Le Dernier Théorème de Fermat

F. PAZUKI

IMB, Université Bordeaux 1, 351 Cours de la Libération, 33405 Talence, France

1 Introduction

Pierre de Fermat (Beaumont-de-Lomagne 1601 - Castres 1665) a poursuivi des études de droit à Toulouse, Bordeaux puis Orléans et pratique les mathématiques comme un loisir. C'est la traduction en latin des oeuvres de Diophante par Bachet de Méziriac qui l'amène à se passionner pour l'arithmétique. Il démontre plusieurs théorèmes, en conjecture d'autres, annote les carnets de Diophante ; et c'est dans la marge du Livre II, problème 8, qu'il écrit en 1641 les phrases suivantes :

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

On peut traduire par : "Diviser un cube en deux cubes, une puissance 4 en deux puissances 4 ou une puissance quelconque en deux puissances de même dénomination, est impossible. J'ai découvert une démonstration merveilleuse mais je n'ai pas la place de la mettre dans la marge." Cette note est le point de départ d'une formidable aventure humaine et mathématique de plus de 350 ans, qui verra sa conclusion en 1994 lorsqu'Andrew Wiles rectifia sa preuve de la dernière étape. Nous présentons ici l'esquisse de la démonstration du résultat que l'on énonce de nos jours en ces termes :

Théorème : (Fermat-Wiles) Soit n un entier supérieur ou égal à trois. Alors l'équation :

$$x^n + y^n = z^n$$

n'admet pas de solution (x, y, z) avec x, y et z entiers naturels non nuls.

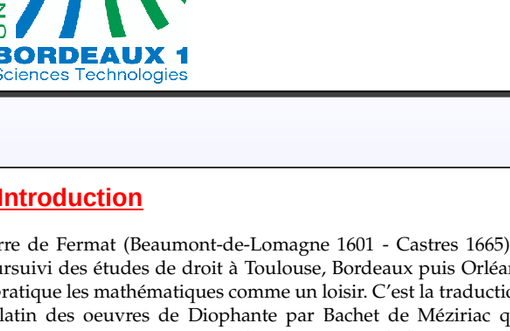

FIG. 1: Pierre de Fermat (1601-1665) et Andrew Wiles (1953 -)

2 Les premiers cas

Voici quelques-uns des premiers résultats obtenus à propos de cette équation. Signalons tout d'abord que lorsque $n = 1$ ou $n = 2$, il y a une infinité de solutions à l'équation de Fermat, que l'on sait paramétrer.

Frénicle de Bessy (1605-1675), en utilisant une indication de Fermat, publie le cas $n = 4$ en 1676 (posthume).

Le cas $n = 3$ sera démontré par Euler (1707-1783).

Legendre (1752-1833) et Dirichlet (1805-1859) traitent le cas $n = 5$.

Sophie Germain (1776-1831) donne un critère de divisibilité permettant de traiter de nouveaux cas.

Le mathématicien Kummer (1810-1893) prouve le théorème pour tout $n \leq 100$ (sauf 37, 59 et 67).

3 Les Courbes Elliptiques

Définition : Une courbe elliptique E définie sur un corps K est une courbe lisse donnée par une équation du type :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

Si la caractéristique de K est différente de 2 et 3 on peut transformer cette équation en :

$$y^2 = x^3 + Ax + B, \quad \text{avec } A, B \in K.$$

On associe à ces courbes les nombres suivants :

- le *discriminant* de E : $\Delta(E) = -16(4A^3 + 27B^2)$. On appellera Δ_{min} le discriminant minimal de E.
- le *conducteur* de E : $N = \prod_p p^{f_p}$ avec :

$$f_p = \begin{cases} 0 \text{ si } E \text{ a bonne réduction en } p, \\ 1 \text{ si } E \text{ a réduction multiplicative en } p, \\ 2 \text{ si } E \text{ a réduction additive en } p. \end{cases}$$

Remarque 1 : lorsque l'équation de E est à coefficients entiers, on peut réduire cette équation modulo un nombre premier p et obtenir ainsi une équation de courbe définie sur le corps résiduel. Si cette équation réduite est toujours lisse (i.e. $\Delta \,(\text{modulo}\, p) \neq 0$), on dira que la courbe est à bonne réduction.
Remarque 2 : les premiers de mauvaise réduction divisent nécessairement le discriminant de la courbe. En particulier il n'y en a qu'un nombre fini et le conducteur est donc un entier. Si la caractéristique est égale à 2 ou 3, f_p peut être plus grand que 2 en réduction additive.

Voici des exemples de courbes elliptiques (définies sur $\mathbb{Q}$) :

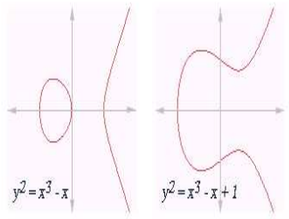

FIG. 2: $E(\mathbb{R})$: Points réels de courbes elliptiques.

Les courbes elliptiques sont munies d'une structure de groupe donnée par la loi corde-tangente dont on voit une illustration ci-dessous. Le neutre O est donné par le point à l'infini.

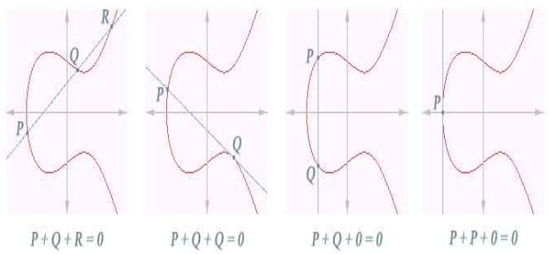

FIG. 3: Loi de groupe.

Remarque 3 : ce dessin illustre ici que la loi est interne et commutative, l'existence d'un élément neutre et le fait que tout élément admet un symétrique. Il faut encore vérifier que la loi est associative (ce n'est pas évident).

4 Les Formes Modulaires

Soit $\mathcal{H} = \{z \in \mathbb{C} \,|\, \text{Im}(z) > 0\}$ le demi-plan de Poincaré. Le groupe de matrices $\text{SL}_2(\mathbb{Z})$ agit sur $\mathcal{H}$ par :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} .z = \frac{az + b}{cz + d}.$$

On voit sur le dessin ci-dessous le demi-plan de Poincaré et un domaine fondamental (en grisé) pour l'action de $\text{SL}_2(\mathbb{Z})$:

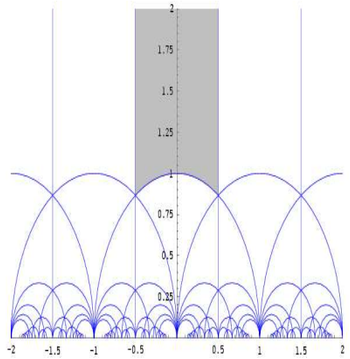

FIG. 4: Demi-plan de Poincaré.

Pour une fonction holomorphe f sur $\mathcal{H}$ et pour une matrice $\gamma \in \text{SL}_2(\mathbb{Z})$ notons :

$$(f|_k\gamma)(z) = \frac{1}{(cz + d)^k} f(\gamma.z).$$

Définition : une forme modulaire f de poids k pour un groupe Γ d'indice fini dans $\text{SL}_2(\mathbb{Z})$ est une fonction holomorphe sur $\mathcal{H}$ vérifiant :
- $f|_k\gamma = f$ pour tout $\gamma \in \Gamma$.
- Pour tout $\delta \in \text{SL}_2(\mathbb{Z})$ la fonction $f|_k\delta$ admet un développement de Fourier du type (avec N un entier strictement positif) :

$$(f|_k\delta)(z) = \sum_{n \geq 0} a(n) e^{2\pi i n z / N}.$$

Exemple : soit $z \in \mathcal{H}$, on pose alors : $q = e^{2i\pi z}$. La fonction :

$$\Delta(z) = q \prod_{n=1}^{+\infty} (1 - q^n)^{24}$$

est une forme modulaire de poids 12 (pour $\Gamma = \text{SL}_2(\mathbb{Z})$).

On considérera dans la suite uniquement l'espace $S_2(\Gamma_0(N))$ (avec $N \geq 1$ un entier) des formes modulaires de poids $k = 2$ pour le sous-groupe de $\text{SL}_2(\mathbb{Z})$ suivant :

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) |\ c \equiv 0 \,(\text{modulo } N) \right\}.$$

On sait exhiber une formule générale pour la dimension de $S_2(\Gamma_0(N))$. En particulier pour $N = 2$ on retiendra :

$$\dim_{\mathbb{C}}(S_2(\Gamma_0(2))) = 0,$$

i.e. il n'existe pas de forme modulaire non nulle de poids 2 et de niveau 2.

5 La Preuve

5.1 Premières remarques

Nous allons tout d'abord procéder à des réductions du problème.

Réduction 1 : on sait résoudre l'équation de Fermat pour $n = 1, 2$ en donnant une paramétrisation des solutions et par la négative pour $n = 3, 4$. Il suffit donc de considérer $n \geq 5$.

Réduction 2 : il suffit de considérer les cas où n est premier.

On raisonne à partir de maintenant par l'absurde en supposant l'existence d'un triplet (a, b, c) tel que $a^p + b^p + c^p = 0$ avec $abc \neq 0$ et a, b, c premiers entre eux, $p \geq 5$ un premier.

Réduction 3 : on peut se restreindre sans perte de généralité au cas où $a \equiv -1 \,(\text{modulo } 4)$ et $2|b$.

5.2 Courbe de Hellgouarch-Frey

L'idée générale est de construire une courbe basée sur ce triplet d'entiers vérifiant des propriétés impossibles. On va considérer, en suivant les idées originales de Hellgouarch et Frey, la courbe elliptique :

$$E_{a^p,b^p,c^p} \ : \ y^2 = x(x - a^p)(x + b^p).$$

On obtient alors :

$$\begin{cases} \Delta_{min} = 2^{-8}(abc)^{2p} \\ N = \prod_{\substack{l|abc \\ l \text{ premier}}} l = 2\text{rad}_2(abc) \end{cases}$$

5.3 Les théorèmes de Wiles et de Ribet

Le théorème de Wiles (1994) affirme qu'il existe une forme modulaire non nulle f de poids 2 et de niveau N naturellement associée à la courbe E_{a^p,b^p,c^p} de conducteur N.

Le théorème de Ribet (1987) affirme que dans cette situation la forme modulaire non nulle de poids 2 associée à E_{a^p,b^p,c^p} est en fait de niveau N_p avec :

$$N_p = \frac{N}{\prod_{\substack{l||N \\ p|\text{ord}_l(\Delta)}} l}.$$

On calcule alors :

$$N_p = \frac{N}{\text{rad}_2(abc)} = 2.$$

La combinaison des théorèmes de Wiles et de Ribet fournit donc l'existence d'un élément non nul dans l'espace $S_2(\Gamma_0(2))$. Or $S_2(\Gamma_0(2)) = \{0\}$. C'est la contradiction cherchée. Il n'existe donc pas de triplet d'entiers (a, b, c) non trivial tel que $a^p + b^p + c^p = 0$.

Remarque 4 : dans les théorèmes de Wiles et de Ribet, associer une forme modulaire à une courbe elliptique se fait via la théorie des *représentations galoisiennes*. Mais la marge est ici trop exigüe...

6 Références

- *Introduction aux mathématiques de Fermat-Wiles*, Y.Hellegouarch, Dunod 2e éd. (2001).
- *Modular Forms and Fermat's Last Theorem*, G.Cornell, J.Silverman, G.Stevens, Springer (1997).
- *Quadrature*, Trimestriel n°22 (1995).
- *The Arithmetic of Elliptic Curves*, J.Silverman, Springer 106 (1986).