2π (un angle), les points d'une courbe elliptique sont paramétrés par une variable complexe modulo deux périodes. Il en résulte que les points de p-division ne sont plus sur une droite mais dans un plan. Mais abordons, comme nous l'avions promis, les courbes elliptiques.

L'introduction des courbes elliptiques

Prenons une courbe elliptique représentée par la cubique d'équation : $y^2 = x^3 + a_2x^2 + a_4x + a_6$. La courbe est définie sur les rationnels si a_2, a_4 et a_6 sont rationnels. De plus il ne faut pas que le second membre de l'équation ait une racine double ; dans le cas contraire, la cubique possède un point multiple et n'est pas une courbe elliptique.

Comme les points de la courbe sont paramétrés par une variable complexe modulo deux périodes, ces points forment un groupe commutatif dont l'élément nul est le point de paramètre 0. Habituellement on choisit le paramétrage pour que l'élément nul du groupe soit le point à l'infini de la courbe. Les points rationnels de la courbe elliptique sont ceux dont les coordonnées sont rationnelles. Un théorème d'Abel explique comment construire le composé de deux points, et les points rationnels forment un groupe pour cette loi de composition *(voir la figure 3)*.

Pour les amateurs de courbes elliptiques, un des thèmes d'étude des années 1960 était une conjecture de Beppo Levi. Cette conjecture affirme, entre autres, que pour toutes les courbes elliptiques définies sur les rationnels, il existe un majorant de l'ordre des points rationnels. L'ordre d'un point P étant le plus petit entier n non nul tel que P composé avec lui-même n fois soit nul.

Les points rationnels d'ordre $2p^2$ doivent être particulièrement fascinants puisque B.A. Demjanenko et moi-même avons étudié ces points entre 1965 et 1970. À notre grand étonnement l'existence de ces points entraînait celle d'une solution non triviale de l'équation de Fermat d'exposant p.

En 1969, j'ai pensé à renverser l'approche : j'ai essayé de démontrer que, si l'équation de Fermat avait un triplet solution a,b,c, tous non nuls, alors la courbe elliptique dont l'équation est $Y^2 = X(X - a^p)(X + b^p)$ aurait des points d'ordre p intéressants. Si le nombre c n'apparaît pas dans cette équation c'est qu'il se déduit des deux autres par l'équation de Fermat $a^p + b^p = c^p$. La courbe sera désignée dans la suite par $E(A,B,C)$, avec $A = a^p$, $B = b^p$ et $C = -c^p$: certains auteurs la désignent sous le nom de «Courbe de Frey». Remarquons que l'on ne peut donner d'exemple de courbe $E(A,B,C)$ correspondant à une solution non triviale de l'équation de Fermat puisqu'il n'en existe pas. On peut toutefois en donner pour des équations voisines comme $x^p + y^p = 2z^p$.

Nous sommes ainsi passés du problème de Fermat de degré p à un problème sur les points d'ordre p de la courbe elliptique $E(A,B,C)$. Là encore, les mathématiciens ont élargi le problème : au point (a,b,c) ils ont fait correspondre une courbe elliptique $E(A,B,C)$, et l'on est passé ainsi d'un objet algébrique, un point $(u,v) = (a/c, b/c)$ de la courbe $u^p + v^p = 1$ à un objet «transcendant», la courbe $E(A,B,C)$.

Le passage à une dimension supérieure pour démontrer un théorème avait été utilisé avec profit par Desargues *(voir la figure 1)*. Cette démonstration fameuse par sa simplicité illustre l'intérêt de changer de «point de vue». Toutefois, une théorie plus générale que la théorie précédente n'est intéressante que si elle donne des résultats imprévus : dans le cas contraire, elle est stérile et sans portée.

Les courbes elliptiques éliminent de façon particulièrement élégante les solutions triviales de l'équation de Fermat : en effet, la courbe $E(A,B,C)$

LES FORMES MODULAIRES

La fonction thêta définie pour $|q| < 1$ par :

$$\theta(q) = \sum q^{n^2}$$

a été étudiée par Euler et Jacobi.
Si l'on pose $q(z) = e^{\pi i z}$, avec $z = x + iy$, $y > 0$, on obtient les équations fonctionnelles :

(1) $$\theta(q(z)) = \theta(q(z + 2))$$

(2) $$\theta(q(-1/z)) = (z/i)^{1/2}\, \theta(q(z))$$

La série de Dirichlet qui est associée à θ n'est autre que la célèbre fonction dzéta de Riemann :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad \text{pour } \mathrm{Re}(s) > 1$$

Euler a établi que cette fonction possède un "produit eulérien", c'est-à-dire un produit ne portant que sur les nombres premiers :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p} (1 - p^{-s})^{-1}$$

L'équation fonctionnelle de la fonction thêta conduit à celle de ζ, et le produit eulérien de ζ conduit à de nouvelles propriétés de θ !
Le 24 avril 1828, Jacobi découvrit l'identité :

$$\left(\sum q^{n^2}\right)^4 = 1 + 8 \sum A(m) z^m, \text{ où } A(m) = \sum d, \; d \text{ divisant } m \text{ et } \not\equiv 0 \bmod 4$$

qui lui permit de donner instantanément le nombre de représentations d'un entier positif comme somme de quatre carrés !
L'équation *(2)* entraîne l'équation fonctionnelle :

$$\frac{\Gamma(s/2)}{\pi^{s/2}}\, \zeta(s) = \frac{\Gamma((1 - s)/2)}{\pi^{((1 - s)/2)}}\, \zeta(1 - s)$$

publiée par B. Riemann en 1859.
La célèbre "hypothèse de Riemann" affirme que les zéros de $\zeta(s)$, qui ne sont pas -2, -4, -6, etc., se trouvent sur l'axe de symétrie de cette équation (la droite correspondant à la partie réelle de s égale à 1/2) : c'est une des grandes conjectures que notre époque lègue au prochain siècle.

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 :

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

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 :

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

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 $\exp (\tau) = e^{2i\pi\tau}$, 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-