Courbes elliptiques et équation de Fermat

Fabien Pazuki

Novembre 2004

Table des matières

Introduction

Aux alentours de 1640 Pierre de Fermat écrit dans une marge d'un de ses cahiers d'arithmétique :

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

Ce fut le point de départ d'une aventure mathématique qui s'est achevée il y a dix ans, en 1994, date à laquelle le dernier "théorème" de Fermat encore à l'étude fut démontré. On peut y associer de très nombreux noms de mathématiciens, Fermat, Euler, Sophie Germain, Kummer, mais aussi plus récemment Frey, Shimura, Taniyama, Weil, Serre, Ribet, Taylor, Wiles.

Le but de cet exposé est de présenter quelques grandes lignes de la preuve du dernier théorème de Fermat. C'est Andrew Wiles qui, en démontrant la conjecture de Taniyama-Weil en 1994, a apporté la conclusion à cette quête de 350 ans. Rappelons donc le fameux :

Théorème 0.1. *Soit $n \geq 3$ un entier naturel. Alors l'équation :*

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

n'admet aucune solution $(x, y, z) \in \mathbb{Z}^3$ avec $PGCD(x, y, z) = 1$ et $xyz \neq 0$.

1 Présentation des objets

1.1 Courbes elliptiques

Définition : On appelle *courbe elliptique* une courbe algébrique admettant un modèle de Weierstrass, i.e. donnée par une équation de la forme suivante :

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

Une telle courbe est dite définie sur $\mathbb{Q}$ si les coefficients a_i sont rationnels pour tout i.

On associe à ces courbes les nombres suivants :

– Le discriminant Δ de la courbe E : c'est un polynôme en les coefficients a_i du modèle de Weierstrass de E. Par exemple lorsque la courbe est du type $E : y^2 = x^3 + Ax + B$ on a alors $\Delta(E) = -16(4A^3 + 27B^2)$. Si Δ est nul la courbe est singulière. On notera Δ_{min} le discriminant d'un modèle minimal.

– Le conducteur N de la courbe qu'on définit de la façon suivante : posons tout d'abord

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

avec δ_p un nombre égal à zéro lorsque la carastéristique du corps de définition est différente de 2 ou 3. On pose alors (le produit est fini) :

$$N = \prod_p p^{f_p}.$$

1.2 Formes modulaires

Soit $\mathcal{H} = \{z \in \mathbb{C} | Im(z) > 0\}$ le demi-plan de Poincaré. Pour une fonction holomorphe f sur $\mathcal{H}$ et pour une matrice $\gamma \in GL^+(2, \mathbb{R})$ notons :

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

Définition : Une *forme modulaire* f de poids k pour un groupe Γ d'indice fini dans $SL(2, \mathbb{Z})$ est une fonction holomorphe sur $\mathcal{H}$ vérifiant :

– $f|_k\gamma = f$ pour tout $\gamma \in \Gamma$.

– Pour tout $\delta \in SL(2, \mathbb{Z})$ la fonction $f|_k\delta$ admet un développement de Fourier du type (avec M un entier positif) :

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

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

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

2 Présentation de la preuve

2.1 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.

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

2.2 Courbe de 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 :

$$\Delta_{min} = 2^{-8}(abc)^{2p},\ N = \prod_{l|abc} l = 2rad_2(abc).$$

2.3 Les théorèmes de Wiles et de Ribet

Le théorème de Wiles 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 affirme que dans cette situation on peut en fait associer naturellement à E_{a^p,b^p,c^p} une autre forme modulaire non nulle de poids 2 mais de niveau N_p avec :

$$N_p = \frac{N}{\prod\limits_{\substack{l||N \\ p|ord_l(\Delta)}} l}.$$

On calcule alors :

$$N_p = \frac{N}{rad_2(abc)} = 2.$$

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.

3 Conclusion

On ne dit rien ici du contenu exact des théorèmes de Wiles et de Ribet, encore moins de leurs preuves respectives. On se bornera à indiquer que l'étude des représentations du groupe $Gal(\overline{\mathbb{Q}}|\mathbb{Q})$ a joué un rôle clef dans cette histoire.

Références

[1] G.Cornell, J.H.Silverman, G.Stevens. Modular forms and Fermat's Last Theorem, *Springer-Verlag* (1997).

[2] Hellegouarch. Invitation aux mathématiques de Fermat-Wiles, *Dunod* (2001).

[3] J-P.Serre. Cours d'arithmétique, *Presses Universitaires de France* (1995).

[4] J.H.Silverman. The Arithmetic of Elliptic Curves, *Springer-Verlag*(1986).

[5] J.H.Silverman. Advanced topics in the arithmetic of elliptic curves, *Springer-Verlag* (1994).