π, e^{π} et $\Gamma(1/4)$

Démonstration d'une conjecture centenaire.

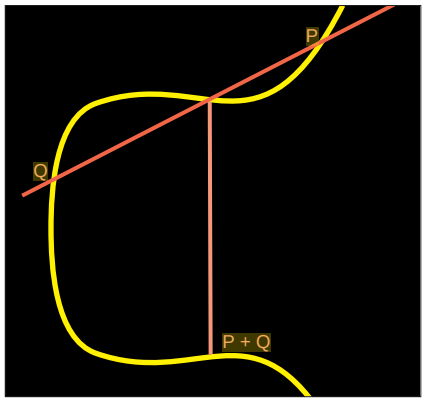
La démonstration du théorème de Fermat, par Andrew Wiles, avait mis en vedette les courbes elliptiques, composées de points dont les coordonnées x et y vérifient des équations de la forme $y^2 = 4x^3 - g_2x - g_3$. Aujourd'hui des mathématiciens français et russe obtiennent de nouveaux résultats liés à ces courbes et à l'«invariant modulaire» qui leur est associé.

Qu'est-ce que l'invariant modulaire? Tout commence par le paramétrage des courbes elliptiques : on sait qu'on peut aussi les définir par un seul paramètre, un nombre complexe z (un nombre que l'on associe à un point d'un plan, au lieu de l'associer à un point d'une droite) et par une fonction p dite de Weierstrass. L'abscisse x de tout point de la courbe s'écrit sous la forme $p(z)$, tandis que l'ordonnée correspondante s'écrit sous la forme $p'(z)$, où p' est la fonction dérivée de p.

Ce paramétrage étant fait, les mathématiciens ont défini une sorte d'addition des points de la courbe, en associant un point noté $P + Q$ à deux points P et Q de la courbe : si le point P a pour coordonnées $(p(z), p'(z))$ et si le point Q a pour coordonnées $(p(t), p'(t))$, alors le point $P + Q$ a pour coordonnées $(p(z + t), p'(z + t))$. Géométriquement, le point $P + Q$ s'obtient en traçant la droite qui passe par les points P et Q ; cette droite coupe la courbe elliptique en un troisième point, dont le symétrique par rapport à l'axe des abscisses est la somme $P + Q$.

Peut-on classer les diverses courbes elliptiques? Les mathématiciens utilisent à cette fin la fonction p et ses périodes. Une fonction d'une variable réelle, comme le sinus, a une période unique, égale en l'occurrence à 2π ; mais les fonctions p sont des fonctions de la variable complexe, et elles ont deux périodes de base. Le nombre $J(q)$ nommé invariant modulaire est défini à partir de leurs périodes ; il indique les ressemblances entre les courbes elliptiques : deux courbes ayant le même invariant modulaire ont des comportements identiques pour la loi d'addition de leurs points.

En 1969, Kurt Mahler, de l'Université de Canberra, avait conjecturé que l'invariant modulaire $J(q)$ est transcendant quand q est algébrique. Un nombre est transcendant s'il n'est pas algébrique, c'est-à-dire s'il n'est racine d'aucune équation polynomiale à coefficients entiers. S'il n'est pas besoin d'être grand mathématicien pour vérifier que $\sqrt{2}$ est algébrique (puisqu'il est racine de l'équation $x^2 = 2$), la démonstration de la transcendance d'un nombre est souvent très difficile : il a fallu attendre 1882 pour savoir que le nombre π est transcendant. La conjecture de Mahler a intéressé de nombreux théoriciens des nombres : en démontrant cette conjecture, on obtient la transcendance d'une famille infinie de nombres.



On définit une addition de points appartenant aux courbes elliptiques. Pour classer de telles courbes selon la façon dont leurs points s'additionnent, on utilise une fonction nommée invariant modulaire.

Avec Katia Barré-Sirieix, Guy Diaz et Georges Philibert, nous avons démontré la conjecture de K. Mahler en février 1995. Notre résultat a fait quelque bruit dans la communauté mathématique, parce qu'il résolvait un problème ancien, mais il a surtout ouvert une voie nouvelle pour l'étude de questions difficiles, et il est à l'origine de résultats spectaculaires : Yuri Nesterenko, de l'Université de Moscou, talonné par Patrice Philippon, de l'Université Paris VI, ont démontré l'indépendance algébrique des nombres π, e^{π} et $\Gamma(1/4)$, où la fonction Γ d'Euler prolonge la fonction factorielle aux nombres fractionnaires. Cela signifie que, si P est un polynôme de trois variables à coefficients entiers non tous nuls, le nombre $P(\pi, e^{\pi}, \Gamma(1/4))$ n'est pas nul. L'indépendance algébrique de π et e^{π} qui découle du travail de Y. Nesterenko et P. Philippon est un résultat dont les mathématiciens rêvaient depuis près d'une centaine d'années!

François GRAMAIN
Université de Saint-Étienne