

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.