard/Pluriel, 2011.

[Wei83] André Weil, *Number Theory — An approach through history from Hammurapi to Legendre*, Modern Birkhäuser Classics, Birkhäuser Verlag, 1983.