L'histoire de la théorie (algébrique) des nombres

4TMQA01U Maths, sciences et société

Felix Henson, Sylvain Callewaert

Semestre automne 2023-24

Table des matières

> ... j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir.
>
> *Pierre de Fermat*

1 Introduction

On dit parfois que la chimie n'est que la physique appliquée, et que la physique n'est rien que les mathématiques appliquées.[12] Mais on pourrait bien dire qu'au cœur des maths il existe un domaine de pureté absolue, soit la théorie des nombres. Bien que le concept de « nombre » soit une invention humaine, les civilisations étudient les nombres et leurs propriétés depuis l'antiquité. Un exemple notable est la Grèce antique, où les méthodes de géométrie à la règle et au compas ont mené à des questions sur la constructibilité des nombres – une propriété qu'on comprend aujourd'hui par le biais de l'algèbre moderne. La quadrature du cercle et la duplication du cube sont des problèmes bien connus qui datent de cette époque. Cette étude a fortement enrichi le domaine de l'algèbre, et par conséquent a eu un grand impact sur les sciences plus largement.

Les problèmes et résultats de la théorie des nombres concernent souvent les entiers, les nombres algébriques et les nombres premiers. Aujourd'hui, le domaine se répartit en plusieurs branches, principalement la « théorie algébrique » et la « théorie analytique », dépendant des approches à ces concepts. Nous examinons dans ce mémoire principalement le coté algébrique, avec comme guide le dernier théorème de Fermat.

2 Avant Fermat

2.1 Diophante d'Alexandrie

Diophante d'Alexandrie est un mathématicien de langue grec de l'antiquité tardive (∼200-300 après J.C.), parfois considéré comme étant le « père de l'algèbre ». On ne sait pas grand-chose de sa vie. Même son œuvre n'est que partiellement connu, tous les ouvrages nous étant parvenus ne sont que fragmentaires. Des volumes des *Arithmétiques*, le travail qui l'a fait passer à la postériorité, seulement 6 étaient connus à l'époque de Fermat sur les 13 annoncés par l'auteur lui-même dans le préambule. Dans les années 60, on a découvert 4 autres – pas les copies originales, mais une traduction arabe.

Malgré le manque d'informations sur l'homme, les calculs de Diophante ont conduit, des centaines d'années plus tard, à ce qu'on appelle aujourd'hui *l'analyse diophantienne* – un domaine qui fait partie de la théorie des nombres. Il s'intéresse principalement aux solutions entières à des polynômes

aux coefficients entiers – appelés aujourd'hui des *équations diophantiennes*. Cela peut paraître simple, mais en fait il ne peut exister aucun algorithme pour trouver des solutions a une équation diophantienne quelconque (cf. la solution au $10^{\text{ème}}$ problème de Hilbert). Pour cette raison, de nombreux problèmes difficiles en théorie des nombres prennent la forme d'une équation diophantienne.

L'une des équations que considère Diophante est $x^2 + y^2 = z^2$. Probablement l'équation diophantienne la plus connue aujourd'hui, son lien avec des triangles rectangles était alors bien connu depuis des siècles [13]. Diophante cherche des solutions dans $\mathbb{Q}$ à partir d'un z connu, et ne s'appuie pas sur des méthodes géométriques. Voici sa méthode :

Problème. *(Diophante, 2.VIII) Partager un carré proposé en deux carrés.*

Méthode. Proposons de partager 16 en deux carrés. On note x^2 le premier de ce carrés. Alors l'autre nombre est $16 - x^2$. Il faut donc trouver $x \in \mathbb{Q}$ tel que $16 - x^2$ est un carré. Considérons $(ax - \sqrt{16})^2$, $a \in \mathbb{N}$. En particulier on considère le cas $a = 2$ et on identifie cette expression avec ce deuxième nombre, soit $(2x - 4)^2 = 16 - x^2$. Donc on a $5x^2 = 16x$, d'où $x = \frac{16}{5}$. C'est à dire, $16 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2$. □

Cette démonstration bénéficie ici de l'écriture algébrique moderne, qui n'existait pas à l'époque de Diophante. Dans le texte original, il pose et résout ses problèmes en mots et en son propre écriture quasi-algébrique, qui fournit des raccourcis pour des concepts communs tels que des puissances ou l'égalité. On voit aussi qu'il n'essaye pas de décrire une solution générale à ses problèmes, se concentrant ici sur le cas particulier du carré 16. En effet, les *Arithmétiques* est plutôt un livre d'exercices, une suite de problèmes, chacun avec ses propres conditions, résultat particulier, et méthode de résolution personnelle ; ce n'est pas un traité d'algèbre comme on verrait aujourd'hui. Par conséquent, bien que Diophante ait sans doute inspiré les idées de la théorie des nombres, il a fallu attendre pour avoir des résultats plus généralisés.

2.2 Al-Karaji

Au $\text{IX}^{\text{ème}}$ siècle vit à Bagdad le mathématicien Al-Kwharizmi qui va être un des fondateurs de l'algèbre moderne. Dans ses traîtés il est le premier à

chercher des solutions d'équations linéaires et quadratiques à l'aide d'opérations, de transformation et de combinaisons qu'il définit clairement. Ses contributions aux mathématiques sont nombreuses et notables, l'usage du zéro comme nombre, les bases du calcul logarithmique, etc. et ses recherches ne se limitent pas au seul domaine des mathématiques (astronomie, géographie, ...).

Cependant, en son temps il n'existe pas encore de traduction en arabe de Diophante, qui lui est, par conséquent, inconnu. En effet il faut attendre le début du X$^{\text{ème}}$ siècle, sois plus de cinquante ans après le décès de Al-Kwharizmi, pour que les ouvrages du mathématicien grec soit traduits et étudiés de nouveau. C'est notamment Al-Karaji et ses disciples qui vont s'en emparer et vont les poursuivre, en cherchant notamment à toujours généraliser.

Abu Bakr Muhammad ibn al-Hasan al-Karaji vécut lui aussi à Bagdad et c'est là qu'il publia ses travaux les plus important. On ne sait pas grand chose de sa vie, il occupa probablement un poste officiel à la cour avant de se retirer et de finir sa vie loin de la ville. On ne connaît de lui que onze oeuvres, dont quatre traitant de mathématiques. Ses recherches vont changer l'approche des mathématiques, comme un de ses disciples l'expliqua plus tard, ses idées consistaient à « opérer sur les inconnues au moyen de tous les instruments arithmétiques comme l'arithméticien opère sur les connus »

Problème. *(Al-Karaji, III.36-38) [Trouver $x, y \in \mathbb{Q}$ tels que]* $x^2 + y^2 = 9$

Méthode. On a $9 - x^2 = y^2$. Posons $y = 2x - 3$, alors $9 = x^2 = 4x + 9 - 12x$, donc $x = \frac{12}{5}$. Alors $y = \frac{24}{5} - 3 = \frac{9}{5}$. Donc $\left(\frac{24}{5}\right)^2 + \left(\frac{9}{5}\right)^2 = 9$. □

3 Fermat et la théorie algébrique des nombres

3.1 Pierre de Fermat

En 1601, Pierre de Fermat naît à Beaumont-de-Lomagne, dans le sud-ouest de la France. Il étudie à l'université de Toulouse avant de partir vivre à Bordeaux, où il commence ses recherches mathématiques. Ensuite, il étudie la loi en Orléans avant de revenir à Toulouse en 1631. C'est alors qu'il est nommé au parlement de Toulouse, et il restera magistrat jusqu'à sa mort en 1665.

Pendant sa vie il ne publie presque rien de mathématique ; il écrit à Pascal :

> Quelle que soit la part de mon travail qui mérite d'être publiée, je ne veux pas que mon nom y paraisse. [24]

Cependant, il est en contact avec de nombreux mathématiciens bien connus, à qui il envoie des lettres contenant ses résultats – parfois en forme de problèmes à résoudre et souvent sans démonstration. C'est par le biais de ces correspondances que, malgré son emploi peu mathématique, il réussit à devenir célèbre parmi les mathématiciens de l'époque. Par exemple, son *petit théorème* vient d'une correspondance entre lui et mathématicien parisien Bernard Frénicle de Bessy en 1640.

Theorème 3.1 (Petit théorème de Fermat, formulation moderne)**.** *Si p est un nombre premier et a un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p (i.e. $a^{p-1} \equiv 1 \mod p$.)*

Démonstration. C'est une conséquence du théorème de Lagrange (bien que ce dernier ne soit pas encore découvert à l'époque). On considère $a \mod p$ comme élément de $(\mathbb{Z}/p\mathbb{Z})^\times$, groupe multiplicatif d'ordre $p-1$. Alors l'ordre de a divise l'ordre du groupe par le théorème de Lagrange, donc en particulier $a^{p-1} \equiv 1 \mod p$. En effet, l'une des démonstrations d'Euler consiste à étudier les restes modulo p des puissances de a, ce qui est à peu près ce que fait la démonstration ci-dessus. [2] □

Ce théorème décrit un propriété utile des nombres premiers, et par conséquent il décrit une façon de vérifier si un nombre est composé : pour $n \in \mathbb{N}$, s'il existe $a \in \mathbb{N}$ tel que $n \nmid a$ et $n \nmid a^{n-1}$, alors n n'est pas premier. C'est la base des tests de primalité de Fermat et de Rabin-Miller. Les nombres premiers sont un intérêt clé de la théorie des nombres, et sont le sujet principal de l'hypothèse de Riemann, un problème ouvert en la théorie analytique.

Fermat déclare son petit théorème en termes de suites géométriques, mais ne le démontre pas. Il écrit plûtot :

> Cette proposition est généralement vraie en toutes progressions et en tous nombres premiers ; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.[3]

C'est cette habitude de ne pas écrire entièrement les démonstrations à ses théorèmes qui mènera au mystère autour de son dernier théorème plus tard.

3.1.1 Le dernier théorème

En plus de ses correspondances, Fermat écrit des idées dans la marge de sa copie des *Arithmétiques*, une traduction latine faite en 1621 d'un œuvre jusque-là oublié par l'occident. Après sa mort, son fils publie sa copie avec ses notes incluses, et c'est ici que se trouve sa fameuse conjecture.

Dernier théorème de Fermat (FLT). *L'équation*

$$x^n + y^n = z^n \,;\, xyz \neq 0, \tag{1}$$

n'a pas de solution pour $x, y, z \in \mathbb{Z}$, $n \geq 3$.

Fermat dit avoir trouvé une démonstration « merveilleuse » pour ce résultat, mais il ne la détaille pas à cause des marges trop étroites. On appelle sa conjecture le « dernier théorème » car dans les 100 ans qui ont suivi la mort de Fermat, les mathématiciens contemporains ont réussi à prouver tous ses conjectures sauf 2 : celle des nombres « premiers de Fermat », qui s'est avérée fausse, [1] et le FLT.

Problème. *Montrer que l'équation* (1) *n'a pas de solution dans le cas* $n = 4$.

La démonstration de ce résultat repose sur deux autres résultats, présentés ci-dessous en forme de lemmes.

Lemme 3.2 (Euclide, *Éléments* X29, Lemme 1)**.** *Soit* $x, y, z \in \mathbb{N}$ *un triplet pythagoricien primitif. Alors il existe* $u, v \in \mathbb{N}^*$ *avec* $u > v$*, premiers entre eux, tels que l'un d'entre eux est pair et l'autre impair, et :*

$$x = 2uv,\ y = u^2 - v^2,\ z = u^2 + v^2$$

.

Lemme 3.3 (Fermat, extrait d'une lettre à Huygens)**.** *L'aire d'un triangle rectangle ne peut pas être un carré.*

C'est les *Arithmétiques* qui inspirent Fermat à démontrer ce fait, puisque Diophante y présente de nombreux triangles dont les aires ont des propriétés liés aux carrés – par exemple un triangle dont l'aire diffère d'un carré par un entier donné – mais il n'en présente aucun dont l'aire est exactement un carré. C'est le seul cas du FLT qui a été démontré par Fermat lui-même.

1. Les nombres de Fermat sont les entiers de la forme 2^{2^n} pour un entier n. Fermat conjecture que tous ces nombres sont premiers, ce qui est vrai pour $n \in [[1, 5]]$, mais pas pour $n = 6$.

Démonstration du lemme 3.3. La preuve consiste en une descente infinie. Prenons un triangle rectangle aux côtés rationnels a_0, b_0, c_0 dont l'aire $\frac{a_0 b_0}{2}$ est un carré. On peut multiplier les côtés par un dénominateur commun pour obtenir trois entiers, puis les diviser par leur pgcd pour obtenir un triplet pythagoricien primitif a, b, c. Comme on a multiplié a_0 et b_0 par la même quantité, on a que $\frac{ab}{2}$ est un carré.

Par le lemme d'Euclide, on a $a = 2uv, b = u^2 - v^2, c = u^2 + v^2$ où $u, v \in \mathbb{N}^*$ ont les propriétés décrites dans le lemme 3.2. On a donc $\frac{ab}{2} = uv(u-v)(u+v)$. Il est simple de vérifier que ces quatre facteurs n'ont aucun diviseur en commun. Par l'unicité de la factorisation dans $\mathbb{Z}$, on en déduit que $u, v, u-v$, et $u+v$ sont des carrés. Donc $(u-v)(u+v) = b$ est un carré (disons $b =: w^2$) comme produit de deux carrés, d'où $v^2 + w^2 = u^2$. C'est un nouveau triplet pythagoricien, primitif car $\text{pgcd}(u, v) = 1$, donc on peut refaire les étapes qu'on vient de faire.

On pose $v = 2u_1v_1, w = u_1^2 - v_1^2, u = u_1^2 + v_1^2$ comme avant. On a déjà établi que $u = u_1^2 + v_1^2$ est un carré (disons $u =: w_1^2$) car il divise $\frac{ab}{2}$, d'où le nouveau triplet pythagoricien u_1, v_1, w_1. Le triangle rectangle associé à ce triplet a comme aire $\frac{u_1 v_1}{2} = \frac{v}{4}$. On sait que v est un carré, donc cet aire est aussi un carré (et plus petit que $\frac{ab}{2}$). On a trouvé un nouveau triangle rectangle aux côtés naturels dont l'aire est un carré, et ce triangle est plus petit que celui de départ (i.e. aux côtés a, b, c). On a donc une descente infinie, ce qui est impossible.

□

Démonstration du FLT pour $n = 4$ (Fermat). On considère le triangle rectangle aux cotés $a^4 - b^4$, $2a^2b^2$, et $a^4 + b^4$, où $a, b \in \mathbb{N}^*$. On vérifie facilement qu'il satisfait le théorème de Pythagore. On suppose qu'il existe $c \in \mathbb{N}^*$ tel que $a^4 - b^4 = c^2$. Alors l'aire du triangle est $\frac{1}{2} \cdot 2a^2b^2(a^4 - b^4) = a^2b^2c^2$ par hypothèse, or cet aire est un carré, ce qui contredit le lemme 3.3. Donc l'équation $a^4 - b^4 = c^2$; $a, b, c \in \mathbb{N}^*$ n'a pas de solution. En posant $x^2 = c$, $y = b$, $z = a$ on obtient que (1) n'a pas de solution pour $n = 4$. □

Près de 100 ans après la mort de Fermat, Leonhard Euler publie une démonstration pour le cas $n = 3$ dans son *Algèbre*. Dans son travail il utilise l'anneau $\mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$, en particulier il utilise la factorisation $p^2 + 3q^2 = (p + i\sqrt{3}q)(p - i\sqrt{3}q)$. Il dit que si le terme à gauche est un cube, alors les deux facteurs à droite sont aussi des cubes car ils sont premiers entre eux. Par contre, ceci n'est pas *a priori* vrai, puisque la factorisation

n'est pas unique dans $\mathbb{Z}[i\sqrt{3}]$ (par exemple, $2 \cdot 2 = 4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$). Il semblerait qu'Euler n'ait pas remarquer cette subtilité, mais heureusement Gauss reformule la démonstration en utilisant $\mathbb{Z}[j]$ (où j est une racine primitive cubique de l'unité), ce qui est bien un anneau factoriel. [2]

3.2 Sophie Germain

Sophie Germain est née en 1776 dans une famille de la bourgeoisie parisienne. Elle découvre les mathématiques à l'adolescence en lisant des ouvrages dans la bibliothèque familiale, ça devient pour elle une véritable passion et elle va se former en autodidacte, apprenant même le latin afin d'étudier les travaux des plus grands noms de son temps, ce qui va lui donner de solides connaissances en théorie des nombres. Au cours de sa vie elle va correspondre avec des mathématiciens, notamment Legendre et Gauss, et même finir par être reconnue, bien que difficilement, par le monde académique.

En 1815, l'Académie des Sciences va proposer comme sujet pour son prochain prix des Mathématiques le dernier théorème de Fermat. C'est comme ça que Sophie Germain va se pencher sur le problème.

Elle va commencer par remarquer que si un nombre premier $p \neq 2$ divise n on peut réécrire l'équation comme : $(x^q)^p + (y^q)^p = (z^q)^p$ avec $q \in \mathbb{N}$, ce qui, en redéfinissant les arguments, donne :

$$x^p + y^p = z^p$$

et d'autre part que si n n'est divisible par aucun nombre premier impair alors c'est une puissance de 2, donc 4 divise n, et on peut alors se ramener au cas $n = 4$, déjà démontré. Il suffit donc de considérer les cas où p est un nombre premier impair.

Germain va alors premièrement dégager deux cas différent du dernier théorème de Fermat :

— Quand p ne divise pas xyz
— Quand p divise xyz

Ses travaux vont se concentrer sur celui ou p ne divise pas xyz.

Proposition 3.4. *Soit p et q deux nombres premiers distincts et différents de 2 tels que :*

2. Un anneau factoriel est un anneau où la factorisation d'un élément en éléments irréductibles est unique, à multiplication par un élément inversible près. Par exemple, tout entier relatif peut s'écrire de façon unique comme $(\pm 1)p_1 p_2 \cdots p_r$ où chaque p_i est premier. $\mathbb{Z}[i\sqrt{3}]$ n'est donc pas factoriel.

1. *p n'est pas congrue à un entier relatif à la puissance p modulo q*

2. *si $x^p + y^p + z^p \equiv 0 \mod q$ pour $x, y, z \in \mathbb{Z}$, alors q divise x, y ou z*

Alors le premier cas du dernier théorème de Fermat est vrai pour l'exposant p.

Pour pouvoir démontrer cette proposition on a besoin d'introduire les relations de Barlow-Abel.

On suppose qu'il existe des entiers x, y, z, différents de 0 et solution de l'équation $x^p + y^p + z^p = 0$, alors

$$-z^p = x^p + y^p$$
$$x^p + y^p = (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - ... - xy^{p-2} + y^{p-1})$$

On note $Q_p(x,y) = \sum_{k=0}^{p-1} x^k(-y)^{p-k-1}$ et l'on remarque que, si $x + y \neq 0$ et si p est impair alors $Q_p(x,y) = \frac{x^p+y^p}{x+y} =$ est un entier relatif.

Lemme 3.5. *Si x, y sont premiers deux à deux avec n, alors*

$$pgcd(Q_n(x,y), x+y) = pgcd(n, x+y)$$

Proposition 3.6 (Relations de Barlow-Abel)**.** *Si x, y et z sont des entiers relatifs premiers entre eux satisfaisant l'équation $x^p + y^p + z^p = 0$, et si $p \neq 2$ ne divise pas z, alors il existe $t, t_1 \in \mathbb{Z}$ tels que :*

$$x + y = t^p, \ \frac{x^p + y^p}{x+y} = t_1^p, \ z = -t_1 t,$$

avec $p \nmid t \cdot t_1$ et $pgcd(t, t_1) = 1$

Démonstration. De part le petit théorème de Fermat on a :

$$x + y + z \equiv x^p + y^p + z^p = 0 \mod p$$

donc $x + y \equiv -z \mod p$ et $p \nmid x + y$. On a $pgcd(Q_n(x,y), x+y) = 1$ d'après le lemme, et par factorisation unique alors il existe t et t_1 tel que $x + y = t^p$ et $Q_p(x,y) = \frac{x^p+y^p}{x+y} = t_1^p$. De plus, $t^p t_1^p = (tt_1)^p = (x+y)Q_p(x,y) = (-z)^p$, donc $z = -tt_1$. □

Proposition 3.4. De l'hypothèse 2, q divise un seul des x, y, z, supposons que que $q \mid x$ On applique les relations de Barlow-Abel à chacun des x, y, z, on obtient donc :

$$x + y = t^p,\ \frac{x^p + y^p}{x + y} = t_1^p,\ z = -t_1 t,$$
$$y + z = r^p,\ \frac{y^p + z^p}{y + z} = r_1^p,\ x = -r_1 r,$$
$$z + x = s^p,\ \frac{z^p + x^p}{z + x} = s_1^p,\ z = -s_1 s.$$

On peut les réécrire comme $2x = -r^p + s^p + t^p \equiv 0 \mod q$ De par l'hypothèse 2, q divise r, s ou t, or si $q \mid t$ alors $q \mid x + y$ et q divise y. Pareillement si q divise s alors $q \mid x + z$, donc q divise z, ce qui n'est pas possible, donc $q \mid r$, et l'on a les congruences suivantes :

$$y \equiv -z \mod q;$$
$$t_1^p \equiv y^p - 1,\ \text{car } (x + y)t_1^p = x^p + y^p;$$
$$r_1^p \equiv pt_1^p \mod q,\ \text{car } r_1^p = \frac{y^p + z^p}{y + z} \equiv py^p - 1 \equiv pt_1^p \mod q$$

Comme $q \nmid z$, q ne divise pas t_1, on peut donc trouver un rationnel t' tel que $t_1 t' \equiv 1 \mod q$, ce qui donne

$$t'^p r_1^p \equiv t'^p t_1^p p \mod q (r_1 t')^p \equiv p \mod \tag{2}$$

Ce qui contredit directement la première hypothèse. □

Theorème 3.7 (Théorème de Sophie Germain)**.** *Si p est un nombre premier différent de deux tel que $2p + 1$ est également premier, alors le premier cas du théorème de Fermat est vrai pour p.*

Démonstration. On cherche à montrer que la proposition 3.4 est vrai pour p et $q = 2p + 1$.

1) Si $p \equiv a^p \mod q$ alors, en appliquant le symbole de Legendre on a :

$$(\frac{a}{q}) = \pm 1 \equiv a^{(q-1)/2} = a^p \equiv p \mod q$$

alors $p \equiv \pm 1 \mod q$, ce qui est impossible.

2) On suppose que $x^p+y^p+z^p \equiv 0 \mod q$ et $q \nmid xyz$. Comme $p = (q-1)/2$ de par le petit théorème de Fermat on a :

$$x^p \equiv \pm 1 \mod q, \tag{3}$$
$$y^p \equiv \pm 1 \mod q, \tag{4}$$
$$z^p \equiv \pm 1 \mod q \tag{5}$$

Donc $0 = x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \mod q$, ce qui est impossible et conclut la démonstration. □

3.3 Gabriel Lamé et Ernst Kummer

Gabriel Lamé naît a Tours en 1795. Il étudie à l'École Polytechnique et ensuite l'École des Mines à Paris et pendant ce temps, bien que toujours étudiant, il commence à publier des articles. Au cours de sa carrière longue et variée, il tombe sur le théorème de Fermat pendant ses travaux sur les coordonnées curvilignes, en particulier en étudiant l'équation $\left(\frac{x}{a}\right)^n + \left(\frac{y}{b}\right)^n = 1$, ce qui donne (1) avec $z = a$ lorsque $a = b$. En 1840 il publie une démonstration du théorème pour le cas $n = 7$ (et tous multiples de 7 non divisibles par 2, 3 ou 5). Ses méthodes ont une base plus simple que les démonstrations d'Euler et Germain : après diviser le problème en deux cas – celui où 7 ne divise ni x, ni y, ni z (le premier cas), et celui ou 7 divise un de ces nombres (le deuxième cas) – sa preuve repose seulement sur des propriétés de divisibilité des nombres naturels. L'explication de sa preuve ci-dessous est basée sur le résumé trouvé dans [6].

Démonstration de Lamé du FLT pour $n = 7$, premier cas. On part de l'équation $x^7+y^7 = z^7$ avec x, y, z non-nuls et premiers entre eux. Ensuite on trouve des expressions pour x^7, y^7, z^7 en termes des autres variables en réarrangeant l'équation de base et en développant ; on a

$$x^7 = (z-y)X,\ y^7 = (z-x)Y,\ z^7 = (x+y)Z,$$

avec

$$\begin{aligned} X =& (z-y)^6 + 7y(z-y)^5 + 3\cdot 7y^2(z-y)^4 + 5\cdot 7y^3(z-y)^3 \\ &+ 5\cdot 7y^4(z-y)^2 + 3\cdot 7y^5(z-y) + 7y^6, \end{aligned}$$

et des expressions similaires pour Y et Z.

On traite maintenant le premier cas. L'hypothèse implique que les deux termes $(z-y)$ et X dans l'expression pour x^7 sont premiers entre eux, et donc ces termes sont des septième puissances. Il en est de même pour les expressions pour y^7 et z^7. Donc on peut définir :

$$\begin{array}{lll} x = m\mu & X = m^7 & z - y = \mu^7 = a \\ y = n\nu & Y = n^7 & z - x = \nu^7 = b \\ z = p\rho & Z = p^7 & x + y = \rho^7 = c, \end{array}$$

avec m, n, p, μ, ν, ρ premiers entre eux. On dispose maintenant de l'égalité

$$x + y - z = \mu(m - \mu^6) = \nu(n - \nu^6) = \rho(p - \rho^6),$$

donc $x + y - z$ est divisible par μ, ν, et ρ, donc par $P := \mu\nu\rho$. On écrit $x + y - z = A\mu\nu\rho = AP$ pour un entier A. On en déduit la relation

$$\rho^7 - \nu^7 - \mu^7 = 2A\mu\nu\rho.$$

Lamé utilise cette relation pour déduire que 7 divise $16A^7$, donc 7 divise A. Il démontre aussi que A est un carré (disons B^2), et obtient finalement les équations suivantes :

$$\begin{aligned} c - b - a &= 2B^2P \\ a^2 + b^2 + c^2 - ba - ca + ab &= BD \\ abc &= P^7 \\ 3(a^4 + b^4 + c^4) + 10(b^2c^2 + c^2a^2 + a^2b^2) &= \frac{16}{7}B^{14}, \end{aligned}$$

pour un certain entier D. Par élimination on obtient :

$$7\left(\frac{B^6}{7}\right)^1 - D^2 = P^2(7B^6P^2 - 5B^2D - P^6). \tag{6}$$

Il est possible de vérifier que B est impair et divisible par 7, que P est pair et que D est impair. Donc, comme P est divisible par 2, l'expression à droite de eq. (6) est divisible par 4, tandis que l'expression à gauche ne l'est pas. C'est une contradiction. □

La démonstration du deuxième cas commence de façon similaire, avec quelques petites différences dans les systèmes d'équations, notamment l'apparition des puissances de 7 dans les systèmes d'équations. Par contre, on ne

peut pas utiliser la divisibilité directement pour finir l'argument, il faut plutôt utiliser la descente infinie appliquée aux équations de la forme $t^2 = u^2 + 7v^2$ pour t, u impairs, v pair, et t, u, v premiers entre eux.

En 1847, à l'Académie des sciences, Lamé déclare être proche d'une démonstration généralisée du FLT. Il donne une esquisse verbale de ses méthodes, mais attire plusieurs critiques. Une de ces critiques vient d'Ernst Kummer, qui remarque une faille subtile mais importante dans le raisonnement de Lamé.

Démonstration proposé par Lamé en 1847. On travaille dans l'anneau

$$\mathbb{Z}[\zeta] = \left\{ \sum_{k=0}^{n-1} x_k \zeta^k \mid x_0, \ldots, x_{n-1} \in \mathbb{Z} \right\},$$

où ζ est une racine primitive $n^{\text{ème}}$ de l'unité (par exemple $\zeta = e^{\frac{2\pi i}{n}}$). Dans cet anneau on peut factoriser (1) :

$$x^n + y^n = \prod_{k=0}^{n-1} (x + \zeta^k y) = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y) = z^n.$$

Les facteurs $(x + \zeta^k y)$ sont premiers entre eux, donc on a nécessairement que chacun est une $n^{\text{ème}}$ puissance d'un autre nombre dans $\mathbb{Z}[\zeta]$, puisque leur produit est une $n^{\text{ème}}$ puissance. À partir d'ici et de certaines relations entre les facteurs, Lamé déduit une contradiction. □

Les détails de la fin de sa démonstration ne sont pas particulièrement pertinents, puisque Lamé, comme Euler cent ans avant, tombe dans un piège logique. Le fait de supposer que chaque facteur dans la décomposition de $x^n + y^n$ est une $n^{\text{ème}}$ puissance nécessite que cette factorisation en termes premiers entre eux soit unique, une propriété qui est toujours vraie dans $\mathbb{Z}$ mais non nécessairement dans un anneau quelconque. En effet, Kummer a déjà démontré en 1844 que l'anneau $\mathbb{Z}[\zeta]$ n'est pas factoriel dans le cas $n = 23$. Suite à l'annonce par Lamé de sa démonstration, Kummer envoie à Liouville, un membre de l'académie des sciences, une lettre exprimant ses soucis, et la prétendue preuve tombe à l'eau.

Inspiré par le manque de factorisation unique dans ces anneaux, Kummer se met à travailler sur une manière de la restaurer. Son idée est celle des « nombres idéaux », des éléments qu'on ajouterait à un anneau pour le rendre

factoriel. Par exemple, si on considère $\mathbb{Z}[i\sqrt{5}]$, alors $3\times 7 = 21 = (1+2\sqrt{5})(1-2\sqrt{5})$. Kummer propose qu'il existe des nombres idéaux p_1, p_2, p_3, p_4 tels que

$$p_1p_2 = 3,\ p_3p_4 = 7,\ p_1p_3 = (1+2\sqrt{5}),\ p_2p_4 = (1-2\sqrt{5}),$$

qui donne la décomposition unique $21 = p_1p_2p_3p_4$.[28] Cependant, Kummer ne précise pas tous les détails de sa théorie, ce qui limite son utilité.

Ensuite, Richard Dedekind redéfinit l'idée de Kummer en termes ensemblistes ; il appelle ces ensembles des *idéaux* d'un anneau. Dans ce qu'on appelle aujourd'hui les *anneaux de Dedekind*, ces structures donne une factorisation unique en termes d'ensembles même si l'anneau n'est pas factoriel. On a donc une décomposition unique de l'idéal engendré par un élément quelconque en idéaux dits *premiers*. Non seulement la théorie de Dedekind est-elle mieux définie que celle de Kummer, les idéaux sont aujourd'hui une partie intégrante de l'algèbre commutative, et permettent de créer de nouveaux anneaux par le biais des quotients.

Kummer réussit aussi à démontrer le FLT pour tous les nombres premiers dits « réguliers ». Un nombre premier p est appelé régulier si et seulement s'il ne divise pas les numérateurs des nombres de Bernouilli $B_2, B_4, \ldots, B_{p-3}$. Il se trouve que ce critère est assez difficile à vérifier, et tandis que Kummer est convaincu qu'il existe une infinité de nombres premiers réguliers, on ne sait toujours pas aujourd'hui si tel est le cas. De toute façon, c'est un bon exemple d'une démonstration du FLT pour une grande classe de nombres, ce qui est encore peu ordinaire à l'époque.

3.4 Andrew Wiles et la fin du FLT

Les concepts qui mènent finalement à une démonstration du théorème de Fermat sont en fait bien plus avancés que ce qu'ont utilisé les mathématiciens du XIX$^{\text{ème}}$ siècle. L'étincelle qui déclenche tout est une conjecture faite en 1955 par mathématicien japonais Yutaka Taniyama. Il pense qu'il y aurait un lien entre deux structures mathématiques qui n'ont, a priori, rien à voir l'un avec l'autre : les courbes elliptiques et les formes modulaires. Avec Gorō Shimura, ils précisent la conjecture, qui reçoit le nom de la « conjecture de Taniyama-Shimura ».

Conjecture de Taniyama-Shimura (T-S). *Toute courbe elliptique sur $\mathbb{Q}$ est modulaire.*

À l'époque, la conjecture est reconnue mais elle est considérée trop difficile à aborder. Pour la comprendre on aura besoin de quelques définitions. [3] L'explication ci-dessous est basée sur une partie d'une présentation par Kenneth A. Ribet [18].

Definition. *Une* courbe elliptique *(sur un corps K) est une courbe algébrique définie par les solutions (x, y) d'une équation de la forme $y^2 = x^3 + ax + b$, où $a, b \in K$, ainsi qu'un point « à l'infini » que l'on note $\mathcal{O}$.*

Remarques.
1. *Une cubique de la forme $x^3 + dx^2 + ex + f$ peut être réduit à la forme à droite ci-dessus en posant $x' = x + \frac{d}{3}$.*
2. *Une courbe elliptique a une structure de groupe additive où $\mathcal{O}$ est l'élément neutre.*

Definition. *On appelle* discriminant *d'une cubique $(x-\alpha)(x-\beta)(x-\gamma)$ le carré du produit des différences des racines, i.e. $[(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)]^2$. On appelle* singulière *(resp. non singulière) une courbe elliptique de discriminant 0 (resp. discriminant non nul).*

Definition. *Pour une courbe elliptique sur $\mathbb{Q}$ et un nombre premier ℓ, on peut choisir une équation aux coefficients entiers pour cette courbe et la réduire modulo ℓ. Si, après cette procédure, on obtient une équation non singulière, on dit que la courbe a* bonne réduction *modulo ℓ. Sinon, on parle de* mauvaise réduction.

Exemple. *On considère la courbe elliptique définie par $y^2 = x^3 - x + 1$. Le discriminant de la cubique à droite est -23. Il est alors logique (et vrai) que cette courbe a mauvaise réduction modulo 23. En fait, elle a bonne réduction modulo tous les nombres premiers sauf 2 et 23.*

Si E est une courbe elliptique définie sur $\mathbb{Q}$ qui a bonne réduction modulo ℓ, alors la courbe $E \mod \ell$ a au plus $\ell^2 + 1$ points (car il y a ℓ choix pour chacun de x et y, en plus du point $\mathcal{O}$). On note $|E(\mathbb{F}_\ell)|$ le nombre de points de E modulo ℓ.

Definition. *Soit E une courbe elliptique sur $\mathbb{Q}$. On pose $a_\ell = \ell + 1 - |E(\mathbb{F}_\ell)|$ pour tout ℓ premier tel que E a bonne réduction modulo ℓ. On dit que E est* modulaire *lorsqu'il y a une forme modulaire définie par une série entière dont les coefficients sont exactement les a_ℓ.*

3. Pour comprendre la conjecture, il est beaucoup plus important de connaître des propriétés des courbes elliptiques que celles des formes modulaires.

Exemple. *La forme modulaire associée à la courbe* $y^2 = x^3 - x + 1$ *est*

$$q - 3q^3 - 2q^5 - 4q^7 + 6q^9 + 2q^{11} - 5q^{13} + 6q^{15} + \dots,$$

avec $q = e^{2\pi i\tau}$ *où* $\tau \in \mathbb{C},\ \mathrm{Im}(\tau) > 0$.

Il est important de noter qu'en 1955, il n'y avait aucune raison de penser que le dernier théorème de Fermat serait lié aux courbes elliptiques, ni aux formes modulaires. Il a fallu attendre quelques décennies pour que le lien soit découvert.

En 1975, Yves Hellegouarch étudie les ordres (dans le sens de la structure de groupe) des points sur des courbes elliptiques. Il remarque dans une publication que s'il existe une courbe elliptique sur $\mathbb{Q}$ qui a un point P d'ordre $2p^2$ (i.e. $2p^2P = \mathcal{O}$) avec $p > 3$ premier, alors l'équation (1) a des solutions (pour $n = p$).[8] C'est la première fois que l'on voit la possibilité de construire un contre-exemple au FLT en utilisant les courbes elliptiques.

Dans les années 1980, mathématicien allemand Gerhard Frey considère la courbe elliptique $y^2 = x(x - a^p)(x + b^p)$ associée à l'équation $a^p + b^p = c^p$, où $p \geq 5$ est un nombre premier, on appelle aujourd'hui cette courbe la « courbe de Frey ». Il remarque que cette courbe a plusieurs qualités étranges. Certaines de ces qualités nécessitent une bonne connaissance des courbes algébriques pour être appréciées, mais une en est assez facilement comprise avec l'aide de quelques outils de plus.

Remarques.

1. *Il existe souvent une « meilleure façon » d'écrire une courbe elliptique E, qui s'appelle la* forme minimale. *C'est l'équation qui donne une courbe elliptique isomorphe à E telle que cette nouvelle courbe a bonne réduction au plus grand nombre de points possible.*
2. *Le discriminant de la forme minimale d'une courbe elliptique s'appelle le* discriminant minimal.
3. *Il existe differentes sortes de courbes elliptiques, parmi lesquelles les courbes* semi-stables. *Les courbes semi-stables sont particulièrement pertinentes dans l'histoire du FLT.*

Definition. *Le* conducteur *d'une courbe elliptique semi-stable est le produit des diviseurs premiers du discriminant minimal de cette courbe.*

La courbe de Frey est bien une courbe semi-stable, de discriminant minimal $\Delta := \frac{(abc)^{2p}}{256}$ et de conducteur $N := \prod_{\ell | abc,\, \ell \text{ premier}} \ell \leq abc$. Il se trouve

que $\frac{\Delta}{N} \geq \frac{(abc)^{2p-1}}{256}$ croît de manière exponentielle avec p, mais ceci contredit une conjecture de Szpiro qui dit que, pour tout ε positif, Δ serait majoré par un multiple de $N^{6+\varepsilon}$ – i.e. que le discriminant minimal et le conducteur devraient être « proche » l'un de l'autre.[27] Frey, face à ces faits surprenants, conjecture alors que si cette courbe existe, elle n'est pas modulaire. Par contre, son raisonnement s'appuie sur des idées nouvelles et jusque-là non démontrées.

En 1985, Jean Pierre Serre écrit une lettre, dans laquelle il raffine les propositions de Frey. Il dit que si on parvenait à démontrer un certain résultat, on prouverait incontestablement que la conjecture T-S implique le FLT. Il estime ce résultat « tout petit » (surtout par rapport à une éventuelle démonstration de la conjecture T-S), et il l'appelle donc ε. Pour cette raison, la conjecture précisée de Serre obtient le nom *conjecture epsilon*.

Ken Ribet commence presque immédiatement à travailler sur la conjecture epsilon. Il se concentre d'abord sur un cas particulier, ce qu'il trouve plus raisonnable que d'essayer de s'attaquer au problème entier tout de suite. Une fois ce cas démontré, Ribet essaye en vain pendant plusieurs semaines de démontrer le cas général. Lors d'un congrès au campus de UC Berkeley en 1986, il parle de ses idées à Barry Mazur, qui lui dit qu'il l'a en fait déjà démontré, car les arguments que Ribet utilise pour le cas particulier s'étendent facilement au cas général sans quasiment aucun changement. [19] La *conjecture epsilon* devient ainsi le *théorème de Ribet*.

Le héros de l'histoire du dernier théorème de Fermat est Andrew Wiles. Né à Cambridge au Royaume-Uni en 1953, il est fasciné depuis son adolescence par l'énigme du théorème de Fermat, grâce au livre *The last problem* de E.T. Bell. Cependant, une fois devenu mathématicien, il se rend compte que Fermat n'a de toute évidence jamais su démontrer sa proposition. Malgré ceci, suite à la démonstration par Ribet de la conjecture epsilon, il est convaincu que la conjecture T-S (et par conséquent le FLT) est non seulement vraie, mais aussi démontrable avec les outils mathématiques qui lui sont disponibles. En particulier, il n'a qu'à prouver que la courbe de Frey est modulaire pour prouver le FLT par l'absurde.

Wiles travaille en secret sur le problème pendant des années, et ne parle de son travail qu'à sa femme, jusqu'en 1993 où, lors d'une série de trois présentations, il révèle son œuvre achevé au monde mathématique. Sa démonstration montre que les courbes elliptiques semi-stables sont modulaires, ce qui implique le FLT. Malheureusement, comme tous ceux qui ont tenté

de démontrer le théorème avant lui, Wiles a fait une erreur dans sa démonstration. Pourtant, après un an de plus de travail, il présente une version améliorée (en collaboration avec son ancien étudiant Richard Taylor) de sa preuve, qui est enfin validée. Le dernier théorème de Fermat est ainsi vaincu.

Theorème 3.8 (Wiles, Taylor)**.** *Toute courbe elliptique semi-stable est modulaire.*

Après la finalisation de cette preuve, des anciens étudiants de Wiles – Richard Taylor, Brian Conrad et Fred Diamond – ainsi que Christophe Breuil, publient une série d'articles démontrant les cas restants de la conjecture T-S. En 2001 elle devient finalement un théorème.

Theorème 3.9 (Théorème de modularité)**.** *Toute courbe elliptique est modulaire.*

3.5 L'avenir – le programme de Langlands

Bien que très impressionnante, le théorème de modularité ne représente qu'une petite partie d'un phénomène bien plus grand dans la théorie des nombres. Ce phénomène s'appèlle le *programme de Langlands*, qui a ses racines dans une lettre que Robert Langlands envoie à André Weil en 1967.

Robert Langlands naît en Colombie-Britannique au Canada en 1936. Il obtient son doctorat à Yale aux États-Unis en 1960 et passe les 7 prochaines années comme professeur associé à Princeton, avant de partir en Turquie pendant une année. C'est pendant cette période qu'il commence à formuler les idées qui deviendraient son « programme ».

Langlands se rend compte de certains liens entre différentes structures mathématiques, en particulier entre des problèmes en analyse harmonique et des problèmes analogues en théorie des nombres. Il conjecture l'existence d'une « correspondance » entre ces deux mondes mathématiques, mais n'a pas les moyens de la démontrer. Un bel exemple de cette correspondance est bien le théorème de modularité, qui donne un lien direct entre les courbes elliptiques (du côté théorie des nombres) et les formes modulaires (du côté analyse harmonique). Plus généralement, le programme conjecture un lien entre les représentations galoisiennes (théorie des nombres) et les formes automorphes (analyse harmonique).

Un tel lien est prisé parce qu'il ouvre les portes à de nouvelles façons de résoudre des problèmes. Par exemple, on peut utiliser ce qu'on sait d'une certaine courbe elliptique pour déduire des conclusions sur la forme modulaire

qui y est associée. De plus, on peut transformer un problème de l'analyse harmonique, posé en termes des formes modulaires, en un problème algébrique posé en termes des courbes elliptiques. C'est ce puissance qui fait du programme de Langlands un domaine de recherche actif dans le monde des mathématiques modernes, et on espère qu'il peut continuer de faire avancer la théorie des nombres à l'avenir.

Références

[1] Diophante d'Alexandrie et Paul Ver Eecke. *Diophante d'Alexandrie. Les six livres arithmétiques et le livre des nombres polygones*. Desclée de Brouwer, 1926.

[2] Leonhard Euler. *Theoremata circa residua ex divisione potestatum relicta*. 1761.

[3] Pierre de Fermat, Paul Tannery et Charles Henry. *Œuvres de Fermat, tome deuxième, correspondance*. Paris : Gauthier-Villars et cie, 1894, p. 206-209.

[4] Edward Frenkel. *The Langlands Program - Numberphile*. 2023. URL : https://www.youtube.com/watch?v=4dyytPboqvE&t=484s (visité le 20/12/2023).

[5] Gerhard Frey. « Links between stable elliptic curves and certain Diophantine equations ». In : *Annales Universitatis Saraviensis. Series Mathematicae* 1.1 (1986).

[6] Catherine Goldstein. « Gabriel Lamé et la théorie des nombres : « une passion malheureuse » ? » In : *Bulletin de la Sabix* 44 (2009). URL : http://journals.openedition.org/sabix/690.

[7] Yves Hellegouarch. *Invitation aux Mathématiques de Fermat-Wiles*. 2e éd. Dunon, 2001.

[8] Yves Hellegouarch. « Points d'ordre $2p^h$ sur les courbes elliptiques ». In : *Acta Arithmetica* 26.3 (1975), p. 253-263. URL : http://eudml.org/doc/205313.

[9] G. Lamé. « Mémoire d'analyse indéterminée, démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers ». fr. In : *Journal de Mathématiques Pures et Appliquées* 1e série, 5 (1840). URL : http://www.numdam.org/item/JMPA_1840_1_5__195_0/.

[10] Serge Lang. « Some History of the Shimura-Taniyama Conjecture ». In : *Notices of the American Mathematical Society* 42.11 (1995).

[11] Franz Lemmermeyer. *Jacobi and Kummer's Ideal Numbers*. 2011. arXiv : 1108.6066 [math.NT].

[12] Randall Munroe. *xkcd: Purity*. 2008. URL : https://xkcd.com/435 (visité le 10/01/2024).

[13] Otto Neugebauer. *The Exact Sciences in Antiquity*. Mineola, NY : Dover Publications, nov. 1969, p. 36.

[14] Joseph Oesterlé. « Nouvelles approches du « théorème » de Fermat ». In : *Astérisque* 161-162 (1988). URL : http://www.numdam.org/item/SB_1987-1988__30__165_0/.

[15] Erich Reck. *Dedekind's Contributions to the Foundations of Mathematics*. 2020. URL : https://plato.stanford.edu/entries/dedekind-foundations/#AlgNumThe (visité le 13/01/2024).

[16] Paulo Ribenboim. « The Early History of Fermat's Last Theorem ». In : *13 Lectures on Fermat's Last Theorem*. Springer New York, 1979, p. 9-10. ISBN : 978-1-4684-9342-9. DOI : 10.1007/978-1-4684-9342-9_1.

[17] Kenneth A. Ribet. « From the Taniyama-Shimura Conjecture to Fermat's Last Theorem ». In : *Annales de la Faculté des sciences de Toulouse : Mathématiques*. 5e sér. 11 (1990).

[18] Kenneth A. Ribet. *Kenneth A. Ribet, "A 2020 View of Fermat's Last Theorem"*. 2020. URL : https://www.youtube.com/watch?v=mq9BS6S2E2k (visité le 05/12/2023).

[19] Kenneth A. Ribet. *The Bridges to Fermat's Last Theorem - Numberphile*. 2015. URL : https://www.youtube.com/watch?v=nUN4NDVIfVI (visité le 12/12/2023).

[20] E. F. Robertson et J. J. O'Connor. *Al-Karaji - biography*. 1999. URL : https://mathshistory.st-andrews.ac.uk/Biographies/Al-Karaji/ (visité le 17/10/2023).

[21] E. F. Robertson et J. J. O'Connor. *Diophantus of Alexandria*. 1999. URL : https://mathshistory.st-andrews.ac.uk/Biographies/Diophantus/ (visité le 17/10/2023).

[22] E. F. Robertson et J. J. O'Connor. *Gabriel Lamé*. 2000. URL : https://mathshistory.st-andrews.ac.uk/Biographies/Lame/ (visité le 10/01/2024).

[23] E. F. Robertson et J. J. O'Connor. *Robert Phelan Langlands*. 2023. URL : https://mathshistory.st-andrews.ac.uk/Biographies/Langlands/ (visité le 09/01/2024).

[24] Simon Singh. *Fermat's Last Theorem*. Fourth Estate, 1997.

[25] Ian Stewart et David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. 4e éd. Chapman et Hall/CRC, 2015.

[26] John Stillwell. *Numbers and Geometry*. Springer-Verlag, 1998, p. 131-133.

[27] Andrew Sutherland. *18.783 Elliptic Curves, Lecture 26*. MIT OpenCourseWare. 2017. URL : https://dspace.mit.edu/bitstream/handle/1721.1/122962/18-783-spring-2017/contents/index.htm?sequence=9&isAllowed=y.

[28] Michel Waldschmidt. *MM020 Théorie des Nombres, 5ème fascicule*. 2011. URL : https://webusers.imj-prg.fr/~michel.waldschmidt/articles/pdf/TdN2011fascicule5.pdf (visité le 13/01/2024).

[29] Andrew Wiles. *Andrew Wiles - The Abel Prize interview 2016*. 2017. URL : https://www.youtube.com/watch?v=cWKAzX5U85Q&t=102s (visité le 10/01/2024).

[30] Andrew Wiles. *Andrew Wiles Acceptance Speech - The Abel Prize*. 2019. URL : https://www.youtube.com/watch?v=PLuLpE0OZGU (visité le 10/01/2024).

[31] Andrew Wiles. *Andrew Wiles: Fermat's Last theorem: abelian and non-abelian approaches*. 2020. URL : https://www.youtube.com/watch?v=4t1mgEBx1nQ (visité le 04/12/2023).

[32] Andrew Wiles. « Modular Elliptic Curves and Fermat's Last Theorem ». In : *Annals of Mathematics* 141.3 (1995), p. 443-551. ISSN : 0003486X. URL : http://www.jstor.org/stable/2118559 (visité le 04/12/2023).

[33] Andrew Wiles. *The Langlands Programme - Andrew Wiles*. 2023. URL : https://www.youtube.com/watch?v=ZFOPxZtlkig (visité le 04/12/2023).