

FORMES MODULAIRES ET COURBES ELLIPTIQUES

La théorie d' Eichler-Shimura associe à la forme modulaire f :

$$f = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2$$

la courbe elliptique $y^2 - y = x^3 - x^2$.

Ceci signifie qu'en écrivant :

$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + \dots = \sum a_n q^n,$$

le nombre des points modulo p de cette courbe (y compris le "point à l'infini") est égal à $p + 1 - a_p$ (à condition que p ne divise pas 11).

Pour l premier, différent de 11, l'opérateur de Hecke T_l est défini par :

$$T_l(\sum a_n q^n) = \sum a_{ln} q^n + l \sum a_n q^{ln}$$

On vérifie que

$$T_l(f) = a_l f,$$

ce qui signifie que f est un vecteur propre de l'opérateur T_l .

La propriété de f qui lui vaut le qualificatif de "modulaire" est l'équation fonctionnelle suivante :

$$f[\exp(a\tau + b/c\tau + d)] = (c\tau + d)^2 f[\exp(\tau)],$$

où $\exp(\tau) = e^{2\pi i \tau}$, τ est un nombre complexe dont la partie imaginaire est positive, $(a, b; c, d)$ est une matrice de quatre entiers, telle que 11 divise c et $ad - bc = 1$ (elle n'est pas évidente !).

admet un point double si et seulement si le polynôme $X(X - A)(X + B)$ admet une racine double, c'est-à-dire si et seulement si $ABC = (abc)^p = 0$.

Le reste du programme consistait à voir ce que l'on pouvait savoir des point d'ordre p de la courbe $E(A, B, C)$. J'ai constaté, en 1969, que leurs coordonnées engendraient un corps algébrique qui ressemblait beaucoup au corps cyclotomique engendré par ζ_p . Les courbes $E(A, B, C)$ ainsi associées aux solutions hypothétiques non triviales de l'équation de Fermat fourniraient, à l'aide de leurs points de p -division, des représentations du groupe de Galois absolu qui sont trop belles pour exister.

Dès leur naissance, on soupçonnait que les courbes $E(A, B, C)$ étaient des juments de Roland (dans Roland Furieux, la jument de Roland possède toute les qualités sauf l'existence). Mais comment le prouver ?

C'est alors que Gerhard Frey est intervenu en 1985 : dans un manuscrit non publié intitulé «Modular Elliptic Curves and Fermat's Conjecture», il conjecturait que les courbes $E(A, B, C)$ ne pouvaient pas satisfaire la conjecture de Taniyama Weil : décidément l'Histoire aime les marges !

Les formes modulaires

On m'a rapporté une boutade du grand mathématicien M. Eichler : il aurait dit qu'il n'y avait que cinq opérations fondamentales en arithmétique : l'addition, la soustraction, la multiplication, la division et... les formes modulaires.

Les formes modulaires sont des fonctions de la variable complexe vérifiant des équations fonctionnelles (voir l'encadré de la page 95). On en trouve des vestiges fragmentaires dans l'*Ars Conjectandi* de Jacques Bernoulli (1713), puis quelques beaux spécimens, dont la fonction θ dans Euler (1748), dans l'*Introductio in Analysis Infinitorum*, où apparaissent également des séries de Dirichlet et où l'on trouve aussi l'expression sous forme de produit eulérien de la fonction ζ de Riemann. On reste pantois devant la boîte de Pandore ouverte par Euler. Son *Algèbre* fourmille aussi d'équations diophantiennes, de courbes et d'intégrales elliptiques.

Peut-être est-ce dans Euler que le mathématicien allemand E. Hecke a fait ses achats. Il a relié l'équation fonctionnelle et le développement en produit de la fonction ζ de Riemann, à d'étranges propriétés de la fonction θ .

Ses études joueront un rôle crucial dans la démonstration du théorème de Fermat-Wiles.

Les formes modulaires se comportent comme des organismes, leurs propriétés étant liées de manière stricte et harmonieuse par l'action d'un groupe. Celles qui nous intéressent ici sont vecteurs propres d'opérateurs très importants ici, les opérateurs de Hecke (voir l'encadré ci-contre).

La conjecture de Taniyama-Weil

Depuis les années 1950, on savait associer à une courbe elliptique une série de Dirichlet, que l'on appelait la fonction L de cette courbe elliptique et qui recelait de nombreuses informations sur les points rationnels de cette courbe. Hecke avait montré, par ailleurs, comment associer à certaines séries de Dirichlet des formes modulaires de telle sorte que si les premières possèdent un produit eulérien (un produit sur les nombres premiers), les secondes sont vecteurs propres des opérateurs de Hecke. Toutefois les informations sur les fonctions L étaient trop fragmentaires pour démontrer dans le cas général l'existence de la forme modulaire.

En 1955, la voix de Taniyama s'éleva dans le désert pour annoncer que toute courbe elliptique devait provenir d'une forme modulaire. Cette prophétie, prématurée et vague, ne suscita guère d'intérêt à l'époque...

Il est bon de s'arrêter ici pour évoquer des questions de style. Un des thèmes récurrents de notre histoire est que la contribution des mathématiciens français est marquée de positivisme. Le philosophe Auguste Comte, pape du positivisme au XIX^e siècle, voyait dans le développement historique de la science trois stades successifs : le stade théologique, le stade métaphysique, et le stade positif. Dans ce dernier stade seulement la théorie est vérifiable, on dirait aujourd'hui falsifiable selon Popper. La théorie doit être suffisamment précise pour être mise en défaut si elle est imparfaite.

C'est en ce sens qu'André Weil a apporté une contribution essentielle à la conjecture de Taniyama. En s'appuyant sur la théorie d'Eichler Shimura, il a su préciser comment on devait chercher la forme modulaire associée à une courbe elliptique.

La scène était dressée pour le spectacle, mais le temps semblait avoir sus-

pendu son vol. On ne savait que faire des courbes elliptiques $E(A,B,C)$ que l'on pouvait associer à une hypothétique solution non triviale de l'équation de Fermat.

L'explosion de 1986 et le théorème de Wiles

On a dit que le coup de baguette magique fut donné en 1985 par G. Frey, alors professeur à l'Université de Sarrebruck. G. Frey conjecturait que nos courbes $E(A,B,C)$ devaient contredire la conjecture de Taniyama, et, merveille des merveilles, la communauté mathématique le crut ! Jean-Pierre Serre, d'ordinaire si prudent, tira le «coup de feu qui fit le tour du monde» en publiant de profondes conjectures dont découlait le théorème de Fermat. Peu de temps après, en 1987, B. Mazur et K. Ribet prouvèrent ces conjectures pour la représentation hypothétique du groupe de Galois absolu qui serait liée à une solution non triviale de l'équation de Fermat, mais à une condition : il fallait que la courbe $E(A,B,C)$ vérifie la conjecture de Taniyama.

Stimulé par le théorème de Ribet, le mathématicien britannique Andrew Wiles s'embarqua seul pour un long voyage sur des «océans étranges de pensée».

La navigation fut rude, et ce n'est qu'en 1991 que quelques oiseaux dans le ciel signalèrent la proximité d'une terre. En 1992, il pensait arriver près du but, et le 21 juin 1993, à l'Institut Newton, il annonça que le théorème de Fermat était démontré.

Las, l'annonce était prématurée, et les oiseaux disparurent de l'horizon. Un autre mathématicien aurait sans doute abandonné, mais A. Wiles n'écoula que son courage et son collègue R. Taylor ; celui-ci l'incitait à revenir sur sa route. C'est alors que, le 19 septembre 1994, il vit en un éclair la solution tant cherchée : un procédé découvert par Ehud de Shalit ouvrait un chemin plus direct vers la conjecture de Taniyama pour les courbes $E(A,B,C)$.

Un chef-d'œuvre est né et un mythe est mort : le théorème de Fermat est enfin démontré. De plus, le travail d'Andrew Wiles ouvre la voie à un vaste continent de recherches futures où de nombreuses conjectures restent à prouver.

Par ailleurs, la liste des équations diophantiennes abordables par la méthode des courbes $E(A,B,C)$ est loin

LES DIFFÉRENTES ROUTES EMPRUNTÉES DEPUIS FERMAT

LA ROUTE DES PIÉTONS

Cette route a été empruntée par Fermat lui-même pour l'exposant 4, puis par Lamé et Lebesgue pour l'exposant 7.

On se ramène à l'impossibilité de la résolution en nombres entiers des équations $t^2 = r^4 + 4s^4$ lorsque n est égal à 4, et $t^2 = r^4 - 3/4r^2s^2 + 1/7s^4$, lorsque n est égal à 7 (rst différent de zéro) et on procède par descente infinie.

LES FORMES QUADRATIQUES

On peut penser que, pour les exposants p premiers impairs, Fermat associait à son équation la forme quadratique $X^2 + (-1)^{(p+1)/2}pY^2$. C'est du moins ainsi que procédèrent Euler pour p égal à 3, puis Legendre et Dirichlet pour p égal à 5.

LES EXTENSIONS CYCLOTOMIQUES

Depuis De Moivre au XVIII^e siècle, on sait factoriser $x^p + y^p$ en produit de facteurs du premier degré en x et y , et cela conduit à considérer l'ensemble des nombres déduits par additions, soustractions et multiplications de $\zeta_p = e^{2\pi i/p}$, c'est-à-dire l'anneau des entiers cyclotomiques. C'est ainsi que Kummer parvint à démontrer l'assertion de Fermat pour tous les nombres premiers "réguliers". Malheureusement on ne sait pas démontrer qu'il existe une infinité de tels nombres.

L'APPROCHE ELLIPTIQUE

Elle est beaucoup plus récente que les précédentes (26 ans) et fait l'objet de cet article.

REMARQUES

- 1) Les trois premières méthodes font usage de la descente infinie pour prouver le second cas (défini dans l'article).
- 2) Une forme quadratique apparaît dans la route des piétons pour l'exposant 7.
- 3) Le nombre quadratique $((-1)^{(p-1)/2}p)^{1/2}$ apparaît implicitement dans la seconde méthode : il appartient à l'anneau des entiers cyclotomiques.
- 4) Finalement le corps des nombres cyclotomiques est contenu dans le corps engendré par les coordonnées des points de p -division de la courbe $E(A,B,C)$.

d'être close. Pourtant les solutions d'une équation aussi voisine du théorème classique, que $x^n + y^n = 2z^n$ ne peuvent être étudiées directement par cette méthode puisque cette équation possède la solution non triviale (1,1,1). Fermat n'est sans doute pas aussi mort qu'on le suppose, et sa note marginale suscitera peut-être d'autres découvertes.

À ce stade du panorama et après deux articles portant sur le sujet, le lecteur a une idée sur le comment du théorème de Fermat. Le pourquoi de ces recherches peut lui sembler énigmatique : il nous semble que cette question ne peut être examinée en termes logiques et que le pourquoi des mathématiques reste et restera un choix artistique. Le mathématicien Emil Artin exprime avec force ce point de vue : «Nous pensons tous que les mathématiques sont un art... Certes les mathématiques sont logiques : chaque conclusion est tirée des résultats qui précèdent. Cependant la totalité de l'affaire, l'œuvre d'art véritable, n'est pas linéaire ; et, ce qui est bien pire, sa

perception ne peut être qu'instantanée. Nous avons tous éprouvé, en de rares occasions, une impression d'exaltation en réalisant que nous avions permis à nos auditeurs de voir, l'espace d'une seconde, l'architecture complète d'une question, et toutes ses ramifications.»

Yves HELLEGOUARCH est professeur de mathématiques à l'Université de Caen.

Catherine GOLDSTEIN, *Un théorème de Fermat et ses lecteurs*, Presses Universitaires de Vincennes, 1995.

Grand théorème de Fermat, in *Quadrature*, n°22, été 95.

Séminaire Bourbaki, Exposés de Jean-Pierre Serre et Joseph Oesterlé. Juin 1995.

Yves HELLEGOUARCH, *Points d'ordre $2p^h$ sur les courbes elliptiques*, in *Acta Arithmetica* XXVI, 1975.

K.A. RIBET, *Galois Representations and Modular Forms*, in *Bulletin of the American Society*, Octobre 1995.